S.Y. YUSUPOV,
A.A. GANIYEV, O.N. BEKMIRZAYEV

KOMPYUTER TIZIMLARI VA TARMOQLARINI BUZISH VA HIMOYALASH

O‘ZBEKISTON RESPUBLIKASI
OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT
TEXNOLOGIYALARI UNIVERSITETI

S.Y. YUSUPOV, A.A. GANIYEV, O.N. BEKMIRZAYEV

KOMPYUTER TIZIMLARI VA TARMOQLARINI BUZISH VA HIMOYALASH

O‘quv qo‘llanma

O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi tomonidan oliy o‘quv yurtining “5330300 – Axborot xavfsizligi (sohalar bo‘yicha)” ta’lim yo‘nalish talabalari uchun o‘quv qo‘llanma sifatida tavsiya etilgan

TOSHKENT
«IQTISOD-MOLIYA»
2023

UO'K: 004.056(075.8)
KBK 32.811.4ya73

Yu91 Kompyuter tizimlari va tarmoqlarini buzish va himoyalsh: O'quv qo'llanma / **S.Y.Yusupov, A.A.Ganiyev, O.N.Bekmirzayev;** – T.: «Iqtisod-Moliya», 2023. – 232 b.

Taqrizchilar:

J.X.Djumanov – *Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universitetining "Kompyuter tizimlari" kafedrasi mudiri, t.f.d.*

B.A.Allaberganov – *O'zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi yetakchi mutaxassisi.*

Ushbu o'quv qo'llanmada kompyuter tizimlari va tarmoqlarini buzishning asosiy turlari, tarmoq tahdidlari va hujumlarining turlari, dasturiy ta'minot, elektron pochta va parollarni buzish usullari, shuningdek, axborotni himoya qilishning asosiy prinsiplari, vositalari, hakerlik va hujumlardan himoya qilish usullari, Ilovalarda hujumlarning ba'zi turlari, xakerlik hujumlarida ishlatiluvchi apparat va dasturiy vositalar yoritib berilgan. Har bir bo'limda qisqacha xulosa va o'z-o'zini nazoratlash savollari berilgan.

O'quv qo'llanma "5330300 – Axborot xavfsizligi (sohalar bo'yicha)" ta'lim yo'nalishi talabalari uchun mo'ljallangan bo'lib axborot xavfsizligini ta'minlash sohasida faoliyat yuritayotgan mutaxassislar uchun ham foydali.

UO'K: 004.056(075.8)
KBK 32.811.4ya73

ISBN 987-9943-8703-5-2

MUNDARIJA

KIRISH

Saytlarni buzish, parollar va maxfiy ma'lumotlarni o'g'irlash, masofadan buzib kirishlar bugungi kunda tez-tez uchrab turmoqda. Aslida, ommaga e'lon qilingan buzg'unchilik ma'lumotlari haqiqiy xakerlik hodisalarining birozgina qismini tashkil etmoqda.

Rivojlangan davlatlar iqtisodiyot tarmoqlarining biron-bir sohasini zamonaviy axborot infratuzilmasisiz tasavvur etish qiyin. Ma'lumki, axborot xavfsizligi muammolari axborot texnologiyalari, kompyuter texnologiyalari, ma'lumot almashishning elektron usullari va obyektning ma'lum tugunlarida maxfiy ma'lumotlarning konsentratsiyasi rivojlanishi bilan ham tobora murakkablashib bormoqda. Axborot xavfsizligini ta'minlashga qaratilgan ko'plab texnik, dasturiy, tashkiliy va boshqa yechimlarning paydo bo'lishi tabiiy holga aylandi.

Axborot xavfsizligini milliy xavfsizlikning birinchi darajali elementiga aylanganini alohida ta'kidlash zarur. Axborotni himoya qilish masalasi, shubhasiz, davlatning ustuvor vazifalaridan biri sifatida ko'rib chiqilishi kerak.

Respublikamizda davlat va iqtisodiy boshqaruvda axborot texnologiyalarini rivojlantirish bilan bir qatorda, axborot xavfsizligiga alohida e'tibor qaratilmoqda. O'zbekiston Respublikasi Prezidenti Sh.M.Mirziyoyevning 2017-yil 8-fevraldagi "Qonun hujjatlarini tatbiq etish tizimini tubdan takomillashtirish chora-tadbirlari to'g'risida"gi qarorida va 2017–2021-yillarda O'zbekiston Respublikasini yanada rivojlantirish strategiyasida qator vazifalar belgilab berildi, jumladan "... axborot xavfsizligi va axborotni himoya qilish tizimini takomillashtirish, axborot sohasidagi tahdidlarga o'z vaqtida va yetarli darajada qarshi turish". Ushbu vazifalarni amalga oshirish muhim muammolardan biri hisoblanadi.

Ushbu o'quv qo'llanma kompyuter tizimlari va tarmoqlaridagi xakerlik hujumlarining asosiy turlari, shuningdek, axborotni himoya

qilishning asosiy prinsiplari, xakerlik va hujumlardan muntazam ravishda himoya qilish usullarini tizimli taqdim etishga bag‘ishlangan.

Birinchi bob kompyuter tizimlari va tarmoqlarini buzishning asosiy turlari, hujum qilish usullari, kompyuter viruslari turlariga bag‘ishlangan.

Ikkinchi bo‘limda Internet orqali masofadan hujumlar, hujumning bosqichlari, xakerlik hujumlari uchun dasturiy va apparat vositalar ko‘rib chiqilgan hamda xakerlik hujumlari va guruhlariga misollar keltirilgan.

Uchinchi bob tarmoq tahdidlari va hujumlariga, simsiz qurilmalar va android platformasidagi hujumlarga bag‘ishlangan.

To‘rtinchi bobda dasturiy ta’minot xavfsizligi masalalari, dasturlarni buzish texnologiyalari va usullari ko‘rib chiqilib. Dastlabki kod va dastur tuzilishini tiklash usullari va tavsiflari keltirilgan.

Beshinchi bobda elektron pochta va parollarni buzish usullari batafsil yoritilgan. Shuningdek, elektron pochta tizimlari bilan bog‘liq tadqiqotlar va Windows tizim parolini buzish usullari ko‘rib chiqildi.

Oltinchi bobda axborot xavfsizligining asosiy prinsiplari, axborot xavfsizligi vositalari, shuningdek, maxfiy ma’lumotlarning tarqalishidan himoya qilish va ma’lumotlar bazasini himoya qilish masalalari ko‘rib chiqilgan. Kompyuter viruslaridan himoylanishning dasturiy vositalari va asosiy chora-tadbirlari berilgan.

Yettinchi, xulosa bobida kompyuter hujumlarini aniqlashning qanday vositalari mavjudligi, saytni xakerlik hujumidan qanday himoya qilish to‘g‘risida ma’lumotlar jamlangan. Hujumlarga qarshi kurash usullari va simsiz tarmoqlarni himoya qilish usullari keltirilgan.

I-BOB. KOMPYUTER TIZIMLARI VA TARMOQLARINI BUZISHNING ASOSIY TURLARI

1.1. Asosiy tushunchalar

"Axborotlarni buzish" yoki ***"ma'lumotlarga hujum"*** ushbu harakatga ta'rif berish oson emas, chunki axborotlar asosan elektron shaklda bo'lib, yuzlab turlarda beriladi. Axborotga alohida fayl, ma'lumotlar bazasi, undagi bitta yozuv va dasturiy ta'minot to'plami sifatida ham qarash mumkin. Mazkur obyektlarning barchasi ma'lum bir ijtimoiy guruhning hujum ta'siriga tushushi va xavf ostiga qolishi ehtimoldan xoli emas.

Har qanday axborot obyektini saqlash, unga kirishni qo'llab-quvvatlash va foydalanish ruxsatini ta'minlashda uning egasi yoki vakolatli shaxs ushbu ma'lumotlar bilan ishlash qoidalarini o'rnatadi. O'rnatilgan qoidalarni buzish axborotga nisbatan qasddan hujum qilish sifatida tasniflanadi.

Buzish yoki xakerlik hujumi so'zi tor ma'noda "xavfsizlik tizimini buzishga urinish" va keng ma'noda "aqliy hujum", murakkab masalalarni hal qilish yo'lini topishga yondashish, deb tushuniladi. Aqliy hujum natijasida muammolar yechimi uchun noan'anaviy usullarni o'ylab topish yoki mavjud usullarga o'zgartirish kiritish orqali ularni optimallashtirish mumkin.

Buzish va hujum qilish tushunchalari bilan bog'liq ayrim atamalarni keltiramiz.

"Cracker" hujumi – masofaviy/mahalliy hisoblash tizimidan nazoratni qo'lga olish (huquqlarni kuchaytirish), beqarorlashtirish yoki xizmat ko'rsatishdan voz kechishga undaydigan harakat.

"Crack" – dasturiy ta'minotni buzish imkonini beruvchi dastur. Qoidaga ko'ra, krek ommaviy foydalanishga mo'ljallangan va buzish ko'rinishlaridan biri.

"Cracker" – krek yaratish bilan shug'ullanuvchi kishi.

Buzg'unchi – bu oldindan tayyor krek yoki uning yordamisiz dasturni buzadigan kishi.

"Patch" – kompyuter fayllarida muayyan o'zgarishlarni avtomatik tarzda kiritish uchun mo'ljallangan ma'lumotlar. Xususan, path yoki yangilanish *(update)* dasturiy ta'minot xatoliklarini tuzatish yoki uning finksionalligini o'zgartirish uchun ishlatiladigan ma'lumotlarni o'z ichiga olgan avtomatlashtirilgan alohida dasturiy vosita.

Bundan tashqari, ijro etiluvchi faylga o'zgartirishlar kiritish (masalan, ro'yxatdan o'tish zarurligi to'g'risida eslatish), dasturning funksional imkoniyatlarini kamayishi bilan bog'liq dasturiy tomondan bo'ladigan ko'ngilsiz harakatlarni to'xtatish maqsadida kiritiladi.

Shunday qilib, kompyuter tizimini ***buzish yoki hujum qilish*** – bu tajovuzkor tomonidan muayyan zaiflikni topish va ulardan foydalanish harakatidan iborat jarayondir. Boshqacha aytganda, ***hujum – tahdidni amalga oshirish.***

Xavfsizlikka tahdidning uchta asosiy turi mavjud: ***oshkor bo'lish, butunlikka nisbatan tahdid va xizmat ko'rsatishdan voz kechish.***

Oshkor bo'lishga nisbatan tahdid, axborotning bilishi lozim bo'lmagan shaxslarga ma'lum bo'lishi. Kompyuter xavfsizligi termonalogiyasi nuqtayi nazaridan oshkor bo'lish tahdidi yuqori o'rin tutib, kompyuter tizimida saqlanadigan yoki bir tizimdan ikkinchisiga uzatilgan vaqtda ba'zi konfidensial ma'lumotlatga kirish ruxsati qo'lga kiritilganda yuzaga keladi. Ba'zan "oshkor bo'lish" so'zi o'rniga "o'g'rilik" yoki "sirqib chiqish" so'zlari ishlatiladi.

Butunlikka nisbatan tahdid kompyuter tizimida saqlanadigan yoki bir tizimdan ikkinchisiga uzatiladigan ma'lumotni qasddan o'zgartirish (modifikatsiya qilish yoki o'chirish)ni o'z ichiga oladi. Odatda, davlat tuzilmalarida oshkor bo'lishlikka duch kelish ehtimoli ko'proq, biznes va tijorat tuzilmalarida esa butunlikka nisbatan ko'proq tahdid kuzatiladi.

Xizmat ko'rsatishdan voz kechish tahdidi muayyan xatti-harakatlar natijasida hisoblash tizimidagi bir qancha resurslarga kirishni cheklash natijasida yuzaga keladi. Aslida, xizmatni cheklab qo'yish tahdidi vaqt jihatidan doimiy xarakterga ega bo'lib, natijada so'raladigan

resurs hech qachon qabul qilinmaydi yoki uning uzatish vaqti kechiktirilishi mumkin. Bunday hollarda, manbadan foydalanish tugaganligi kelib chiqadi.

1.2. Kompyuter tizimlarini buzish usullari

Kompyuter buzg'unchiliklari yoki hujumlari har kuni sodir bo'ladi. Shunchaki kompyuteringizni Internet tarmog'iga ulang va kimdir sizning tizimingizga kirishga harakat qiladi. Na reklama, na havolalar kompyuterga e'tibor qaratmasa ham, u doimo skanerdan o'tkaziladi. Agar kompyuter biznes maqsadlari uchun ishlatilsa, masalan, savdo, notijorat, ta'lim yoki harbiy saytni qo'llab-quvvatlash uchun ishlatiladigan hollarda tajovuzkorlar tomonidan ko'proq e'tibor beriladi.

Aksariyat hujumlar kompyuterlarning oddiy tekshiruv amaliyotlarini bajarib, ularning asl maqsadi xavfsizlikning zaifliklarini topishdir. Biroq, har kuni matbuotda ta'kidlanayotgani kabi, darhaqiqat tez-tez amalga oshirilayotgan murakkab hujum ssenariylari mavjud. Bir yil mobaynida AQShning ko'plab yirik banklari mijozlar hisoblari holati to'g'risidagi ma'lumotlarni ko'rish imkoniga ega bo'lgan xakerlar qurboni bo'ldi. Buzg'unchilar Internet-do'konlaridan mijozlarning ko'plab kredit karta raqamlarini o'g'irlab ketishdi. Ular E-tijorat kompaniyalaridan mijozlar kredit karta ma'lumotlarini oshkor qilmaslik evaziga tez-tez pul talab qildilar. Mahsulotlarni real vaqtda sotadigan ko'plab firmalar, axborot kompaniyalari va Internet-do'kon saytlarini vaqtinchalik to'xtatishga majbur bo'ldilar va natijada mijozlar boshqa firmalar xizmatlariga murojaat qilishdi.

Kompyuter hujumi tasnifi

Biz "kompyuter hujumi" haqida so'z yuritganimizda, odamlarning kompyuterga ruxsatsiz kirishi uchun dasturlarni ishga tushirishini tushunamiz. Hujumlarni tashkil qilish shakllari juda xilma-xildir, lekin umuman olganda, ularning barchasi quyidagi toifalarga kiradi:

• *Kompyuterga masofadan tajovuz qilish*: Internet (yoki mahalliy tarmoq) orqali boshqa kompyuterga ruxsatsiz kirishni ta'minlaydigan dasturlar;

• *Kompyuterga lokal tajovuz qilish*: ular ishlayotgan kompyuterga ruxsatsiz kirishni ta'minlaydigan dasturlar;

• *Masofadan kompyuterni bloklash*: Internet tarmog'i orqali masofadan turib barcha kompyuterning ishini bloklash yoki undagi alohida dasturni bloklaydigan dasturlar (ko'pincha kompyuterni funksiyasini tiklash uchun qayta ishga tushirish kerak);

• *Kompyuterni mahalliy bloklash*: ular ishlayotgan kompyuterni bloklaydigan dasturlar;

• *Tarmoq skanerlari*: qaysi kompyuterlar va dasturlar hujumlarga uchrashga moyilligi mavjudligini aniqlash bilan bog'liq tarmoqlar haqidagi ma'lumotlarni to'playdigan dasturlar;

• *Dastur zaifliklari skanerlari*: ma'lum bir turdagi hujumga zaif kompyuterlarni qidirishda Internetdagi katta kompyuter guruhlarini tekshiradigan dasturlar;

• *Parolni ochuvchilar:* oson taxmin qilish orqali shifrlangan parol fayllaridagi parollarni aniqlash dasturlari. Hozirgi kunda kompyuter parollarini shu qadar tezkor aniqlashi mumkinki, ayni paytda ko'pgina murakkab darajadagi parollarni aniqlanayotganligi buni yaqqol ko'rsatmoqda;

• *Tarmoq analizatorlari* (*snifferlar*): tarmoq trafigini tinglaydigan dasturlar. Odatda ularda foydalanuvchi nomlari, parollar va kredit karta raqamlarini avtomatik ravishda trafikdan olish imkoniyati mavjud.

Ma'lumki, har qanday universal kompyuter tizimining dasturiy ta'minoti uchta asosiy komponentdan iborat: operatsion tizim (OT), tarmoq dasturiy ta'minoti (TDT) va ma'lumotlar bazasini boshqarish tizimi (MBBT). Shuning uchun, kompyuter tizimlari himoyasini buzishga qaratilgan barcha harakatlarni uchta guruhga bo'lish mumkin:

• ma'lumotlar bazasini boshqarish tizimi darajasidagi hujum;

• operatsion tizim darajasidagi hujum;

• tarmoq dasturiy ta'minoti darajasidagi hujum:

Ma'lumotlar bazasini boshqarish tizimi darajasidagi hujum

Ma'lumotlar bazasini boshqarish tizimini himoyalash eng oson vazifalardan biri hisoblanadi. Buning sababi, MBBT qat'iy ichki tuzilishga ega va uning elementlari bilan bajariladigan operatsiyalar aniq

belgilangan. Bunda to'rtta asosiy harakat mavjud: *elementni qidirish, joylashtirish, o'chirish va almashtirish*. Boshqa operatsiyalar yordamchi va kamdan-kam ishlatiladi. Aksariyat hollarda, xakerlar operatsion tizim darajasidagi kompyuter tizimi himoyasini chetlab o'tib, operatsion tizim vositalari yordamida MBBT fayllariga kirishni afzal ko'rishadi. Ammo, yetarli darajada ishonchli himoya mexanizmlari mavjud bo'lmagan yoki xatolarni o'z ichiga olgan MBBT ning noto'g'ri testlangan versiyasi yoki xavfsizlik siyosatini belgilashda MBBT administratori tomonidan xatolar sodir etilgan hollarda, xakerlar MBBT darajasida qo'llaniladigan muhofazani to'laqonli yengib o'tishlari mumkin bo'ladi.

Bundan tashqari, MBBTda maxsus usullarni qanday qo'llash kerakligini bilish uchun ikkita hujum ssenariylari mavjud. Birinchi holda, MBBT soni maydonlari bo'yicha arifmetik operatsiyalarning natijalari kichik songacha yaxlitlanadi va farq MBBT boshqa yozuvida yig'iladi (qoida bo'yicha, ushbu yozuv xakerning bankdagi shaxsiy hisob raqamini o'z ichiga oladi va yaxlitlangan sonli maydonda esa boshqa bank mijozlari hisob raqamlarini saqlaydi). Ikkinchidan, xaker faqatgina statistik ma'lumotlar mavjud bo'lgan MBBT yozuvlari maydoniga kira oladi. MBBTga qilinadigan xaker hujumi g'oyasi – so'rovni zimdan shakllantirish bo'lib, statistikani to'plovchi yozuvlar to'plami birgina yozuvdan iborat bo'ladi.

Operatsion tizim darajasidagi hujumlar

Operatsion tizimni himoya qilish, MBBTdan farqli o'laroq, juda murakkab jarayon. Aslida zamonaviy operatsion tizimlarning ichki strukturasi juda murakkab va shuning uchun tegishli xavfsizlik siyosatiga rioya qilish juda qiyin masala.

Hech kim kompyuter texnologiyalari sohasidagi barcha yangiliklardan xabardor bo'lishi kerakligi bilan bahslashmaydi. Shuningdek, yuqori malakali bo'lish ham foydadan xoli emas. Ammo, xakerlik san'ati faqatgina eng "mukammal" kompyuter muhofazasini buzishdan iborat emas. Faqat ma'lum bir himoya tizimidagi zaiflik nuqtani topish kerak xolos.

Muayyan xaker hujumi algoritmini amalda qo'llash muvaffaqiyatlari, asosan, ushbu hujumning maqsadi bo'lgan muayyan

operatsion tizimning arxitekturasi va konfiguratsiyasiga bog'liq. Biroq, deyarli har qanday operatsion tizim duchor bo'ladigan hujumlar mavjud:

• ***parolni o'g'irlash:***

foydalanuvchi operatsion tizim bilan ishlash huquqini beruvchi parolni kiritganda qarab kuzatish (xatto parol kiritish vaqtida ekranda ko'rsatilmasa ham, xaker osonlikcha klaviaturada foydalanuvchining barmoq harakatlarini kuzatish orqali parolga ega bo'lishi mumkin);

tarmoqqa ulanganda parolni eslab qolishni istamaydigan foydalanuvchi tomonidan ushbu parolni saqlagan fayldan parol olish (odatda, bunday parol shifrlanmagan shakldagi faylda saqlanadi);

foydalanuvchilar unutmaslik uchun kalendarlar, daftarlardan yoki kompyuter klaviaturalari orqasida yozilgan parolni qidirish;

tashqi tashuvchilardan parol ma'lumotlarini o'g'irlash (diskret yoki operatsion tizimga kirish uchun mo'ljallangan foydalanuvchi parolini saqlaydigan elektron kalit);

barcha mumkin bo'lgan parol variantlarini to'liq qidirish;

maxfiy parollar mavjudligi to'g'risida ma'lumotlardan foydalanib, ma'lum bir foydalanuvchining bilimini o'z ichiga olgan, uning ismi, familiyasi, telefon raqami, tug'ilgan sanasi va h.k. eng ko'p ishlatiladigan parollarning lug'atlarini ishlatib, belgilarning paydo bo'lish chastotasi bo'yicha parol tanlash; har bir klassdan bitta parol tekshiriladi, bu qidiruv vaqtini sezilarli darajada kamaytiradi;

• ***kompyuterning qattiq disklarini skanerlash*** – xaker doimiy ravishda kompyuterning qattiq disklarida saqlangan har bir faylga kirishga harakat qiladi; agar disk maydoni yetarli darajada katta bo'lsa, administrator fayllar va kataloglarga kirish ruxsatlarini tavsiflaganda, hech bo'lmasa bitta xatoga yo'l qo'yganligini payqashi, natijada bunday kataloglar va fayllarning xaker tomonidan o'qilishiga olib keladi; izlarni yashirish uchun, xaker bu hujumni boshqa nom ostida tashkil qilishi mumkin: masalan, parolni xaker o'ziga ma'lum bo'lgan foydalanuvchi nomi ostida kiritishi;

• ***"chiqindi" yig'ish*** – agar operatsion tizim vositalari avval o'chirilgan narsalarni qayta tiklashga imkon beradigan bo'lsa, xaker boshqa foydalanuvchilar tomonidan o'chirilgan narsalarga kirish uchun

ushbu imkoniyatdan foydalanishi mumkin: masalan, chiqindi qutilarining ichidagilarning mazmunini ko'rish;

• ***vakolatlarning ortishi*** – dasturiy ta'minot yoki operatsion tizim boshqaruvidagi xatoliklarni qo'llash, xaker joriy xavfsizlik siyosati bo'yicha o'ziga berilgan vakolatlardan ko'proq vakolatni qo'lga oladi:

dasturni vakolatli foydalanuvchi nomi ostida yuklash yoki tizim dasturi (drayver, xizmat ko'rsatish, domen va boshqalar) sifatida amalga oshirish;

tizim dasturlari tomonidan foydalaniladigan dinamik ravishda yuklangan kutubxonani almashtirish yoki bunday kutubxonalarga yo'lni tavsiflovchi muhit o'zgaruvchilarini o'zgartirish;

operatsion tizimning o'ziga tegishli bo'lgan quyi tizimining kodi yoki ma'lumotlarini modifikatsiyasi.

Xizmat ko'rsatishdan voz kechish – ushbu hujumning maqsadi operatsion tizimni qisman yoki butunlay ishdan chiqarishdir:

resurslarni olib qo'yish (xaker dasturi operatsion tizimda mavjud bo'lgan barcha resurslarni ushlab qoladi, keyin cheksiz siklga kiradi);

so'rovlar bilan bombardimon qilish (xaker dasturi muntazam operatsion tizimga so'rovlarni jo'natadi, bu reaksiya muhim kompyuter resurslaridan foydalanishni talab qiladi);

dasturiy ta'minot yoki boshqaruv xatolaridan foydalanish.

Agar kompyuter tizimidagi dasturiy ta'minotda xatolik bo'lmasa va uning administratori operatsion tizim ishlab chiqaruvchilari tomonidan tavsiya etilgan xavfsizlik siyosatini qat'iyan kuzatib borayotgan bo'lsa, mazkur holda yuqorida qayd etilgan barcha xakerlik hujumlari samarasiz bo'ladi. Xavfsizlik darajasini oshirish uchun zarur bo'lgan qo'shimcha chora-tadbirlar asosan ushbu kompyuter tizimi ishlaydigan muayyan operatsion tizimga bog'liq. Shunga qaramay, qabul qilingan chora-tadbirlardan qat'iy nazar operatsion tizim darajasida kompyuter tizimini buzish tahdidini to'liq bartaraf etish mumkin emasligini e'tirof etishimiz kerak. Shuning uchun xavfsizlikni ta'minlash siyosati, himoya bardoshliligi, operatsion tizim uchun

yaratilgan himoya vositalarini xaker yengib o'tgan holda ham, jiddiy zarar yetkaza olmasligi lozim.

Tarmoq dasturiy ta'minoti darajasidagi hujumlar

TDT nisbatan zaif hisoblanadi, chunki xabarlar uzatiladigan aloqa kanali himoyalanmagan va bu kanalga kirish imkoniyatiga ega bo'lgan har bir kishi xabarlarni to'xtatib, o'zlarining maxsus matnlarini jo'natishi mumkin. Shuning uchun, TDT darajasida quyidagi xakerlik hujumlari bo'lishi mumkin:

• ***mahalliy tarmoq segmentini tinglash*** – bir xil mahalliy tarmoq segmentida, unga ulangan har qanday kompyuter boshqa segment kompyuterlardan yuborilgan xabarlarni olish imkoniga ega va shuning uchun xakerning kompyuteri ma'lum bir mahalliy tarmoq segmentiga ulangan bo'lsa, u holda barcha axborot almashinuvi mavjud bo'lgan ushbu segmentdagi kompyuterlar ma'lumotlariga kirish mumkin bo'ladi;

• ***marshrutizatordan xabarlarni tutib olish*** – agar xaker tarmoq marshrutizatoriga imtiyozli kirish huquqiga ega bo'lsa, u holda ushbu marshrutizator orqali o'tadigan barcha xabarlarni to'xtata oladi va hajm jihatidan butunlay tutib olish imkoniyati bo'lmagan holda ham, tanlov asosida o'zida foydalanuvchi parollari va elektron pochtalari saqlangan xabarlarni tutib olishga intiladi;

• ***yolg'on marshrutizator yaratish*** – xaker tarmoqqa maxsus xabarlar yuborish orqali uning kompyuteri tarmoq marshrutizatori sifatida ishlashiga erishadi, undan so'ng u o'zidan o'tib ketadigan barcha xabarlarga kirishni ta'minlaydi;

• ***xabarga ishontirish*** – tarmoqqa yolg'on qaytadigan tarmoq manzili orqali xabarlar jo'natish asosida xaker oldindan o'rnatilgan kompyuter tarmoqlariga ulanishni kompyuterga o'tkazadi va natijada xakerlar kompyuteriga aldov yo'li bilan havolasini yuborgan foydalanuvchilar huquqlarini oladi;

• ***xizmatni rad etish*** – xaker tarmoqqa maxsus turdagi xabarlarni yuboradi, bundan keyin tarmoqqa ulangan bir yoki bir nechta kompyuter tizimlari butunlay yoki qisman ishlamaydi.

1.3. Kompyuter tarmoqlarida buzish turlari

Katta tarmoqlarni buzish oson ish emas, bu maksimal darajada himoyalangan tarmoqlarni qurish yo'llarining maxsus usullarini qo'llashni talab qiladi.

Internetga ulangan har qanday kishi xakerga nisbatan zaif bo'ladi. Misol: kompyuterni tekshiradigan yoki uni virus bilan zararlaydigan "Troyan oti". Antivirus dasturlari, tarmoqlararo ekran va umumiy xavfsizlik choralari, ko'p provayderlar, biznes va bosh sahifa foydalanuvchilari tomonidan xavfni kamaytirish va kompyuterlarni, web-saytlarni va serverlarni potensial xakerlarga imkon qadar kamroq jalb qilish uchun ishlatiladi. Hakerlarning xohishlarini hisobga olgan holda, Internetda faollik oshib, xakerlik hujumlari ehtimolligi oshib borishini taxmin qilish oson. Misol: vaqti-vaqti bilan internetga ulangan bosh sahifa foydalanuvchilarida ustuvor maqsad bo'lmasligi mumkin. Xavfni kamaytirish tartibida quyidagi hujum obyektlari ro'yxatini ko'rsatish mumkin:

1) Axborotni to'plash vositalari

Ma'lumotni to'plash uchun ko'p faol va passiv usullar mavjud. Passiv ma'lumot to'plash IP-manzili xavfsizligini tekshirish, tarmoq infratuzilmasini aniqlash, qo'llaniladigan dastur va xavfsizlik vositalarini aniqlashdan iborat. Xakerning ixtiyorida ma'lumot to'plash uchun katta hajmdagi arsenal mavjud, xususan:

- ***Tarmoqni tadqiq qilish:*** kompyuterning ma'lum zaifliklarini tezlik bilan tekshirish uchun ishlatiladi. Buni amalga oshirish uchun snifferlardan foydalaniladi. Ular tarmoqdagi kompyuterlar o'rtasida ma'lumotlarni uzatish vaqtida parollar va boshqa jo'natmalarni tutib oladi;

- ***Ijtimoiy muhandislik:*** ma'lumot olish uchun har xil manipulyatsiyalar, masalan, pivo tanavvul qilish paytida parollar yoki qayd yozuvlarini qo'lga kiritish;

- ***Ommabop manbalar va chiqindi qutilari***: reklama materiallari va chiqindi konteynerlaridan ma'lumotlarni olish;

- ***Ko'rinmaydigan dasturlar (root kitlar):*** kompyuter xavfsizligini buzish faktini yashirish vositasi.

Tarmoqni tadqiq qilish xakerga hujumni rejalashtirish uchun zarur. Buning uchun skanerlash, foydalanilayotgan ilovalarni va ularning versiyalarini aniqlash, tarmoqda o'rnatilgan topologiyani o'rnatish qo'llaniladi. Tarmoqni tadqiq qilishda IP-adresslar, tarmoq adresslari, kirish huquqi ro'yxatlari, kirish nuqtalari, tarmoqlararo ekranlarning sozlanmalari, ilovalar versiyalari va foydalanuvchilar nomlari eng muhim hisoblanadi.

Ko'pgina xakerlar vositalari axborotni masofadan turib yig'ishda foydalaniladi.

Xakerlar skanerlashning barcha diapazonlaridan foydalanadilar. Ularga portni skanerlash, IP manzillar, marshrutizatorlar (OSPF soxtalashtirish-IP-marshrutizatsiya protokoli va OSPF-eng qisqa yo'lni tanlash protokoli), SNMPni skanerlash (tarmoqni boshqarish protokoli), port va ilovalar tadqiqoti, tarmoqlararo ekranlarni tekshirish, simsiz ulanish nuqtasi, operatsion tizim, o'rnatilgan apparat va IP-stack protokoli kiradi.

"***Ijtimoiy muhandislik***" termini xakerlar tomonidan tanlangan firma xodimlaridan axborot olishda foydalaniladigan har qanday hiylani aniqlash uchun qo'llaniladi. Hech nimadan shubxalanmayotgan personalni yolg'on ma'lumotlar bilan manipulyatsiya qilish, axborot olish uchun har qanday usullardan foydalaniladi. Ular inson tabiatiga bog'liq. Aktiv va passiv ijtimoiy injineriya orasida farq bor. Telefon qo'ng'irog'i keraksiz shubhalarni keltirib chiqarishi mumkin; Ushbu chaqiruv kutilsa nima bo'ladi?

Ijtimoiy muhandislik – ushbu tahdid na serverga va na mijozning mashinasiga, balki mijozning miyasiga qaratilgan hujumdir. Ayniqsa, uni ajralish deb atash mumkin. Agar kerakli ma'lumotlarni, masalan, parolni qo'lga kiritrshni istasangiz, buni bir necha usul bilan amalga oshirishingiz mumkin:

- parolni tiklash formasini ko'rib chiqing, maxfiy savolni toping va ushbu savolga berilgan javobni qurbonimizdan suhbat yoki shaxsiy xabarlar asosida toping;

- biz maktubga login/parol/yangi parol/yangi savol va h.k. yuborish haqida so'rov xabarini qurbonga yuboramiz. Maktub, foydalanuvchi ishonadigan shaklda, bo'lishiga ishonishi mumkin bo'lgan xizmat uslubida rasmiylashtirilishi kerak.

Potensial jabrlanuvchi haqida ma'lumotni ***omma uchun ochiq manbalardan, hamda chiqindi qutilaridan*** olish mumkin. Omma uchun ochiq bo'lgan resurslarning namunaviy misollaridan biri WHOIS ma'lumotlar bazasi, oq sahifalar, munozara arxivlari, resurs egalari to'g'risida ma'lumotni o'z ichiga olgan yangi web-sahifalar; lahzali xabar almashish, xodimlar bilan muloqot qilish, elektron pochta manziliga domenni aniqlash, oq sahifalarni qidirish; Google kabi qidiruv tizimlarida yillar oldin yuborilgan elektron pochta xabarlari orqali; crawlers yoki Google dan foydalanib, Internetdan ma'lumotlarni olish hisoblanadi.

2) Xaker hujumlari

Xaker barcha dastlabki ma'lumotni to'plagach, quyidagi hujumlardan birini boshlash vaqti keladi:

Troyan otlari – sirtdan butunlay qonuniy ko'rinadigan dasturdir, ammo ishga tushirilganidan keyin ba'zi noqonuniy xatti-harakatlarni keltirib chiqaradi. Ular parollarni topish, tizimni bo'lajak hujumlarga xavfsizroq holga keltirish yoki oddiy diskdagi dasturlar yoki ma'lumotlarni o'chirish uchun ishlatilishi mumkin. Troyan otlari virusga o'xshaydi, lekin boshqa fayllarni zararlash yo'li bilan ko'paya olmaydi, kompyuterga joylashadi, masofadan kompyuterga kirishni nazorat qilish imkoniyatini beradi.

Qora tuynuklar – an'anaviy autentifikatsiyani chetlab o'tish va kompyuterga masofadan kirib borish imkonini beradi, ularni tasodifan aniqlashdan yashiradi. Bu dastur o'rnatilishi yoki qonuniy modifikatsiya qilinishi mumkin. Kirish vaqtida ular foydalanuvchi nomlari va parollarning murakkab kombinatsiyalaridan o'tishlari mumkin. Qora tuynuklarning odatiy misollari: NetBus, SubSeven va BackOrifice.

DoS va DDoS hujumlari – tarmoqqa yo'naltirilgan bo'lib, ular foydali trafikni minimal darajaga qisqartirishi yoki umuman to'xtatilishi uchun qo'shimcha so'rovlar bilan to'ldiradi. Ma'lumotlar bazalariga

zarar yetkazishi mumkin bo'lgan viruslar va qurtlardan farqli o'laroq, DoS hujumlari tarmoqni bir muncha vaqt mobaynida buzadi, DDoS hujumlari ilgari zararlangan turli tarmoqli kompyuterlardan foydalanadi. "Zombi" rolini o'ynaydigan kompyuterlar soxta xabarlarni jo'natib, soxta trafikni oshiradi.

DDoS hujumlarining qurbonlari bo'lib, barcha vositalar, yirik web-saytlar, serverlar, yirik kompaniyalar va xizmat ko'rsatuvchi provayderlar hisoblanib, tarmoq o'tkazuvchanligiga to'sqinlik qiladi.

Bufer toshqini – buning sababi beqaror ishlovchi dasturlarning keng tarqalganligi. Bufer – bu dasturning yoki jarayon tomonidan ishlatiladigan, ishga tushirish vaqti haqidagi ma'lumotni saqlaydigan kompyuter xotirasining bir qismi. Kompyuter dastur kodi va ma'lumotlarini ajrata olmagani uchun, bufer to'lib ketishi, xakerning xizmatni o'chirishiga yoki zararli kodni tatbiq qilishga imkon beradi.

Buferda saqlangan ma'lumot miqdori uning hajmidan oshib ketgan holda, qo'shimcha ma'lumotlar o'zgarmaslar, bayroqlar yoki o'zgaruvchilar qo'shni xotira maydonlarida yoziladi.

Brutfors – buzg'unchilikning eng qo'pol, sodda tanlov usuli. Ya'ni, lug'atdan foydalanib dastur, har qanday kombinatsiyalar bo'yicha so'zlarni tartiblaydi va muqobilini to'g'ri topgach, u sizni bu haqda xabardor qiladi va ko'rsatib beradi, shuning uchun siz yaxshi lug'atga ega bo'lsangiz, muvaffaqiyat darajasi ortadi, agar siz parol nimalardan tarkib topganini bilsangiz masalan, faqat harflardan yoki faqat raqamlardan iborat bo'lsa, tanlov soni minimallashadi.

XSS hujumi – serverda mavjud bo'lgan zaiflikka hujum, bu generatsiya qilinadigan HTML server sahifasiga o'zboshimchalik bilan kodni joylashtirish imkonini beradi, bu ixtiyoriy tarkibli narsani o'z ichiga olishi va bu kodni o'zgaruvchi qiymat sifatida qabul qilishi mumkin, bunda filtrlash ishlamayapti, Server bu o'zgaruvchini taqiqlangan belgilar mavjudligi uchun tekshirmaydi -, <,>, ', ". Ushbu o'zgaruvchining qiymati generatsiya qilingan HTML sahifasidan buyruq faylidagi serverga so'rov yuborish orqali o'tkaziladi. Boshqacha aytganda, XSS hujumi serverdagi zaifliklar yordamida, mijozlar kompyuterlarida hujum qilish hisoblanadi.

XSS hujumi ko'pincha cookie fayllarini o'g'irlash uchun ishlatiladi. Unda foydalanuvchilarning saytga tashriflari sessiyasi haqidagi ma'lumotlar saqlanadi, xaker saytdagi foydalanuvchining shaxsiy ma'lumotlarini boshqarish maqsadida ushbu sessiya yakunlanmagan holatda server saytiga murojaat qilishi mumkin bo'ladi. Bunga qo'shimcha ravishda, shifrlangan parol Cookie-larda saqlanadi va zaruriy utilitlarsiz, buzg'unchi istaklari bilan parolni buzishda yetarlicha mashaqqatlarsiz erishib bo'lmaydi.

SQL injection (SQL in'eksiya yoki SQL kodni tatbiq qilish) – saytni buzishning eng xavfli usullardan biri hisoblanadi. SQLni ishlatish orqali buzish bazaviy so'rovga tasodifiy SQL kodini joylashtirishga asoslangan. SQL injection ko'rinishidagi hujumning yuzaga kelishining asosiy sababi SQL so'rovlariga yuborilgan kirish ma'lumotlarining noto'g'ri qayta ishlashidir.

Foydalanilayotgan ma'lumotlar bazasi turiga va "omad" darajasiga qarab, tajovuzkor har qanday jadvallarning mazmunini olish, ma'lumotlarni o'chirish, o'zgartirish yoki qo'shish va ayrim hollarda nafaqat o'qish, balki hujum qilingan serverda saqlangan mahalliy fayllarni o'zgartirish yoki o'zboshimchalik bilan buyruqni bajarishi mumkin. Haqiqatan ham, agar saytda SQL injection hujumni amalga oshirish mumkin bo'lsa, unda sayt ma'lumotlar bazasi bilan ixtiyoriy amaliyotni o'tkazish mumkin. Masalan, parollar o'g'irlash va butun saytga kirish yoki kredit karta raqamlarini o'zgartirish, sayt xizmatlarini haq to'lamasdan olish va yuzlab boshqa ochiq yoki yopiq harakatlar bo'lishi mumkin. Ushbu harakatlarning ba'zilarini siz xatto anglay olmaysiz. Tajovuz qiluvchi sizga birozgina talofat yetkazishi mumkin va kutilmagan vaziyatda esa biznes faoliyatingizni qulatishi ehtimoldan xoli emas. Agar XSS zaifligi – tumov bo'lsa, u holda, SQL injection o'limga olib keluvchi kasallikdir va siz unga qarshi mavjud vositalar bilan himoya qilinishingiz kerak.

Botnet – ma'lum sondagi xostlardan iborat va botlar (avtonom dasturiy ta'minot) ishlayotgan kompyuter tarmog'i. Odatda botnet tarkibidagi bot qurbon kompyuterida yashirin o'rnatiladigan va badniyat shaxsga (botnet "egasiga") kompyuter resurslaridan foydalangan holda ma'lum harakatlarni bajarishga imkon beradigan dasturiy ta'minotdir. Botnetlar ko'pincha spam yuborish, uzoqdagi tizimda parollarni birma-

bir ko'rib chiqish, xizmat ko'rsatishni rad etish kabi noqonuniy yoki ruxsat etilmagan faoliyat uchun foydalaniladi.

Virus egasi kompyuteringizga to'liq kirishni qo'lga oladi va endi sizning kompyuteringiz firibgarning istagi uchun ishlaydi, ya'ni har qanday serverga (saytga) nisbatan qilinadigan DDOS hujumini ishtirokchisiga aylanadi.

Fake (Soxta) – kerakli fayl yoki qaysidir saytga o'xshash bo'lgan aniq nusxa bo'lib, soxta web-saytning aniq nusxasi topilgan sahifani yoki saytni ko'rish uchun, majburiy avtorizatsiyadan o'tish talab qilinadi. Foydalanuvchi login va parollarni o'g'irlash uchun foydalaniladi. Faoliyat prinsipi: jabrlanuvchi saytga bog'lanishni amalga oshiradi, haqiqiy login bilan avtorizatsiyadan o'tadi, saytdagi faylga ma'lumot yuboriladi, tajovuzkor jabrlanuvchining login hamda parolini oladi va saytga kiradi.

Fake so'zi keng ma'noda haqiqiy narsalarga olib boruvchi ixtiyoriy soxtalikdir. Fake parollaringizni o'g'irlash uchun yaratiladi. Agar bitta belgining farqini ko'rmasangiz, unda siz bu haqiqiy sayt deb, o'z login/parolingizni kiritasiz va natijada jabrlanuvchiga aylanasiz.

Fishing (ing. fishing-baliq ovlash) – bu Internet-firibgarlikning bir turi, uning maqsadi foydalanuvchining identifikatsiya ma'lumotlarini olishdir. Bunga parollar o'g'irlanishi, kredit karta raqamlari, bank hisoblari va boshqa maxfiy ma'lumotlar kiradi.

Fishing banklardan, provayderlardan, to'lov tizimlaridan va boshqa tashkilotlardan keladigan soxta e-pochta xabarnomasi bo'lib, har qanday sababga ko'ra, qabul qiluvchidan zudlik bilan shaxsiy ma'lumotlarni uzatish/yangilashni talab qiladi. Buning sabablari turli xil bo'lishi mumkin. Bular ma'lumotlar yo'qolishi, tizimning noto'g'ri ishlashi va h.k.

1.4. Kompyuterga hujum qilish usullari

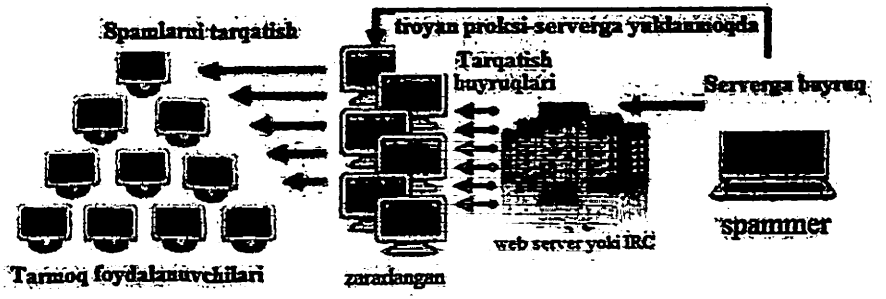
Xakerlik jinoyatchiligining bir nechta turlarini farqlaymiz:

1) reklamali spam-biznes

Bunda proksi server imkoniyatlariga ega troyan dasturlari tatbiq qilingan zararlangan kompyuterlar tarmog'i yaratiladi. Ushbu tarmoqda bir necha ming kompyuterlar jalb qilingan bo'lishi mumkin.

Bunda vaqtning istalgan momentida buzg‘unchi jabrlanuvchidan olgan jo‘natma va manzili asosida o‘z topshiriqlarini bajartira oladi.

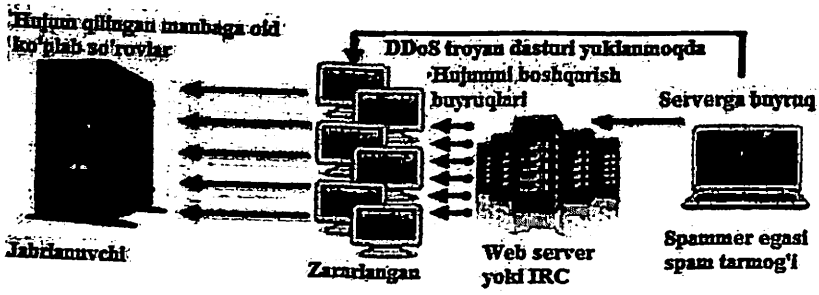
Mavjud “mutanosiblik”: tarqatishning yuqori tezligi, qora ro‘yxat texnologiyasini chetlab o‘tish imkoniyati, spamerning manzilini hisoblashning imkonsizligidir. Ushbu spam texnologiyasining namunali diagrammasi 1-rasmda keltirilgan.



1.1-rasm. DDoS tarmoqli hujumni bo‘lib yuborish va “Zombi” kompyuterlarini yaratish

Barcha zararlangan kompyuterlar tomonidan, serverga nisbatan bir vaqtda yoppasiga katta miqdordagi hujum amalga oshiriladi. Soxta murojaatlar so‘rovlarni qayta ishlovchi server kompyuteriga yuboriladi. Biroq, har qanday resurs cheklovga ega bo‘lgani kabi, yuboriladigan so‘rovlar soni server kompyuterining imkoniyatlaridan kattaroq bo‘lganda, server noto‘g‘ri ishlay boshlaydi yoki osilib qolishi mumkin. Bu holda xostingdagi mijozlar saytlari asta-sekin ochila boshlaydi. Shuningdek, xostingga bo‘layotgan soxta so‘rovlar hujumining ortib ketishi natijasida to‘planib qolgan so‘rovlarni qayta ishlash funksiyasi yo‘qoladi (1.2-rasm).

Ushbu turdagi faoliyat uchun “robots” so‘zidan kelib chiqqan “bot” dasturlari yaratiladi. O‘n minglab kompyuterlar ushbu troyanlar bilan zararlanadi va virus buzg‘unchidan buyruqni olmaguncha kutish holatida bo‘ladi. Bunday ZOMBI tarmoqlar (bot tarmoqlari) xakerlar o‘rtasida talabga aylangan: sotiladi yoki ijaraga beriladi.



1.2-rasm. Bir vaqtning o'zida barcha virusli kompyuterlarning serverga nisbatan ommaviy hujumi

2) DDoS hujumlari

DDoS hujumlari raqibni siqib chiqarish, rahbariyatga po'pisa qilish maqsadida amalga oshiriladi. Odatda, onlayn kazino, do'kon, bukmeykerlar va boshqa resurslar, daromadi uzluksiz onlayn ishlash bilan bog'liq bo'lganlar, bu tahdidga duchor bo'ladi. O'n yillar oldin, bu turdagi jinoyatlar hozirgi kunga nisbatan keng tarqalgan. Hozirgi paytda ushbu hujumga nisbatan muvaffaqiyatli kurash olib borilmoqda. Mening kuzatishlarim va xosting shikoyatlariga binoan, ko'plab resurslar hozirda ko'pincha raqiblar hujumlarni boshdan kechirishmoqda.

3) Pulli SMS yuborish va sizning nomingizdan qo'ng'iroqlar

Ushbu turdagi jinoyatchilikning texnologiyasi juda oddiy. Huquqbuzar, internetda mahsulot xaridlari, ko'rsatilgan xizmat uchun SMS orqali to'lovlarni qabul qilish xizmatlarini ko'rsatuvchi sifatida server ro'yxatidan o'tadi yoki mahalliy telefon provayderi bilan shartnoma tuzadi.

Troyan dasturi pulli SMS yuboradi yoki sizning kompyuteringizdan qo'ng'iroqlarni amalga oshiradi. Pul mablag'lari esa huquqbuzar hisobiga tushadi.

Buning uchun tarmoqdagi virusni tutish ham kerak emas. Ma'lumki, hozirgi vaqtda do'stlaringiz va tanishlaringizga bevosita kompyuteringizdan bepul SMS yuborishni taklif qiladigan juda ko'p bepul dasturlar mavjud. Ushbu dasturni o'rnatib undan foydalansangiz, siz o'zingizning telefon raqamingizni mustaqil ravishda kiritasiz va pulli

xabarlarni jo‘natasiz. Mobil telefon raqamini topish virus uchun muammo emas.

4) Elektron to‘lov tizimlaridan pulni o‘g‘irlash

Bu yerda josus troyan dasturlari ishlaydi. Ular kompyuter tizimida saqlangan kirish kodlari ma’lumotlarini to‘playdi va fayllarni deshifrlaydi so‘ngra, ularni jinoyatchiga yuboradi. So‘nggi vaqtlarda WebMoney, E-Gold kabi to‘lov tizimiga asoslangan himoya usullari maxsus kompleks bo‘lib, murakkab vositalarsiz va jabrlanuvchining qo‘shimcha ma’lumotlarisiz amalga oshirilishiga yo‘l qo‘yilmaydi. O‘g‘rilar o‘g‘irlanadigan summa, tahdid va vositalarga sarflanadigan miqdordan minimal bo‘ladigan vaziyat uchun harakat sxemasini tuzmaydi.

5) Bank kartalaridan axborotni o‘g‘irlash

Bu hozirgi kunda eng ko‘p tarqalgan xakerlik faoliyati turidir. Bu yerda ma’lumki, josus troyan dasturlar, jabrlanuvchining login, parol, karta raqami va kodini qo‘lga kiritish uchun bank saytiga ulanishini kutadi. Josus dasturlar asosan ommabop banklarning qurboni, tovarlar, xizmatlar, transport uchun to‘lov serverlariga tashrif buyuruvchilar uchun dasturlashtirilgan. Siz amalga oshirgan to‘lovdan so‘ng, troyan xostga tashrif buyurgan sahifaning manzili, karta raqami va parolni yuboradi.

Ushbu turdagi jinoyatlarda sizning kompyuteringizda virus bo‘lishi ahamiyatga ega emas. Ayni vaqtda qimmatli ma’lumotlarni kiritishni talab qiladigan ko‘plab soxta web-sahifalar va havolalar mavjud. Buni amalga oshirish uchun turli xil psixologik nomaqbul usullardan tortib, ajoyib yangiliklargacha foydalaniladi. Soxta sahifa sizning kiritgan to‘lov karta, kodi va boshqalar haqidagi ma’lumotlarni buzg‘unchiga darhol bir necha marotaba jo‘natadi.

6) Arxivlash va ma’lumotlarni shifrlash orqali elektron shantaj

Xakerlar kompyuterda ma’lumotlarni to‘plash va ularni juda murakkab kodlar yordamida arxivlovchi dasturlarini ishlab chiqdi. Shundan so‘ng, to‘plangan ma’lumotlar butunlay o‘chiriladi. Troyan nuqtayi nazaridan muhim bo‘lgan alohida fayllar ham kodlanishi mumkin. Bundan tashqari, buzg‘unchi tomonidan ko‘rsatilgan fayllar,

papkalar faqatgina maxsus dastur yoki qo'shimcha kod kiritish yordamida tiklanishi mumkinligi haqidagi xabar yuboriladi. Shuningdek, belgilangan havolada shifrni yechuvchi kodni sotib olish taklifi beriladi.

Ushbu jinoyat eng xavfli usul hisoblanadi. Agar boshqa kompyuterda virus faoliyatini natijalari tuzatilishi mumkin bo'lsa, unda biz murakkab himoya qilish algoritmlariga asoslangan, texnik jihatdan parolni yechib bo'lmaydigan yagona kod bilan ishlashimiz kerak bo'ladi.

7) Mahalliy hujum

Ushbu hujumlar muayyan kompaniya yoki serverni zararlash maqsadida maxsus ishlab chiqilgan virusni yuqtirish yoki ularni tarqatish uchun qilinadigan hujumdir. Buning sababi, har doimgidek, ahamiyatsiz: axborot, hujjatlar, hisob raqamlari, parollarni qo'lga kiritishdir.

Bunday hujumlarga odatda katta firmalar va banklar duch keladi. Bunday kompaniyalarning tarmoqlarini himoyalanganligi odatda, eng yuqori darajada bo'ladi va mahalliy xodimlarning yordamisiz unga kirib bo'lmaydi. Bunday xodimlar insayder deyiladi.

1.5. Operatsion tizimlarni buzish usullari

Operatsion tizimlarga (OS) qarshi amalga oshirilishi mumkin bo'lgan barcha turdagi hujumlar ikkita sinfga bo'linishi mumkin: *mahalliy va masofali hujumlar*.

Mahalliy hujumlar eng samarali va tasirchan hisoblanadi. Hujumkor shaxs tizimga yoki obyektga bevosita jismoniy kirish imkoniga ega bo'lsa yoki mahalliy hujumni amalga oshiradigan obyekt ijrochi bo'lsa, masalan, virusli dastur yoki troyanlarni qo'llagan hollarda kuzatiladi. Boshqa tipdagi mahalliy xakerlar hujjatlarni buzuvchi ("psixologik") kodni o'z ichiga olgan maxsus xabarni yuboradi, foydalanuvchi yoki tizimga ta'sir o'tkazishning yana bir usuli uning kompyuterida buzg'unchiga aloqador bo'lgan dasturni ishga tushurishdan iborat.

Masofali hujumlar eng keng tarqalgan hujumlardan biri bo'lib, unda modem yordamida mahalliy yoki global internet tarmoqlariga ulanish kuzatiladi. Masofali hujumlar samarali bo'lmasdan, eng yomon holatlarda, tarmoqqa ulangan kompyuterning bir me'yorda ishlashini buzadi, uni qayta yuklash yoki foydalanuvchi saqlashga ulgurmagan ma'lumotlarni o'chirib yuborilishiga olib keladigan DoS (Xizmatni rad etish) hujumi bilan tugaydi, natijada ma'lumotlar o'chadi. Hujum amalga oshirilgan kompyuter muayyan tashkilotning serveri bo'lsa, u holda uning ishini to'xtatilishi kompaniyaga katta zarar keltirishi mumkin. Modem aloqasidan foydalangan holda Internetga ulanishni amalga oshiruvchi ishchi stansiyalarga hujum qilish tajovuzkorlarga yetarlicha qiyinchiliklar tug'diradi.

Viruslar va troyanlar orqali mahalliy hujumlarga yo'l qo'ymaslik uchun tizimni va elektron pochtani kuzatuvchi antiviruslardan foydalanish maqsadga muvofiq.

Masofali va mahalliy hujumda kompyuterga kirib borish umumiy tuzilishga ega. Hozirgi vaqtda kompyuterlarga suqilib kirishda, tizim dasturlash va OT arxitekturasi bilimlariga asoslangan murakkab texnologiyalardan foydalaniladi. Odatda, suqilib kirishning uslublarini topishda, buzg'unchiga operatsion tizim, o'rnatilgan ilovalar, tizim xizmatlarini va jabrlanuvchi kompyuterda ishlaydigan dasturlarni tadqiq qilishda bir necha oy sarflanishi lozim.

Biroq, har bir tizimga kirishning aniq yo'lidan farqli o'laroq, buzg'unchi "bufer toshib ketishi" (*buffer overflow*) deb ataladigan usulni qo'llaydi. Ushbu usul dasturiy ta'minot orqali xakerlar dasturini ishga tushirishdan iborat, masalan, masofadan boshqarish yordam xizmati, tarmoqni nazorat qilish yoki xatto kompyuter qurilma drayverini yuklash kabilar.

Ushbu buzish texnologiyasining mohiyati, tizimda muntazam yoki tez-tez ishlatiladigan dasturni, masalan, hodisaga javoban, nafaqat axborotni o'z ichiga olgan ma'lumotlarni, balki ushbu tizimga xakerlar tomonidan tuzilgan dasturni "ilova" qilishdir. Jabrlanuvchi kompyuter dasturlari ma'lumotlari bilan birgalikda xakerlar tomonidan taqdim

etilgan taklifni ham qabul qiladi va maxsus so‘rovdan so‘ng xaker tarmoq dasturi mustaqil ishga tushadi.

Ko‘pincha, bu maqsadlarga erishish uchun ma’lumotlar stekka qo‘yish kabi, ma’lumotlarni olish jarayonidan chiqqanda, qurbon dasturida tarmoq buzg‘unchisi dasturini ishga tushirish, metodikasidan foydalaniladi. Xatto eng sodda dasturda ham xakerlar buferlarni to‘ldirishlari va maqsadli kodlarini yozishi mumkin bo‘lgan yuzlab o‘rinlar bo‘lishi mumkin. Ishlab chiqaruvchilar dasturiy mahsulotlaridagi bunday joylarni tezda topishga harakat qiladilar va ularni tezda tuzatadilar, ammo shunga qaramasdan izlanuvchi xakerlar yangi va yangi zaifliklarni topishni davom etmoqda.

Xakerlar o‘zlarining dasturlarini kompyuterda yuklashga muvaffaq bo‘lganda, ular o‘ylaydigan birinchi narsa quyidagilardir: tizimingizda qanday huquqlar bor va ular bu huquqlar bilan o‘z vazifalarini bajaradimi yoki yo‘qmi, chunki Windows XP-dagi barcha jarayonlar turli xil huquqlarga ega. Ko‘pincha, xakerlar dasturning nomidan ishlayotgan huquqlarga ega bo‘ladilar.

Agar tajovuzkorlar masofaviy hujumda ba’zi tarmoq xizmatlarini cheklash uchun buferni qayta yuklash usulidan foydalansa, unda tizimda faqatgina uning nomidan va uning huquqlari bo‘yicha ishlash mumkin bo‘ladi (ehtimol, bu *SYSTEM* yoki xizmatlar tizim sozlamalaridan kelib chiqib boshqa guruh bo‘lishi mumkin). Shuning uchun, tizimni himoya qilish maqsadida, yuklangan ilovalar va xizmatlar faqat ular uchun zarur bo‘lgan huquqlar ostida bo‘lishiga intilishi kerak.

Shu bilan birga, xakerlar (tarmoq krakerlari) buni anglagan holda, ikki tomonlama hujumni amalga oshiradilar, bu avvalo masofadan hujum qilish va qurbonlik tizimiga kirish, so‘ng tizimda ularning huquqlarini oshirishdir. Bunga zarur huquqlarga ega chiqish obyektni ikkinchi mohiyat bo‘yicha buzish orqali erishiladi. Ikkinchidan, kompyuterga kirish imkoni oldindan ta’minlanganligi sababli buzish lokal hujum sanaladi. Mahalliy hujumlar ko‘proq huquqlarni egallash, ya’ni tizim boshqaruvchisining huquqlari uchun amalga oshiriladi. Shuning uchun ham xakerlarni tizimga kirib borishini chegaralash uchun qo‘shimcha to‘siqlarni qo‘yish, bu tizim uchun barcha foydalanuvchilar

faqatgina haqiqatda zaruriy bo'lgan huquqlar bilan ishlashlarini ta'minlash kerak.

Agar xakerlar tizim administratori yoki Power Users tajribali foydalanuvchilar guruhi huquqlarini olgan bo'lsa, unda tizim ular tomonidan boshqarilishi, muhim ma'lumotlarning to'liq yo'qolishi yoki tijorat ma'lumotlarining kompaniya tashqarisida tarqalishiga olib kelishi mumkin.

1.6. Kompyuter viruslari

Kompyuter viruslari va u bilan qanday kurashish kerak? Bu mavzu bo'yicha o'nlab kitoblar va yuzlab maqolalar yozilgan, o'nlab (yoki balki yuzlab) kompaniyalarning yuzlab (yoki minglab) mutaxassislari kompyuter viruslariga qarshi kurashish bilan shug'ullanmoqdalar. Ko'rinishidan bu mavzu unchalik murakkab emas va shu qadar diqqat markazida bo'ladigan mavzu emas. Biroq, bu unday emas. Kompyuter viruslari ma'lumotlar yo'qolishining eng keng tarqalgan sabablaridan biri bo'lib kelgan va shunday bo'lib qolmoqda. Viruslar tashkilotlar va korxonalar ishiga to'sqinlik qiladigan holatlar mavjud. Bundan tashqari, kompyuter virusi odamning o'limiga olib kelgan bir hodisa qayd etildi - Gollandiyadagi shifoxonalardan birida, bemor virusni yuqtirganligi va noto'g'ri ma'lumot berganligi sababli bemorga morfinni o'ldiradigan dozasini olgan.

Raqobat qiluvchi antivirus kompaniyalarining ulkan sa'y-harakatlariga qaramay, kompyuter viruslari tufayli yo'qotishlar kamaymaydi va har yili yuz millionlab dollarga teng astronomik qiymatga yetadi. Bunday hisob-kitoblar aniq baholanmaydi, chunki bunday hodisalarning faqat bir qismi ma'lum.

Shuni yodda tutish kerakki, antivirus dasturlari va apparatlari viruslardan himoya qilishning to'liq kafolatini bermaydi. Odam-kompyuter tandemining boshqa tomonidagi vaziyat deyarli yomon. Foydalanuvchilar ham, professional dasturchilar ham ko'pincha "o'zini himoya qilish" qobiliyatiga ega emaslar va virus haqida fikrlari ba'zan yuzakidir. Demak, kompyuter virusi nima?

Kompyuter virusi – bu maxsus yozilgan dastur bo'lib, uning majburiy (zaruriy) xususiyati bu o'zining nusxalarini yaratish (asl nusxa bilan bir xil emas) va ularni kompyuter tarmoqlariga va/yoki fayllariga, kompyuter tizimining maydonlariga va boshqa bajariluvchi qismlariga yuborish qobiliyatidir. Bunday holda, nusxalar keyinchalik tarqatish qobiliyatini saqlab qoladi.

Viruslarni quyidagi asosiy xususiyatlarga ko'ra sinflarga bo'lish mumkin:

yashash joyi;

operatsion tizim (OT);

ish algoritmining xususiyatlari;

halokatli imkoniyatlar.

Muhiti bo'yicha viruslarni quyidagilarga bo'lish mumkin:

fayl;

yuklanuvchi;

makro;

tarmoqli

Fayl viruslari turli xil yo'llar bilan (eng keng tarqalgan virus turi) bajariluvchi fayllarni zararlaydi yoki fayllarni ikkinchi nusxasini (hamroh viruslari) yaratadi yoki fayl tizimi tashkiliy xususiyatlaridan (link - viruslari) foydalanadi.

Yuklanuvhi viruslar o'zlarini diskning yuklash sektoriga (yuklash sektori) yoki qattiq diskning tizim yuklash vositasi (Master Boot Record)ga yozadi yoki ko'rsatkichni boot-sektoriga o'zgartiradi.

Makro-viruslar mashhur muharrirlarning hujjatlar fayllari va bir nechta jadvallarini zararlaydi.

Tarmoq viruslari tarqalish uchun kompyuter tarmoqlari va elektron pochtalarning protokollari yoki buyruqlaridan foydalanadi. Ko'p kombinatsiyalar mavjud. Masalan: fayllarni yuklash viruslari, ikkala faylni ham, disklarning yuklash sektorlarini ham zararlaydi. Bunday viruslar, qoidaga ko'ra, ancha murakkab ish algoritmiga ega, ko'pincha tizimga kirishning asl usullarini, yashirin va polimorfik texnologiyalarni qo'llaydi. Bunday kombinatsiyaning yana bir misoli tarmoq makro

virusidir, bu nafaqat tahrirlanadigan hujjatlarni buzadi, balki ularning nusxalarini elektron pochta orqali ham yuboradi.

Zararlangan operatsion tizim (aniqrog'i obyektlari infeksiyaga duchor bo'lgan OT) bu viruslarni sinflarga bo'lishning ikkinchi darajasidir. Har bir fayl yoki tarmoq virusi biron-bir yoki bir nechta OT fayllarini yuqtiradi – DOS, Windows, Win95/NT, OS/2 va boshqalar. Makro viruslar Word, Excel, Office 97 fayl formatlarini yuqtiradi. Yuklanuvchi viruslari, tizimlarning ma'lumotlarini disklarning yuklash tarmoqlarida joylashishi uchun maxsus formatlarni maqsad qiladi.

Viruslar ish algoritmining xususiyatlari orasida quyidagilarga alohida e'tibor qaratiladi:

- rezidentlik;
- stels-algoritmlaridan foydalanishi;
- o'z-o'zini shifrlash va polimorfizm;
- nostandart usullardan foydalanish.

Rezident virus. Kompyuterga virus yuqqanda, rezident virusi o'z rezident qismini RAMda qoldiradi, shundan so'ng u operatsion tizimning zararlangan obyektlarga chaqiruvlarini to'xtatadi va ularga kirib boradi. Rezident viruslar xotirada qoladi va kompyuter o'chirilgunga qadar yoki operatsion tizim qayta ishga tushmaguncha faol bo'ladi. Rezident bo'lmagan viruslar kompyuter xotirasini zararlamaydi va cheklangan vaqt davomida faol bo'lib qoladi. Ba'zi viruslar virusni tarqatmaydigan kichik rezident dasturlarni xotirada qoldiradi. Bunday viruslar norezident hisoblanadi.

Makro viruslarni rezident deb hisoblash mumkin, chunki ular zararlangan tahrirlovchi ishlaganda butun vaqt kompyuter xotirasida bo'ladi. Bunday holda, operatsion tizimning rolini muharrir o'z zimmasiga oladi va "operatsion tizimni qayta ishga tushirish" tushunchasi muharrirdan chiqayotgandek qabul qilinadi.

Ko'p sathli operatsion tizimlarda DOS virusi yashovchisining "umri" virusni yuqtirgan DOS oynasi yopilgan vaqt bilan cheklanishi mumkin va ba'zi operatsion tizimlarda yuklanish viruslarining faolligi OT disk drayverlari o'rnatilgan vaqt bilan cheklanadi.

Stels dan foydalanish – algoritmlar viruslarni o'zlarini tizimda to'liq yoki qisman yashirish imkonini beradi. Eng ko'p uchraydigan stels algoritmlar OT infeksiyalangan obyektlarni o'qish/yozish uchun so'rovlarni to'xtatishdir. Bunday holda, stels viruslar ularni vaqtincha davolaydi yoki infeksiyalanmagan ma'lumotlarni vaqtincha "almashtiradi". Makro viruslar uchun eng mashhur usul makroslarni ko'rish menyusiga murojaatlarning oldini olishdir. Dastlabki fayllarga asoslangan stels viruslardan biri "Frodo" virusi edi, birinchi yuklanuvchi stels virusi "Brain" bo'lgan.

O'z-o'zini shifrlovchi va polimorfizm virusi deyarli barcha turdagi viruslar tomonidan virusni aniqlash protsedurasining murakkabligini oshirish uchun ishlatiladi. Polimorf viruslar (polimorfik), signaturasi bo'lmagan viruslarni aniqlash ancha qiyin, ya'ni doimiy kod bo'limlarini o'z ichiga olmaydi. Aksariyat hollarda bir xil polimorf virusning ikkita namunasi bir-biriga mos kelmaydi. Bunga virusning asosiy tanasini shifrlash va shifrlovchi dasturga o'zgartirish kiritish orqali erishiladi.

Viruslarda turli xil *nostandart* usullar viruslarni OT ning yadrosida (VIRUS virusi singari) chuqur yashirish, ularning doimiy nusxalarini aniqlanishdan (TRUO, Trout2 viruslari) himoya qilish va virusni davolashni qiyinlashtirish uchun tez-tez ishlatiladi (masalan, o'z nusxalarini Flash-BIOS-ga joylashtirish orqali) va h.k.

Viruslarni zararlilik xususiyatlariga ko'ra quyidagilarga bo'lish mumkin:

zararsiz, ya'ni, kompyuterning ishlashiga hech qanday tasir ko'rsatmaydi (tarqalish natijasida diskdagi bo'sh xotira kamayishi bundan mustasno);

zararli emas, ularning ta'siri diskdagi bo'sh xotiraning kamayishi va grafik, ovoz va hokazo effektlar bilan cheklanadi;

kompyuterni jiddiy ishlamay qolishiga olib keladigan xavfli viruslar;

juda xavfli viruslar, operatsion algoritmda protseduralar dasturlarning yo'qolishiga, ma'lumotlarning yo'q qilinishiga, kompyuter xotirasining tizim zonalarida ishlashi uchun zarur bo'lgan ma'lumotlarni

o‘chirib tashlashga olib kelishi mumkin va xatto tasdiqlanmagan kompyuter afsonalaridan biri aytganidek, tezkor ishdan mexanizmlarning harakatlanuvchi qismlari – rezonansga kirish va ba’zi turdagi qattiq disklarning boshlarini yo‘q qilinishiga sabab bo‘ladi.

Virus algoritmida tizimga zararli bo‘lgan biror vaj topilmasa ham, ushbu virusni to‘liq ishonch bilan zararsiz deb atash mumkin emas, chunki uni kompyuterga kiritish oldindan aytib bo‘lmaydigan va ba’zan halokatli oqibatlarga olib kelishi mumkin. Demak, virus, har qanday dastur singari, ham fayllarni, ham disk sektorlarini buzadigan zararli kodlarga ega (masalan, “DenZuk” virusi, bir qarashda umuman zararsiz, 360K disketa bilan juda ravon ishlaydi, ammo katta hajmli disketadagi ma’lumotlarni yo‘q qilishi mumkin). Hozirgacha “COM yoki EXE”ni ichki fayl formati bo‘yicha emas, balki uning kengayishi bilan belgilaydigan viruslar paydo bo‘ldi. Tabiiyki, agar format va nom kengaytmasi mos kelmasa, zararlanishdan keyin fayl ishlamay qolishi mumkin. Windows-da yoki boshqa kuchli dasturiy ta’minotli tizimlarda ishlayotganingizda, DOS-ning yangi versiyalaridan foydalanganda, rezident virusni va tizimni “siqib qo‘yishi” mumkin. Yuklanuvchi viruslar; Makro viruslar; Polimorf viruslar; Boshqa “zararli dasturlar”; Rezident viruslar; Tarmoq viruslari; Stels viruslar; Fayl viruslari; IRC qurtlari.

1.7. Josus dasturlar

Bizning vaqtimiz axborotni ishonchli saqlashning turli xil shakllari bilan ajralib turadi. Pul, qog‘oz va hujjatlarni saqlashda odamlar seyf va banklardan foydalanadilar, idoralar va kvartiralarni himoya qilish uchun esa soqchilarni ishga olishadi, signalizatsiya va kuzatuv o‘rnatishadi, kuzatuvlar qiladilar. Biroq, ishbilarmonlar shaxsiy kompyuterlarida saqlangan ma’lumotni xavfsizligi uchun juda kam vaqt va pul sarflashadi.

Internetga ulanganda, kompyuter egasi kompyuterni allaqachon xavf ostiga qo‘yganiga shubha qilmaydi. Har qanday tajovuzkor foydalanuvchi ushbu kompyuterga ulanishi va maxsus dasturlar yordamida nafaqat saytlar, fayllar va papkalarga tashrif buyurish

tarixini, balki kodlar, parollar, loginlar va boshqalar saqlanuvchi fayllarni ham ko'rishlari va ulardan nusxa olishi mumkin. Bundan tashqari, xaker yashirincha josus dasturlarni qo'llab tizimning keyingi o'zgarishlari haqidagi ma'lumotlarni qabul qilib turish imkoniyatiga ega bo'ladi.

Bunday holatlardan qochish, kompyuterda saqlangan ma'lumotlarning hech bo'lmaganda minimal darajada xavfsizligini ta'minlash bo'yicha ma'lumotga ega bo'lishingiz talab etiladi.

Josus dasturlar (Spyware) foydalanuvchi kompyuteridagi ma'lumotlarni to'playdi va uni elektron pochta orqali yuboradi, bu kompyuterni buzish deb ataladi.

So'nggi yillarda ushbu turdagi dasturlar keng tarqaldi va rivojlandi, bu esa foydalanuvchilar uchun katta xavf tug'diradi.

Josus dasturlari quyidagicha bo'ladi:

- kompyuter yuklanishiga xalaqit beruvchi;
- xabar matnini o'zgartiruvchi;
- foydalanuvchi klaviatura orqali kiradigan barcha ma'lumotlarni yozib olish;
- qaysi fayl va saytlarga tez-tez tashrif buyurganligini yozib olish;
- har bir xabarga reklama qo'shish;
- ekranni rasmga olish, buferni nazoratlash;
- barcha ma'lumotlarni ixtiyoriy pochta qutisiga yuborish.

Bundan tashqari, ular kompyuterning tezligiga ta'sir qiladigan tizim resurslaridan juda talabchan.

Josus dasturlar jarayon ro'yxatida ko'rinmagani uchun, ular faqat maxsus Anti Spyware dasturlar yoki bilimlar yordamida aniqlanishi mumkin.

Ko'p hollarda spyware dasturlar foydalanuvchi kompyuteriga fayllarni almashish tarmoqlari orqali bepul dasturlar bilan birga kirib oladi. Ulardan odatda marketologlar, raqobatchilar yoki faqat havaskorlar foydalanadi. Masalan, foydalanuvchi brauzerni bosh sahifa manzili o'zgartirilganda dastur yuklanishi bilanoq doimiy ravishda mazkur saytga tashrif buyuriladi.

Josus dasturlarni bir nechta turga ajratish mumkin:

Internet Spyware – ushbu turdagi dasturiy ta'minot ulanishlar, barcha tashrif buyurilgan resurslar, elektron pochta xabarlarini yuborish

va qabul qilish, onlayn-do'konlardan qilingan xaridlar haqidagi ma'lumotlarni to'playdi;

HDD Spyware – ushbu turdagi dasturlar foydalanuvchining qattiq diskida saqlangan ma'lumotlarni skanerlaydi;

Keylogger – ilovaning ishlash paytida foydalanilgan tugmachalar haqida ma'lumot saqlash uchun mo'ljallangan. Ushbu turdagi dasturlardan foydalangan holda siz parollar, loginlar va h.k. kiritishlarni kuzatib borishingiz mumkin;

Cookies Spyware – cookies fayllar haqida ma'lumot to'playdi.

Yuqorida sanab o'tilgan josus vositalardan foydalanib, ayg'oqchilar, osonlik bilan parollarni va kodlarni o'qib oladi, masalan, Internet orqali plastik karta vositasida tovarlar yoki xizmatlar haqini to'lashda, WebMoney yoki boshqa to'lov tizimlariga kirish parollarini o'g'irlashni amalga oshiradi.

Asosiy xulosalar

Kompyuter tizimini buzish yoki unga tajovuz qilish-buzg'unchilar tomonidan amalga oshiriladigan, muayyan zaiflikni topish va undan foydalanishdan iborat harakatlardir. Boshqacha aytganda, hujum-tahdidni amalga oshirishdir.

Xavfsizlikka tahdidning uchta asosiy turi mavjud: oshkor bo'lish, butunlik va xizmatdan voz kechish.

Oshkor bo'lish tahdidi, axborotning bilishi lozim bo'lmagan shaxslarga ma'lum bo'lishi.

Butunlikka nisbatan tahdid kompyuter tizimida saqlanadigan yoki bir tizimdan ikkinchisiga uzatiladigan ma'lumotni qasddan o'zgartirish (modifikatsiya qilish yoki o'chirish)ni o'z ichiga oladi.

Xizmat ko'rsatishdan voz kechish tahdidi muayyan xatti-harakatlar natijasida hisoblash tizimidagi bir qancha resurslarga kirishni blokirovka qilish natijasida yuzaga keladi.

"Kompyuter hujumi" deganda odamlarning kompyuteriga ruxsatsiz kirish uchun dasturlarni ishga tushirishini tushunamiz.

Kompyuter tizimlari himoyasini buzishga qaratilgan barcha harakatlar uchta guruhga bo'linadi: ma'lumotlar bazasini boshqarish tizimi darajasidagi hujum, operatsion tizim darajasidagi hujum, tarmoq dasturiy ta'minot darajasidagi hujum;

Operatsion tizimlarga (OT) qarshi amalga oshirilishi mumkin bo'lgan barcha turdagi hujumlar ikkita sinfga bo'linishi mumkin: mahalliy va masofali hujum.

Mahalliy hujumlar, eng samarali va tasirchan hisoblanadi. Hujumkor shaxs tizimga yoki obyektga bevosita jismoniy kirish imkoniga ega bo'lsa yoki mahalliy hujumni amalga oshiradigan obyekt ijrochi, masalan, virusli dastur yoki troyanlarni qo'llagan hollarda kuzatiladi. Boshqa tipdagi mahalliy xakerlar xujjatlarni buzuvchi ("psixologik") kodni o'z ichiga olgan maxsus xabarni yuboradi, foydalanuvchi yoki tizimga ta'sir o'tkazishning yana bir usuli uning kompyuteriga buzg'unchiga aloqador bo'lgan dasturni ishga tushurishdan iborat.

Masofali hujumlar eng keng tarqalgan hujumlardan biri bo'lib, modem yordamida mahalliy yoki global internet tarmoqlariga ulanishda kuzatiladi.

Spyware foydalanuvchi kompyuteridagi ma'lumotlarni to'playdi va uni elektron pochta orqali yuboradi, bu kompyuterni buzish deb ataladi.

Nazorat savollari

1. "Axborotlarni buzish" yoki "ma'lumotlarga hujum" nima?
2. "Axborotlarni talon-taroj qilish" yoki "ma'lumotlarga hujum qilish" bilan bog'liq qanday atamalar mavjud?
3. Xavfsizlikka tahdidlarning asosiy turlari qanday?
4. Hujumlarni tashkil qilish toifalarini sanab o'ting.
5. Ma'lumotlar bazasini boshqarish tizimining darajasida hujumlarni shakllantirish.
6. Operatsion tizim darajasida hujumlarni shakllantirish.
7. Tarmoq dasturiy ta'minot darajasida hujumlarni shakllantirish.
8. Xaker hujumlari uchun imkoniyatlar ro'yxati.
9. Jinoyatchilikning qanday turlarini xakerlar biladi?
10. Operatsion tizimlarni buzishning qanday usullari mavjud?
11. Spyware dasturining mohiyati nimadan iborat?

II-BOB. TARMOQ XATARLARI VA HUJUMLARI

2.1. Tarmoq hujumlarining ba'zi turlari

Tarmoq hujumlari ular boshqaradigan tizimlar kabi xilma-xildir. Ba'zi hujumlar juda murakkab. Boshqalarini esa oddiy operator tomonidan ham amalga oshirilishi mumkin, xatto uning faoliyati qanday oqibatlarga olib kelishi mumkinligini oldindan aytib bo'lmaydi. Hujum turlarini baholash uchun siz TPC/IP protokoliga xos bo'lgan ba'zi cheklovlarni bilishingiz kerak. Internet, davlat idoralari va universitetlar o'rtasidagi muloqotni o'rnatish, o'quv jarayoni va tadqiqotlar o'tkazish uchun yaratilgan. Ushbu tarmoq yaratuvchilari qanchalik keng tarqalishi mumkinligini bilishmagan. Natijada internet protokoli (IP)ning dastlabki versiyalari spetsifikatsiyasida xavfsizlik talablari mavjud emas edi. Aynan shuning uchun ko'plab dastlabki IP lar zaif hisoblanadi. Ko'p yillar o'tib, ko'plab shikoyatlar kelib tushdi (RFC-Request for Comments), nihoyat, ular IP uchun xavfsizlik vositalarini joriy qila boshladilar. Biroq, IP-himoya vositalari dastlab ishlab chiqilmaganligi sababli, barcha dasturlarni ushbu protokolda mavjud bo'lgan xavflarni kamaytiradigan turli xil tarmoq protseduralari, xizmatlar va mahsulotlar bilan to'ldirildi. Quyida biz hujum turlarini qisqacha muhokama qilamiz va ular bilan kurashishning yo'llarini sanab o'tamiz.

1) Operatsion tizim va dasturiy ta'minot tuynuklariga hujum

Ushbu turdagi tarmoq hujumlarini eng keng tarqalgan buzg'unchilik turi deb hisoblashimiz mumkin: operatsion tizimlar va dasturiy ta'minotlardagi zaifliklarni qanday aniqlangan bo'lsa, ushbu zaifliklar ham shunday aniqlanadi, chunki dasturlash tillari qudratli emas. Ma'lum bo'lgan faktlar: kod hajmi qanchalik katta bo'lsa, unda xatolar borligi ehtimoli ham shunchalik katta. Shunday qilib, tizim qanchalik murakkab bo'lsa xatoliklar bo'lishi shunchalik ehtimollidir.

Ochiq kodga asoslangan ilovalar, dasturiy xatoliklarni bartaraf etish nuqtayi nazaridan nihoyatda mutanosib hamda ishonchli dasturiy

kod etaloni hisoblanadi. Yangi paydo bo'lgan xatolarni tuzatish uchun doimo yangilanishlar chiqarib turiladi va qarabsizki hammasi ham u darajada mushkul emas.

Qanday dasturiy ta'minot kodlari xatosi tizimga tashqaridan hujum qilish uchun xavf tug'diradi? Eng xilma-xillari. Yaqqol bir misol sifatida buferni to'lib ketishiga olib keluvshi dastur kodining xatosini keltirishimiz mumkin. Ushbu muammo (bufering to'lib ketishi) eng ko'p zaifliklarning ildizida joylashgan va tarmoq dasturiy ta'minot xavfsizligi sohasida eng keng tarqalgan zaiflik hisoblanadi. Ushbu zaifliklar asosan, kompyuter qurtlari (masalan, CodeRed, Slammer, Lovesan) va viruslar kabi zararli dasturlarda faol foydalaniladi. Ushbu zaifliklardan DDoS-hujumlarini keng ko'lamda uyushtirishda foydalaniladi.

Ushbu turdagi hujumlarni uyushtirish uchun maxsus pochta dasturlari-pochta bomba mashinalari qo'llaniladi. Bu kabi ilovalar elektron pochtani qaytish manzili soxta bo'lgan xabarlar bilan to'ldiradi. Xatto xatning sarlavhasi (HEAD) orqali ham qaytarish manzilini belgilash juda qiyin, chunki jo'natuvchining IPsi sarlavhada ko'rsatilganlar bilan hech qanday bog'liqligi mavjud emas. Ayyor rejani amalga oshirish uchun buzg'unchi foydalanuvchi, faqatgina jabrlanuvchining elektron pochta manzilini bilishi yetarli bo'ladi.

2) Kompyuter qurtlari, viruslar va troyan dasturlari yordamida amalga oshiriluvchi tarmoq hujumlari

Virus bilan zararlanishning belgilari odatda quyidagilar hisoblanadi: ijrochi fayllarning zararlanishi (EXE, COM), yuklanishdagi anomal xulq-atvor, "disklarni mo'jizaviy formatlanishi", tizimdagi uzulishlar va h.k.

Troyan otlari yordamidagi tarmoq hujumlarining mohiyati juda oddiy: zararli dastur keyinchalik ma'lum funksiyalardan foydalangan holda qurbonning mashinasiga tushadi, keyinchalik uning funksional tarkibiga qarab shaxsiy ma'lumotni o'g'irlaydi va keyin ma'lumotlarni dastur egasiga yuboradi, tizimni masofadan boshqaradi (backdoor (orqa eshik) deb nomlangan, proksi-server bo'lib xizmat qiladi (albatta, nima uchunligi tushunarli), DDoS hujumlarida ishtirok etadi va h.k.

A 311 Death Full (bekdor) – ko‘plab xususiyatlarga ega yangi, rivojlangan masofaviy boshqaruv tizimlari:

- o‘rnatishdan so‘ng, dastur tizim ilovalari ostida ishlaydi;
- o‘rnatilgan paytdan e’tiboran ko‘zga ko‘rinmaslik;
- tinglash portlarining ko‘rinmasligi;
- fayl tizimida to‘liq va mukammal boshqarish: nusxa ko‘chirish, nomini o‘zgartirish, fayl va papkalarni o‘chirish, yangi papkalar yaratish;
- berilgan fayllar/papkalarni ma’lum bir niqob bilan (shu jumladan, yangilanish), shuningdek, bitmap tasvirlarni barcha oynalarning ust qismida ko‘rsatish va serverning ichki vositalaridan foydalanib WAV fayllarini namoyish qilish, (mos fayl nomi ustiga sichqonning o‘ng tugmasini bosganingizda, menyuda qo‘shimcha bo‘lim ko‘rsatiladi) fayllarni to‘g‘ridan to‘g‘ri fayl-menejeri orqali elektron pochtaga yuborish;
- sichqoncha tugmasini bir marta bosish bilan dasturlarni ishga tushirish, fayl xususiyatlarini ko‘rish/o‘zgartirish, ro‘yxatga olish va kitobini boshqarish (Windows 2000/XP da, SYSTEM huquqidagi boshqaruv faqat qayta yuklanishdan keyin bajariladi): yaratish, qayta nomlash, kalitlarni va parametrlarni o‘chirish;
- kompyuterni qayta ishga tushirish/o‘chirish/foydalanuvchini tizimdan chiqishi;
- disklarni o‘chirish va monitorni o‘chirish/yoqish. “Shartlar, aytilganidek, keraksiz”.

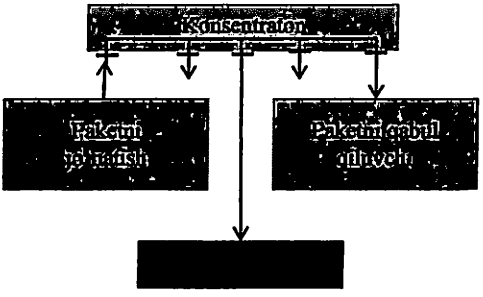
Kompyuter qurtlari vositasida tashkil etilgan tarmoq hujumlariga to‘xtalganda, quyidagilarni aytish kerak: kompyuter qurtlarni tarqatish mexanizmining asoslari bu ko‘p sonli dasturiy teshiklardir, yangi avlod ko‘pincha yangi qurtlarni yaratadi. Hodisalarning mantig‘iga ko‘ra, taxmin qilish mumkin: yangi teshik-yangi qurtdir. Biroq, biz Internetdagi yirik epidemiyaning sababi bo‘lgan kompyuter qurtlarining ko‘pgina modifikatsiyasini esdan chiqarmasligimiz kerak.

3) Paketlar Snifferlari

Paketlar snifferlari – bu tarmoq kartasida foydalanuvchi ilova dasturi hisoblanadi va promiscuous mode rejimida ishlaydi (bu rejimda

jismoniy kanallar orqali olingan barcha paketlar tarmoq adapteri tomonidan qayta ishlashga yuboriladi). Bu holatda sniffer muayyan domen orqali uzatiladigan barcha tarmoq paketlarini o'zida saqlagan holda uzatadi. Hozirgi kunda snifferlar tarmoqlarda butunlay huquqiy asosda ishlamoqda. Ular muammolarni bartaraf qilish va trafikni tahlil qilish uchun ishlatiladi. Ba'zi tarmoq ilovalari ma'lumotlarni matn formatida (telnet, FTP, SMTP, POP3, va h.k.lar) uzatayotgani sababli siz foydali va ba'zida maxfiy ma'lumotlarni (masalan, foydalanuvchi nomlari va parollarini) topish uchun snifferdan foydalanishingiz mumkin.

Login va parollarning ushlab qolinishi xavflidir, chunki foydalanuvchilar ko'pincha bir nechta ilovalar va tizimlarga kirish uchun bir xil login va parollardan foydalanadilar. Ko'p foydalanuvchilar odatda barcha resurslarga va ilovalarga kirish uchun bitta parolga ega. Agar dastur mijoz/server rejimida ishlayotgan bo'lsa va autentifikatsiya ma'lumotlari tarmoq orqali o'qilishi mumkin bo'lgan matn formatida uzatilsa, ushbu ma'lumot boshqa korporativ yoki tashqi resurslarga kirish uchun ishlatilishi mumkin. Xakerlar inson zaifliklarini juda yaxshi bilishadi va ulardan foydalanadi (hujum usullari ko'pincha ijtimoiy muhandislik usullariga asoslanadi). Ular juda ko'p resurslarga kirish uchun bir xil parolni ishlatishimizdan xabardor va shuning uchun ular ko'pincha muhim ma'lumotlarga kirish uchun parolni topishda muvaffaqiyat qozonishadi. Eng yomoni, xaker tizim darajasida foydalanuvchi resursiga kirishga muvaffaq bo'ladi va uning yordamida tarmoq va uning resurslariga kirish uchun istalgan vaqtda foydalanilishi mumkin bo'lgan yangi foydalanuvchi yaratiladi.



2.1-rasm. Sniffing

Quyidagi vositalardan foydalangan holda paketlarni sniffer qilish xavfini kamaytirish mumkin:

Autentifikatsiya – kuchli autentifikatsiya vositalari to'plamni sniffingdan himoya qilishning birinchi usuli hisoblanadi. "Kuchli" autentifikatsiya deganda aylanib o'tilishi qiyin bo'lgan usuli nazarda tutilmoqda. Bunday autentifikatsiyaga misol sifatida-bir martalik parollarni aytish mumkin (OTP-One-Time Password). OTP siz bilgan sizda bor narsalar bilan birlashtirilgan ikki faktorli autentifikatsiya texnologiyasidir. Ikki faktorli autentifikatsiyaga oddiy misol-bu, avvalo sizning plastik kartangiz va siz kiritgan PIN-kod bilan sizni aniqlaydigan bankomatning ishidir. OTP da autentifikatsiya qilish uchun PIN-kod va shaxsiy kartangiz ham talab qilinadi. "Karta" (token) – bu bitta tasodifiy bir martalik parolni ishlab chiqaruvchi apparat yoki dasturiy vosita. Agar xaker bu parolni sniffer yordamida bilib qolsa, bu ma'lumotlar foydasiz bo'ladi, chunki hozirgi holatda parol ishlatilgan va foydalanishdan chiqarib yuborilgan bo'ladi.

Kommutatsiyalanuvchi infratuzilma – tarmoq muhitida paketlarni snifferlash bilan kurashishning yana bir usuli bu kommutatsiyalanuvchi infratuzilmani yaratishdir. Misol uchun, agar barcha tashkilotlarda kommutatsiyalanuvchi ethernet ishlatiladigan bo'lsa, xakerlar faqat bog'langan portga keluvchi trafikka kirish ruxsatini qo'lga kiritishi mumkin. Kommutatsiyalanuvchi infratuzilma sniffing xavfini bartaraf qilmaydi, lekin uning jiddiyligini sezilarli darajada kamaytiradi.

Anti-snifferlar – Sniffingga qarshi kurashishning uchinchi usuli bu tarmoqda ishlayotgan snifferlarni aniqlovchi apparat yoki dasturlarni o'rnatishdir. Ushbu vositalar tahdidni to'liq bartaraf eta olmaydi, ammo boshqa ko'plab tarmoq xavfsizligi vositalari kabi ular umumiy himoya tizimiga kiritilgan. "Anti-snifferlar" deb ataluvchi dasturlar "qo'shimcha" trafiklarni qayta ishlashning oldini olish uchun xostlarning aloqaga chiqish vaqtlarini hisoblab chiqadi.

Kriptografiya-Paketlarni sniffinglash bilan kurashishning eng samarali usuli bo'lib paketlarni ushlab qolishning oldini olomaydi va snifferlar ishini taniy olmaydi, lekin bu ishni foydasiz qilib qo'yadi. Agar aloqa kanali kriptografik jihatdan xavfsiz bo'lsa, demak, xaker

xabarni emas, balki shifrlangan matnni (ya'ni tushunarsiz bitlar ketma-ketligini) ushlab qoladi. Tarmoq darajasidagi Cisco kriptografiyasi IPSec protokoliga asoslanadi. IPSec-bu IP dan foydalanadigan qurilmalar o'rtasida xavfsiz aloqa uchun standart usul. Boshqa kriptografik tarmoq boshqaruv protokollariga SSH (Secure Shell) va SSL (Secure Socket Layer) protokollari kiradi.

4) IP-spufing

IP-spufing, korporatsiya ichida yoki tashqarisida xaker o'zini vakolatga ega foydalanuvchi sifatida tanishtirganda paydo bo'ladi. Bu ikki usulda amalga oshirilishi mumkin. Birinchi holatda, xaker vakolatli foydalanuvchining IP manzillar oralig'ida joylashgan IP-manzil yoki muayyan tarmoq resurslariga kirishga ruxsat berilgan vakolatli tashqi manzildan foydalanishi orqali bo'lishi mumkin. IP-spufing xurujlari ko'pincha boshqa hujumlar uchun boshlang'ich nuqtadir. Klassik misol – bu DoS hujumidir, u xakerning haqiqiy identifikatsiyasini yashiradigan notanish adresidan boshlanadi.

Odatda, IP-spufing mijoz va server ilovalari orasidagi o'zaro aloqa qurilmalari orasidagi uzatiladigan normal ma'lumot oqimiga noto'g'ri ma'lumot yoki zararli buyruqlar kiritish bilan cheklanadi. Ikki tomonlama muloqot uchun, xaker yolg'on IP-manzilga paketlarni yo'naltirish uchun barcha marshrutlash jadvallarini o'zgartirishi kerak bo'ladi. Ba'zi xakerlar, xatto ilovalardan javob olishga harakat qilishmaydi. Agar asosiy vazifa tizimdan muhim faylni olish bo'lsa, ilovalarning javoblari muhim emas.

2.2-rasm. IP-spoofing sxemasi

Xaker agarda marshrutlash jadvallarini o'zgartirsa va to'g'ridan to'g'ri trafikni noto'g'ri IP-manzilga yo'naltirsa, u holda xaker barcha paketlarni qabul qiladi va ularga avtorizatsiya qilingan foydalanuvchi kabi javob berishga qodir bo'ladi.

Spufing tahdidi quyidagi chora-tadbirlar bilan qisqartirilishi mumkin (lekin bartaraf etilmaydi):

Kirish nazorati – IP-spufingni oldini olishning eng qulay usuli – bu kirishni boshqarishni to'g'ri sozlashdir. IP-spufing samaradorligini kamaytirish uchun, tashqi tarmoqdan kelgan va tarmoqning ichida joylashgan bo'lishi kerak bo'lgan asl manzilga ega bo'lgan har qanday trafikni o'chirish uchun kirish boshqarishini sozlash darkor. Bu faqat ichki manzillar vakolatli bo'lgandagina IP spufing bilan kurashishga yordam berishini unutmang. Agar tashqi tarmoq manziliga ruxsat berilgan bo'lsa, ushbu usul samarasiz hisoblanadi.

RFC 2827 Filtrlashi – Sizning tarmog'ingiz foydalanuvchilari tomonidan boshqa tarmoqlar orqali spufing qilishga urinishlarini to'xtatishingiz mumkin (va yaxshi "tarmoq fuqarosi" bo'lishingiz mumkin). Buning uchun manba manzili tashkilotingiz IP manzillaridan biri bo'lmagan har qanday chiquvchi trafikni rad etishingiz kerak, "RFC 2827" deb nomlanadigan bunday filtrlash provayderingiz (ISP) tomonidan amalga oshirilishi mumkin. Natijada, ma'lum bir interfeysda kutilgan manba manziliga ega bo'lmagan barcha trafiklar bekor qilinadi. Misol uchun, agar bir ISP 15.1.1.0/24 IP-manziliga ulanishni ta'minlasa, u filtrni sozlashi mumkin, shunda bu interfeysdan faqat 15.1.1.0/24 dan kelgan trafik ISP routeriga ruxsat etiladi. Barcha provayderlar ushbu turdagi filtrlarni tanitmaguncha, uning samaradorligi imkon qadar kamroq bo'ladi. Bundan tashqari, filtrlangan qurilmalardan qanchalik uzoqda bo'lsa, aniqroq filtrlashni amalga oshirish juda qiyin bo'ladi. Misol uchun, RFC 2827 ni kirish router darajasida filtrlash asosiy trafik manzilidan (10.0.0.0/8) barcha trafikni o'tkazishni talab qiladi, tarqatish darajasida esa (ushbu arxitekturada) siz trafikni aniqroq aniqlab olishingiz mumkin bo'ladi (manzil-10.1.5.0/24).

IP-spufingga qarshi kurashning eng samarali usuli paketni sniffinglashda bo'lgani kabi, bir xil: hujumni mutlaqo samarasiz qilish

kerak. IP-spufing faqatgina autentifikatsiyalangan IP-manzillarga asoslangan holda ishlaydi. Shu sababli, qo'shimcha autentifikatsiya usullarini kiritish ushbu turdagi hujumni foydasiz qiladi. Qo'shimcha autentifikatsiya qilishning eng yaxshi turi kriptografik usul hisoblanadi. Mumkin bo'lmagan holatda esa, bir martalik parollar bilan ikki faktorli autentifikatsiya qilish yaxshi natijalar beradi.

2.2. Web-serverlar xavfsizligi xatarlarini tasniflash

Web-serverlarini xavfsizligi xatarlari - web-serverlarning asosiy sifatli xususiyatlarini (sifatlarini) texnik jihatdan qayta ko'rib chiqishda mumkin bo'lgan buzilishlarga: maxfiylik, konfidensiallik, butunlik va kirish ruxsati. Zamonaviy tasniflash iyerarxik tuzilishga ega. Hujum sinfining nomi o'zbek tilida ham, ingliz tilida ham taqdim etiladi.

1. Autentifikatsiya (Authentication) – web-server autentifikatsiya qilish mexanizmlarida zaifliklarni chetlab o'tish yoki ekspluatatsiya qilishga qaratilgan hujumlarni tasniflaymiz:

1.1. Saralab olish (Brute Force). Ishga tushirish yoki oddiygina "shafqatsiz" sinov va xatolikning avtomatlashtirilgan jarayonidir, uning asosiy vazifasi foydalanuvchi nomi, parol, kredit karta raqami, shifrlash kaliti va boshqalarni topishdir. Ko'p tizim zaif parollar yoki shifrlash kalitlarini ishlatishga imkon beradi. osongina taxmin qilingan yoki lug'atlarda joylashgan parollarni tanlashga qaratilgan;

1.2. Yetarli bo'lmagan autentifikatsiya (Insufficient Authentication). Ushbu zaiflik, web-server buzg'unchiga muhim ma'lumotlarni yoki server funksiyalarini to'g'ri autentifikatsiya qilmasdan kirishiga ruxsat berganida paydo bo'ladi. Bunday turdagi hujumlar ko'pincha tarmoq orqali ma'muriy interfeys orqali amalga oshiriladi;

1.3. Xavfsiz parolni tiklash (Weak Password Recovery Validation). Ushbu zaiflik web-server buzg'unchiga ruxsatsiz ravishda boshqa foydalanuvchilarning parollarini olish, o'zgartirish yoki ularni qaytarib olish imkonini berishi tufayli amalga oshiriladi. Odatda, web-serverda autentifikatsiya qilish foydalanuvchi parolini yoki parol

frazasini eslab qolishini talab qiladi. Kuchli xavfsizlik siyosatida faqat foydalanuvchi parolni bilishi mumkin va uni aniq eslab qolishi kerakligiga qaraladi.

2. Avtorizatsiya (Authorization). Ko'plab saytlar muayyan kontent yoki dastur vazifalariga faqat muayyan foydalanuvchilarga ruxsat beradi. Boshqalar uchun ruxsat cheklangan bo'lishi kerak. Turli texnikalardan foydalangan holda, tajovuzkor o'zining imtiyozlarini kengaytirish va himoyalangan resurslardan foydalanish huquqini qo'lga kiritishi mumkin;

2.1. Seans identifikatsiyasi boshorat qiymati (Credential/Session Prediction). Boshqa foydalanuvchilarning sessiyalarini to'xtatishga imkon beradi. Bunday hujumlar foydalanuvchining noyob sessiya identifikatorini bashorat qilish yoki taxmin qilish yo'li bilan amalga oshiriladi. Ushbu hujum, shuningdek, seansni to'xtatib qo'yish (seansni o'g'irlash), agar muvaffaqiyatli bo'lsa, buzg'unchiga web-serverga buzilgan foydalanuvchining huquqlari bilan so'rov yuborish imkonini beradi.

Sessiya identifikatori cookie-fayllarda, yashirin manzili maydonlarida yoki URL-larda saqlanadi. Agar hujum qiluvchi seans identifikatorini yaratish uchun foydalaniladigan algoritmni aniqlay olsa, u holda quyidagi harakatlar bajarishi mumkin:

– joriy sessiya identifikatoridan foydalangan holda serverga ulanish;

– keyingi sessiya identifikatorini hisoblash yoki topish;

– qabul qilingan cookie fayl identifikator qiymatini/yashirilgan manzili/URL maydonini tayinlash.

2.2. Yetarli bo'lmagan avtorizatsiya (Insufficient Authorization) web-server buzg'unchiga muhim ma'lumotlar yoki funksiyalarga kirishga ruxsat berganida paydo bo'ladi, unga kirish cheklangan bo'lishi kerak. Foydalanuvchi tomonidan muvaffaqiyatli autentifikatsiyadan o'tish u serverning barcha funksiyalari va tarkibiga kirishni anglatmaydi degani emas. Autentifikatsiya qilishdan tashqari, erkin foydalanishni boshqarish kerak. Avtorizatsiya jarayoni usuli, foydalanuvchi, xizmat yoki dasturning qanday harakatlar qilishi mumkinligini belgilaydi.

3. Mijozlarga hujum (Client-side Attacks). Sayt tashrifi vaqtida foydalanuvchi va server o'rtasida texnologik va psixologik jihatlar o'rtasida ishonch munosabati o'rnatiladi. Oddiy ma'noda, foydalanuvchi saytni qonuniy xavfsiz tarkib bilan ta'minlashni kutadi. Bundan tashqari, foydalanuvchilar saytdan hujumlarni kutishmaydi. Ushbu ishonchdan foydalangan holda, tajovuzkor server mijozlariga hujum qilish uchun turli usullardan foydalanishi mumkin:

3.1. Kontentni almashtirish (Content Spoofing). Qusur – kontentning qo'pol o'rnini bosishi jarayoni. Spoofing tarkibining muayyan texnikasi yordamida, tajovuzkor foydalanuvchini web-server tomonidan ishlab chiqarilgan va tashqi manbadan uzatilmaganligiga ishonish uchun majburiy holga keltiradi. Ba'zi web-sahifalar dinamik HTML-kod yordamida yaratiladi. Masalan, ramkaning joylashishi

<frame src = "http: // foo. example / file.html">

quyidagi URL parametrida o'tkazilishi mumkin:

https: //foo.example/page? frame_src = http: //foo.example/file.html

Buzg'unchilar framesrc parametrining dastlabki qiymatini frame_src=http://attacker.example/spoof.html bilan o'zgartirishi mumkin;

3.2. Saytdagi skript (Cross-site Scripting, XSS). Cross sayt Skriptning zaiflik mavjudligi buzg'unchiga serverning ishlaydigan kodini jo'natish imkonini beradi va u foydalanuvchining brauzeriga yo'naltiriladi. HTML/JavaScript odatda bunday kodni yozish uchun ishlatiladi, lekin VBScript, ActiveX, Java, Flash va hokazolardan foydalanish mumkin:

- doimiy (saqlangan);
- doimiy bo'lmagan (aks ettirilgan).

Ularning orasidagi asosiy farq shuki, aks ettirilgan versiyada kodning serverga uzatilishi va mijozga qaytishi HTTP so'rov kesimida va saqlanganda esa turli xillarda amalga oshiriladi.

4. Ma'lumotlarni fosh etish (Information Disclosure). Ushbu klassdagi hujumlar web-ilovalar haqida qo'shimcha ma'lumot olishga qaratilgan. Ushbu zaifliklardan foydalangan holda, buzg'unchiga

ishlatilgan dasturiy ta'minotni aniqlash, mijoz va server versiyasi raqamlari va o'rnatilgan yangilanishlar aniqlanishi mumkin. Boshqa hollarda axborot oqimi vaqtinchalik fayllar yoki zaxira nusxalarini joylashtirishni o'z ichiga olishi mumkin. Ko'pgina holatlarda, bu ma'lumotlar foydalanuvchining ishlashi uchun talab qilinmaydi. Ko'pgina serverlar haddan ortiq miqdordagi ma'lumotlarga kirishni ta'minlaydi, ammo xizmat ma'lumotlarining miqdorini kamaytirish kerak. Hujum qilishga mo'ljallangan dastur haqida qanchalik bilimga ega bo'linsa, tizimni obro'sizlantirsh shu qadar osonroq bo'ladi:

5. Ma'lumotlar sirqib chiqishi (Information Leakage). Server muhim ma'lumotni e'lon qilgan vaziyatda ushbu zaiflik paydo bo'ladi, masalan, ishlab chiqaruvchilar yoki xatolar haqidagi xabarlar tizimni obro'sizlantirish maqsadida foydalanilishi mumkin. Qimmatlilik, niyati buzuq nuqtayi nazaridan, HTML sharhlari, xatolik haqidagi xabarlar yoki oddiygina ochiq holda bo'lgan xabarlarni jamlagan ma'lumotlardir. Ruxsat berilgan axborotni tahlil qilish, niyati buzuq razvedkani amalga oshirishi va server kataloglari tuzilishi haqida tasavvur paydo qilish, foydalanilgan SQL so'rovlar, asosiy jarayonlar va server dasturlari nomlarini aniqlash imkonini beradi.

6. Mantiqiy hujumlar (Logical Attacks). Ushbu sinfning hujumlari dasturning funksiyalaridan yoki uning ishlash mantig'idan foydalanishga qaratilgan. Ilova mantig'i-muayyan harakatlar bajarilayotganda dasturning kutilayotgan jarayoni. Masalan, parolni tiklash, hisob qaydnomasini rasmiylashtirish, auksion savdolari va elektron tijorat tizimidagi operatsiyalar. Ilova foydalanuvchidan muayyan vazifani bajarish uchun bir necha ketma-ket xatti-harakatlarni to'g'ri bajarilishini talab qilishi mumkin. Hujum qiluvchi bu mexanizmlardan o'z maqsadlari yolida chetlab o'tishi yoki undan foydalanishi mumkin.

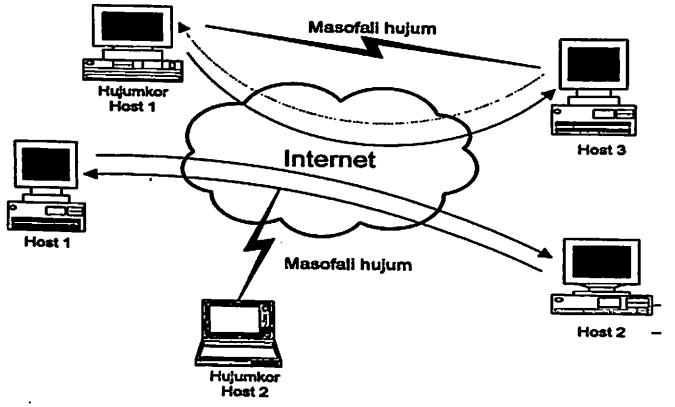
7. Jarayonni tekshirishning zaifligi (Insufficient Process Validation). Ushbu sinfning zaifliklari server dastur operatsiyalarining ketma-ketligini yetarlicha tekshirmasa paydo bo'ladi. Agar foydalanuvchining sessiya holati va ilovani to'g'ri tekshirilmagan bo'lsa, dastur qalloblik maqsadidagi zaiflikka aylanishi mumkin.

Ilovaning ayrim funksiyalariga kirish jarayonida foydalanuvchi ma'lum tartibda bir qator harakatlarni amalga oshirishi kutiladi. Agar ba'zi xatti-harakatlar noto'g'ri yoki noto'g'ri tartibda bajarilgan bo'lsa, unda butunlikni buzish mumkin bo'ladi. Bunday funksiyalarning namunalari transfer, parolni tiklash, xaridni tasdiqlash, hisob qaydlarni yaratish va h.k.

2.3. Masofali hujumlarning tasnifi

Internet taraqqiyoti ushbu tarmoq orqali taqdim etilayotgan imkoniyatlardan foydalanadigan tashkilotlar va odamlarning sonini oshishiga olib keldi. Ammo Internetning keng tarqalganligi xavfsizlik muammosiga qiziqishning ortishi va uning asosiy qoidalarini qisman o'zgarishiga sabab bo'ldi. Gap shundaki, Internet buzg'unchiga butun dunyo bo'ylab ruxsatsiz kirish va tizimlarning ishini izdan chiqarishni amalga oshirishda hech qanday qiyinchilik tug'dirmaydi.

Masofaviy hujum deganda dasturiy ta'minot yordamida Internet-kanallar orqali yuborilgan ma'lum hajmli Internet-paketlarning masofaviy axborotga ta'siri tushuniladi (2.3-rasm).



2.3-rasm. Internet orqali masofaviy hujum

Ma'lumki, hujum – bu tahdidni amalga oshirishdir. Odatda Internet muhitidagi tahdidlar quyidagilardir:

– ***tarmoq tarkibiy qismlaridan birining ishdan chiqishi.*** Uskuna va dasturiy ta'minotdagi xatoliklar yoki loyihalashdagi kamchiliklar natijasida tarmoq tarkibiy qismlaridan birining ishlamay qolishi xizmat ko'rsatishni rad etilishiga yoki xavfsizlikni buzilishiga olib kelishi mumkin. Autentifikatsiya serverlari tomonidan avtorizatsiya qilishning yolg'ondan rad etilishi yoki tarmoqlararo ekranning ishdan chiqishi xavfsizlikka ta'sir qiladigan xatolarning namunalaridan biridir;

– ***ma'lumotni skanerlash.*** Xakerlar yoki avtorizatsiyadan o'tgan foydalanuvchilar tomonidan muhim ma'lumotlarning ruxsatsiz ko'rilishi turli xil mexanizmlar orqali amalga oshirilishi mumkin – ya'ni noto'g'ri manzillangan elektron pochta xabarlari, printerda bosmalash, ruxsatlarni boshqarishni noto'g'ri konfiguratsiyalash, bir xil identifikatordan bir necha kishilarning birgalikda foydalanishi va boshqalar;

– ***axborotdan noto'g'ri foydalanish*** – axborotdan vakolat doirasidan tashqari boshqa maqsadlarda foydalanish xizmatni rad etish, keraksiz xarajatlar, obro'ning yo'qotilishiga olib kelishi mumkin. Jinoyatchilar tizim ichidagi va tashqi foydalanuvchilar bo'lishi mumkin;

– ***axborotni ruxsatsiz o'chirish, o'zgartirish yoki oshkor qilish*** – ma'lumotlar ishonchliligini qasddan yo'q qilish, konfidensial ma'lumotlarning oshkor bo'lishi yoki butunligi talabining buzilishiga olishiga olib kelishi mumkin;

– ***suqilib kirish*** – ruxsat etilmagan shaxslar yoki tizimning xizmat ko'rsatishni rad etishiga hamda hodisadan so'ng jiddiy talofat va xarajatlarga olib keladigan hujum;

– ***maskarad*** – tashkilotni moliyaviy yo'qotish va muammolar girdobiga yetaklovchi xizmatlar yoki axborotni o'g'irlash, moliyaviy tranzaksiyalarni ko'zlash va o'zini vakolatga ega foydalanuvchi sifatida ko'rsatishga urinish.

Har qanday tarmoq axborot tizimining asosiy xususiyati uning tarkibiy qismlari ma'lum joyda taqsimlanishi va ularning o'zaro aloqasi jismoniy (tarmoq ulanishlarini ishlatish) va dasturiy jihatdan (xabar mexanizmidan foydalangan holda) amalga oshiriladi. Bunday holda, barcha boshqaruv xabarlari va ma'lumotlar tarmoq ulanishlari orqali almashinuv paketlari shaklida uzatiladi. Tarmoq orqali uzatilgan paket

sarlavha va ma'lumotlar maydonidan iborat bo'lib, paket sarlavhasi paketga almashinuv protokoli bilan aniqlangan xizmat ma'lumotlarini va murojaat qilish, uni identifikatsiya qilish, boshqa ko'rinishga o'zgaritirish va boshqa ma'lumotlarni o'z ichiga oladi. Bu xususiyat ushbu bo'limda ko'rib chiqiladigan Infratuzilmaga va IP-tarmoqlar protokollariga masofaviy hujumlarning asosiysidir.

Axborot tizimlariga uzoqdan ta'sirlar (hujum) bir nechta belgilar bilan ifodalanadi. Ularning mohiyatini va bajarilish shartlarini ko'rib chiqish uchun quyidagi tasniflash taklif etiladi.

Ta'sir tabiati bo'yicha masofaviy hujumlar quyidagilarga bo'linadi:

- passiv ta'sir qilish;
- faol ta'sir qilish.

Axborot tizimiga passiv ta'sir tizimning ishlashiga to'g'ridan to'g'ri ta'sir qilmasligi, lekin himoyalangan ma'lumotlarga kirish siyosatini buzishi mumkin. Uning taqsimlangan tizimning ishlashiga ta'sir yetishmasligi sababli, masofadan passiv ta'sirni aniqlashni deyarli imkoni yo'q. Axborot tizimidagi passiv masofali ta'sirga misol tariqasida, tarmoqdagi aloqa kanalini tinglash va uzatilgan ma'lumotni ushlab qolinishini keltirish mumkin.

Tizim resurslariga *faol ta'sir* qilish – tizimning ishlashiga bevosita ta'sir qiladi (konfiguratsiya o'zgarishi, noto'g'ri ishlash va h.k.) va uning xavfsizlik siyosatini buzadi. Faol ta'sirning alohida xususiyati passiv ta'sir bilan solishtirganda, uni aniqlash (katta yoki kichik darajada murakkablik bilan) imkoniyatining mavjudligidir. Bunday ta'sir natijasiga misol qilib xizmatdan voz kechishni keltirish mumkin.

Ta'sirni amalga oshirish maqsadiga ko'ra, masofadan qo'zg'atilgan hujumlar quyidagi maqsadlarga yo'naltirilishi mumkin:

- axborot konfidensialligining buzilishi;
- ma'lumotlar yaxlitligi buzilishi;
- tizimning ishlamay qolishi (mavjud emasligi).

Axborot tizimiga deyarli har qanday zararli ta'sirning asosiy natijasi axborotdan ruxsatsiz foydalanishni ta'minlashdir. Bunday kirish axborotni egallash yoki buzish orqali amalga oshiriladi. Axborotni

qo'lga olish imkoniyati unga kirish imkoniyati ham mavjudligini anglatadi, lekin uni o'zgartirish (modifikatsiyalash) mumkin emas. Natijada axborotni qo'lga olish uning maxfiyligi buzilishiga olib keladi. Axborotni egallashning bir misoli tarmoq trafigini tahlil qilishdir (avtorizatsiyalangan tarmoq trafigini tahlili bilan adashtirmaslik lozim).

Axborotni buzilishi, tajovuzkorning tizim obyektlari orasidagi axborot oqimi ustidan to'liq nazorat o'rnatishi va/yoki ishonchli foydalanuvchi nomidan ma'lumotlarni uzatish imkoniga ega bo'lsagina amalga oshirilishi mumkin.

Ta'sir boshlanishining holatiga ko'ra, ta'sirni boshlash uchun uchta shart mavjud:

• *hujum obyekti so'roviga ko'ra hujum qilish.* Bunday holatda, tajovuzkor potensial hujum obyektidan muayyan turdagi so'rovlarni yuborishini kutadi va bu ta'sirni boshlash sharti bo'ladi. Bunday so'rovlarga DNS va ARP talablari misol bo'la oladi;

• *hujum qilinadigan obyektga kutilgan hodisaning boshlanishidagi hujum.* Tajovuzkor masofaviy nishonning operatsion tizimining holatini doimiy ravishda kuzatib boradi va ma'lum bir hodisa sodir bo'lganda tizimga ta'sir qiladi;

• *shartsiz hujum.* Bu holatda, hujumni boshlash hech qanday shartsiz, ya'ni hujum darhol va tizimning holati, hujum qilingan obyektdan mustaqil ravishda amalga oshiriladi. Tajovuzkor hujumni boshlash tashabbuskoridir.

Hujumchining hujum qilingan obyektga nisbatan joylashuviga binoan, ushbu belgiga muvofiq ta'siri ham ichki segmentli, ham segmentlararo ravishda amalga oshiriladi.

Masofaviy hujum nuqtayi nazaridan tajovuzkorni va hujum obyektini bir-biriga nisbatan joylashuvi, ya'ni ular bir xil yoki turli segmentlarda joylashganligi muhimdir. Ichki segmentli hujumda, nomidan ma'lum bo'lganidek, tajovuzkor va hujum obyekti bir xil segmentda. Segmentlararo hujumda tajovuzkor va hujum obyekti turli segmentlarda joylashgan. Bu tasnifning xususiyati hujumning "uzoqlik darajasi" haqida so'z yuritishga imkon beradi.

Amalda, segmentlararo hujumni ichki segmentli hujumga qaraganda amalga oshirish juda qiyin. Biroq, segmentlararo masofaviy hujum ichki segmentli hujumdan ko'ra ko'proq xavf tug'diradi, chunki hujum qilingan obyektdan tajovuzkorning uzoqligi hujumni qaytarishga qaratilgan chora-tadbirlarga sezilarli ta'sir qiladi.

Simsiz yechimlarda ichki segmentli va segmentlararo hujumning muvaffaqiyatli amalga oshishining ehtimoli sezilarli darajada oshadi. Simli va simsiz tarmoqlar o'rtasidagi asosiy farqlardan biri simsiz tarmoqning oxirgi nuqtalari o'rtasida maydonni to'liq nazorat qilish juda qiyin. Juda keng doirali tarmoqlarda, simsiz muhit hech qanday nazorat qilinmaydi. Simsiz tarmoqlar kabi ochiq va boshqarilmaydigan muhitda eng keng tarqalgan muammo anonim hujum qilish imkoniyatidir.

Buzg'unchilar va hujum qilinadigan obyektlar sonining nisbati bo'yicha masofadan turib hujum quyidagi sinflarga bo'linishi mumkin:

- "birga-bir" ta'sir-hujum bir buzg'unchi tomonidan yagona maqsadga qaratilgan;
- "birga-ko'p" ta'sir-hujum bir buzg'unchi tomonidan bir nechta narsalarga qarshi amalga oshiriladi;
- "ko'pga-bir" ta'sir;
- "ko'pga-ko'p" ta'sir.

So'nggi ikki holatda hujum bir yoki bir nechta obyektga nisbatan turli xil kompyuterlardan bir necha tajovuzkorlar tomonidan amalga oshiriladi (taqsimlangan yoki kombinatsiyalashgan ta'sirlar).

2.4. Hujumlarni amalga oshirish bosqichlari

Hujumning amalga oshirishning keyingi bosqichlarini farqlashimiz mumkin:

– hujumdan oldin dastlabki harakatlar yoki "ma'lumot yig'ish";
– xususan "hujumni amalga oshirish";
– hujumni tugatish.

Odatda, hujum haqida gapirilganda, birinchi va oxirgi bosqich haqida unutib, ikkinchi bosqich nazarda tutiladi. Ma'lumot yig'ish va

hujumni tugatish ("izlarni o'chirish"), o'z navbatida, hujum ham uch bosqichga bo'linishi mumkin.

Ma'lumot yig'ish – hujumni amalga oshirishning asosiy bosqichidir. Ushbu bosqichda hujumkorning samarasi hujumning muvaffaqiyati uchun kalit hisoblanadi. Birinchidan, hujumning maqsadi tanlanadi va u haqida ma'lumot to'planadi (operatsion tizimning turi va versiyasi, ochiq portlar va ishlaydigan tarmoq xizmatlari, o'rnatilgan tizim va dasturiy ta'minot hamda uning konfiguratsiyasi va boshqalar). Keyin esa tajavuzkorning ta'siri orqali unga kerakli natija olib keladigan hujum qilinadigan tizimning eng zaif joylari aniqlanadi. Tajovuzkor hujum maqsadi bilan bo'gliq barcha kanallarini aniqlashga urinadi. Bu nafaqat amalga oshirilayotgan hujum turini, balki uni amalga oshirish manbasini ham tanlashga imkon beradi. Misol uchun, hujum qilinadigan uzel Unix va Windows NT boshqaruvidagi ikkita server bilan o'zaro harakat qiladi. Hujum uzeli bir server bilan ishonchli aloqaga ega, ammo boshqasi bilan emas. Hujumchi qaysi serverga hujumni amalga oshirishiga qarab, bu hujumni faollashtiriladi, amalga oshirish vositasi tanlanadi va hokazo. So'ng olingan ma'lumotlarga va istalgan natijaga qarab, eng katta ta'sir ko'rsatadigan hujum tanlanadi.

Misol uchun: SYN Flood, Teardrop, UDP Bomb-xostning ishdan chiqarish; CGI skripti-xostga kirish va ma'lumotni o'g'irlash; PHF-parol faylini va masofaviy parolni topish va h.k.

Routerlarda xavfsizlik devorlari yoki filtrlash mexanizmlari kabi an'anaviy himoya vositalari, birinchi va uchinchi bosqichlarni butunlay "unutgan" holda faqatgina hujumning ikkinchi bosqichida kuchga kiradi. Bundan kelib chiqadi-ki, ko'pincha kuchli va qimmatbaho himoya vositalari bilan ham, hujumni to'xtatish juda qiyin. Bunga yaqqol misol-taqsimlangan hujumlardir. Birinchi bosqichda xavfsizlik vositalarini ishga tushirish, ya'ni hujum qilingan tizim haqida ma'lumot to'plash imkoniyatini cheklash mantiqan to'g'ri bo'lar edi. Bu esa, hujumni butunlay oldini olmasada, hech bo'lmasa tajovuzkorning ishini sezilarli darajada murakkablashtirishi mumkin. Shuningdek, an'anaviy usullar amalga oshirib bo'lingan hujumlarni aniqlashga va ular amalga oshirilganidan so'ng zararni baholashga imkon bermaydi, ya'ni

hujumning uchinchi bosqichida ishlamaydi. Bundan xulosa qilsak, bunday hujumlarning oldini olish choralarini oldindan ko'ra olishning imkoni mavjud emas.

Kerakli natijaga qarab, buzg'unchi hujumning birinchi yoki boshqa bosqichiga e'tiborini jamlaydi. Misol uchun, xizmatni rad etish uchun hujum qilingan tarmoq batafsil tahlil qilinadi, undagi mavjud bo'shliqlar va zaifliklar aniqlanadi; axborotni o'g'irlash uchun hujum qilinayotgan xostlarga oldin aniqlangan zaifliklar yordamida yashirincha kirishga e'tibor qaratiladi.

Hujumlarni amalga oshirishning asosiy mexanizmlarini ko'rib chiqamiz. Bu hujumlarni aniqlash usullarini tushunish uchun muhimdir.

Hujumlarni amalga oshirishning birinchi bosqichi hujum qilingan tizim yoki uzel haqida ma'lumot yig'ishdir. Tarmoq topologiyasi, hujum qilinadigan xostning operatsion tizimining turi va versiyasini, shuningdek, mavjud tarmoq va boshqa xizmatlarni belgilash va hokazolarni aniqlash kabi amallarni o'z ichiga oladi. Ushbu harakatlar turli usullar bilan amalga oshiriladi.

Ushbu bosqichda, tajovuzkor hujumning taxminiy nishoni atrofidagi tarmoq muhitini o'rganadi. Bunday joylar, masalan, "jabrlangan" Internet-provayderining yoki hujum qilinadigan kompaniya ofisining masofali saytlari bo'lishi mumkin. Ushbu bosqichda tajovuzkor "ishonchli" tizimlar (masalan, sheriklar tarmog'i) manzillarini va hujumga bevosita bog'liq bo'lgan xostlarni (masalan, ISP router) aniqlashga urinishi mumkin. Bunday xatti-harakatlarni aniqlash juda qiyin, chunki ular uzoq vaqt davomida va himoya vositasi (xavfsizlik devorlari, hujumlarni aniqlash tizimlari va boshqalar) orqali kuzatiladigan maydon tashqarisida amalga oshiriladi.

Buzg'unchilar tomonidan ishlatiladigan tarmoq topologiyasini aniqlashning ikkita asosiy usuli mavjud:

- TTL modulyatsiyasi (TTL modulation);
- marshrut yozuvi (record route).

Birinchi usul Unix uchun traceroute va Windows uchun tracert-dasturidan foydalanadi. Ular IP-paket sarlavhasida Time to Live ("yashash vaqti") maydonidan foydalanadi, bu tarmoq paketi o'tgan

routerlarning soniga qarab o‘zgaradi. Ping utilita dasturi ICMP paketining yo‘nalishini qayd etish uchun ishlatilishi mumkin. Odatda, tarmoq topologiyasi xavfsizlik konfiguratsiya noto‘g‘ri sozlangan ko‘plab tarmoq qurilmalarida o‘rnatilgan SNMP protokoli yordamida aniqlanishi mumkin. RIP dan foydalanib, tarmoqdagi marshrut jadvali va hokazo haqida ma’lumot olish mumkin. Ushbu usullarning ko‘pchiligi tarmoq xaritalarini yaratish uchun zamonaviy boshqaruv tizimlari (masalan, HP OpenView, Cabletron SPECTRUM, MS Visio va boshqalar) tomonidan qo‘llaniladi. Tarmoq xaritasini yaratish uchun hujumchilar tomonidan ham xuddi shunday usullar muvaffaqiyatli ishlatilishi mumkin.

Xostni identifikatsiya qilish odatda Ping yordamchi dasturini ishlatib ICMP protokolini ECHO_REQUEST buyrug‘i yuborib amalga oshiriladi. ECHO_REPLY javobli xabar xostning mavjudligini bildiradi. Fping yoki nmap kabi ko‘plab xostlarni parallel identifikatsiyalash jarayonini avtomatlashtirish va tezlashtirish uchun bepul dasturlar mavjud. Ushbu usulning xavfli tomoni ECHO_REQUEST so‘rovlari xostning standart vositalari tomonidan aniqlanmasligi hisoblanadi. Buning uchun trafikni tahlil qilish vositalari, xavfsizlik devorlari yoki hujumni aniqlash tizimlaridan foydalanish kerak.

Bu xostlarni aniqlashning eng oson usulidir. Biroq, uning ikkita kamchiligi bor, ya’ni:

1. Ko‘pgina tarmoq uskunalari va dasturlari ICMP paketlarini bloklaydi va ularni ichki tarmoqqa kiritmaydi (yoki aksincha, ularni chiqarib yubormaydi). Masalan, MS Proxy Server 2.0 ICMP paketini o‘tkazishga ruxsat bermaydi. Natijada to‘liq bo‘lmagan tasvir yuzaga keladi. Boshqa tomondan, ICMP paketini to‘sib qo‘yish buzg‘unchiga “birinchi mudofaa chizig‘i” – routerlar, xavfsizlik devorlari va boshqalar borligi haqida ma’lumot beradi.

2. ICMP so‘rovlaridan foydalanish, ularning manbaini osonlik bilan aniqlash imkonini beradi, bu albatta, tajovuzkorning vazifasiga qo‘shilmaydi.

Tarmoq segmentida turli xostlarni aniqlash imkonini beruvchi yana bir usul bu tarmoq kartasining "aralash" rejimidan foydalanishdir. Biroq, tarmoq segmentining trafigi tajovuzkorga o'z xostidan mavjud bo'lmaydigan holatlarda qo'llanilmaydi, ya'ni bu usul faqat lokal tarmoqlarda qo'llaniladi. Xostlarni identifikatsiyalashning yana bir usuli DNS-razvedkasi bo'lib, nom xizmat serveriga murojaat qilish orqali korporativ tarmoqdagi xostlarni aniqlash imkonini beradi.

Masofadagi OTni aniqlashning asosiy mexanizmi TCP/IP stekining, turli xil operatsion tizimlarda turlicha amalga oshirilganini hisobga olgan holda, talablarga javob berishini tahlil qilish hisoblanadi. Har bir masofaviy xostga o'rnatilgan operatsion tizimni aniqlash uchun TCP/IP stekiga maxsus so'rovlar va javoblar yuboriladi.

Hujum qilinayotgan xost haqida ma'lumot to'plash bosqichidan oldingi qadam uning vazifasini belgilaydi, masalan, xavfsizlik devori yoki web-server funksiyalarini bajarilishi. Ushbu qadam faol xizmatlar, xost nomlari, tarmoq topologiyasi va h.k. haqida to'plangan ma'lumotlar asosida amalga oshiriladi.

Oxirgi qadam *zaifliklarni izlashdir*. Ushbu bosqichda, tajovuzkor turli xil avtomatlashtirilgan vositalarni qo'llab yoki qo'pol hujumni amalga oshirish uchun ishlatilishi mumkin bo'lgan zaifliklarni aniqlaydi. Bunday avtomatlashtirilgan vositalar sifatida Shadow Security Scanner, nmap, Retina va boshqalar ishlatilishi mumkin.

Hujumni amalga oshirish – aynan shu vaqtdan boshlab hujum qilingan xostga kirishga urinish boshlanadi. Shu bilan birga, kirish to'g'ridan to'g'ri bo'lishi mumkin, ya'ni uzelga kirish va xizmat ko'rsatishni rad etishni amalga oshirish asosidagi bilvosita kirish bo'lishi mumkin.

To'g'ridan to'g'ri kirishga qaratilgan hujumlarni amalga oshirish ikki bosqichga bo'linishi mumkin:

- *suqulib kirish;*
- *nazoratni o'rnatish.*

Suqulib kirish – perimetrni himoya qilishni (masalan, xavfsizlik devori) yengish demakdir. Bu turli yo'llar bilan amalga oshirilishi

mumkin. Misol uchun, "tashqariga qaraydigan" kompyuter xizmatining zaifligini yoki zararli mazmunli e-mail (makro virus) yoki Java appletlar yuborish orqali foydalanish. Bunday kontent xavfsizlik devoridagi "tunnel" deb ataladi (VPN tunnellari bilan aralashmaslik uchun), undan tajovuzkor o'tib ketadi. Ushbu bosqichga administratorning yoki boshqa foydalanuvchilarning maxsus yordamchi dasturlari (masalan, L0phtCrack yoki Crack) yordamida parolini tanlashi mumkin.

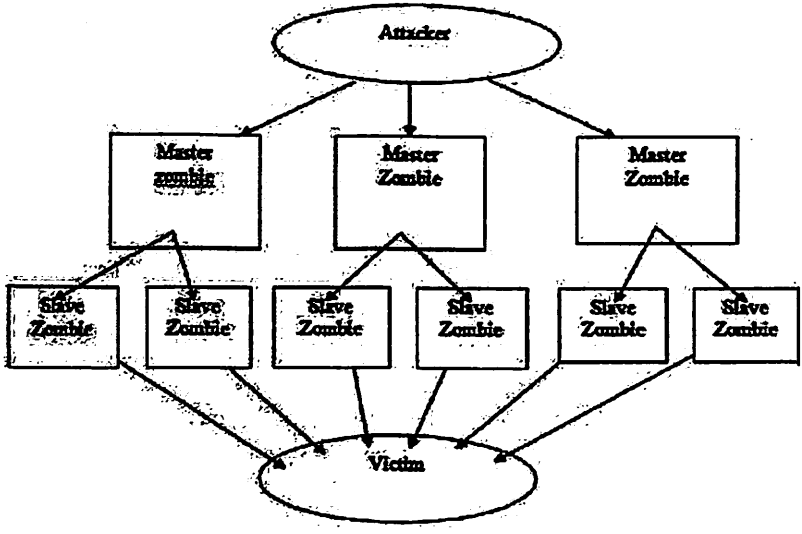
Kirishdan keyin, tajovuzkor hujum qilingan xost ustidan *nazoratni* o'rnatadi. Buni Troyan dasturi yordamida (masalan, NetBus yoki BackOrifice) amalga oshirish mumkin. Nazorat o'rnatilib va "izlar tozalangan"dan so'ng, tajovuzkor hujum qilingan kompyuterdan, egasiga bildirmay, barcha kerakli ruxsatsiz harakatlardan masofadan foydalanishi mumkin. Shu bilan birga, operatsion tizim qayta ishga tushirilgandan so'ng ham korporativ tarmoq xostini boshqarish tashkil etilishi kerak. Buni yuklash fayllaridan birini almashtirish yoki boshlang'ich fayllaridagi yoki tizim yozuvlaridagi zararli kodiga ulanishni o'rnatish orqali amalga oshirish mumkin. Ta'kidlash joizki, hujumkorning ikkinchi bosqichda ikkita maqsadi bo'lishi mumkin. Birinchidan, xostning o'zida va undagi ma'lumotlarga ruxsatsiz kirishga imkon topish. Ikkinchidan, boshqa xostlarga qo'shimcha hujumlarni amalga oshirish maqsadida xostga ruxsatsiz kirish huquqini olish. Birinchi maqsad, faqat ikkinchisi bajarilgandan so'ng amalga oshiriladi. Ya'ni, birinchi navbatda tajovuzkor boshqa hujumlar uchun bazani yaratadi va bundan keyin boshqa xostlarga kiradi. Bu yashirish yoki hujumning manbasini topish qiyinlashishi uchun zarurdir.

Hujumni tugatish – hujumni yakunlash bosqichi tajovuzkor tomonidan "izlarni o'chirish"dir. Odatda qayd yozuvi jurnallaridan va boshqa harakatlardan tegishli yozuvlarni olib tashlanib hujum qilingan tizim dastlabki "eski" holatga qaytariladi.

2.5. DoS va DDoS hujumlari

DoS (Ing. *Denial of Service*-Xizmatni to'xtatib qoyish) – xaker hujumi hisoblash tizimning huquqiy foydalanuvchilariga taqdim etilgan

tizim resurslariga (serverlarga) kira olmaydigan shartlar yoki ushbu tizimdan foydalanishni qiyinlashtiruvchi sharoitlarni yaratish uchun bajariladi. Tizimning so‘rovlarni rad etilishi tizimni egallashga qaratilgan qadam bo‘lishi mumkin (agar favqulodda holatlarda dasturiy ta’minot muhim axborotlarni-masalan, versiya, dastur kodining bir qismi va h.k.). Ammo bu odatda iqtisodiy bosimga qaratilgan bo‘ladi: daromad keltiruvchi sodda xizmatlar, provayder hisobidan va hujumdan qochish uchun choralar sezilarli darajada “maqsad” cho‘ntakka ta’sir qiladi. Bugungi kunda DoS va DDoS hujumlari eng ommabop bo‘lib, ular qonuniy jihatlarda ko‘rsatilgan muhim dalillar qoldirmasdan deyarli har qanday tizimni to‘xtatib qo‘yishiga qodir. (2.4-rasm).



2.4-rasm. DoS hujumi sxemasi

DoS, shubhasiz, xaker hujumlarining eng mashhur hujum turidir. Bundan tashqari, ushbu turdagi hujumlarga qarshi yuz foizlik himoya yaratish juda qiyin. Xatto xakerlar orasida DoS hujumlar unchalik ahamiyatli hisoblanmaydi va ularni ishlatish “Xaker”lar orasida obro‘sizlanishni keltirib chiqaradi, chunki DoS hujumni tashkillashtirish uchun ma’lumot va malakali bo‘lish shart emas. Biroq, bu amalga

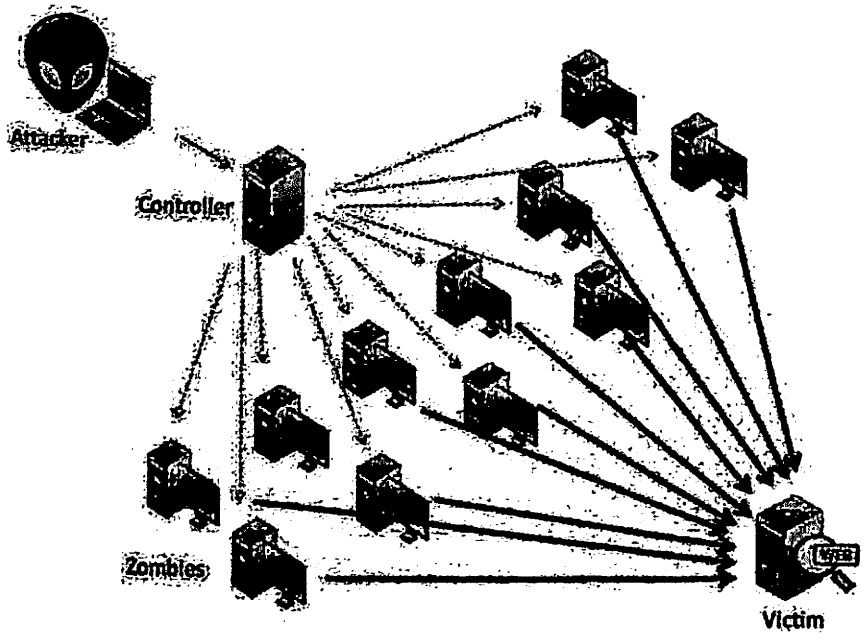
oshirishning oddiyligi va tarmoq xavfsizligi uchun ma'sul bo'lgan rahbarlarning e'tiborini jalb qilish uchun yetarlicha sabab bo'la oladigan katta zarar hisoblanadi.

DoS hujumlari boshqa hujum turlaridan farq qiladi. Ular sizning tarmog'ingizni qo'lga olish yoki ushbu tarmoqdan biron-bir ma'lumot olish uchun mo'ljallanmagan. DoS hujumi tarmog'ingizni, operatsion tizim yoki dasturning foydalanuvchanligini cheklab qo'yib, tarmog'ingizdan an'anaviy foydalanishni to'xtatadi.

Ba'zi server ilovalari (masalan, web-server yoki FTP-server)dan foydalanilganda, DOS hujumlari ushbu ilovalar uchun mavjud bo'lgan barcha ulanishlarni band qilish va oddiy foydalanuvchilarga xizmat ko'rsatishda tarmoqni band holatda keltirish bilan chegaralab qo'yadi. DoS hujumlar TCP va Internet Control Message Protocol (ICMP) kabi standart Internet protokollarini ishlatishi mumkin. Aksariyat DoS hujumlar dasturiy ta'minot xatoliklari yoki xavfsizlik teshiklariga bog'lanib qolmagan, balki tizim arxitekturasining umumiy zaiflik tomonlaridan foydalanadi. Ba'zi hujumlar tarmoq ishlashini bekor qiladi, uni nomaqbul va keraksiz paketlar bilan to'ldiradi yoki tarmoq resurslarining mavjud holati haqida noto'g'ri ma'lumot beradi. Ushbu turdagi hujumni oldini olish murakkab bo'lib, provayder bilan muvofiqlashtirishni talab qiladi. Tarmog'ingizni to'ldirishga mo'ljallangan trafik provayder tomonidan to'xtatilmagan bo'lsa, unda tarmoqning kirish qismida buni amalga oshira olmaysiz, chunki butun tarmoqli kengligi band bo'ladi. Ushbu turdagi hujum bir vaqtning o'zida bir nechta qurilmalar orqali amalga oshirilganda, uni taqsimlangan DoS hujumi deb hisoblashimiz mumkin (DDoS-distributed DoS) bo'ladi.

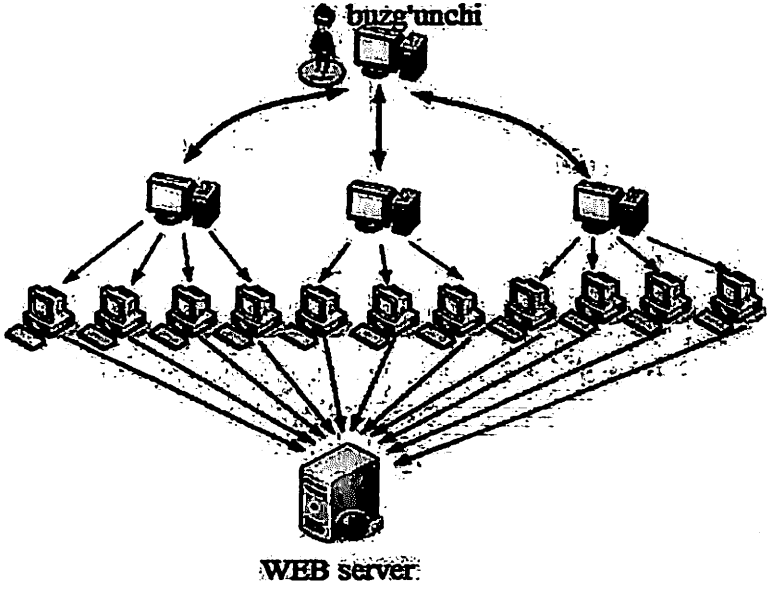
Ushbu turdagi hujumlarda xizmat ko'rsatishdan voz kechishga olib keladigan xatolar yuzaga kelishga yoki xizmatni chegaralashga olib keladigan himoya choralaridan foydalaniladi. Oddiy DoS uslubi samarali bo'lmagan joyda DDoS ishlatiladi. Buni amalga oshirish uchun bir nechta kompyuterlar birlashtirilib, har bir kishi jabrlanuvchi tizimiga

qarshi DoS hujumini amalga oshiradi. Birgalikda bu DDoS hujumi deb ataladi (2.6-*rasm)*.



2.5-rasm. DDoS hujumining ko'rinishi

Birinchidan, tajovuzkor potensial zaif tugunlarni aniqlash uchun maxsus tayyorlangan skript yordamida katta tarmoqni ko'zdan kechiradi. Topilgan zaif nuqtalar o'rganiladi, ushbu zaif nuqtalarga hujum qilinadi va natijada xaker administrator huquqlariga ega boladi. Nazorat o'rnatilgan uzellarga zimdan ish olib boruvchi troyan dasturlari o'rnatiladi. Endilikda bu kompyuterlar zombi kompyuterlar deb ataluvchi DDoS hujumining potensial ishtirokchilariga aylanganligini xatto uning foydalanuvchisi ham payqamaydi. Keyinchalik, tajovuzkor kompyuterga ma'lum buyruqlarni jo'natadi va ular o'z navbatida hujum qilinuvchi ya'ni pirovard server va kompyuterga qarshi kuchli hujumni amalga oshiradi.



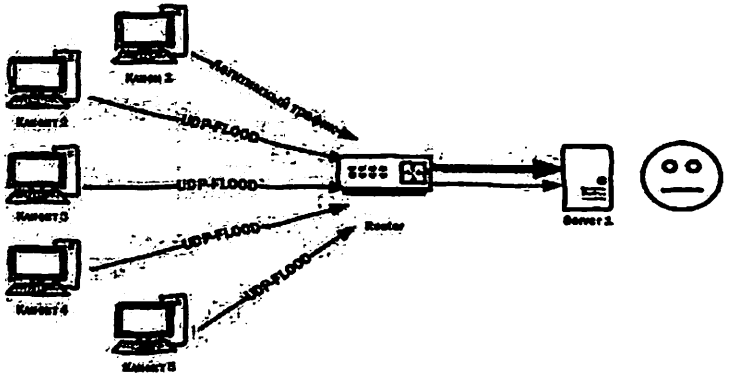
2.6-rasm. DDoS hujumi web-serveri

DoS va DDoS boshqa tarmoq hujumlari o'rtasidagi asosiy farq nima? Mazmunan bunday hujumlar qandaydir konfidensial axborotni qidirish yoki joriy tarmoqdan foydalanishning ruxsatini to'liq nazoratga olishni maqsad qilmagan. Ushbu turdagi hujumlar, avvalambor, paketlarni qayta ishlash yoki tizim resurslarini sarf qilish orqali tizim normal ishlashiga putur yetkazadi.

Bunday hujumlar bir nechta ko'rinishlarga ega:

1. **UDP flood (User Datagram Protocol)** muayyan tizim manziliga ko'p sonli UDP paketlarni yuborish bilan amalga oshiriladi, qo'shimcha komponentli TCP protokoli paketlarni to'g'ri kafolatli yetkazilishini emas, ulanish xizmati ketma-ketlikni datagrammalanmagan holda amalga oshiriladi.

ICMP flood – ICMP protokoliga hujum (Internet Control Message protokoli-xatolar haqida xabar beruvchi va tarmoq uzellari o'rtasida aloqani ta'minlovchi TCP/IP protokollari to'plamidagi majburiy nazorat protokoli). Aynan ICMP protokoli TCP/IP muammolarini topish va tuzatish uchun Ping vositasidan foydalanadi.



2.7-rasm. UDP flood

Smurf – Pingni ifodalaydi – ICMP so'rovlar bu spam-paketlarni yolg'on manba manzili yordamida ommaviy havola qilingan manzilga yo'naltiradi. Smurf hujum negizida manzil bo'yicha ommaviy havolalar yo'naltirilgan Smurf-Ping-so'rovlar yotadi. Ushbu so'rov paketlarida ishlatiladigan soxta manba manzili tajovuzkorning manzili bilan bir xil bo'ladi. Ping so'rovlarini ommaviy yo'nalishlardan qabul qiluvchi tizimlar qay tarzda bo'lishidan qat'iy nazar, unga javob beradi (albatta, kimdan, nega so'rov keldi).

TCP SYN Flood, agar mijoz TCP serveriga ulanishni o'rnatmoqchi bo'lsa, muayyan ketma-ketlikda xabarni almashish talab etiladi. Birinchidan, mijoz tizimi serverga SYN paketini yuboradi. Shundan so'ng, server SYN paketni qabul qilganligini tasdiqlaydi va mijozga SYN-ACK xabarini yuboradi. Mijoz aloqa o'rnatilishini yakunlaydi va ACK xabariga javob beradi va keyin ma'lumotlar almashinuvini qayta davom ettirishi kerak bo'ladi. Server tizimi mijozga tasdiqlash (SYN-ACK) xabarini yuboradi, ammo hali ACK xabarini olmagan nuqtada, yarim ochiq ulanish o'rnatiladi.

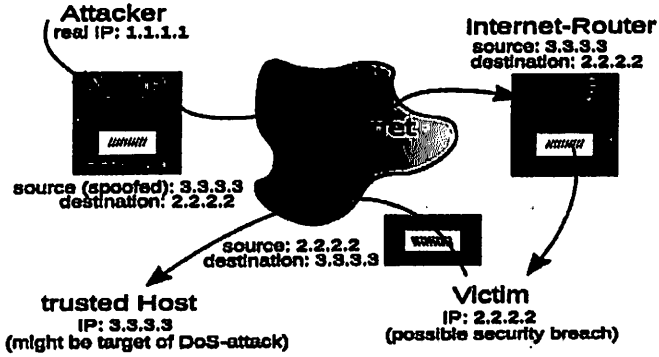
Ping of Death hujumlari juda katta miqdorda IP-paketlarni qabul qilganda oldindan javob qilish tizimini band qilishdir. TCP/IP 65 KB hajmdagi maksimal hajmini qo'llab-quvvatlaydi. **Ping of Death** tizimni qulatishi, muzlatishi va qayta ishga tushirishi mumkin.

Tribe Flood Network (TFN) va **Tribe Flood Network 2000 (TFN2K)** bir yoki bir necha maqsadlarda ko'p manbalardan DOS

hujumiga muvofiqlashtirilgan yuklanuvchi taqsimlangan vositalar muhiti sanaladi. TFN hujumidan foydalanish-manbaning soxta manzili yordamida paketlarni generatsiyalash imkoniyatini beradi. Hujum mexanizmi quyidagicha: Niyati buzuq foydalanuvchi bosh kompyuterga TFN serverlar yoki domenlar ro'yxatiga tajovuz qilish haqida buyruq yuboradi. So'ngra domenlar DoS hujumining belgilangan turini bir yoki bir necha jabrlanuvchining IP manzili bo'yicha generatsiya qiladi. IP manzil va hujum manba portlari paket o'lchami kabi tasodifiy holatlarda o'zgarishi mumkin.

Stacheldracht (so'zma-so'z "tikanli sim»), tajovuzkor va Stacheldraht bosh serveri, avtomatik yangilash agentlari o'rtasidagi aloqani shifrlash, shu jumladan TFN, bir necha DOS hujumi xususiyatlarini o'zida birlashtiradi. Hujumning dastlabki bosqichi ko'p sonli tizimlarga faol ommaviy hujum qilishni nazarda tutib undan keyinchalik hujumlar paytida foydalanishni ko'zlaydi. Keyingi so'nggi bosqich tizimni "bo'ysundirish" bir yoki bir nechta obyektlarga hujum qilish uchun ishlatiladigan oxirgi bosqich.

IP-Spoofing (IP-manzillar soxtalashtirish) hujumi – bu DoSning bir turi emas, ammo shunga qaramay, bu kabi hujumlar DDoSni tashkil qilishda bo'lgani kabi, IPni yashirish zarur bo'lganda keng qo'llaniladi *(2.8-rasm)*.



2.8-rasm. IP-spoofing xurujlari

MAC spoofing hujumlari. Mac-adresni soxtalashtirish uchun ishlatiladi. Ushbu turdagi hujum MAC adres filtrlash vositasi yordamida

ruxsatni cheklagan holda buzg'unchi mashinasi ishonchli mashina sifatida qabul qilinganda amalga oshiriladi.

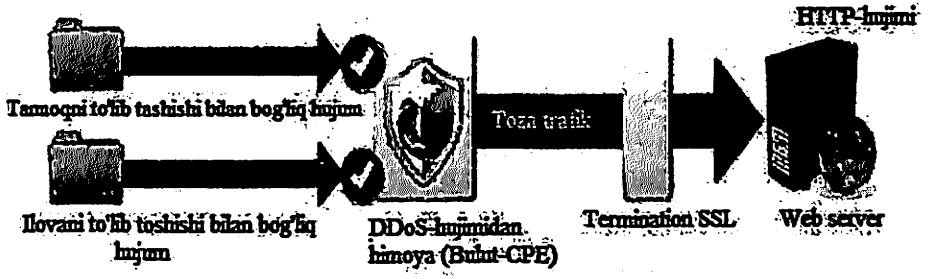
Password attacks (Parolni buzish uchun hujum) hujumida turli xil usullardan foydalanish mumkin: frontal hujum yoki Brute Force-deb ataluvchi parol tanlovchisidan. "Brute Force" – ko'p urunishli autentifikatsiya imkoniyati mavjud bo'lgan hollarda ushbu hujum mos keladi: Elektron pochta qutilari, FTP qayd yozuvlari, SAM-fayllar, PWL-fayllar, UIN va hokazo. Hujumda barcha to'g'ri bo'lishi mumkin bo'lgan belgilar kombinatsiyalari ko'rib chiqiladi.

Packet sniffers – muayyan domen orqali yuborilgan barcha tarmoq paketlarini qo'lga olish uchun "tartibsiz rejimda" tarmoq adapteridan foydalanadigan dasturdir. Tarmoqlarni tahlil qilish va nosozliklarni bartaraf qilish uchun paketlardagi sniffers tarmoqlarda qonuniy foydalaniladi. Biroq, ba'zi tarmoq dasturlari ma'lumotlar matnini ochiq shaklda (telnet, FTP, SMTP, POP3 va h.k.) yuborganligi sababli, sniffing paketlar paketlarni foydalanuvchi nomlari va parollari kabi muhim ma'lumotlarni qo'lga kiritilishiga olib kelishi mumkin.

2.6. HTTPS va SSL-hujumlari

DoS/DDoS hujumlariga qarshi kurashishda ikkita qarash mavjud. Birinchisi, hujumni tarmoqqa chuqur kirib borishidan oldin uni imkon qadar tezroq to'xtatish kerak. Ikkinchisi, bu juda achinarli biroq, barcha trafikni tekshirishuvdan o'tkazish talab etiladi. HTTPS protokoli asosida hujumlarni amalga oshirish oson emas.

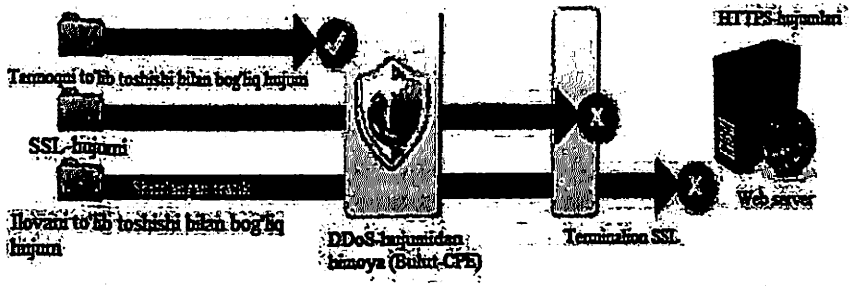
Nima uchun HTTPS hujumi bunday xavf tug'diradi? HTTP protokoliga o'xshash protokoldan foydalanganligiga qaramasdan, u mutlaqo boshqa tahdid darajasini keltirib chiqaradi. Buning sababi shundaki, qoida bo'yicha, HTTP hujumlarini mijoz uskunasida (CPE) joylashgan bulutli yoki ideal holatni, u yerda joylashgan DDoS himoya tizimi yordamida aniqlash va yo'q qilish mumkin (2.9-rasm). Bunday yechimlar dastur darajasidagi HTTP yoki tarmoqni band qilish hujumlariga qarshi kurashishi mumkin.



2.9-rasm. HTTP – hujumi, tizim xavfsizligidan qaytgan DDoS-hujumi

Ammo, xuddi shu hujumlar HTTPS protokoli yordamida amalga oshirilganda, masala boshqacha tus oladi. Tarmoq oqimi to'xtashi mumkin; ma'lumotlar to'la shifrlanmagan va SYN oqimi, masalan, HTTPS-da, HTTP-da bo'lgani kabi ko'rinadi. Biroq, dasturlarga qarshi qaratilgan hujumlarni aniqlash murakkab jarayondir.

HTTPS hujumlarini bulutda yoki mijoz uskunasida joylashgan xavfsizlik tizimlari yordamida aniqlab bo'lmaydi. Ilova darajasida HTTPS trafigi shifrlanadi va shuning uchun uni xavfsizlik mexanizmlari tomonidan aniqlab bo'lmaydi. Bundan tashqari, HTTP unikal SSL-ga ega hujumlarga qarshi himoyasiz hisoblanadi.



2.10-rasm. HTTPS protokoliga hujum

2.10-rasmda ko'rsatilgandek, shifrlangan HTTPS trafigi odatda faqat web-serverda yuklamani muvozanatlashtiruvchida yoki SSL terminatsiya uchun mo'ljallangan moslamada deshifrlanadi. Ushbu

obyektlar, odatda, trafikni DoS hujumlaridan himoya qiluvchi tizimlar tekshiradigan darajadan keyingi (bulutda yoki CPEda) tarmoqqa joylashadilar:

Tashkilotlar o'zlarining SSL kalitlari va sertifikatlarini MSSP bulutiga o'zlari istamagan holda topshirishga rozi bo'lishlari sababli, ushbu harakat ma'lum xavflarni keltirib chiqarishi mumkin, chunki bulutda joylashgan DoS himoya tizimi shifrlangan trafikni tahlil qila olmaydi va shuning uchun hujumni aniqlab bo'lmaydi.

CPE qurilmasi ma'lumotlarni shifrlangan shaklda ko'radi biroq, uni tahlil qila olmaydi. Shunday qilib, buzg'unchi maqsadga erishganidan so'ng hujumni sezish juda kech bo'lishi mumkin.

HTTPS hujumlaridan tashqari, SSL qatlamiga xos bo'lgan va to'g'ridan to'g'ri SSL aloqa mexanizmiga qaratilgan hujumlar ham mavjud.

Odatda, xavfsiz ulanishni o'rnatish uchun SSL-tasdiqlash faqat bir marta amalga oshiriladi. Hujum uchun yangi maxfiy kalitni o'rnatishda "qayta kelishuv" protokol variantidan foydalaniladi. SSL-ni qayta tasdiqlash maqsadida takroriy so'rovlarni yuborish bilan, tajovuzkor serverning protsessoriga ishlamay qolguncha maqsadli yuklamani sezilarli darajada oshiradi.

Agar server "qayta kelishuv" parametrini qo'llab-quvvatlamasa, buzg'unchi yangi SSL ulanishlarini ochishi mumkin, bu esa xuddi shunday ta'sirga olib keladi. SSL hujumi asimmetrikdir – server tomonidan tasdiqlashni amalga oshirish uchun zarur bo'lgan manbalar tasdiqlashni so'ragan (hujumchi) qurilma tomonidan talab qilingan manbadan 15 marta katta.

HTTPS protokoli deyarli barcha web-saytlar tomonidan qo'llab-quvvatlanadi va pul o'tkazmalari u bilan himoyalangan moliyaviy web-saytlarning muhim tarkibiy qismi hisoblanadi. HTTPS hujumlarini aniqlashning murakkabligini hisobga olib, bunday hujumlar keskin o'sishi kutilmoqda va tashkilotlarga, ayniqsa moliya sohasida faoliyat yurituvchilarga ushbu muammoga qarshi kurashish uchun yechimlarni qo'llashlari tavsiya etiladi.

Simsiz qurilmalarga hujum

LAN (Local Area Network) – lokal tarmoq. O'zaro axborot almashish muhiti orqali bog'langan, bir-biriga yaqin binolardagi (chegaralangan hududdagi) ko'plab kompyuterlar to'plamidan hosil bo'lgan tarmoq.

WLAN (Wireless LAN) – simsiz lokal tarmoq.

Shunday qilib, xavfsizlikning markazlashtirilgan siyosatiga qo'shimcha ravishda, haqiqatan ham xavfsiz tarmoqni yaratish imkonsiz bo'lsa, quyidagi masalalarga alohida e'tibor qaratish lozim.

Xavfsiz almashinuv protokollaridan foydalanish (FTP va telnet kabi matnli protokollar aniq tahdid ekanligi sir emas) va ma'lumotlar tunnellanish, masalan, SSH orqali.

Ishonchli kriptografik algoritmlar yordamida muhim ma'lumotlarni shifrlash.

Ikkita xavfsizlik brandmaueri tomonidan xizmat ko'rsatiladigan DMZ (zararsizlantirilgan hududlar) mavjudligini o'z ichiga olgan tarmoq arxitekturasidan foydalanish. DMZ to'liq ishonchli bo'lmagan tarmoq qismiga ishora qiladi. DMZni yaratish g'oyasi ichki tizimni (bu holda bizning xavfsiz LAN) Internetga kirishdan himoya qilishdir.

IDS (Buzib kirishni aniqlash tizimi), IPS (Intruzion profilaktika tizimi)dan foydalanish. Ideal holatda, bunday tizim kirishga urinish paytida signal beradi (yoki IPS-o'zi oldini olishga urinadi).

NAT-dan foydalanish (LAN ulanish manzilini tashqi ulanishning IP-manziliga o'tkazish texnologiyasi). Shubhasiz, NAT xavfsizlik funksiyasi ichki tizimlarning manzillarini tashqi tarmoqdan nozik mijozlar va ikki faktorli autentifikatsiya tizimi bilan tashqi vositalarni himoya qilish (buzg'unchilar xavfini sezilarli darajada kamaytiradi).

MAC Sniffing&Spoofing

Bunday hujumlar bo'lishi mumkin, chunki paketlarni uzatish paytida, xatto WEP yoqilgan bo'lsa ham, MAC-manzili tarmoq orqali ochiq holda uzatiladi. Natijada, MAC manzil to'xtatib qolinishi mumkin. Keyinchalik, xaker soxta MAC-dan foydalanib, APga murojaat qiladi. Shunday qilib, ACL-ga asoslangan autentifikatsiya bekor qilinadi.

Access Point Spoofing

Ushbu turdagi hujumda yolg'on kirish nuqtasidan foydalanib mijozni o'ziga jalb etadi. Tergov kabi parollar va barcha ma'lumotlar buzg'unchiga taqdim etiladi. Ushbu hujumni muvaffaqiyatli amalga oshishi uchun buzg'unchi kirish nuqtasi signali asl AP signali quvvatidan nihoyatda kuchli bo'lishi lozim.

Plaintext-hujum

Qo'llash uslubi: hujumkor kirishdagi jo'natmani biladi va shifrlangan javobni nusxalaydi. Ushbu holatda – faqat kalit talab etiladi. Buning uchun hujumkor tarmoqqa ma'lumotning bir qismini yuboradi va javobni oladi. Javob sifatida qabul qilingan 24-bit uzunlikdagi vektordan kalitni generatsiyalashda foydalaniladi.

2.7. Android platformasiga nisbatan hujumlar

Mobil qurilmalar orqali foydalanuvchilar xavfsizlik jihatidan ehtiyotkor bo'lishni talab qiluvchi katta ahamiyatga ega bo'lgan xizmatlardan foydalanish imkoniyatiga egadirlar (masalan, mobil banking, to'lovlar va mobil identifikatorlar). Shunga ko'ra, xakerlarga yaxshi ma'lumki, autentifikatsiya ma'lumotlarini uyali aloqa vositasida tashkillashtirish orqali qimmatbaho online resurslarga ruxsatsiz kirish imkoniyatiga ega bo'ladi. Ayniqsa, xakerlar ijtimoiy tarmoqlarga kirish uchun moliyaviy ma'lumotlar, mobil tarmoqlardagi shartnoma ma'lumotlarni qo'lga kiritish maqsadida moliyaviy ma'lumotlarga kirish ruxsatini qo'lga olishga harakat qiladi. Bir tomondan, bu urunish shaxsiy ma'lumotlarni to'liq o'g'irlanishi uchun yetarli bo'lishi mumkin.

Bugun dunyodagi ko'plab mobil smartfonlar egalari Android platformasidan foydalanadilar. Shuning uchun, "Xakerlar" ko'proq Android platformasini buzib va unga hujum qiladilar.

Lekin Android-tizimini buzish murakkab jarayon bo'lib, juda ko'p foydalanuvchilar o'z hujjatlari va boshqa turdagi ma'lumotlarini ushbu tizimda saqlashga harakat qiladilar. Shunga mos holda xakerlar shaxsiy Android platformasini buzish orqali o'z mablag'laridan foydalanishlari mumkin.

Ba'zi ishlab chiquvchilar Android platformasining zaif nuqtalarini aniqlash uchun hujumlardan foydalanadilar.

Android operatsion tizimi zaifliklari

Android-smartfon, planshetlar, o'yin konsollari va boshqalar uchun mo'ljallangan OT bo'lib, 2008-yilda paydo bo'lgan. Taxminan 2 milliarddan ortiq foydalanuvchilarga ega. Bu raqam ko'zni quvontiradi. Ma'lumki, dasturiy ta'minot qanchalik keng tarqalgan bo'lsa, buzg'unchilik maqsadlarida tajovuzkorlar uning kamchilik va zaif nuqtalarini o'rganishga harakat qiladi. Android OS xavfsizligi bo'yicha munozaralar juda uzoq vaqt davom etmoqda. Ushbu tizim kimdir uchun yomon hisoblansa, yana kimdir aynan shu OT ni ma'qul ko'radi va uning kamchiliklarini deyarli sezishmaydi.

Android viruslari endilikda yangilik bo'lib qolmay, bu ro'yxatning boshidan "SMS-troyan" o'rin olgan. Ularning maqsadi qisqa raqamlarga qimmatli xabarlarni yuborishdir. Sizning hamyoningizdagi bu manipulyatsiyaga sarflangan mablag' hujumchilarga o'tadi.

Ushbu turdagi dasturlar odatda bir-biridan farq qilmaydi, ba'zi bir interfeys elementlari va pulning o'tkazilishi kerak bo'lgan hisob raqamlari bundan mustasno. Ko'pincha, bu zararli dasturlar ommaviy o'yin turlari va dasturlari ostida yashirinadi.

Shunga bog'liq holda, iste'molchilar apparatning turli funksional imkoniyatidan foydalanish huquqiga ega bo'lishi bilan Android qurilmalari keng ishlatiladi. OTning yangilanishi bilan yangi funksionallik paydo bo'ladi va ilgari topilgan zaifliklar tuzatiladi. Ko'p hollarda sobiq flagman OT yoki dasturiy ta'minotning yangi versiyasini qabul qila olmaydi va shuning uchun mumkin bo'lgan tahdidlardan himoyalanmaydi.

Android tizimining arxitekturaviy tuzilmasi, dastlab barcha dasturlarni tizim fayllarini o'zgartirish imkoniyatini istisno qilish uchun cheklangan erkin foydalanish huquqlari bilan chiqariladi.

Android tizimi mukammal emas, chunki funksional va apparat innovatsiyalarining o'sishi bilan yangi bo'shliqlar, aniqroq aytganda, zaifliklar paydo bo'ladi. Android planshet yoki smartfondan foydalanishda duch kelishi mumkin bo'lgan asosiy muammolardan biri

– super foydalanuvchi yoki root huquqlarini olish imkoniyatidir. Ushbu vazifani bir nechta harakatlar bilan amalga oshiruvchi juda ko‘p dastur, skript va modullar mavjud.

Root huquqlaridan doimiy foydalanish juda xavfli bo‘lmay, u butun tizimni nazorat qilish uchun foydalanuvchilar tomonidan tez-tez ishlatiladi. Zararli dasturlar yaratish uchun ushbu zaifliklarni ishlatsangiz, holat butunlay boshqacha tus oladi.

Eksployt – vositasida root huquqlarini olish uchun xuddi shunday dasturiy modul va ssenariylarni ishlatish orqali hujumchilar qurilmani to‘liq nazorat qiladilar. Masalan, ular foydalanuvchi ishtirokisiz va roziligisiz virus dasturlarini to‘liq o‘rnatishi mumkin.

Android operatsion tizimida troyan virusi ular orasidagi farq va xavf darajasini aniqlash maqsadida uning 4 ta turini ko‘rib chiqamiz.

1) Triada troyan virus.

Birinchi virus 2017-yil mart oyida paydo bo‘lgan bo‘lib, Triada deb nomlanadi. Triada tizimli fayllarni o‘zgartirish uchun root imtiyozlari orqali faol ishlatiladigan modulli troyandir. Bundan tashqari, virus ko‘pincha qurilmaning RAM-da o‘rnashib, uni aniqlash oson emas.

Qurilmada virus paydo bo‘lgandan so‘ng, birinchi navbatda tizim haqidagi ma’lumotlarni to‘plashni boshlaydi, keyin to‘plangan ma’lumotlarni buyruq serveriga yuboradi.

Troyandan xabar olingach, buyruqlar serveri uni zaryadlanadigan qurilmaning shaxsiy identifikatorini o‘z ichiga olgan konfiguratsiyalar va xakerning server bilan bog‘lanishlari va modullarni o‘rnatishi kerak bo‘lgan sozlamalar to‘plami mavjud bo‘lgan fayl yuboriladi. Moduli o‘rnatilgandan so‘ng, troyan telefon xotirasidan o‘zini o‘chirib yuboradi va faqat qurilmaning RAM-da qoladi.

Triadni aniqlash qiyin, chunki u Zygote jarayonini o‘zgartiradi. Zygote Android operatsion tizimining asosiy jarayonlaridan biri bo‘lib, u boshqa ilovalar uchun asos bo‘lib xizmat qiladi. Triada Zygotga yetib kelishi bilan u qurilmaga o‘rnatilgan har bir ilovaning bir qismiga aylanadi. Triada tizimi ishlaydigan jarayonlar ro‘yxatlari va o‘rnatilgan

paketlardan o'z modullarini yashirish uchun tizim fayllarini o'zgartirishi mumkin.

Triada kiruvchi xabarlarni ham filtrlash imkoniyatiga ega bo'ladi. Ba'zi ilovalarni xarid qilishda internetda SMSdan foydalanishadi. Foydalanuvchilar xabarlarni ko'ra olmaydilar, chunki ular dasturni emas, balki SMS-xabarlarni o'qish dasturi bilan qayta ishlanadi.

Ushbu uslub foydalanuvchi hisobidan pulni olish uchun ishlatiladi. Trojan moliyaviy xabarlarni modifikatsiya qiladi, shuning uchun pullar ishlab chiqaruvchilar hisobiga emas, balki jinoyatchilar hisobiga tushadi. Shuning uchun jabrlanuvchi qurilmada biror narsa noto'g'ri ekanini sezmaydi va hech narsadan tashvishlanmaydi.

2) Godless Trojan virusi

Trend Micro kompaniyasi Godness virusning yangi versiyasini aniqladi, Android operatsion tizimining 5.1 versiyasidan oldingi smartfonlar va planshetlar himoyasiz edi. Bu dunyodagi barcha Android qurilmalarning taxminan 90 %ini tashkil etadi.

Godless troyani negizida bir necha eksploytdan va root android-root-tools boshlang'ich ochiq kodli frameworkdan foydalanadi. Virus mustaqil tarzda qurilmani buzadi va har xil turdagi hujumlarni amalga oshiradi. Bundan tashqari, viruslar Google Play ilovalardan foydalangan holda tarqaladi.

Zararlangan ilovani smartfon yoki planshetga o'rnatish natijasida, virusli kod Android tizimli fayllariga kirish va root huquqini qo'lga kiritilishiga olib keladi. Virus kodining bir qismi qurilmalarga yuklab qo'yiladi va boshqa barcha komponentlar masofadan xakerlar buyrug'i bilan serverlardan yuklab olinadi. Virus, mashhur o'yinlarning soxta nusxalari, chiroq ilovasi, Wi-Fi signal kuchaytirgichi kabi kichik, ammo ommabop dasturlarda keng tarqalgan.

3) Faketoken troyan virusi

Dastlabki hujum 2016-yil iyul oyida uyushtirilgan bo'lib, asosan Rossiya, Ukraina, Germaniya va Tailanddagi jami 27 mamlakatdagi 16 mingdan ortiq foydalanuvchilar jabrlangan. Virus odatda, Adobe Flash Player kabi turli xil dastur va o'yinlar ko'rinishida tarqaladi.

Troyan operatsion tizimning himoya mexanizmlari bilan o‘zaro muloqotda bo‘lishga qodir, masalan, boshqa ilovalar oynasini yopish yoki SMS bilan ishlash uchun odatiy murojaat huquqini talab qilish. Android operatsion tizimining so‘nggi versiyalarida ham Faketoken foydalanuvchi ma’lumotlarini o‘g‘irlashi mumkin.

Tizim ishga tushirilgach, troyanchi qurilma administratori huquqlarini (root huquqi) so‘raydi. Agar foydalanuvchi rozi bo‘lmasa, Faketoken bu huquqlarni so‘rab olgan oynani qayta ishga tushiradi va so‘rovni rad etish uchun deyarli hech qanday imkoniyat qoldirmaydi. Administrator huquqlariga ega bo‘lgan Faketoken zarur ruxsatnomalarni so‘rashni boshlaydi: foydalanuvchining SMS-ga, uning fayllari va kontaktlariga kirish, SMS yuborish va qo‘ng‘iroqlarni amalga oshirish hamda h.k. Ushbu so‘rovlar ham ijobiy qaror qabul qilishdan avval foydalanuvchiga doimiy ravishda ko‘rsatiladi.

Troyan boshqa dasturlarning ustidagi oynalarni ko‘rsatish huquqini so‘raydi. Bu uning fishing sahifalarini ko‘rsatish orqali qurilmani bloklashi va foydalanuvchi ma’lumotlarini o‘g‘irlashi uchun kerak. Troyan ishini tayyorlash bosqichida yakuniy so‘rov SMS orqali ishlash uchun so‘rov berish huquqini talab qiladi – bu Faketoken tomonidan foydalanuvchiga Androidning zamonaviy versiyalarida SMSlarni o‘g‘irlamasligidan bexabar qolishiga imkon beradi. Buning uchun troyan SMS bilan ishlash uchun kerakli foydalanuvchi imkoniyatlarini amalga oshiradi. Shuni aytib o‘tish joizki, ba’zi qurilmalarda va Android versiyalarida Faketoken orqali SMS-xabarni yuborishga urinish xatolarga olib keladi. Natijada, foydalanuvchi SMS bilan ishlovchi ilovani qo‘lda o‘zgartirmaguncha SMS xabarlar yuborib bo‘lmaydi. Troyan buni ma’qullamaydi va u bu huquqni yana o‘zi uchun so‘rashni boshlaydi.

Troyan ishida, shuningdek, ilova yorliqlarini manipulyatsiyasini ham ko‘rish mumkin. Faketoken ishga tushgandan so‘ng ijtimoiy tarmoqlar, messenjerlar va brauzerlar bilan bog‘liq bir nechta ilovalar belgisi ostidagi arxivni yuklab qo‘yadi. Keyinchalik, joriy ilovalarni o‘rniga o‘zining yangi yorliqlarini yaratishga harakat qiladi.

Ishchi yorliqlar o‘rnatilganidan so‘ng, troyan ishining keyingi bosqichi foydalanuvchi ma’lumotlarini o‘g‘irlash boshlanadi. Faketoken 77 xil qurilma lokalizatsiyasi uchun turli tillardagi iboralarni o‘z ichiga olgan ma’lumotlar bazasini serverdan yuklab oladi. Agar foydalanuvchi troyan xabari havolasini bosgan bo‘lsa, troyan akkauntidan parolni o‘g‘irlash uchun mo‘ljallangan masalan, Gmail kabi, fishing sahifasini ochadi. Bundan tashqari, xuddi shu sahifada, troyanlar asl Gmail ilovasini parolni o‘g‘irlash maqsadida blokirovka qiladi. Ko‘pgina zamonaviy mobil troyanchilar singari, Faketoken ham asl Google ilovasini bir-biriga mos tushadi. Faketoken jabrlanuvchi bank kartasi ma’lumotlarini o‘g‘irlash uchun Google Play asl ilovasini o‘zining fishing sahifasi bilan berkitadi. Bundan tashqari, troyan hujum qilingan ilovalarning ro‘yxatini va hujum qiladigan ilovalar uchun fishing sahifalarini boshqaruvchi serverdan yaratilgan HTML shabloni sahifasini olishi mumkin. Troyanlar o‘zi uchun troyan serverdan HTML-sahifaning ba’zi usullariga murojaat huquqini olish qobiliyatini ishga tushiradi. Natijada, fishing funksiyasidan tashqari qurilma ma’lumotlari, shu jumladan, Gmail akkaunti manzili va eng yomoni qurilma holatini ishlab chiqaruvchining boshlang‘ich parametrlariga qaytarib qo‘yilishi mumkin.

4) Marcher Trojan virusi

Virus 2013-yildan beri ma’lum bo‘lib, Marcher Google Play ostiga fishing- sahifalari yashirib, hech narsadan shubhalanmaydigan foydalanuvchilardan bank kartalari ma’lumotlarini tortib olishga harakat qilgan.

Asosiy xurujlar – mashhur ilovalarning soxta versiyalariga aloqador havolalarga ega bo‘lgan SMS yoki MMS xabarlaridir. Marcher WhatsApp, Netflix, Super Mario Run va shunga o‘xshash dasturlarni muvaffaqiyatli taqlid qilmoqda. Ushbu link rasmiy Google Play katalogiga olib kelmaydigan uchinchi tomon saytlariga yetaklaydi. Zararli dasturiy ta’minotni o‘rnatganingizdan so‘ng, foydalanuvchi administratorning huquqlari va imkoni bo‘lgan hamma narsalarga kirish huquqini beradi. Agar virus jabrlanuvchini ogohlantirmasa, Marcher tizimdagi o‘z o‘rnini muvaffaqiyatli mustahkamlaydi.

Troyan ikki asosiy vazifaga ega: turli maqsadli dasturlarning oynalariga ishonchli fishing - sahifalarni ko'rsatish, shuningdek, onlayn bank identifikatsiya kodlarini qo'lga kiritishda foydalanuvchi SMS-xabarlarining mazmunini diqqat bilan kuzatishdir. Troyan, Instagram, Play Store, Facebook, Skype, Viber, WhatsApp Messenger va Gmail kabi ilovalarning yuqori qismida fishing sahifalarini ko'rsatib, bank kartasi ma'lumotlarini o'g'irlashga urinadi. Antiviruslar Marcherga qarshi kuchsizdir, chunki virus xavfsizlik yechimlarini aldash uchun oddiy usullardan foydalanadi. Qurilmada ishlaydigan antivirusni aniqlagan holda, troyan foydalanuvchi dasturini ochishga ruxsat bermaydi va jabrlanuvchini uy ekraniga majburan qaytaradi. Antivirus tahdidni aniqlasa ham, foydalanuvchining ruxsati keyingi harakatlar uchun talab qilinadi, so'ngra antivirus muammoni hal qilish va o'zaro ta'sir o'tkazish uchun hech narsa qila olmaydi. Operatsion tizimning boshqa versiyalari foydalanuvchilari ham virusga chalingan bo'lsada, tajovuzkorlar asosan e'tiborni Android 6.0.1 ga qaratmoqda.

2.1-jadval

Mobil troyanlarning farqlari

Nomlanishi	OT versiyasi	Qurbon turi	Root huquqi	Virus vazifasi	Tarqalishi
Triada	4.4.2	Dasturchi, foydalanuvchi	+	Pulni o'g'irlash uchun SMS-xabarlar	Ilovalar
Godless	5.1.	Foydalanuvchi	+	Foydalanuvchi haqida josuslik	Ilovalar
Faketoken	5.0	Foydalanuvchi	+	Ma'lumotlarni o'g'irlash	Dasturlar va ilovalar
Marcher	6.0.1	Foydalanuvchi	+	Soxta sahifalarga havola qilingan SMSva MMS	Ilovalar

2.1-jadvalda mobil troyanlarning turli viruslar va operatsion tizim versiyalaridagi ishi ko'rsatilgan. Ijtimoiy muhandislik va fishing sahifalari usullari qurboni bo'lgan troyanlari hech qanday shubhaga

bormaydigan foydalanuvchilar bo'ldi. Virusni butunlay nazorat qilish uchun super user huquqlarini talab qiladi. Virusning vazifalari pulni o'g'irlash, aloqa raqamlari, elektron pochta parollari va foydalanuvchi harakatlarining kuzatuvidir. Troyanlar foydali ilovalar va dasturlar ko'rinishida qurilmaga kirishdi.

So'nggi yillarda mobil telefonlar bir qancha boshqa zararli dasturlar bilan bog'liq kiberjinoyatchilik muammolarini o'sishi va yorqinroq tus olishi ta'kidlanmoqda.

2012-yilda paydo bo'lgan mobil qurilmalar uchun 5 ta eng xavfli zararli dasturlarning ro'yxati aniqlandi:

FakeInst

Fake Instagram, Opera Browser, Skype kabi mashhur ilovalar sifatida namoyon bo'ladi va foydalanuvchi nomidan pulli raqamlarga SMS yuboradi. FakeInst oilasida RuWapFraud, Depositmobi, Opfake va JiFake kabi ko'plab imkoniyatlar mavjud. Androidda zararli dasturlarning umumiy sonini oltmish foizi FakeInst oilasiga mansub bo'lib, geografik jihatdan u Rossiyada va dunyoning boshqa mamlakatlarida ham namunalari mavjud.

SMSZombie

Ro'yxatda yaqindagina Xitoyda aniqlangan so'nggi bir necha hafta ichida 500 mingdan ortiq qurilmaga zarar yetkazgan SMSZombie dasturi ham bor. U China Mobile onlayn to'lovlar tizimiga SMS xabar yuboradi. To'lov miqdori, chastotasi va maqsadi-zararli dasturni ishlab chiquvchi tomonidan nazorat qilinadi. O'rnatishdan so'ng, u qurilmaning administrator imtiyozlarini oladi va bundan keyin SMSZombie o'chirish deyarli imkonsiz.

NotCompatible

Aprelda Lookout Mobile Security tomonidan kashf qilingan, Lookout xavfsizligi bilan bog'liq dasturlar yetakchi menejeri DerekHalliday ta'kidlaganidek, NotCompatible web-saytlardan foydalanib zararli dasturni tarqatishning asosiy usuli sifatida ishlatadigan birinchi qismi.

"Android-brauzer virusli web-saytga tashrif buyurganida NotCompatible avtomatik ravishda yuklab qo'yiladi", deydi u. Yuklab

olingan ilovani o'rnatish uchun foydalanuvchini ishontirish maqsadida tizimni yangilanishi ostiga yashirinadi.

Agar u muvaffaqiyatli o'rnatilgan bo'lsa, "NotCompatible" maxsus tarmoqlarga kirishga ruxsat berishi mumkin, bu viruslar Android qurilmasini ushbu tarmoqlarga ulaydi va undan keyin himoyalangan ma'lumotlarga yoki tizimning o'ziga kirish uchun foydalanish mumkin, deydi Halliday.

Android Bmaster

Androidga tekshirilgan ilovalar bilan birga o'rnatiladi. Yil boshida Bmaster Android Marketga aloqasi bo'lmagan ilovalar sifatida sanalgan. Jabrlanganlarning aksariyati Xitoylik edi. Qurilmada zararli dastur telefonning xotirasidan konfidensial ma'lumotlarni o'g'irlaydi, jumladan, Cell ID, manzil kodi va IMEI raqami, so'ng foydalanuvchi nomidan pulli raqamlarga SMS yuboradi.

"Android Bmaster komandasi va boshqaruv serverlari tahlili shuni ko'rsatdiki, ushbu dasturning ishlash muddati davomida botnet ga ulangan zararlangan qurilmalar soni bir necha yuz mingni tashkil etdi", deydi Symantec Security Response direktori Kevin Haley. "Ixtiyoriy kunda 10 000 dan 30 000 gacha foydani yetkazib beradigan zararlangan qurilmalar soni yil sayin barqaror oshib borganda millionlab dollar foyda keltirishi uchun yetarli bo'lgan.

LuckyCat

LuckyCat – bu Yaponiyadagi aerokosmik va energetika sanoati sohalarida, shuningdek, Tibet aktivistlariga qarshi hujumni maqsad qilgan kompaniya. Zararlangan hududlarni ko'paytirish maqsadida hujumchilar Android platformasiga mo'ljallangan hujumning yangi versiyasini yozdilar.

Ilova o'rnatishdan so'ng, ekranda "testService" matnli qora belgini ko'rsatadi va qurilmadan ma'lumotlarni o'qishga imkon beradigan bo'shliqni yaratadi.

"LuckyCat – bu Android platformasiga qaratilgan birinchi APT (advanced persistent threat) - deydi mutaxassislar. Bu Android platformasidagi barcha qurilmalariga qaratilgan troyan oti bo'lib, bo'shliqni yaratadi va zararlangan qurilmadan ma'lumotni o'qiy boshlaydi.

Android OT bilan ishlashdagi xavfsizlik muammolaridan biri bu inson faktori bo'lib, loqaydlik, e'tiborsizlik, o'ziga ishonish va manmanlik, erta yoki kech ixtiyoriy aqlli tizim xavf ostiga qolishi ehtimoldan xoli emas.

Asosiy xulosalar

Tarmoq hujumlari xilma-xilligi: Operatsion tizim va dasturiy ta'minotlarning tuynuklariga asoslangan hujumlar; Kompyuter qurtlari, viruslar va troyan dasturlari yordamida amalga oshiriluvchi tarmoq hujumlari.

Web-serverlarini xavfsizligi xatarlari – web-serverlarning asosiy sifatli xususiyatlarini (sifatlarini) texnik jihatdan qayta ko'rib chiqishda mumkin bo'lgan buzilishlari: maxfiylik, konfidensiallik, butunlik va kirish ruxsati.

Web-serverlar xavfsizligiga nisbatan tahdidlar tasnifi: Autentifikatsiya (tanlov, yetarli bo'lmagan autentifikatsiya, parollarni tiklash xavfi); Avtorizatsiya (sessiya identifikatorini bashorat qilish, yetarli bo'lmagan avtorizatsiya); Mijozlarga hujum (kontentni almashtirish, ssenariylarni saytlararo bajarilishi); ma'lumotlarni fosh bo'lishi; Ma'lumotlar sirqib chiqishi; Mantiqiy hujumlar; Jarayonni tekshirishning zaifligi.

Masofaviy hujum-dasturiy ta'minot yordamida Internet-kanallar orqali yuborilgan ma'lum hajmli Internet-paketlarning masofaviy axborotga ta'siri tushuniladi.

Odatda Internet muhitidagi tahdidlar quyidagilardir: Tarmoq tarkibiy qismlaridan birining ishdan chiqishi, ma'lumotni skanerlash, axborotdan noto'g'ri foydalanish, axborotni ruxsatsiz o'chirish, o'zgartirish yoki oshkor qilish, suqilib kirish, maskarad.

Ta'sir tabiati bo'yicha masofaviy hujumlar quyidagilarga bo'linadi: *passiv ta'sir* qilish (tizimning ishlashiga to'g'ridan to'g'ri ta'sir qilmasligi, lekin himoyalangan ma'lumotlarga kirish siyosatini buzishi mumkin) va *faol ta'sir* qilish (tizimning ishlashiga bevosita ta'sir qiladi va uning xavfsizlik siyosatini buzadi).

Hujumlarni amalga oshirish bosqichlari: Hujumdan oldin dastlabki harakatlar yoki "ma'lumot yig'ish", xususan "hujumni amalga oshirish" va hujumni tugatish.

DoS hujumi – xaker hujumi hisoblash tizimning huquqiy foydalanuvchilariga taqdim etilgan tizim resurslariga (serverlarga) kira olmaydigan shartlar yoki ushbu tizimdan foydalanishni qiyinlashtiruvchi sharoitlarni yaratish uchun bajariladi.

Simsiz qurilmalarga qaratilgan hujumlar turlari: MAC Sniffing&Spoofing, Access Point Spoofing, Plaintext-hujumi. Android OT uchun quyidagi troyan viruslari mavjud: Triada, Godless, Faketoken, Marcher.

Mobil qurilmalar uchun eng xavfli zararli dasturlar: FakeInst, SMSZombie dasturi, NotCompatible, Android Bmaster, LuckyCat.

Android OT bilan ishlashdagi xavfsizlik muammolaridan biri bu inson faktori bo'lib, loqaydlik, e'tiborsizlik, o'ziga ishonish va manmanlik, erta yoki kech ixtiyoriy aqlli tizim xavf ostiga qolishi ehtimoldan xoli emas.

Nazorat savollari

1. Tarmoq hujumlarining xilma-xilligini izohlang.

2. Pochta bombardimoni dasturi vazifasi nimadan iborat?

3. Qurtlar, viruslar, troyan otlaridan foydalanib qilinadigan tarmoq hujumlaridagi virusdan zararlanish alomatlari.

4. Web-serverlarga qaratilgan hujumlar sinflari.

5. Internet muhitidagi xatarlarning namunaviy turlarini ayting.

6. Ta'sir jihatidan masofali hujumlar nimaga qaratilgan?

7. Jinoyat obyektidan farqli o'laroq buzg'unchi tutgan o'rin bo'yicha qanday choralar qo'llaniladi?

8. Jinoyat obyekti va uning soni jihatidan kelib chiqib qanday qarshi chora sinflari mavjud?

9. Hujumni amalga oshirish bosqichlarini tushuntiring.

10. Simsiz qurilmalarqa qaratilgan hujumlar turlari.

11. Android platformasidagi hujum asoslari.

12. Android OT bo'shliqlari.

13. Mobil troyanlar farqlarini tariflang.

14. Android OT bilan ishlash xavfsizlik masalalari nimalardan iborat?

III-BOB. DASTURIY TA'MINOTNI BUZISH

3.1. Dasturiy ta'minot xavfsizligi

Dasturiy ta'minot xavfsizligi (DTX) bu keng ma'noda dasturiy ta'minotning o'ziga xos, xususan kompyuter tizimiga turli xil salbiy ta'sir ko'rsatmasdan ishlash xususiyati tushuniladi. DTX darajasi ma'lum sharoitlarda uning ishlashi davomida funksional jihatdan mos keladigan natijaga erishish ehtimoli degan ma'noni anglatadi. Funksional yaroqsiz natijaga olib keladigan sabablar turli xil bo'lishi mumkin: kompyuter tizimlaridagi xatoliklar, dasturchilar va operatorlarning xatosi, dasturiy ta'minotdagi nuqsonlar. Bunday holda, nuqsonlar odatda ikki turga bo'linadi: qasddan va kutilmagan. Birinchisi, qoida sifatida, tajovuzkor harakatlarning natijasi, ikkinchisi-insonning noto'g'ri harakatlari.

Qasddan sodir etiladigan nuqsonlardan himoya qilish muammolarini o'rganishda quyidagi masalalarni hal qilish muqarrar:

– kim bajariladigan dastur kodiga zararli ta'sirning dasturiy nuqsonlarini amaliy ravishda joriy etishi mumkin;

– bunday kamchiliklarni ishlab chiqadigan subyektning harakatlarini mumkin bo'lgan sabablari nima;

– dasturiy nuqson mavjudligini qanday aniqlash mumkin;

– dasturiy ta'minot xatosini, qasddan qilingan dasturiy nuqsondan qanday ajratish mumkin;

– kompyuter tizimini ishlatishda zararli dasturiy vositalarni faollashtirishning eng katta oqibatlari qanday.

Professional dasturchilar dasturiy kod xavfsizligi masalasiga doir muammoli savollarning muhimligini ancha vaqt oldin tushunishgan. Dasturiy ta'minot xavfsizligi bo'yicha mutaxassislar amaliyotda ko'rsatilgan materialni qo'llash haqida aniq ma'lumotga muhtojligini tushunamiz. Muammo shundaki, bunday oddiy va ommabop usullar "xavfsiz ishlashni ta'minlash uchun dasturiy ta'minot provayderlari"

tomonidan barcha muammolar uchun universal yechim sifatida ishlatiladi (masalan, "qora quti" deb ataluvchi testlash tizimi ishlash tamoyillari foydalanuvchiga ma'lum emas).

Dasturiy ta'minotning ishlash tamoyillarini aniqlash-bu xavfsizlik siyosat qoidalarini o'rnatish va tizimlashtirish, so'ngra ushbu siyosatni tegishli texnologiya bilan amalga oshirishni o'z ichiga olgan jarayondir. Dasturlarning xavfsiz ishlashini ta'minlash uchun sehrli yoki universal vositalar mavjud emas. Mukammallashgan kodni tekshirish usullari amalga oshirish bosqichida xatolarni aniqlash uchun juda foydalidir, ammo ular amaliyotda tekshiruvlarni almashtirmaydi. Faqat ruxsat etilgan kod bajarilganligini tekshirish kerak bo'lganda, dastur xavfsizligini ta'minlashning takomillashtirilgan usullari ajralmas hisoblanadi, lekin bajariladigan fayllardagi xatolarni aniqlash uchun mos emas.

Aslida, brandmauerlar (firewall) kompyuter tarmoqlarini to'la himoya qila olmaydi. Qasddan qilingan hujumni tekshiruvchi tizim xatolik bilan o'tadi, bu esa ko'plab noto'g'ri signallarga olib keladi. Ko'p sonli mutaxassislarning yillar davomida sarflagan mehnatiga qaramasdan, dastur kodi hali ham buzilmoqda. Nima uchun shunday bo'ladi?

Xavfsizlik dasturlari sotishdagi asosiy omil bu yaxshi reklamadir, masalan: "faqat ushbu mahsulotni sotib oling va biz sizning barcha tashvishlaringizni qabul qilamiz". Demak, siz dasturni sotib oldingiz, va uni o'rnatdingiz... Aksariyat himoya mexanizmlari dasturiy ta'minotdagi xatolarga-muammoning ildiziga hech qanday aloqasi yo'q. Buning o'rniga, ular javob rejimida ishlaydi. *Paketlarni u yoki bu portga o'tishni taqiqlaydi. Belgilangan shablonni o'z ichiga olgan fayllarni kuzatib boradi. Hajmi chegaradan oshib ketgan paket qismlari va paketlarni ko'rilmasdan olib tashlaydi.* Afsuski, tarmoq trafigini filtrlash-muammolarni hal qilishning eng yaxshi usuli emas. Asosiy muammo bu o'tkazib yuborilgan paketlarni boshqaradigan dastur.

Kundalik ishlatiladigan dasturlarda xatolar mavjudligini taxmin qilishimiz mumkin. Ko'plab tijorat tashkilotlarida dasturiy ta'minot birlashtiruvchi rolini o'ynaydi. Albatta, biz tajovuzkorlarni zaif dasturiy

ta'minotga kirishini oldini olishga harakat qilmoqdamiz, ammo muammo chuqurroq va u an'anaviy to'siqlar orqali hal qilinmaydi. Internet davrida tezroq ishlash uchun siz tezroq ma'lumot almashishingiz kerak. Bu ko'proq veb-xizmatlar va tashqi interfeyslarning paydo bo'lishini anglatadi, ya'ni ko'proq ilovalar masofadan turib (shu jumladan, xakerlar uchun) mavjud bo'ladi. Hattoki oddiy foydalanuvchilar ham o'z uylarida, mashinalarida va hatto cho'ntaklarida ishlaydigan dasturiy ta'minot ham hujumga ochiq bo'ladi. Deyarli har birimiz hujum tahdidi ostidamiz.

3.2. Hujum andozalari

Birinchi va eng muhim tarif - *ujum maqsadi* sanaladi. Hujum muvaffaqiyatining yarmi bu maqsadni to'g'ri tanlashga bog'liq. Xaker tomonidan mahalliy yoki uzoqdan hujumga uchrovchi dastur, *hujumkor dasturiy ta'minot* (target software) deb ataladi. Hujumning maqsadi internetga ulangan server, telefonni bog'lovchilari yoki havo mudofaasini boshqaradigan ajratilgan tizim bo'lishi mumkin. Hujum boshlanishidan oldin tanlangan maqsadning zaif nuqtalarini aniqlanadi. Ba'zan bu xavfni baholash (risk assesment) deb ataladi. Agar jiddiy zaif nuqta aniqlansa, u holda hujumning maqsadi tizimni *buzish* uchun juda yaxshi hisoblanadi.

Dasturni amalga oshirgandan so'ng, bu yoki bu ko'rinishdagi natija olinadi. Sinovda programma ishida nosozliklar keltirib chiqaruvchi xatolar aniqlanadi. Dastur chiqishida qanchalik ko'p ma'lumot bersa, undagi ichki xatolik sharoitlarni aniqlash shuncha osonroq bo'ladi va hokazo. *Kuzatuvchanlik*-chiquvchi ma'lumotlarga binoan dasturdagi xatoliklar ehtimolligi aniqlashdir. Kuzatuvchanlik qanchalik yuqori bo'lsa, dasturiy ta'minotning muayyan qismini testlash osonroq bo'ladi. Hech qanday ma'lumot bermaydigan dasturiy ta'minotdagi xatolik vaziyatini aniqlash imkonsiz. Yaxshi kuzatilgan dastur deb, chiqish ma'lumotlarini ichki tuzatish qobiliyatiga ega bo'lgan dasturga aytiladi. Kam kuzatuv talab etadigan dastur tuzatuvchi yordamida o'zgartirilishi va yuqori kuzatilgan dastur darajasigacha yaxshilanishi mumkin. Misol uchun, ma'lumotlar oqimini kuzatish dasturi, hujum maqsad dasturiga ulangan vaziyatda. Dasturiy ta'minotni

buzish texnologiyalari, ayniqsa, masofaviy hujumlarga nisbatan dasturlarni kuzatish g'oyalarini qo'llaydi. Asosiy g'oya dasturning ichki holati haqida maksimal ma'lumotni statik tarzda, dasturning loyihalash bosqichida va dinamik ravishda amalga oshirilganda to'plashdir.

Xavfni aniqlash uchun tizimda zaifliklar topilishi kerak. Jiddiy muammo shundaki, dasturiy ta'minotdagi zaifliklar asosan tasniflanmagan va noaniq bo'lib qolmoqda.

Zaif nuqtalar haqidagi ma'lumotlarning asosiy manbalari bugtraq pochta ro'yxati bo'lib, unda ko'plab hujum dasturlari birinchi marta ommaviy ravishda ko'rib chiqilgan (http://www.bugtraq.com) va CVE (Common Vulnerabilities and Exposures-keng tarqalgan zaif joylar va xatolar) ma'lumotlar bazasi, uning shakllanishi ilmiy xodimlar tomonidan boshqariladi. Shuni e'tiborga olish kerakki, yangi asrning boshlarida bugtraq pochta ro'yxati Symantec tomonidan ma'lumotlar bazalarini tarqatish uchun foydalanadigan tijorat loyihasiga aylandi (ular obuna orqali taqdim etiladi). CVE ma'lumotlar bazasi barcha zaif nuqtalar va xatolar haqidagi ma'lumotlarni bir joyga to'plash uchun yana bir urinishdir. CVE-ning kamchiliklaridan biri bu ma'lumotlarni aniq taqsimlanishining yo'qligidir.

Biz tomondan eslab o'tilgan ikkita forum dasturiy ta'minotdagi xatolar keng tarqalganligini va turli xil dasturiy ta'minot mahsulotlarida takrorlanganligiga ishonch hosil qilish imkonini beradi. Shunday qilib, dasturiy ta'minotda umumiy muammolar mavjud. Bufferni to'lib qolish holati ko'p holatda, qanday dastur bo'lishidan qat'i nazar, bir xil ko'rishga ega.

Mutaxassislarning tasnifiga ko'ra, zaif joylar, *xatolar (bug)* va *noto'g'ri hisoblar (flow)* asosiy xususiyatlariga ko'ra yagona toifaga bo'linadi va yagona hujum namunasini shakllantiradi. Ushbu yondashuv quyidagi taxminlarga asoslangan. Bunday dasturiy xatolar hujumlarni amalga oshirishning usullarining bir xillashuviga olib keladi. Shunday qilib, muayyan zaif joylar emas, balki dasturiy ta'minotning umumiy muammolarini takidlashga harakat qilamiz. Umumiy tasniflash tizimi yordamida siz katta dasturiy ta'minot tizimlarini zaif joylar mavjudligi tadqiq qilishda shablondan foydalanishingiz mumkin. Ushbu shablon

auditorga dasturlardagi muammoli joylarni topishga imkon beradi. Albatta, bunday ma'lumotlar tizimlarni himoya qilish va hujumlarni amalga oshirish uchun foydalidir.

Xatolik (bug) - bu dasturiy ta'minotdagi xatodir. Darhaqiqat, dasturiy ta'minotda xatolik holati bo'lishi mumkin va shuning uchun u hech qachon bajarilmaydi. Xato atamasi ko'plab mutaxassislar tomonidan keng qo'llanilsa-da, biz uni asosan oddiy muammolarni tasvirlash uchun ishlatamiz. Misol uchun, xato C va C++ dasturlarida strepy () funktsiyasidan noto'g'ri foydalanishdir, bu esa bufer to'lib ketishiga olib keladi. Biz xatoni o'z maqsadlari uchun osonlik bilan ishlatilishi mumkin bo'lgan dastur darajasidagi kamchilik deb hisoblaymiz. Xatolar faqat dastur kodida mavjud bo'lishi mumkin. Loyihalash bosqichida qilingan kamchilikni biz xato deb nomlamaymiz. Xatolarni aniqlash uchun kodni skanerlash dasturlari ishlatiladi.

Noto'g'ri hisoblash (flow) ham dasturiy ta'minotning kamchiligidir, ammo bu yerda muammo yanada chuqurroq darajada aniqlanadi. Noto'g'ri hisob-kitoblar odatda oddiy aniq xatolardan ko'ra nozik va sezilmaydigan kamchiliklar deb atash mumkin, masalan, noto'g'ri hisob-kitoblar ketma-ketlik bilan bog'lanish yoki potentsial xavfli tizim chaqiruvidan foydalanish usulida namoyon bo'lishi mumkin. Hisoblash odatda dasturiy ta'minot kodi va butun loyiha bilan bog'liq. Misol uchun, bir nechta klassik noto'g'ri hisob-kitoblar xatolarni qayta ishlash mexanizmi va axborotni tiklash tizimlari bilan bog'liq bo'lib, ularning ishlarida xatolar yuzaga kelganda xavfli vaziyatlar yuzaga keladi. Noto'g'ri dasturlashning yana bir misoli noto'g'ri dasturlash natijasida skriptlardan foydalangan holda hujum deb atash mumkin. Shuni ham takidlash kerakki, dasturiy ta'minotdagi noto'g'ri hisob-kitoblardan xakerlar umuman ishlatilmaydigan holatlar ham mavjud.

Zaif nuqtalar

Xatolar va noto'g'ri hisoblashlar maxsus ishlab chiqilgan 2 tasnifga muvofiq yagona zaif sinf (vulnerability) hosil qiladi. Zaif nuqtalar-tajovuzkorning o'z maqsadlari yo'lidafoydalanishi mumkin bo'lgan dasturiy ta'minotdagi nuqsonlardir.

Xavfsizlik tizimi bilan bog'liq dasturiy ta'minotdagi zaifliklar mahalliy amalga oshirishdagi xatolardan (masalan, C va C dasturlaridagi g e t s () funktsiyasini chaqirganda) va jarayonlararo ta'sir xatolaridan (masalan, vaziyat yuzaga kelishi mumkin bo'lgan xato "nazorat tekshiruvi vaqtida omon qolish uchun poyga kirish imkoniyati va faylni o'zgartirish) loyiha bosqichida amalga oshirilgan yuqori darajadagi kamchiliklardan (masalan, noto'g'ri xatolarni qayta ishlash va xavfli vaziyatlarga olib keladigan uzilishlar, tranzit ishonchli munosabatlarda ob'ektlardan birgalikda ishlatish tizimlaridan noto'g'ri foydalanish) paydo bo'ladi.

Zaifliklar dasturiy ta'minot kodida xato mavjud bo'lgan o'rinda aniqlanishi mumkin. Zaiflik qanchalik murakkab bo'lsa, uni aniqlash uchun ko'proq kod tekshirilishi kerak. Ba'zan faqat bitta dastur kodini ko'rish hech qanday natija bermaydi. Ba'zan siz ushbu kodda nima sodir bo'lganligini tariflashdan ko'ra, tavsiflashning yuqori darajasiga ega bo'lishingiz kerak. Ko'pincha loyihaning tavsifi zarur bo'ladi. Boshqa hollarda kodni bajarish muhitining tafsilotlarini bilishingiz kerak. Dasturlarda odatiy xatolar va dastur arxitekturasining kamchiliklari o'rtasida sezilarli farq borligini aytish kerak. Oddiy xatoni tuzatish uchun odatda bitta kod satri yetarli bo'ladi va arxitekturaviy yechimdagi xatolik dasturning ko'p jihatlariga ta'sir qiluvchi keng ko'lamli o'zgarishlarni talab qiladi.

Hujumlar tobora murakkablashib borayotganligi sababli, muayyan turdagi zaiflikni aniqlash doimiy ravishda o'zgarib turadi. Vaqti-vaqti bilan xatolardan asoslangan hujumlar allaqachon keng tarqalgan bo'lib, bir necha yil oldin ular "ekzotik" deb hisoblangan. Xuddi shunday, "tramplin" ga asoslangan, ikki bosqichli bufer toshqini hujumlari dolzarb ilmiy tadqiqot mavzusi bo'lib kelgan va endilikda ular kundalik hujumlarda qo'llanilmoqda.

3.3. Dasturlarni buzish usullari

Ko'pincha biz yuklab olgan dasturda foydalanish muddatiga cheklovlar yoki bazi funksiyalari cheklangan bo'ladi va foydalanish muddati tugagandan so'ng umuman ishlata olmaymiz.

Odatda bunday dasturlarni ishlab chiquvchilar kuchli xavfsizlik vositalaridan foydalanmaydi. Bu ko'p vaqt va qo'shimcha mablag 'talab qiladi. Bundan tashqari, dasturning himoyasi qanday bo'lishidan qat'iy nazar, krakerlar (buzg'unchilar) uni buza oladi. Shuning uchun o'rtacha dasturiy himoya tajribasiz foydalanuvchilar uchun mo'ljallangan.

Keyinchalik, dasturni muhofaza qilishning turli yo'llarini ko'rib chiqamiz: crackni qidirish, kompyuterda o'rnatilgan sanani o'zgartirish, ro'yxatga olish kitobini (reyster) tahrirlash, dasturning RAMdagi ro'yxatga olish ma'lumotlaridan qidirish.

1) Crackni qidirish.

Buning eng oson yo'li-sizdan avval internetda buzilgan dasturni yoki unga to'g'ri keladigan crackni topish talab etiladi.

Biz dasturning nomini va kalit so'zlarni qidiruv tizimlariga yozamiz (google, yandex, duckduckgo): seriya raqam, crack, key, keygen, serial, patch va shunga o'xshash narsalarni yozamiz. Rus tilida qidiruv natijalarini ko'rsatish uchun kamida bitta ruscha so'zni, masalan: "Скачать, программа" va boshqalarni kiritish kerak.

Ehtimol, siz birinchi urinishdanoq topa olmassiz, biroq dasturni yuklab olish va o'rnatishga (qayta tiklash) biroz vaqt sarflaganingizdan so'ng, siz ijobiy natijaga erishasiz.

Dori vositalarining (tablekta) tarifini va o'rnatilishini diqqat bilan o'qing. Dasturni birinchi marta o'rnatganingiz noto'g'ri bo'lsa, uni butunlay kompyuterdan o'chirish (tozalash) kerak bo'ladi: ro'yxatga olish kitobini tozalash, tuzilgan tizim fayllarini o'chirish, kompyuterni qayta yuklash.

2) Kompyuterda (sistemada) o'rnatilgan sanani o'zgartirish

Dasturning xizmat ko'rsatish vaqtini cheklash usullaridan biri, bu ishlab chiquvchini dasturning ishlash kunlari sonini o'rnatishi hisoblanadi.

Ko'pgina hollarda, tizimni o'rnatishdan oldin sana vaqtini oldinga, masalan, besh yil orqaga o'tkazish kifoya qiladi. O'rnatishdan so'ng, uni asl holatiga qaytaramiz. Natijada, dastur besh yil va ma'lum kunlar uchun ishlaydi.

Tizim vaqtini o‘zgartirish uchun vaqt belgisini bosing va sozlamalarni yil hisoblagichini yuqoriga qarab o‘zgartiring. Ammo shuni ham aytish kerakki, ko‘pgina zamonaviy dasturlarda bu usul ishlamaydi, ishlab chiquvchilar joriy sanasi ko‘pincha BIOS-dan olishni yoki umuman dasturlarni vaqt yoki sanaga bo‘glamaydilar.

3) RegEdit ro‘yxatga olish kitobi parametrlarini o‘zgartirish

Agar dasturdan foydalanishni boshlash soni cheklansa, vaziyat yanada murakkab ko‘rinishga keladi. Bunday holda, xizmat muddatini uzaytirish uchun kompyuter reestrida bir necha oddiy amallarni bajarish kerak.

Avval ushbu usulni sinab ko‘ramiz:

-Regedit dasturini ishga tushiring (Windows 7 da qidiruv punktida, XP da “Пуск”, “Выполнить” qismida), so‘ng reestrni tahrirlash oydasidan HKEY_CURRENT\Software\Program nomini tanlang va File=> Export buyrug‘ini bajaring.

1. Keyinchalik zarurat uchun faylni saqlab qo‘ying.

2. Natijada, dastur diskka ko‘chiriladi, ular ro‘yxatga olinadigan vaqt yozib qo‘yiladi.

3. Keyinchalik, dasturni ishga tushirish chegarasi yugaganidan so‘ng, saqlangan faylni yuqorida ko‘rsatilgan ro‘yxatga olish kalitiga-File => Import buyrug‘i bilan qayta yozish kerak bo‘ladi.

Biroq, reestr bilan ishlashning bu usuli bilan har doim kerakli natijaga erishib bo‘lmaydi. Keyinchalik Windows ro‘yxatga olish kitobini tahrirlash uchun maxsus dasturlardan foydalanishingiz mumkin. Bunday dasturlarga Regmon, Filemon yoki Registry Trash Keys Finder misol bo‘la oladi.

3.4. Boshlang‘ich kod va dastur tuzilishini tiklash

Aksariyat kishilar kompyuter dasturlari bilan juda yuzaki darajada muloqot qilishadi: ular ma’lumotni kiritadilar va natijalarni sabr-toqat bilan kutadilar. Aksariyat dasturlarning umumiy interfeysi juda qisqa bo‘lishi mumkin, ammo dasturlarning asosiy qismi odatda birinchi qarashda ko‘rinadigan darajada ancha chuqurroq ishlaydi. Dasturlarda

juda ko‘p maxfiy kontent mavjud bo‘lib, unga kirish ruxsatini qo‘lga kiritish kattafoyda olish imkonini beradi. Ushbu kontent dasturiy ta’minotni buzishdanda juda murakkab bo‘lishi mumkin, ya’ni buzg‘unchilikni amalga oshirish dasturning mazmuni haqida ma’lum darajada bilimga ega bo‘lishni nazarda tutadi.

Yaxshi xakerning asosiy sifati hujum qilingan dasturiy ta’minot kodining nozikligi va mukammal emasligini oshkor qilish qobiliyatidir. Ushbu jarayon *boshlang‘ich kod va dastur tuzilishini (*reverse engineering) *tiklash* deb ataladi. Shubhasiz, dasturiy ta’minot buzg‘unchilari tayyor dasturiy ta’minot vositalarining yuqori malakali foydalanuvchilaridir. Dasturiy ta’minotni buzishni daholik bilan hech qanday aloqasi bo‘lmay, buzg‘unchilikni amalga oshirishda ham maxsus sifatga ega dasturlar yo‘q. Standart bo‘lmagan dasturni buzish uchun buzg‘unchi hujum qilingan dasturga g‘ayritabiiy usullar bilan ta’sir qilishi kerak. Shunday qilib, hujumda deyarli har doim maxsus vositalar (dizassembler, skript mexanizmlari, kirish generatorlari) ishlatilgan bo‘lsa-da, bu faqat hujum uchun asosdir. Hujum natijasi odatdagidek xakerning qobiliyatiga bog‘liq.

Dasturni buzishda asosiy narsa-tizim ishlab chiquvchilari tomonidan qabul qilingan taxminlarni aniqlash va ushbu taxminlarni o‘z maqsadlari uchun ishlatishdir (shuning uchun dasturiy ta’minotni ishlab chiqish va yaratish vaqtida barcha taxminlarni oshkor qilish juda muhimdir). Dasturning boshlang‘ich kodi va tuzilishini tiklash-bu farazlarni oshkor qilishning ajoyib usulidir. Ayniqsa, hech qanday tekshiruvsiz amalga oshirilgan dasturlardan buzg‘unchilik hujumlarida foydalanish mumkin bo‘ladi.

Nima uchun bu kerak?

Manba kodini tiklash dasturning asl tuzilishi va uning qanday ishlashi haqida ma’lumot olish imkonini beradi. Bu dasturiy ta’minotni buzishda kerak bo‘luvchi boshlang‘ich ma’lumotlardir. Misol uchun, hujum qilinadigan dastur qaysi tizimli funktsiyalardan foydalanadi,

qaysi fayllarga murojaat qiladi, qaysi protokollar asosida ishlayotganligini va lokal tarmoqning boshqa kompyuterlari bilan qanday aloqa o'rnatganligini bilib olishingiz mumkin.

Dasturning boshlang'ich kodini tiklashning asosiy afzalligi dasturning tuzilishini o'zgartirish va uni amalga oshirish jarayoniga ta'sir qilish qobiliyatidir. Texnik jihatdan, bu tuynuk yaratishdir (patching), chunki asl dasturiy ta'minot kodiga tuynuk qo'shiladi. Tuynuklar buyruqlarni qo'shish yoki muayyan vazifani bajarish usulini o'zgartirish imkonini beradi, ya'ni maxfiy xususiyatlarni qo'shish, o'chirish yoki passiv holga keltirish va manba kodida xavfsizlik tizimi bilan bog'liq xatolarni tuzatish imkoniyatini beradi. Xakerlar orasida patch lash ko'pincha nusxa ko'chirishdan himoyalash mexanizmlarini yo'q qilish uchun faol ishlatiladi.

Har qanday vosita singari, dastur boshlang'ich kodini tiklash ham yaxshi va yomon maqsadlar uchun ishlatilishi mumkin.

Manba kodini tiklash vositalari

Manba kodini tiklash g'oyasi butun texnik yechimlar sanoatini rivojlantirishga turtki bo'ldi. Manba kodini tiklash bo'yicha muhandislar, kerakli protokolni aniqlash va bajariladigan dasturlar uchun kodni tiklash bilan bog'liq ko'plab dolzarb va murakkab muammolarni hal qilishadi. Misol uchun, 1980-larda IBM PC shaxsiy kompyuterlari uchun BIOS manba kodini qayta tiklash mumkin edi, bu bozorda shunga o'xshash yechimlarning paydo bo'lishiga olib keldi. Xuddi shu usullar o'yin konsollari sanoatida ham qo'llaniladi (masalan, Sony PlayStation analoglarini yaratish uchun). Chiplarning muvofiqligini ta'minlash uchun Cyrix va AMD Intelning mikroprotsessorlari dasturiy ta'minot va operatsion tamoyillari uchun manba kodini tiklashdi. Biroq, qonun nuqtai nazaridan manba kodini tiklash jinoyat bilan cheklanadi. DMCA va UCITA kabi yangi qonunlar (ko'plab xavfsizlik mutaxassislari tomonidan tanqid qilingan) manba kodini tiklash uchun qattiq cheklovlar qo'yadi. Agar manba kodini tiklash bilan qonuniy ravishda shug'ullanmoqchi bo'lsangiz, ushbu qonunlar bilan tanishib chiqing. Biz manba kodini qayta tiklashning

qonuniyligi haqida yakuniy baho bermaymiz, balki har doim intellektual mulk bo'yicha mutaxassislar bilan maslahatlashishni maslahat beramiz.

Tuzatuvchi

Tuzatuvchi-dasturlash muhit moduli yoki dastur xatolarini izlovchi alohida qo'llanmadir. Sozlagich ketma-ket trassirovka, dasturni bajarish jarayonida o'zgaruvchilarni kuzatish, o'rnatish va o'zgartirish, nazorat nuqtalarini yoki to'xtash shartlarini o'rnatish va olib tashlashni amalga oshirish imkonini beradi. Sozlagich shunchaki dasturning mantiqiy tuzilishini aniqlash uchun ajralmas hisoblanadi. rostlagichning ikkita toifasi mavjud: foydalanuvchi dasturlari sozlagichi va yadro sozlagichi. Foydalanuvchi dasturlari sozlagichi operatsion tizimni boshqaradigan muntazam dastur sifatida ishga tushiriladi va muntazam dasturlar bilan bir xil qoidalarga bo'ysunadi. Shunday qilib, ushbu toifadagi sozlagich faqat foydalanuvchi darajasida amalga oshiriladigan boshqa jarayonlarni sozlashga qodir. Yadro tuzatuvchisi operatsion tizimning bir qismidir va u bilan siz qurilma drayverlarini va hatto operatsion tizimni ham rostlashingiz mumkin. Eng mashhur yadro tuzatuvchilardan biri Softice rostlagichlaridir.

Xatolarni tuzatish vositalari

Hujum jarayoni uchun noto'g'ri kirish ma'lumotlarini taqdim eta oladigan vositalar, bu jarayonning bajarilishida muvaffaqiyatsizlikka olib kelishi uchun xatolarni tuzatish vositasilaridir. Ushbu dasturdagi xatolarni tahlil qilish orqali tasdiqlangan dastur xatolarni aniqlash mumkin. Ba'zi xatoliklar xavfsizlik tizimiga jiddiy ta'sir ko'rsatadi. Ularning yordami bilan xaker xostga yoki tarmoqqa bevosita kira oladi. Xatolarni tuzatuvchi vositalar ikki xil bo'ladi: xostlar va tarmoqlardan foydalanish uchun. Xostlarda xatolarni tuzatish uchun vositalar sozlagich kabi ishlaydi hamda, jarayonlarga ulanishi va dasturning holatini o'zgartirishi mumkin. Xatolarni tuzatish uchun tarmoq vositalari qabul qiluvchiga ta'sir qilish ta'sirini baholash uchun tarmoq trafigini boshqarishga asoslangan.

Garchi klassik xatolarni tuzatish usullari manba kodining o'zgarishi asosida harakat qilsa-da, dastur uchun kirish ma'lumotlarini manipulyatsiya qilishga ko'proq e'tibor qaratadigan zamonaviy vositalar

ham mavjud. Xavfsizlik mutaxassislari orasida Hailstorm (Cenzic kompaniyasidan), Failure Simulation Tool yoki FST (Cigital kompaniyasidan) va Holodeck (Florida Tech kompaniyasidan) dasturlari alohida qiziqish uyg'otdi.

Dizassembler

Dizsassembler-mashina kodini assembler tilidagi kodga o'tkazadi. Assembler tilidagi kod-bu mashina kodining o'qilishi mumkin bo'lgan shakli (hech bo'lmaganda bit satridan ko'ra ko'proq o'qilishi mumkin). Disassembler yordamida siz mashina kodida qanday mashina ko'rsatmalari ishlatilishini bilib olishingiz mumkin. Mashina kodi muayyan apparat arxitekturasiga xosdir (masalan, PowerPC chipi yoki Intel Pentium). Shuning uchun, dizassemblerlar maxsus apparat arxitekturalariga moslab yoziladi.

Dekompilyator

Dekompilator-bu kodni assembler tilida yoki mashina kodini yuqori darajali tillardagi boshlang'ich kodga aylantirish imkonini beruvchi vositadir, masalan, C tiliga o'tkazish. Shuningdek, kodni Java bayt kodi va MSIL (Microsoft Intermediate Language) tilidagi kodni Javaga o'xshagan oraliq tillarga aylantirish uchun dekompilyatorlar mavjud. Ushbu vositalar, masalan, tsikllar, switch operatorlari va if-then konstruktsiyalari kabi yuqori darajadagi kod tuzilishini aniqlashda katta yordam beradi. Yaxshi disassembler / dekompilyator juftligi o'z kodini qayta tiklash natijasini ikkilik kodga qaytarish uchun ishlatilishi mumkin.

3.5. Manba kodini tiklash usullari

Yuqorida aytib o'tilganidek, boshlang'ich kod tadqiqotchi uchun ba'zan ruxsatli, ba'zan esa yo'q. Dasturiy ta'minotning ishlash tamoyillarini tushunish uchun "qora quti" va "oq quti" kabi testlash va tahlil qilish usullari qo'llaniladi. Ushbu usullar manba kodining mavjudligi darajasi bilan belgilanadi.

Dasturiy ta'minotdagi zaif jihatarni topish uchun qanday usul ishlatilganligidan qat'iy nazar, xaker har doim bir nechta bazaviy savollarni o'rganishi kerak:

noto‘g‘ri (yoki umuman bajarilmagan) bajariladigan vazifalar kirish ma’lumotlarining hajmini tekshiradi;

foydalanuvchilar tomonidan kiritilgan ma’lumotlarni formatlash satrlarida o‘tkazib yuborishi yoki qabul qilishi mumkin bo‘lgan xususiyatlar;

vazifalarni formatlash liniyalari chegaralarini tekshirish uchun mo‘ljallangan (masalan, %20s);

sikl orqali foydalanuvchi tomonidan kiritilgan ma’lumotlarni qabul protseduralar;

past darajadagi nusxa ko‘chirish operatsiyalari;

parametr sifatida uzatilgan bufer manzili bilan arifmetik operatsiyalarni ishlatadigan dasturlar;

so‘zsiz “ishonch” bo‘lgan va kirish ma’lumotlarini dinamik rejimda qabul qilgan tizim chaqiriqlari.

“Oq quti” usuli bo‘yicha tadqiqotlar

“Oq quti” usuli bo‘yicha tadqiqotda birinchi navbatda manba kodi tahlil qilinadi. Ba’zan faqat ikkilik kod mavjud, ammo uni dekompilyatsiya qilish, ikkilik koddan olish va uni tadqiq qilish mumkin, bu ham “oq quti”usuli bilan tahlil qilinadi. Ushbu sinov usuli dasturiy ta’minotdagi dasturiy va tadbiq etish xatolarini aniqlashda juda samarali. Ba’zi hollarda, tadqiqot ma’lum andozalar bilan mosliklarni topish uchun va hatto statik analizator bilan avtomatik ravishda amalga oshirilishi mumkin. Ammo “oq quti” usulida bitta kamchilik mavjud. Bu usuldan foydalanganda, aslida mavjud bo‘lmagan (false positive) potentsial zaifliklar ko‘pincha aniqlanadi. Shunga qaramay, manba kodini statik tahlil qilish usullari ba’zi dasturlarni muvaffaqiyatli buzish imkonini beradi.

“Oq quti” usuli bo‘yicha tadqiqotlar o‘tkazish vositalari ikki toifaga bo‘linadi: manba kodini talab qiluvchi va ikkilik kodni avtomatik ravishda dekompilyatsiya qiladigan va shu vaqtdan boshlab ishlashni davom ettiruvchi. IDA-Pro deb nomlangan “oq quti” usuli bo‘yicha kuchli tahlil platformasi manba kodini talab qilmaydi. Xuddi shu narsa SourceScope dasturi uchun ham amal qiladi, bu Java, C va C++ da manba kodi va dasturlarida kuchli xato ma’lumotlar bazasi bilan birga

keladi. Ushbu vositalar tomonidan taqdim etilgan ma'lumotlar dasturiy ta'minot xavfsizligi masalasini tahlil qilishda juda foydali (dasturlarni buzishda).

"Qora quti" usuli bo'yicha tadqiqotlar

"Qora quti" usuli bo'yicha o'rganilganda, ijrochi dasturning kiritilishida turli test ma'lumotlari taqdim etiladi. Ushbu testda faqat dasturni ishga tushirish talab etiladi va manba kodini tahlil qilmaydi. Xavfsizlik nuqtai nazaridan, zararli ma'lumotlar dasturning ishga tushirilishiga olib kelishi mumkin. Agar dastur ba'zi sinovlarni amalga oshirishda uzilish sodir bo'lsa, unda xavfsizlik muammosi aniqlangan deb hisoblanadi.

Shuni esda tutingki, "qora quti" usuli bo'yicha tahlil qilish ikkilik kodga kirmasdan ham amalga oshirilishi mumkin. Shuningdek, dastur tarmoq orqali tahlil qilinishi mumkin. Talab qilinadigan barcha narsa-kirish ma'lumotlarini qabul qilishga qodir bo'lgan ishlaydigan dasturning mavjudligi, ya'ni, agar tadqiqotchi dasturni qabul qiladigan kirish ma'lumotlarini yuborishga va ushbu ma'lumotlarni qayta ishlash natijasini olishga qodir bo'lsa, unda "qora quti" usuli bo'yicha test qilish mumkin. Shuning uchun ko'plab xakerlar buzish ishlarida "qora quti" usulini tanlaydilar.

"Qora quti" usuli bo'yicha dasturni tahlil qilish "oq quti" usuli bilan bo'lgani kabi samarali emas, lekin bu usul amalga oshirish uchun juda oson va yuqori malakaga ega bo'lishni talab qilmaydi. Qora quti usuli bo'yicha test davomida, mutaxassis, dastur ta'sir, berilgan natijalar aniq dasturi kodi ijrosi yo'llarini aniqlash uchun harakat qiladi. Dastur kodidagi foydalanuvchi ma'lumotlarini kiritish uchun haqiqiy joyni tekshirish mumkin emas, ammo qora quti usuli bo'yicha test "oq quti" usuli bilan taqqoslaganda haqiqiy ish muhitida haqiqiy hujumga o'xshaydi.

"Qora quti" usuli bo'yicha tadqiqotlar ishchi tizimda yuzaga kelganligi sababli, u ko'pincha xizmatni rad etish muammolarini tushunish va tekshirish uchun samarali vosita sifatida qo'llaniladi. Testlash usuli, uning ishlash muhitida (agar iloji bo'lsa) ilovaning ishlashini baholashga qodir bo'lgani uchun, u haqiqiy ishlaydigan ishlab

chiqarish tizimida zaif tomonlarni aniqlash uchun ishlatilishi mumkin. Ba'zida "qora quti" tahlil usulida aniqlangan xatolardan xakerlar aniq tarmoqda, aniq tizimda real hujumlarda foydalana olmadi. Misol uchun, hujum xavfsizlik brandmauerini bloklashi mumkin.

Cenzic kompaniyasining "Hailstorm" tijorat platformasi tarmoqqa ulangan tizimlarda ishlaydigan dasturlarni "qora quti" usuli bo'yicha testlash imkonini beradi. Bu operatsion tizimlarda zaif tomonlarni topish uchun ishlatilishi mumkin. Routerlar va kalitlarni tekshirish uchun SmartBits va IXIA kabi maxsus qurilmalar mavjud. TCP/IP to'plamining yaxlitligini tekshirish uchun bepul ISICS dasturidan foydalanishingiz mumkin. "Qora quti" usuli bo'yicha protokollarni tekshirish ROTOS va Spike muhitlari yordamida amalga oshirilishi juda qulay.

"Kulrang quti" usuli bo'yicha tadqiqotlar

"Kulrang quti" usuli bo'yicha olib borilgan tadqiqotlar "oq quti" usullarini va "qora quti" usuli bo'yicha kirish ma'lumotlari yordamida testlash usullarini birlashtiradi. "Kulrang quti" usuli bo'yicha oddiy tahlilning yaxshi namunasi dasturni rostlagich ichida ishga tushirish va ushbu dasturning kirishida turli ma'lumotlarni berish mumkinligidir. Bunday holda, dastur amalga oshiriladi va sozlagich xatolar va noto'g'ri holatlarni aniqlash uchun ishlatiladi. Rational kompaniyasining Purify tijorat dasturi ijro vaqtida batafsil tahlilni ta'minlaydi va asosan xotira ishini o'rganishga qaratilgan. Bu C va C++ dasturlari uchun, ayniqsa, muhim ahamiyatga. Valgrind-bu Linux muhitida ijrochi dasturlarni tahlil qilishni ta'minlovchi bepul qayta tiklagichdir.

Umuman olganda, barcha testlash usullari dasturiy ta'minotdagi xavflarni va potentsial hujumlarni fosh etish imkoniyatlarni ochib beradi. "Oq quti" usuli bo'yicha tahlil qilish ko'plab xatolarni aniqlashga imkon beradi, ammo bu holda hujumning haqiqiy xavfini o'lchash qiyin. "Qora quti" usuli bo'yicha tahlil qilish hujumlarda ishlatilishi mumkin bo'lgan haqiqiy muammolarni ochib beradi. "Kulrang quti" usuli har ikkala usulni maksimal foyda bilan birlashtirishga imkon beradi. "Qora quti" usuli bo'yicha testlar dasturlarni tarmoq orqali tekshirishga imkon beradi. "Oq quti" usuli

bo‘yicha tahlil qilish uchun statik tadqiqotlar uchun manba yoki mashina kodiga kirish talab etiladi. Odatda, “oq quti” usuli potentsial muammoli nuqtalarni aniqlash uchun ishlatiladi va keyinchalik bu muammoli sohalarga qaratilgan hujum dasturlarini yaratish uchun “qora quti” usullari qo‘llaniladi.

Barcha sinov turlaridagi asosiy muammo (“qora quti” usuli va “oq quti” usuli bilan) dasturlarning barcha jihatlarini, ya’ni dasturiy ta’minot sifatini baholash bilan shug‘ullanadigan tashkilotlarning aksariyatini tekshirmaydi, faqat funksiyalarni va xavfsizlikni tekshirish uchun juda oz vaqt sarflashadi. Dasturiy ta’minotni ishlab chiqish bilan shug‘ullanadigan ko‘pgina tijorat firmalarida vaqt cheklovlari, xarajatlarni tejash tufayli dastur sifatini tekshirish jarayoni buziladi, lekin asosan, ishonch dasturni yaratishda sifatni tekshirish ishning asosiy bo‘gini emasligini bildiradi.

So‘nggi vaqtlarda, dasturiy ta’minotga bo‘lgan ahamiyatning ortishi bilan, asosiy e’tibor dasturiy ta’minot sifatini tekshirish jarayoniga qaratilmoqda. Dasturiy mahsulotlarning xavfsizligi, ishonchliligi va ishlashini tekshirishni o‘z ichiga olgan dasturlarni sinash va tahlil qilishda yagona yondashuv ishlab chiqilmoqda. Dasturlarning sifatini boshqarish jarayonida dasturiy ta’minotning hayot davrining dastlabki bosqichida xavflarni aniqlash va boshqarish uchun “oq quti” va “qora quti” usuli bo‘yicha tahlil qo‘llaniladi.

Asosiy xulosalar

Dasturiy ta’minotning ishlash tamoyillarini aniqlash-bu xavfsizlik siyosat qoidalarini o‘rnatish va tizimlashtirish, so‘ngra ushbu siyosatni tegishli texnologiya bilan amalga oshirishni o‘z ichiga olgan jarayondir. Dasturlarning xavfsiz ishlashini ta’minlash uchun sehrli yoki universal vositalar mavjud emas.

Xaker tomonidan mahalliy yoki uzoqdan hujumga uchrovchi dastur, hujumkor dasturiy ta’minot (target software) deb ataladi.

Dasturni muhofaza qilishning turli usullari mavjud: crackni qidirish, kompyuterda o‘rnatilgan sanani o‘zgartirish, ro‘yxatga olish kitobini (reyster) tahrirlash, dasturning RAMdagi ro‘yxatga olish ma’lumotlaridan qidirish.

Yaxshi xakerning asosiy sifati hujum qilingan dasturiy ta'minot kodining nozikligi va elitamasligini oshkor qilish qobiliyatidir. Ushbu jarayon boshlang'ich kod va dastur tuzilishini (reverse engineering) tiklash deb ataladi.

Manba kodini tiklash dasturning asl tuzilishi va uning qanday ishlashi haqida ma'lumot olish imkonini beradi.

Hujum jarayoni uchun noto'g'ri kirish ma'lumotlarini taqdim eta oladigan vositalar, bu jarayonning bajarilishida muvaffaqiyatsizlikka olib kelishi uchun xatolarni tuzatish vositasilaridir.

"Oq quti" usuli bo'yicha tadqiqotlar o'tkazish vositalari ikki toifaga bo'linadi: manba kodini talab qiluvchi va ikkilik kodni avtomatik ravishda dekompilyatsiya qiladigan va shu vaqtdan boshlab ishlashni davom ettiruvchi.

Xavfsizlik nuqtai nazaridan, zararli ma'lumotlar dasturning ishga tushirilishiga olib kelishi mumkin. Agar dastur ba'zi sinovlarni amalga oshirishda uzilish sodir bo'lsa, unda xavfsizlik muammosi aniqlangan deb hisoblanadi.

So'nggi vaqtlarda, dasturiy ta'minotga bo'lgan ahamiyatning ortishi bilan, asosiy e'tibor dasturiy ta'minot sifatini tekshirish jarayoniga qaratilmoqda. Dasturiy mahsulotlarning xavfsizligi, ishonchliligi va ishlashini tekshirishni o'z ichiga olgan dasturlarni sinash va tahlil qilishda yagona yondashuv ishlab chiqilmoqda.

Nazorat savollari

1. Dasturiy ta'minot xavfsizligi farqlari nimada?

2. Hujumkor dasturiy ta'minot nimani angladati?

3. «Dasturiy ta'minotda kuzatuvchanlik» so'zi mazmuni nimada.

4. Dasturiy ta'minot umumiy muammolari namunasi nimani namoyon etadi?

5. Dasturiy ta'minotdagi «xatolik», «yanglishish», «zaif nuqtalar» nima?

6. Dasturiy ta'minotda hujum davomida nimalar kuzatiladi?

7. Dastur himoyasini kuzatish usullarini tariflang.

8.«Manba kodi va dastur tuzilishini tiklash» iborasi ostida nima tushuniladi.

9.Manba kodini tiklash zarurati nimada?

10. Manba kodini tiklashda qanday vositalardan foydalaniladi?

11. "Oq quti" usulida dasturiy ta'minot tadqiq qilishni tarigflang.

12. "Qora quti" usulida dasturiy ta'minot tadqiq qilishni tarigflang.

13. *"Kulrang quti" usulida dasturiy ta'minot tadqiq qilishni tarigflang.*

IV-BOB. ELEKTRON POCHTA VA PAROLLARNI BUZISH USULLARI

4.1. Elektron pochtani buzish usullari

Odamlar har doim maktub yozishgan va bundan keyin ham yozishadi. Agar ilgari xabar yozishda qog'oz va qalam ishlatilgan bo'lsa, bugungi kunda ularni o'rnini klaviatura va elektron pochta qutilari egalladi. Ushbu aloqa usuli juda mashhur bo'lib, deyarli har bir Internet foydalanuvchisi hozirda bir nechta elektron pochta manziliga ega. Quyidagi pochta xizmatlarida *gmail.com. tut.by. mail.ru*, shuningdek *rambler.ru* va hokazolarda, har kuni ko'plab yangi foydalanuvchilar ro'yxatga olinadi.

Bugungi kunda elektron pochta faqat aloqa vositasi bo'lib qolmasdan, balki uning yordami bilan biznes olib boriladi, har xil tovarlar sotib olinadi va sotiladi, turli xil xizmatlar taklif etiladi. Lekin, afsuski, hamma ham elektron pochtani "ezgu" maqsadlarda ishlatmaydi, hozirgi kunda ko'plab firibgarlar va birovni shaxsiy pochta qutisini buzishga qiziqadiganlar mavjud.

Bu kimga va nima uchun kerak? Birinchidan, bu pochta qutisi egasi uchun kerak bo'lishi mumkin – masalan, loginini, parolni va kirishni qayta tiklashga yordam beradigan boshqa ma'lumotlarni unutgan bo'lsa. Ikkinchidan, raqobat, qizg'anish va qiziqish tufayli boshqa birovning maxfiy ma'lumotlariga qiziqqan ko'plab odamlar bor.

Elektron pochtani buzish xizmatlarini taklif qilish orqali bunday vaziyatlarda pul topishni istaganlar ham bor. Qanday qilib ular buni qila oladilar? Aslida, har qanday tizimda o'z zaif joylari bor va elektron pochta xizmatlari ham bundan istisno emas. To'g'ri, elektron pochtani himoya qilishning yangi, yanada rivojlangan usullari doimo paydo bo'ladi, ammo xakerlar ham yangi buzish yo'llarini kashf qilishadi.

Elektron pochtani buzishning bir nechta usullari mavjud, ular quyidagilar:

Troyan dasturlarini ishga tushirish.

Bunda turli xil ayg'oqchi dasturlar orqali xakerlar shaxsiy va konfidentsial ma'lumotlarni o'g'irlashadi. Odatda, ushbu dasturlar qurbonning kompyuteriga ehtiyotkorlik bilan yuklanadi va darhol parollar va loginlarni, shuningdek, serverlar yoki pochta xizmatlari bilan bog'lanish uchun kirish nuqtalarini saqlashni boshlaydi. Bu ma'lumotlarning barchasi o'z maqsadlari uchun foydalanadigan tajovuzkorlarga yuboriladi.

Himoya usullari.

Antivirusni (sifatli va litsenziyalangan) o'rnatish, shuningdek, dastur yangilanishlarini muntazam ravishda kuzatib borish;

Brauzerlarda, shuningdek FTP menejerlarida pochta va boshqa xizmatlar login va parollarni saqlamang (bu xakerlar uchun parollarni o'g'irlashning eng oson usullaridan biridir);

Tarmoqlararo ekranni, ya'ni kompyuter va tarmoq o'rtasida ma'lumot almashish jarayonlarini nazorat qiluvchi tarmoq ekranini o'rnatish. Bu ftp orqali fayllar va elektron pochta xabarlarini ruxsatsiz yuborilishidan himoya qilishning ishonchli usuli. Bunday xavfsizlik devorlaridan biri-Outpost Firewall Pro.

Foydalanuvchini aldash orqali parollarni aniqlash.

Odamlar xatoga yo'l qo'yishadi. Bundan tashqari, ko'pchiligimiz boshqalarga ishonishga moyilmiz. Aslida, bu mutlaqo normaldir, lekin bu ishonuvchanlik, shuningdek, beparvolik firibgarlar xakerlar tomonidan ishlatiladi.

Bunday yolg'onning eng keng tarqalgan namunasi, foydalanuvchi tomonidan uning parollarini, loginlarini va ro'yxatga olish jarayonida ko'rsatgan boshqa ma'lumotlarni ko'rsatish talab qilinadigan pochta xizmati ma'muriyati nomidan xatlarni yuborish deb atash mumkin. Bu odatda juda sodda tushuntiriladi-server ko'chiriladi, uskunalar almashtiriladi va hokazo. Bu holda, xat odatda "begunoh" tahdidni o'z ichiga oladi agar foydalanuvchi xatni e'tiborsiz qoldirsa, pochta tizimidagi hisob qaydnomasi qaytarib olinmaydi.

Xakerlar bunday xatlarni yuborish orqali nima kutishadi? Har bir ikkinchi shaxs o'z akkauntini qadrlaydi va pochta xizmati

ma'muriyatiga ishonadi. Shuni aytish kerakki, firibgarlarning umidlari ko'pincha oqlanadi-bunday xatlarni olganlarning taxminan yarmi akkauntlarini bloklab qo'ymasliglari uchun o'zlarining shaxsiy ma'lumotlarini taqdim etishga tayyordirlar.

Himoya usuli juda sodda, siz doimo oddiy haqiqatni yodda tutishingiz kerak-hech kimga va hech qachon, login va parollar haqida ma'lumot berish kerak emas. Shuni ham yodda saqlash kerakki, ma'muriyat hech qachon foydalanuvchilardan shaxsiy ma'lumotlarini, hatto ularning akkaunt parollarini taqdim etishni talab qilmaydi.

Soxta sahifalarni yaratish

Bunday holda, pochta qutisini buzish uchun xakerlar asl pochta xizmatidan mutlaqo farq qilmaydigan soxta sahifani yaratadilar. Ushbu pochta orqali soxta ma'lumotni ajratib turadigan yagona farq sahifaning URL satridagi bir oz o'zgargan manzildir. Foydalanuvchilar ushbu sahifada Login va parolingizni kiritib, o'zlarini tajovuzkorlarning ixtiyorida qoldiradilar.

Bunday Fake ga misol sifatida Runetda eng mashhur va ommaviy ijtimoiy tarmoqlardan biri bo'lgan VKontakte klonini keltirishimiz mumkin. Ehtimol, har bir kishi uning haqiqiy manzilini biladi bu vkontakte.ru. Lekin soxta sahifaning manzili deyarli bir xil edi-vkontlakte.ru. Bular o'rtasidagi farqni darhol ko'rish qiyin. Bunga soxta sahifa yaratuvchi firibgarlar umid qilishadi.

Ushbu buzish usulidan himoya qilishning yagona usuli, bu oddiy "hushyorlik"dir. Agar siz elektron pochtangizga kirishga harakat qilsangiz, siz to'satdan parol va login kiritishingiz kerak bo'ladi, bundan oldin hushyor bo'ling va sahifaning URL manzilini diqqat bilan ko'rib chiqing. Agar biror shubha bo'lsa, sahifani tark eting va xizmatingizga yana kirishga harakat qiling.

Sifatsiz elektron pochtadan foydalanish.

Yuqorida aytib o'tilganidek, har bir xizmat xakerlar faol foydalanadigan zaif nuqtalarga ega. Xizmatlar ma'muriyati va firibgarlar doimiy ravishda ko'rinmas urush olib boradi, ba'zilari mudofaa usullarini kashf etadi, boshqalari ularni chetlab o'tishni o'rganadi. Natijada akkaunti buzilgan oddiy foydalanuvchilar azob chekmoqda. Bu

yerda savol tug'uladi, pochta xizmatlarning qancha "bo'shliqlari" bor, pochta qutisi buzish shunchalar osonmi?

Ishonchli himoya usullari va yuz minglab foydalanuvchilar tomonidan sinovdan o'tgan pochta xizmatlaridan foydalanish maqsadga muvofiqdir. Shunday qilib, bugungi kunda pochta xizmati yaxshi himoyalangan liderlar *gmail.com* va *mail.ru* sanaladi. Pochta mijozidan foydalanishning yana bir varianti, bu *The Bat* dasturidir.

Parolni topish uchun brutforsdan foydalanish.

Brutfors-bu pochta xizmatidagi akkaunt parollarini avtomatik ravishda barcha ehtimoliy variantlarni tanlab olish uchun yaratilgan maxsus dasturdir.

Himoya usuli - taxmin qilish yoki mantiqiy hisoblash mumkin bo'lmagan murakkab parol ishlatish. Shunday qilib, parollarni taxmin qilishning eng oson usullari bu-tug'ilgan sana yoki telefon raqamini, uy hayvonining laqabini, shuningdek, bir xil raqam yoki harflarni takrorlashni o'z ichiga oladigan parollardir. Zaif parolning eng oddiy namunasi-bu Login bilan bir xil bo'lishi. Eng muhimi, agar parol 7 ta belgidan ortiq bo'lsa va unda turli raqamlar, harflar va turli registrlar ishlatilsa bunday parollarni buzish anchagina vaqt talab etadi.

Nazorat savolidan yordamida parolni tiklash xizmatidan foydalanish.

Har bir inson parolni yoki loginni unutishi mumkinligini tushunib, har bir pochta xizmatining ma'muriyati ushbu ma'lumotni qayta tiklashga yordam beradi va foydalanuvchilarga nazorat savoliga javob berishni taklif qiladi. Bu xizmat odatda, tajovuzkorlar tomonidan keng foydalaniladi, chunki foydalanuvchi odatda nazorat savoliga esidan chiqmaydigan narsani qo'yadi, masalan, onasining qizlik familyasi yoxud uy hayvonining ismi.

Himoya usuli, ro'yxatdan o'tkazish va nazorat savolini ko'rsatishda zaruriy o'ziga xoslikdan iborat. Xizmatlarni taklif etadigan standart savollarni unuting va hech kimni hayoliga kelmaydigan savol tuzing.

Cookiesni buzish.

Har bir kompyuterda Cookie-fayllar, ya'ni barcha tizim ma'lumotlarining ombori bo'lgan tizim fayllari mavjud. Ushbu Cookie fayllari tufayli brauzer yopilgandan keyin parollarni qayta kiritishimiz shart emas, chunki Cookie-fayllarda parollar va loginlar saqlanadi. Ushbu fayllardan xakerlar sizning pochtangizni buzish uchun foydalanishi mumkin.

Himoya usuli, siz xizmatni avtomatik ravishda yopish uchun pochta xizmatidan chiqib ketishingiz kerak bo'ladi. Ya'ni, brauzerni yoki sahifani yopish emas, balki "chiqish" tugmasini bosishingiz kerak.

4.2 Elektron pochtani buzish yo'llari

Har qanday elektron pochtani aslida buzish mumkinmi? Aslida, bu juda oddiy hol, deyarli har qanday elektron pochtani buzishni iloji bo'lishi mumkin. Ammo elektron pochtani buzishning haqiqiy yo'llarini bilishdan oldin quyidagi narsalarni eslab qolishingiz kerak:

– Tabiatan elektron pochtani bitta sehrli tugmani bosish bilan buzadigan dastur yo'q. Shunday qilib, agar siz bunday dasturni sotadigan web-saytni ko'rsangiz, bu yolg'ondir;

– Har qanday elektron pochtani 100-200 AQSH dollari evaziga buzamiz deb taklif qiladigan har qanday saytga hech qachon ishonmang. Odatda, ular firibgarlardir. Sayt yoki sizga xizmat ko'rsatuvchi shaxs haqida mulohazalarni diqqat bilan o'rganing;

– Buzish va himoya borasida tajribalardan shuni aytish mumkinki, elektron pochtani buzishni faqat ikki ishonchli yo'llari mavjud.

Boshqa barcha usullar faqat hiyla-nayranglar bilan yoki ishlamaydiganlar usullardir.

Quyida deyarli har qanday elektron pochtani buzishning ikki ishonchli yo'llari keltirilgan.

1. *Elektron pochtani buzish*: elektron pochtani buzishning eng oson usuli Keylogger (shuningdek, josus dastur deb ataladi). Keylogger jabrlanuvchining kompyuteridagi har bir bosilgan tugmani tadqiq qiluvchi kichik dasturdir. Ushbu usulni qo'llash uchun siz murakkab

narsalarni qilishingiz yoki maxfiy ma'lumotlarga ega bo'lishingiz shart emas. Kompyuterning nima ekanligini biladigan har bir kishi uni ishlatishi mumkin. Actual spy shunday dasturlardan biridir, lekin u pulli.

2. *Elektron pochta akkauntlarni buzishning boshqa usullari.* Elektron pochtani buzishning eng ko'p ishlatiladigan usullaridan biri, pochta web-sahifasining klonini yaratishdir. Gmail yoki Yahoo kabi ko'rinadigan soxta web-sahifalar ko'plab xakerlar tomonidan foydalaniladi natijada, foydalanuvchi nomi va paroli boshqa serverga yo'naltiriladi va siz boshqa web-sahifaga o'tasiz. Bir necha marta biz buni e'tiborsiz qoldiramiz, ammo oxir-oqibat biz shaxsiy ma'lumotlarimizni yo'qotamiz. Biroq, soxta web-sahifani yaratish va uni Internetda ishlatish oson ish emas. Soxta web-sahifani yaratish uchun HTML va php, JSP kabi skript tillari bilish talab qilinadi. Elektron pochtani buzishning eng oson usuli bu keyloggerlardan foydalanishdir.

Parolni buzish mumkin bo'lgan bir nechta usullar:

Har kuni tajovuzkorlar minglab parollarni buzishadi, bu hodisa juda oddiy bo'lib qoldi, bunday yangiliklar hech kimni hayratda qoldirmaydi. Tan olish kerakki sizning parolingiz buzilsa bu juda yoqimsizdir. Shu sababli, kimdir pochta, bank hisoblari, ijtimoiy media hisoblari va hatto Wi-Fi ulanish nuqtasiga ham kirish imkoniyatiga ega bo'ladi. Buning oldini olish uchun, aksariyat hollarda, foydalanuvchilarning aksariyati amal qilmaydigan axborot xavfsizligining asosiy qoidalariga rioya qilish kifoya. Lekin o'zingizni yanada ko'proq himoya qilish uchun, buzish qanday sodir bo'lishini va xavfni qayerdan kutish mumkinligini tushunish maqsadga muvofiq.

Parollarni buzishning keng tarqalgan usuli haqida batafsil ma'lumot beramiz va qanday zaifliklar sizning himoyangizni zaiflashtirishi mumkinligini ko'rsatamiz. Bundan tashqari, parollarni sinab ko'rish va ularni ishonchliligini tekshirish uchun onlayn xizmatlar ro'yxatini taqdim etamiz.

Parollarni qanday buzish mumkin?

Umuman olganda, avtorizatsiya qilish uchun boshqa odamlarning ma'lumotlarini qo'lga kiritishda bir xil usullar qo'llaniladi, bu faqat vaqt

o'tishi bilan biroz takomillashtirilishi mumkin. Ular haqida har bir kishi uzoq vaqtdan beri ma'lumotga ega va saytlarning aksariyati bunga qarshi kurashish va himoya qilishning muayyan usullarini qo'llamoqdalar, bu esa har doim parollarni buzishdan saqlamaydi. Bundan tashqari, bu usullar birlashtirilishi va kombinatsiyalashtirilishi mumkin.

1) Fishing

Bu boshqa odamlar parollarini bilib olishning juda keng tarqalgan va oddiy yo'li hisoblanadi. Uning soddaligiga qaramay, foydalanuvchilarning katta qismi akkauntlarini "o'g'irlanishi" ga imkon beradi.

Tajovuzkor "soxta" web-saytni yaratadi, uning ko'rinishi parollarni o'g'irlash rejalashtirilgan original Internet-resursni ko'chiradi. Keyinchalik u potentsial qurbonlarni ommaviy ravishda jalb qila boshlaydi (masalan, tezkor daromad, kulgili Mushuklar bilan video va boshqa qiziqarli ma'lumotlar haqida postga aloqadorligini ko'rsatadi). Foydalanuvchi unga tanish bo'lgan resursga, masalan, Vkontakte (va aslida bu sayt soxta) ga kiradi va ushbu kontentni ko'rish uchun siz o'z akkauntingizga kirishingiz kerakligini ko'rsatadi. U nima qiladi? Albatta, u o'z Login va parolini kiritadi va "kirish" tugmasini bosadi, darhol tajovuzkor bu ma'lumotlarni oladi va shubhali foydalanuvchi avtomatik ravishda ushbu saytga yo'naltiriladi va avtorizatsiya qilinadi va hech qanday shubha qolmaydi.

Xuddi shu tarzda, qo'llab-quvvatlash xizmatidan sizning elektron pochtangizga xabar xat keladi. Bu xatda sizning akkauntingizga biron-bir sababga ko'ra kirishingiz kerakligini va darhol kirish uchun havolani taqdim etishini aytadi. Foydalanuvchi ushbu saytga kiradi va yuqorida aytib o'tilganidek, hamma narsani takrorlaydi.

Shunga qaramay, qurbonlarning kompyuterlariga yashirincha tushadigan ba'zi zararli dasturlar ishlashi mumkin. Bunday viruslar mahalliy kompyuterda sozlamalarni o'zgartiradi va saytning asl nusxalari o'rniga o'z saytini sezdirmay ko'chiradi. Manzil satrida saytning aniq domeni hatto, garchi bu soxta bo'lsada shunday amalga oshiriladi.

Bu yerda asosiy faktor, insonning e'tiborsizligi hisoblanadi. Shunday qilib, bir nechta oddiy qoidalar sizni bunday baxtsizlikdan saqlab qolishi mumkun:

Agar pochtangizda sizning hisobingizga tashrif buyuruvchi shaxs akkauntiga o'tish taklif etilsa, unda u yuborilgan manzilga e'tibor bering. Ehtimol, bu aslida juda o'xshash bo'lishi mumkun, lekin hali ham u kichik farqlar bilan ajralib turadi (masalan, support@vk.com o'rniga support@vk.nz). To'g'ri manzil mavjudligi ham to'liq xavfsizlik kafolatini bermaydi.

Parol va login ma'lumotlarini kiritishda brauzeringizdagi manzil satriga e'tibor bering. Siz avtorizatsiyadan o'tishingiz kerak bo'lganda resursning haqiqiy manzili kerak boladi. Pochta holatida bo'lganidek, manzil juda o'xshash bo'lishi mumkin, lekin unda keraksiz yoki o'xshash belgilar bo'lishi mumkin. Asl saytni o'zi bilan almashtirgan virus bilan zararlangan bo'lsa ham, har qanday narsa soxta ma'lumotlarni ajratish uchun juda tabiiy ko'rinadi. Shuning uchun biz sayt bilan bog'liq holda shifrlash mavjudligiga ham e'tibor qaratishimiz kerak. Ushbu HTTP protokoli mavjud emasligi bilan namoyon bo'ladi. Bundan tashqari, manzil panelidagi o'ng yoki chap burchagida qulf ko'rsatiladi, agar siz ustiga bosgan bo'lsangiz, ulanish haqida qo'shimcha ma'lumot paydo bo'ladi, shunda siz saytning haqiqiyligiga ishonch hosil qilishingiz mumkin. Ko'pgina katta saytlar kirish paytida shifrlangan kalitdan foydalanadi, shuning uchun e'tiborli bo'ling.

Shuni takidlash kerakki, fishing hujumlari va parollar tanlash faqat inson tomonidan qo'lda bajarilmayapti. Ushbu maqsadlar uchun millionlab parollarni avtomatik ravishda tanlab oladigan va minglab elektron pochta va shaxsiy xabarlarni jo'natadigan maxsus dasturiy ta'minot ishlatiladi. Bu esa buzilgan akkauntlarni sezilarli darajada oshiradi va ushbu "ish" bo'yicha sarflangan vaqtni qisqartiradi. Bundan tashqari, xakerning faoliyatini yashirish uchun ushbu dasturlar yashirincha o'rnatiladi va boshqa foydalanuvchilarning maxsus serverlari va kompyuterlarida ishlaydi.

2) Parollarni qidirish.

Soddaligiga qaramasdan juda keng tarqalgan usul. Parolni tanlash Brute Force "qo'pol kuch" atamasi deb nomlanadi. Xaker uchun bu yerda muvaffaqiyatli harakatlarning ulushi juda kam va tasodifiy bo'lsada, uning ommaviy xarakteriga va vakolatli yondashuviga qaramasdan, bunday hujumlar hatto juda ko'p zararlarni keltiradi.

So'nggi yillarda bunday hujumlarning samaradorligi sezilarli darajada oshdi. Buning sababi shundaki, juda katta miqdordagi parollarni qabul qilgan xakerlar ularni tahlil qilishdi va foydalanuvchilar tomonidan ko'p qo'llaniladigan parollar "lug'at"ini tuzishdi. Shu sababli, parollar tanlash kamroq vaqt talab etadi va katta ta'sir ko'rsatadi. Internet tarmog'ida oddiy parollar bilan tajribasiz foydalanuvchilar qanchalik ko'p bo'lsa, muvaffaqiyat darajasi ham shuncha ko'p bo'ladi.

Shu bilan birga, agar hujum maxsus buzg'unchi dasturiy ta'minotdan foydalanib maxsus akkauntga amalga oshirilsa, 8 ta belgidan iborat parol bir necha kun ichida o'chirilishi mumkin. Agarda parol sifatida juda oddiy nom va tug'ilgan kun kabi ma'lumotlar ishlatilgan bo'lsa (bu juda tez sodir bo'ladigan bo'lsa), bunday parollar bir necha daqiqada buziladi.

Barcha saytlarda turli parollardan foydalanishga harakat qiling. Qoidaga ko'ra, agar biror bir resursdagi akkaunt buzilsa, zudlik bilan olingan parol yuzlab boshqa saytlarda tekshiriladi. Natijada, siz bir xil parollardan foydalansangiz, boshqa xizmatlardagi boshqa hisoblaringizning bir nechtasini ham buzishi mumkin. Har doim, pochta xizmatlari va ijtimoiy tarmoqlarda parolni qo'lga kiritgach, boshqa bir qator internet-resurslar bilan bog'liq boshqa buzg'unchilik to'lqinlari ham bor.

3) Saytni buzish orqali parollarni olish.

Keling, parolingizni olishda tajovuzkorlar ishlatadigan jiddiy va murakkab usullarga murojaat qilaylik. Oddiy saytlarning asosiy qismi foydalanuvchi parollarini shifrlangan holatda-xesh shaklida saqlaydi. Ya'ni, ro'yxatdan o'tish paytida sizning parolingiz ma'lum algoritm bilan ishlov beradi va parolni qaytarib olishga deyarli imkonsiz bo'lgan

raqamlar va belgilar bilan bog'liq bo'lmagan bir qatorga aylanadi. Saytga har safar kirganingizda, Siz kiritgan parol bir xil algoritm bilan qayta ishlanadi va agar ular mos keladigan bo'lsa, siz sahifangizga kirasiz.

4) Josus dasturiy ta'minot (SpyWare).

Bu foydalanuvchiga sezdirmasdan tizimga o'rnatiladigan zararli dastur bo'lib, birinchi galda kompyuter egasi va turli saytlarga kirishda ishlatiladigan foydali ma'lumotlarni to'plashda josuslik vazifalarini bajaradi.

Ular turli xil shakllarda bo'lib, turli usullar bilan harakat qiladi. Amalda ular o'zlarini ko'rsatmaydilar va hatto antiviruslar ularni sezmaydilar. Siz parolingizni boshqalar bilan baham ko'rganingizni o'zingiz ham bilmaysiz.

Zararli josus dasturlar ta'siridan saqlanish uchun, boshqa barcha viruslarga o'xshash qoidalar qo'llaniladi: shubhali saytlardan qoching, Internetdan yuklab olganingizni kuzating, faqat rasmiy saytlardan dasturiy ta'minotni yuklab oling va muntazam ravishda kompyuteringizni zararli dasturlardan tekshirib turing.

5) Parolni tiklashning ijtimoiy injiniring va ayyorona usullari.

Ijtimoiy injiniring-bu dasturiy ta'minotni emas, balki inson ongini buzishdir. Bu juda g'alati ko'rinadi, lekin butun insoniyatning ruhiyatining o'ziga xos xususiyatlaridan foydalanib, ayg'oqchiga kerakli ma'lumotni olishga imkon beradi. Internetda ushbu usulning juda ko'p sonli misollarini topishingiz mumkin, bu juda qiziqarli mavzu bo'lib, ushbu mavzu bo'yicha ko'proq maqolalar qidirishingiz va ularni o'qib olishingiz mumkin.

Keling, parollarni olishda ijtimoiy injiniring qanday ishlatilishini ko'rib chiqamiz. Ko'pchiligimizga ma'lumki, maxfiy savolga javob berish orqali parolimizni qayta tiklash mumkin bo'lgan ko'p saytlar borligini bilamiz: onaning qizlik nomi, birinchi mashina, sevimli rang, uy hayvoni nomi va shunga o'xshash. Hatto ehtiyotkorlik ko'rsatib, bu haqda hech qachon ijtimoiy tarmoqlardagi begona shaxslarga yozmagan bo'lsangiz ham, (hatto do'st) barcha kerakli ma'lumotlarni topish jarayonida bo'lgani kabi vkontakte tarmog'i yordamida siz bilan

tanishish, uchrashish, ishonchga kirib olish oson bo'ladi. Firibgarlarga ko'ngilchan foydalanuvchilarning o'zlari login va parollar, kredit karta raqamlari va boshqa ko'plab foydali ma'lumotlarni aytishga undaydigan, (odatda qo'llab-quvvatlaydigan va hushyorlikni maxsus texnika bilan uyg'otadiganlar kabi ko'rinadigan) juda oqilona usullar mavjud.

Parol buzilganligini qanday bilish mumkun?

Tarmoqda xakerlar ma'lumotlar bazalariga kiritilgan parolni tekshiradigan bir necha manbalar mavjud. Ulardan eng mashhurlari:

- https://haveibeenpwned.com
- https://breachalarm.com
- https://pwnedlist.com/query

4.1-rasm. haveibeenpwned.com resursi

Agar parol ma'lumotlar bazasida sizning qidiruv ma'lumotingiz bilan mos keluvchi ma'lumot topilgan bo'lsa, darhol parolingizni yangi, ayniqsa, ishonchli va murakkabiga almashtirish tavsiya etiladi.

4.3. Elektron pochta tizimi bilan ayyorlik

Elektron pochta xavfsizlik qoidalarini buzilishi yoki tarmoqqa jiddiy hujum qilishda doimo muayyan rolni o'ynaydi. Har bir virus, har qanday zararli dasturiy ta'minot, har bir fishing xabari asosiy transport mexanizmi yoki tizimga hujum qilishdagi kirish usullari sifatida elektron

pochta xabarlaridan foydalanadi. Elektron xabarlar boshqa aloqa turlari (masalan, SMS yoki lahzali xabarlar) kabi ommabop bo'lmasligi mumkin, biroq bu korporativ va hukumat dunyosida keng qo'llaniladigan vositachidir. Endi biz e-mail haqidagi g'oyani va uni qanday qilib qurol yoki himoya vositasi sifatida foydalanish mumkinligini diqqat bilan ko'rib chiqamiz.

Tarmoqqa ulanishda bir nechta kirish nuqtalarini bilishimiz kerak. Agar biz faqat bitta kirish nuqtasiga tayansak, ishlatilayotgan zaiflik aniqlangan bo'lsa, nima qilamiz? Tarmoqqa kirishning bir nechta nuqtalari bizni ushbu tarmoqni boshqa joyga ko'chirish uchun ko'proq erkinlik beradi. Yondashuv yo'llari juda muhim, bu haqda tushuntirishimiz kerak.

Tashkilot tomonidan elektron pochta yoki tarmoq orqali kirish uchun ishlatiladigan nomlar tomonidan yaratilgan sxema haqida bilish bizga katta afzallik beradi. Foydalanuvchi nomini bilish orqali biz bu foydalanuvchining parolini olishga e'tibor qaratsak bo'ladi.

Aksariyat tashkilotlar (qisman barchasi) bir sxemadan foydalanadilar: *«ism. familiya@kompaniyanomi.com»*.

Ba'zilar dastlabki birikma va lastname@callname.com kombinatsiyasidan foydalanishadi. Boshqalari familiya va birinchi boshlang'ich kombinatsiyasidan foydalanadi, keyin @ name.com. Bu juda shoshqaloqlik, shunday emasmi? Bundan keyin, elektron pochta foydalanuvchisini kiritmang. Bu juda keng tarqalgan xatodir. Tarmoqdagi tashkilotlar foydalanuvchilarga kim, qayerda ishlayotgani va nima qilayotganini aniqlash imkonini beradigan katalogga ega. Ushbu ichki katalog buzg'unchilar uchun oltin koni. Har bir foydalanuvchi haqida ko'proq ma'lumot olish uchun Facebook yoki boshqa ijtimoiy tarmoqlarda profillarni ko'rishingiz mumkin. Dam olish vaqtida, nima qilishlari, sevimli mashg'ulotlari va ulardan foydalanishlari mumkin bo'lgan parollar turlari haqida boshqa narsalarni bilib olishingiz mumkin. Ushbu ma'lumot, agar siz bu kishilarga nisbatan ijtimoiy injineriyadan foydalanishni xohlasangiz foydali bo'ladi (masxaralash yoki foyda uchun).

E-pochta manzillarini to'plashni va elektron pochtani xakerlik vositasi sifatida ishlatishi savollarini ko'rib chiqamiz. E-pochtani buzish ijtimoiy muhandislik bilan chambarchas bog'liq (biz bu haqda yana bir marta xabar qilamiz). The Social Engineering Automation Kit (SEAK) http://www.seak.com.ar/ saytidagi ijtimoiy injineriyani avtomatlashtirish to'plami tarmoq yoki web-saytdagi elektron pochta manzillarini topish uchun qidiruv tizimlaridan foydalanishga mo'ljallangan. SEAK - bu qidiruv tizimlarining web-sahifalar va tarmoqdagi o'rinlarini izlashga imkon beruvchi Perl skriptlarining to'plami bo'lib, ular topadigan barcha elektron pochta manzillarini ko'rsatadi. SEAK odamlarni qidirish uchun ham ishlatilishi mumkin. SEAKga o'xshash bir qancha dasturlar mavjud. Ular Esearchy deyiladi. Uni http://hithub.com/Freedom Coder/ESearchy-ng manzilidan yuklab olishingiz mumkin. Esearchy bilan SEAK funksional jihatdan bir xil, lekin uni Windowsda qo'llash mumkin; Ushbu dastur hujjatlarni izlaydi. Esearchy matn ichida yashirilgan parollarni, shuningdek, jamoatchilik uchun ochiq bo'lgan elektron pochta manzillari kabi boshqa foydali ma'lumotlarni izlaydi.

Maltego utilitasi-sud tajribasida analizator sifatida ishlatilishi mumkin bo'lgan ochiq kodli dasturdir. Maltego ochiq manbalardan ma'lumot topishga yordam beradi, ma'lumotlarni tahlil qilish va ma'lumotlar uzatish uchun qulay bo'lgan grafik ko'rinishidagi ma'lumotlarni ko'rsatadi. Umumiy holda, Maltego bilan siz odamlar va guruhlar, web-saytlar, domenlar, tarmoqlar va onlayn xizmatlar (masalan, sevimli ijtimoiy tarmoqlar) o'rtasidagi haqiqiy munosabatlarni tahlil qilishingiz mumkin.

Shuningdek Google qidiruv tizimidan foydalanishingiz mumkin. Ishchi profil haqidagi barcha ma'lumotni ko'rishni istasangiz, quyidagi buyruqlardan foydalanishingiz mumkin:

site: www.google.com intitle:"Google Profile" "Companies I've worked for" "at company_name".

Gpscan-ushbu qidiruvni avtomatlashtiradigan va yanada ko'proq natijalarga erisha oladigan Rubyda yozilgan dastur. Yuqoridagilardan kelib chiqib Gpscan razvedka va ijtimoiy muhandislik uchun kuchli

vosita bo‘lib qolmoqda. Siz Gpscan-ni http://www.digininja.org/projects/gpscan.php manzilidan topishingiz mumkin.

Misollar

2007 yilda “Fortune 500” kompaniyasining bosh ijrochi direktori yuqori malakali xodimlardan birining xatini oldi. “Kimdan” maydonidagi xatda: maktub kompaniyaning ichki tarmog‘iga yuborilganligi aniq bo‘ldi. “Mavzu” maydonida:” energiya sarfini qanday kamaytirish mumkin” degan matn bor edi. Bosh direktor ushbu elektron pochta xabarini ochganda, undagi ilova va havolani ko‘radi. Direktor ilovani ochdi, lekin u ekranida hech narsa ko‘rmadi va xatni yopdi. Bir necha oydan keyin FBI bosh direktorga o‘zining shaxsiy kompyuterida zararli dasturiy ta’minotni yuqtirganligi uchun kompaniyadan bir necha terabayt ma’lumot o‘g‘irlanganini ma’lum qildi. FBI bu “zararli ta’sirni kamaytirish” mavzusidagi maktub ekanligini tasdiqladi. Ushbu xabar soxta edi.

Shu kabi holatlar har kuni sodir bo‘ladi. Amakingiz sizga qo‘ng‘iroq qilib elektron pochtasiga nega buncha ko‘p reklama yuborganingizni so‘raydi. Maktabda, do‘stingiz sizdan befoyda reklamalar qabul qiladi. Nima uchun siz buncha spam-xabarlarni yuborasiz?!

E-pochta manzilingiz soxtalashtirilgan yoki elektron pochta dasturingiz buzilgan bo‘ladi. E-pochta manzilingiz buzilganligini tekshirish uchun yuborilgan xabarning sarlavhasini ko‘ring. Biz bu darsda ilgari nima qilishni bilib oldik. Endi o‘z bilimlaringizni amalda qo‘llang. Sizdan maktub olgan har bir kishidan sizni to‘liq (faqat xabarning matni emas) qaytarib yuborish uchun so‘rang. Sarlavha sizning elektron pochta manzilingiz o‘zgartirilganligini yoki yo‘qligini ko‘rsatadi.

E-pochtadagi javob va jo‘natilgan maydonlarga qarang. O‘tgan mashqlarda ko‘rganimizdek, ushbu maktub siz yoki boshqa birov tomonidan yuborilganligini ko‘rsatadi.

Maxfiylik to‘g‘risida gap ketganda, webmail shaxsiy hayotga qayg‘urishdan ko‘ra eng oxirgi o‘rinda turadi. Veb-xizmatdan sizning barcha xabarlaringiz, kontaktlar, kalendar yozuvlari va ushbu

ma'lumotni olishga imkon beruvchi qonuniy hujjatlar asosida boshqa ma'lumotlarni taqdim etishni so'rashingiz mumkin. An'anaviy, lekin foydali bo'lgan, o'zingizdan boshqa nom ostida elektron pochta hisobini yaratish ayyorligidir. Yashirin xabarlarni jo'natmoqchi bo'lganlar elektron pochtangizga kirishlari kerak. Siz elektron pochta xabarini yaratishingiz va uni qoralama sifatida saqlashingiz mumkin. Siz hech qachon xabar jo'natmaysiz, faqat ba'zi kontent bilan qoralama yarating xolos. Maktubingiz sizning akkauntingizda qoladi, lekin uni hech qachon jo'natilmaganligi sababli kuzatib bo'lmaydi. "Qabul qiluvchi" ushbu akkauntga kiradi va xabarnomani o'qiydi. Qoralama xabarni o'qib bo'lgandan keyin uni o'chirishi yoki o'zgartirilishi-bunda siz uchun yangi xabar yaratilishi mumkin. Bu to'psiz ping-ponga o'xshaydi. Shuningdek, siz ham Google umumiy hujjati bilan ishlashingiz mumkin.

4.4. Parolni buzish usullari

Kompyuter ma'lumotlarining eng keng tarqalgan himoyasi parolga asoslangan himoya hisoblanadi. Parolni muhofaza qilishni amalga oshirishda tizimga kirish, dasturni ishga tushirish, ma'lumotlarga kirishni talab qilish parol so'rovi bilan birga kiritiladi va keyin kiritilgan parolni original bilan taqqoslanadi.

Parol-bu alifbo va maxsus belgilarning belgilar ketma-ketligi. Ketma-ketlik eng qisqa va eng uzun uzunlikdagi cheklovni ta'minlashi kerak.

Zudlik bilan biz parollarni himoyalashni faqat tor doiradagi foydalanuvchilar uchun mo'ljallangan ma'lumotlarni himoyalashda foydalanish mumkinligini takidlaymiz. Masalan, bu tarzda himoyalangan dasturlar keng tarqalgan bo'lib foydalanilganda, kamida bitta qonuniy foydalanuvchi tajovuzkorga parolni taqdim etishi ehtimoli juda yuqori, bu himoyalangan ilovani ommaviy tarzda foydalanish uchun yetarli bo'ladi.

Parolingiz xavfsiz deb o'ylaysizmi? Qayta o'ylang. Agar siz parolingizni va ma'lumotlarni imkon qadar xakerlardan himoya qilishni istasangiz, parollarni buzishda ishlatiladigan usullar bilan tanishib chiqing. Agar bunday jinoyat turlari sizni ularning diqqatidan chetda

qoldiradi deb hisoblasangiz yoki ular hech qachon parolingizni topa olmasligiga ishonsangiz, bu qarashlaringoz qanchalik noto'g'ri ekanini bilishingiz mumkin.

1. Lug'at yordamida hujum

Buning uchun lug'atda qidirilivchi kutilmagan syurpriz- syurpriz so'zlaridan tarkib topgan oddiy fayldan foydalaniladi. Boshqacha qilib aytganda, bu hujum turi ko'plab odamlar parol sifatida foydalanadigan so'zlarni tanlash orqali o'tadi.

Masalan, "simsimochil" yoki "mansuperadministratori" birgalikda to'plangan so'zlardan iborat parollardan foydalanish buzishdan qutqarmaydi-ehtimol, xakerlar buning uchun bir necha soniya sarflaydi.

2. To'la tanlov hujum uslibi (qo'pol kuch)

Bu usul lug'at asosidagi hujumiga o'xshaydi, lekin qo'shimcha bonus bilan, albatta, lug'atda mavjud bo'lmagan so'zlarni topa oladigan, aaa1-zzz10 gacha bo'lgan barcha alfanumerik birikmalarni tanlovini o'tkazadigan xakerlik hujumi.

Bu tezkor usul emas, biroq sizning parolingiz bir nechta belgidan iborat bo'lsa, unda natijada parolingiz ochiladi. To'la tanlov usuli kompyuter qo'shimcha hisoblash quvvatini, shu jumladan, GPU grafik kartangizning imkoniyatlaridan foydalanib, masalan, tarmoqlangan hisoblash modellari va zombi botnetlardan foydalanib, soddalashtirilishi mumkin.

3. Kamalak jadvali asosidagi hujum

Kamalak jadvali-zamonaviy tizimlar tomonidan ishlatiladigan oldindan hisoblangan xeshlarning (shifrlangan parollarning raqamli mazmuni) ro'yxati. Jadval xeshlash algoritmlarining ixtiyoriy turi uchun barcha parollar kombinatsiyalarini o'z ichiga olgan xeshlardan tarkib topadi. Kamalak jadvali yordamida parolni buzish uchun sarflanadigan vaqt, ro'yxatdan xeshlangan parolni topish vaqtiga nisbatan aniqlanadi. Shunga mos holda, jadvalning o'zi juda katta bo'lib uni ko'rib chiqish uchun jiddiy hisoblash qobiliyatini talab qiladi. Agar topishga harakat qilayotgan xesh, aralashgan algoritmni qo'llashdan oldin parolga

tasodifiy belgilarni qo'shish bilan murakkablashsa, u ham foydasiz bo'ladi.

Murakkab kamalak jadvali imkoniyatlari to'g'risida gapirish muhim, ammo ular juda katta bo'lganda, ularni amalda qo'llash qiyin kechar edi. Ular, ehtimol, oldindan belgilangan "tasodifiy o'zgaruvchilar" to'plami bilan ishlaydi, shuning uchun parol 12 belgidan kamroq bo'lishi kerak emas, aks holda jadval o'lchami davlat darajasidagi xakerlar uchun ham nihoyatda katta bo'ladi.

4. Fishing

Buzg'unchilikning eng oson usuli-foydalanuvdan parolini so'rashdir. Fishing xabari o'quvchini hech qanday shubhaga bormasdan soxta onlayn banking saytlari, to'lov tizimlari yoki boshqa saytlarda "xavfsizlik bilan aloqador biror bir muammoni bartaraf etish" niqobi ostida shaxsiy ma'lumotlarni kiritishni talab etadi.

Foydalanuvchi o'z parolini buzg'unchini qiynamasdan nega aynan o'zi xabardor qiladi?

5. Ijtimoiy injiniring

Ijtimoiy injiniring fishing bilan bir xil konseptsiyaga rioya qiladi-pochta qutisini ishlatmasdan, real dunyoda "foydalanuvchidan parolni so'rash"ni ijro etadi.

Ijtimoiy injiniringni mohiyati-AT xavfsizligi mutaxassisi sifatida ofisga qo'ng'iroq qiladi va tarmoqdan foydalanish parolini so'raydi. Siz buni qanchalik tez-tez takrorlanishidan hayratga tushasiz. Ayrim jinoyatchilar ushbu savolga administratordan yuzma-yuz javob olish uchun kompaniyaga kelishdan oldin kostyum kiyishi va birka taqishi lozim bo'ladi.

6. Zararli dasturlar

Barcha klaviaturadan kiritiluvchi va ekranda aks etuvchi ma'lumotlarni qamrab olib, ularni tasvir nusxalarini xakerga yuboradigan zararli dastur.

Ba'zi zararli dasturlar mijozning veb-brauzerida mavjud parol faylini qidiradi, keyin bu faylni nusxalaydi (yaxshi shifrlanganlardan tashqari) bunda foydalanuvchining sahifa tarixida saqlangan parollarni osonlik bilan qo'lga kiritish mumkin bo'ladi.

7. Offline hujum

Parolni xavfsiz deb tasavvur qilish oson, uch yoki to'rtta muvaffaqiyatsiz paroldan so'ng foydalanuvchilarni blokirovka qiluvchi tizimlarni cheklash orqali himoyalangan bo'lsa, bu ham avtomatik parolni aniqlash dasturlarini blokirovka qilishga imkon beradi. Ko'pgina parollarning xavfga uchrashi "obro'sizlangan" tizimdan qabul qilingan parollar faylida xeshlar to'plamidan foydalanib offline rejimda amalga oshiriladi. Buni ko'plab faktlar inkor etmagan hollarda, balki bu haqiqat bo'lishi mumkin.

Ko'pincha, ushbu qurbonlik foydalanuvchining barcha muhim fayllarini xeshlash parollari bilan birga va server tizimiga xakerlarning kirishini ta'minlovchi uchinchi tomonni himoyasini chetlab o'tish orqali obro'sizlanishga olib keladi. Parol buzg'unchilari maqsadli tizim yoki shaxsiy foydalanuvchilarni xabardor qilmasdan kodni buzishda qancha vaqt sarflanishidan qat'iy nazar urinishda davom ettiradilar.

8. Yelkaning ustunini ushlab turish

Kur'yer niqobi ostidagi o'ziga ishongan xaker, konditsionerlarga texnik xizmat ko'ratuvchi mutaxassis yoki boshqa har qanday xodim sifatida ofis binosiga kirib oladi.

Ofis binosiga kirishi bilanoq, xizmat ko'rsatuvchi personal rasmiy kiyimi uni ofisning ixtiyoriy nuqtasida hech qanday qarshiliklarsiz harakatlanishiga imkon beradi. Bu ularga xodimlar tomonidan haqiqiy kiritilgan parollarni yozib olish imkonini beradi, shuningdek, ko'pchilik odamlar kompyuterlar monitorlariga to'g'ridan-to'g'ri parollarni yopishqoq stikerlarga yozib qo'yadilar bu esa istalgan barcha parollarni ko'rish imkoniyatini beradi.

9. "O'rgimchaklar" usuli.

Tajribali xakerlar korporativ parollarning ko'pchiligi biznes bilan bog'liq so'zlardan tashkil topganligini angladilar. Korporatsiyaning adabiyotlarini o'rganish, web-saytlar materiallari, raqobatchilarning saytlari va hatto mijozlar ro'yxati xakerlarni "o'q-dorilar" bilan maxsus so'zlar ro'yxatini tuzish uchun ishlatilishi mumkin.

Haqiqiy tajribali xakerlar jarayonni avtomatlashtiradilar va kalit so'zlarni aniqlash, buzish uchun ro'yxatlar yaratish va qayta ishlash

uchun yetakchi qidirish mexanizmlari tomonidan ishlatiladigan veb-ga asoslangan ilovalarni ishga tushirishdi.

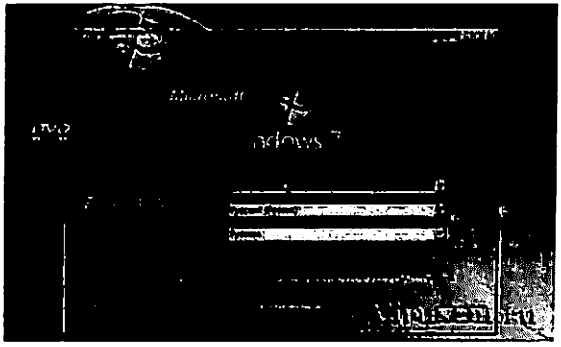
10. Taxmin

Parol buzuvchilarning eng yaxshi do'sti, albatta, foydalanuvchilarning taxminlaridir. Agar ushbu vazifani bajarish uchun mo'ljallangan dastur yordamida haqiqiy tasodifiy parol yaratilgan bo'lsa, foydalanuvchi "tasodifiy" parolni o'xshash biror narsa eslatmaydi.

Buning o'rniga, biz yoqtirgan narsalarga hissiy munosabatimiz tufayli, ehtimol, biz yaratgan "tasodifiy" parollar bizning manfaatlarimizga, sevimli mashg'ulotlariga, uyda oziq-ovqat nomlari, oila va shunga o'xshash narsalarga asoslangan bo'ladi. Aslida, parollar odatda ijtimoiy tarmoqlarda gaplashishni istagan barcha narsalarga asoslanadi va hatto bizning profilimizga kiritiladi. Parol krakerlari, bu ma'lumotlarga qarashlari va lug'at yoki qo'pol kuch usuliga murojaat qilmasdan, iste'molchi darajasidagi parolni buzishga urinayotganda bir nechta, odatda to'g'ri deb taxmin qilishadi.

4.5. Windows tizimi parolni tiklash yo'llari

Endi Windows 7 tizimida parollarni qayta tiklash usuli haqida so'z yuritamiz. Bu usul Windowsning boshqa versiyalarida qo'llanilishi mumkin bo'lsada, farq faqat quyidagi rasmlarda va menyu elementlarining matnida seziladi. Umuman olganda, tartiblar bir biriga o'xshash.



4.2-rasm. Windows 7 tizimi asosiy oynasi

Parolni unutish, bu ishni ona platasini almashtirishgacha yetib borishi mumkin. Windows tizimining qayd yozuvi parolini ochish holatida hamma narsa juda oson. Bizga buning uchun DVD o'rnatish diski (Windows) va 10 daqiqa vaqt talab etiladi.

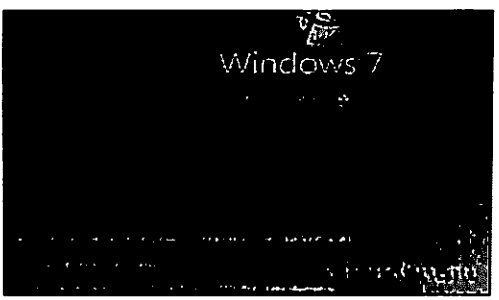
Shunday qilib, vaqt ketdi:

1. Kompyuterni yuklang, qora ekran yonib-qora bo'lgach, "Press ??? to enter Setup" yozuvi paydo bo'lishini kuting, ??? belgisi o'rnida mos paydo bo'luvchi tugmani(bular "Delete", "F2", "F8 bo'lishi mumkin) bosing. Bu kompyuterni (ona plata) ishlab chiqaruvchisi bilan farq qiladi. BIOS-ga kirish uchun qo'shimcha menyu punkti ham mavjud.

2. BIOS-da, ona karta turiga qarab, rasm tasvirlari turlicha bo'lishi mumkin, lekin shunga qaramay, biz *Boot* qismini qidiramiz va kompyuterni CDROM drayveri yordamida yuklaymiz. Menyudan First Boot Device elementini qidiramiz, sukut holatida u yerda HDD tanlangan bo'ladi. Sozlash uchun bosing: biz kvadratcha CDROMning qarama-qarshi tomonida ekanligiga ishonch hosil qilishimiz lozim.

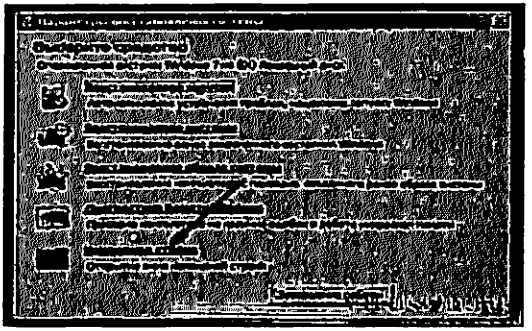
3. Diqqat! O'rnatish diskini qabul qilish holatidaligini tekshiring. BOIS sozlamalarini saqlash uchun F10 tugmachasini bosing, sozlash saqlanadi va kompyuter yangi parametrlar asosida ya'ni, qattiq diskdan emas, balki CD, DVD qabul qilish qurilmasidan qayta yuklanadi.

4. Kompyuter qayta yuklanadi va Windows o'rnatilishi boshlanadi. Quyida paydo bo'lgan muloqot oynasidan "Восстановление системы" bandini tanlaymiz.



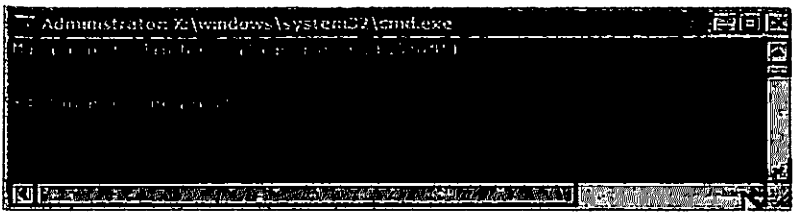
4.3-rasm. oynasidan "Восстановление системы" bandini tanlaymiz

5. Ochilgan “Параметры восстановления системы” oynasidan “Командная строка” buyruqlar ko‘rsatmasini tanlang.



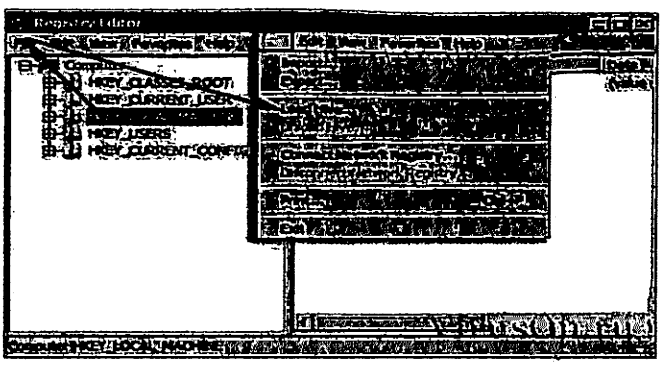
4.4-rasm. “Параметры восстановления системы” oynasi

6. Qora buyruqlar oynasida regedit buyrug‘ini kiriting (yozing) va Enter tugmasini bosing, shu bilan “Редактор реестра”ni oching.



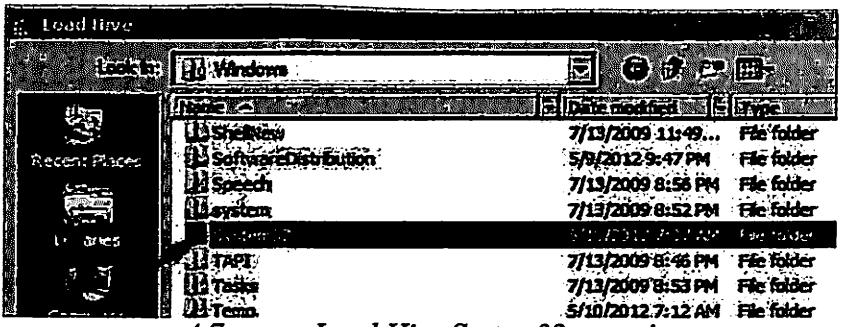
4.5-rasm. Qora buyruqlar oynasi

7. HKEY_LOCAL_MACHINE elementini sichqoncha yordamida tanlab,yuqori suzuvchi Fayl (File) menyusini bosing va ochilgan menyudan “Загрузить куст (ветвь)”, ing. Load Hive buyrug‘ini tanlang.



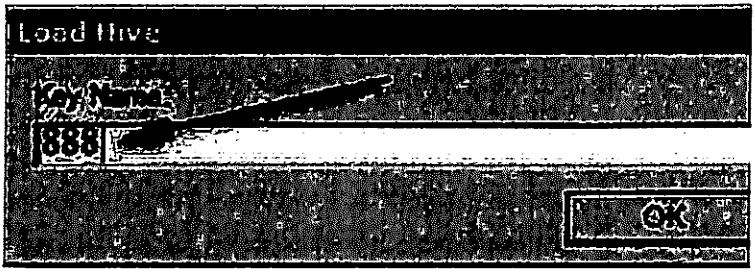
4.6-rasm. Registry Editor HKEY_LOCAL_MACHINE oynasi

8. Ochiq oynada My Computer (Kompyuter) ni bosing va C:/yoki D:/tizimli diskni tanlang. Umuman olganda, sukut bo'yicha DISK:/Windows/System32/ config/SYSTEM manzilida joylashgan tizim faylini qidiramiz.



4.7-rasm. Load Hive System32 oynasi

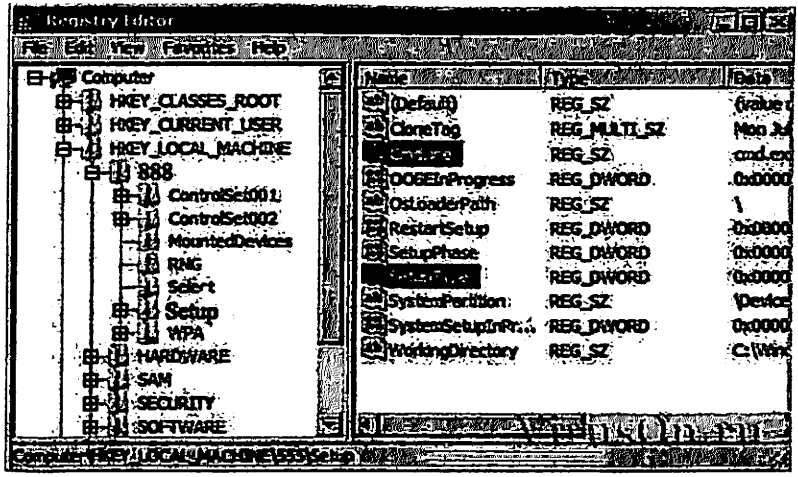
9. Sichqoncha tugmasini ikki marta bosish orqali SYSTEM faylini ishga tushiring. Kichik darchani har qanday qiymat bilan to'ldiramiz, lekin biz uni eslaymiz. 888 raqamidagi rasmda OK tugmasini bosing.



4.8-rasm. Load Hive ning key name oynasida

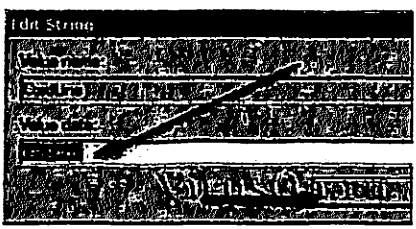
10. Biz yana ro'yxatga olish muharriridamiz. HKEY_LOCAL_MACHINE\ MENU VALUE\Setup-ni qidiramiz. Setup papkasini ustiga bosib, uni tanlang.

11. CmdLine parametrini qidirmoqdamiz. Sichqoncha bilan ikki marta bosing, "Edit String" (Edit String) oynasida biz cmd.exe yozamiz va OK tugmasini bosamiz.



4.9-rasm. HKEY_LOCAL_MACHINE\MENU VALUE\Setup oynasi

12. SetupType parametrini qidiramiz. 11-xatboshiga o'xshash amallarni bajaring. O'rnatilgan 0 qiymatini 2 ga o'zgartiring va OK tugmasini bosing.



4.10-rasm. Edit String parametridan cmd.exe yozish oynasi

13. O'zgarishlarni amalga oshirgandan so'ng, yaratilgan papkani "VALUE" (888-sonli rasmda)-ni tanlab, yuqoridagi "File" (Fayl) menyusidan "Выгрузить куст (ветвь)", ing. Unload Hive elementini bosing. Reestrni tahrirlash oynasini yoping va "Параметры восстановления системы" oynasidan "Перезагрузить" tugmasini bosing.

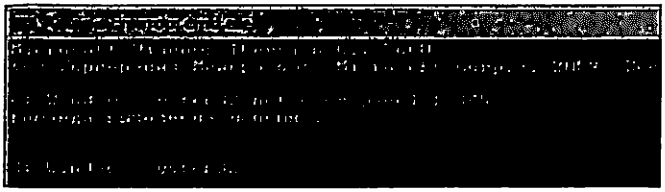
Tizim qayta ishga tushirilgandan so'ng, kompyuter an'anaviy tarzda emas, buyruq qatorini kiritish rejimida paydo bo'ladi.

Biz Windows tizimi parolini buzish ustida ishlashni davom ettiramiz.

Variant-1-Foydalanuvchi nomi mavjud, lekin parol yo'q.

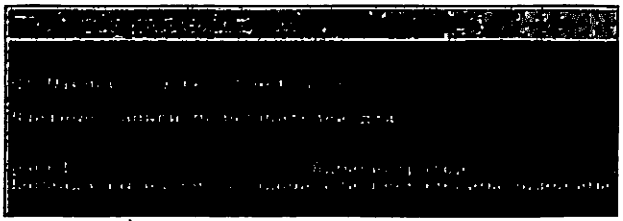
Parolni o'zgartirish (asl holatini tiklash) uchun buyruq qatorida rasmda bo'lgani kabi, **net user NAMEuser NEWParol**-ni kiriting va **Enter** tugmasini bosing.

Agar loginda bo'sh joy bo'lsa, uni qo'sh tirnoqlarga olib qo'ying.



4.11-rasm. Administrator: cmd.exe oynasida parolni tiklash

Variant 2-Siz, albatta, parolni yoki foydalanuvchi nomini eslay olmaysiz. Bunday holda, **net user** buyrug'ini kiriting va **Enter** tugmasini bosing. Buyruq bajariladi, ushbubuyruq tizimning barcha foydalanuvchilarini (ularning hisoblarini) topadi va ko'rsatadi.



4.11-rasm. Administrator: cmd.exe oynasida parolni tiklash

net user buyrug'ida parametr bo'lmaganligi sababli, buyruq satrida xato paydo bo'ladi, ammo bu og'riqli emas.

Sizning keyingi harakatlaringiz uchun istalgan foydalanuvchi nomini tanlab va satrni to'ldirishingiz mumkin. Agar siz yangi foydalanuvchi qayd yozuvi yaratishni xohlamasangiz va ushbu nomni o'z holicha qoldiramiz.

Foydalanuvchi nomi va yangi parolni kiritish orqali buzilgan tizimda yangi hisob yaratish:

Buyruqning satrini ketma-ket (har biri 1,2,3 raqamisiz) kiritib, har kiritilgan qatordan so‘ng Enter ni bosing:

Windows 7 rus tilida:

1. net user ИМЯпользователя НОВЫЙпароль
2. net localgroup Администраторы ИМЯпользователя
3. net localgroup Пользователи ИМЯпользователя

Windows 7 ingliz tilida:

net user add

net localgroup Administrators add

net localgroup Users delete

So‘ngra, qora buyruqlar oynasini yoping va Windows 7 yangi parametrlar bilan yuklashni davom ettiradi.

Login va parol maydonlarida yangi ma’lumotlarni kiriting, ularni buyruq satrida yaratdingiz va siz ushbu parolni qayta-qayta takrorlaysiz.

Asosiy xulosalar

E-pochtani buzishning quyidagi usullari mavjud: Troyanlarni ishga tushirish, aldash orqali foydalanuvchi parollarini topish, soxta sahifalarni yaratish, sifatsiz elektron pochtadan foydalanish, parolni topish uchun brutforsdan foydalanish, Cookies fayllarni buzish.

Deyarli har qanday elektron pochtani keylogger (josuslarga qarshi dastur deb ham ataladi) yordamida yoki elektron pochta orqali web-sahifaning klonini yaratish orqali buzish mumkin.

E-pochtani buzish usullari: fishing, parollarni tanlash, saytni buzish orqali parollarni olish, parodlarni, josus dasturiy ta’minot, parolni tiklashning ijtimoiy injiniring va ayyorona usullari.

Pochta qutisini buzish bu ijtimoiy injinering bilan chambarchas bog‘liq.

Parolni buzishning eng keng tarqalgan usullar quyidagilardir: Lug‘at yordamida hujum, to‘la tanlov hujum uslibi (qo‘pol kuch), kamalak jadvali asosidagi hujum, fishing,ijtimoiy injiniring, fishing, ijtimoiy injiniring, zararli dasturlar, offline hujum, yelkaning ustunini ushlab turish, “O‘rgimchaklar” usuli, taxminiy usullar.

Windows operatsion tizimida o'rnatilgan kompyuter foydalanuvchisi parolini qayta tiklash tizim parolini buzish orqali amalga oshiriladi.

Nazorat savollari

1. *Elektron pochtani buzish kimga va nimaga kerak?*
2. *Elektron pochtani buzish usullarini ayting.*
3. *Elektron pochtani himoyalash usullarini tavsiflang.*
4. *Elektron pochta qanday vositalar yordamida buziladi.*
5. *Parollar qanday buziladi?*
6. *Parol buzilganligini qanday aniqlash mumkin?*
7. *Parollarni buzishning keng tarqalgan usullarini ayting.*
8. *Windows operatsion tizimi o'rnatilgan kompyuter foydalanuvchisi parolini buzishning qanday usulini bilasiz?*

V-BOB. AXBOROTNI HIMOYA QILISH TAMOYILLARI

5.1. Axborotni himoya qilishning asosiy tamoyillari

Axborot bugungi kunda muhim resurs bo'lib, uning xavf-xatarga uchrashi noxush oqibatlarga olib keladi. Kompaniya konfidensial ma'lumotlarini qo'lga kiritilishi moliyaviy yo'qotish tahdidi bilan bog'liq, chunki olingan ma'lumotlar raqobatchilar yoki tajovuzkorlar tomonidan ishlatilishi mumkin. Bunday noxush holatlarning oldini olish uchun barcha zamonaviy firmalar va tashkilotlar axborot himoya qilish usullaridan foydalanadilar.

Bugungi kunda kompyuter ma'lumotlarini muhofaza qilish deganda axborotning yaxlitligini tekshirish masalalarini hal etuvchi usullar va vositalar, kompyuter resurslari, unda saqlanadigan dasturlar va ma'lumotlarga, shuningdek, dasturiy ta'minot mahsulotlaridan ruxsatsiz foydalanishni istisno qiluvchi chora tadbirlar majmui tushuniladi.

Axborot xavfsizligini ta'minlashning asosiy tamoyillari quyidagilardan iborat:

- *tizimlilik;*
- *murakkablik;*
- *himoyalashning uzluksizligi;*
- *yetarlilik;*
- *boshqaruv va qo'llashdagi moslashuvchanlik;*
- *himoyalash mexanizmlari va algoritmlarining ochiqligi;*
- *himoyalash choralari va vositalarini qo'llash qulayligi.*

Tizimlilik tamoyili tajovuzkorlarni, tahdidlarni ro'yobga chiqarish uchun mavjud va kelajakda sodir bo`lishi mumkin bo'lgan kanallarni hisobga olish zarurligini nazarda tutadi.

Murakkablik tamoyili. Axborot xavfsizligi (AX) mutaxassislari kompyuter tizimlarini himoya qilish uchun keng ko'lamli chora-tadbirlar, usullar va vositalarga ega. Murakkablik tamoyili birlashtirilgan

himoya tizimini qurishda axborot xavfsizligi vositalari (AXV) tizimi ishini muvofiqlashtirishni, turli xil AX tizimlarini biriktirishdagi zaif nuqtalarni yo'q bo'lishi, tahdidlarni amalga oshirish mumkin bo'lgan barcha kanallarni qamrab oladi.

Himoyalashning uzluksizligi tamoyili. Axborotni muhofaza qilish-bir martalik hodisa emas, balki hayotning barcha bosqichlarida tegishli choralar ko'rishni o'z ichiga olgan doimiy maqsadli jarayondir. Masalan, ko'pchilik jismoniy va texnik vositalar o'zining vazifasini ishonchli ijro etishi uchun muntazam tashkiliy qo'llab-quvvatlashni talab qiladi (ismlarni, parollar, shifrlash kalitlarini o'z vaqtida o'zgartirish va saqlashni ta'minlash va boshqalar).

Yetarlilik tamoyili. Umuman olganda mutlaq xavfsizlikni ta'minlovchi himoya tizimini yaratish juda ham mushkul, tizimni buzish vaqt va pul masalasidir. Masalan, ixtiyoriy kriptografik xavfsizlik vositasi mutlaq barqarorlikni kafolatlamaydi, biroq axborotni himoyalash jihatidan vaqt bo'yicha axborotning konfidensialligini ta'minlaydi.

Boshqaruv va qo'llashdagi moslashuvchanlik tamoyili xavfsizlik darajasini o'zgartirish mumkinligini anglatadi. Muayyan ish sharoitlarida avtomatlashtirish tizimlari, uning xavfsizligini ta'minlaydigan axborot xavfsizligi vositalari muhofazalashning yetarli darajada bo'lishini qisman ta'minlaydi. Himoya tizimini boshqarish va qo'llashning moslashuvchanligi avtomatlashtirilgan tizim egalarini avtomatlashtirish tizimlarining ish sharoitlarini o'zgartirganda himoya vositalarini yangilariga almashtirish bo'yicha keskin choralarni ko'rish zaruratidan xalos qiladi.

Himoyalash mexanizmlari va algoritmlarining ochiqligi tamoyili. Shuni takidlash lozimki, axborotni muhofazalash vositasi tuzilmasini va uning quyi tizimlarining ishlash algoritmlari konfidensialligi hisobidan ta'minlash funksional jihatdan imkonsiz. Himoya algoritmini bilish tajovuzkorni yengish yoki himoya qarshiligini kamaytirilishiga yo'l qo'ymasligi kerak.

Himoyalash choralari va vositalarini qo'llash qulayligi tamoyili himoya mexanizmlari foydalanuvchanlik jihatidan intuitiv va qulay bo'lishi lozim.

Axborotlarni muhofazalash texnologiyalari, axborotni tutib olinishi yoki yo'qotilishini oldini olishning zamonaviy usullariga asoslangan. Himoya qilishning oltita asosiy usuli mavjud:

1) To'sish;
2) Niqoblash;
3) Tartibga solish;
4) Boshqarish;
5) Majburlash;
6) Ogohlantirish.

Ushbu usullarning barchasi yo'qotishlarni bartaraf etish va turli xil tahdidlarni muvaffaqiyatli aks ettiruvchi axborotlarni himoyalashning ishonchli texnologiyalarini ishlab chiqishga qaratilgan.

To'sish-axborotni tizimlarini jismoniy muhofaza qilish usuli bo'lib, tajovuzkorni himoyalangan hududga kirishiga imkon bermaydi.

Niqoblash-ma'lumotlarni ruxsat etilmagan shaxslar tomonidan idrok etmasliklari uchun yaroqsiz bo'lgan shaklga keltirishni o'z ichiga oladi. Shifrni yechishda tamoyillarni bilish talab etiladi.

Boshqarish-axborot tizimining barcha tarkibiy qismlari ustidan nazoratni amalga oshiradigan axborotni himoya qilish usullari.

Tartibga solish-axborot tizimlarini muhofaza qilishning eng muhim usuli bo'lib, maxsus ko'rsatmalarning kiritilishini nazarda tutadi. Unga ko'ra himoyalangan ma'lumotlar bilan barcha manipulyatsiyalarni amalga oshirish mumkin.

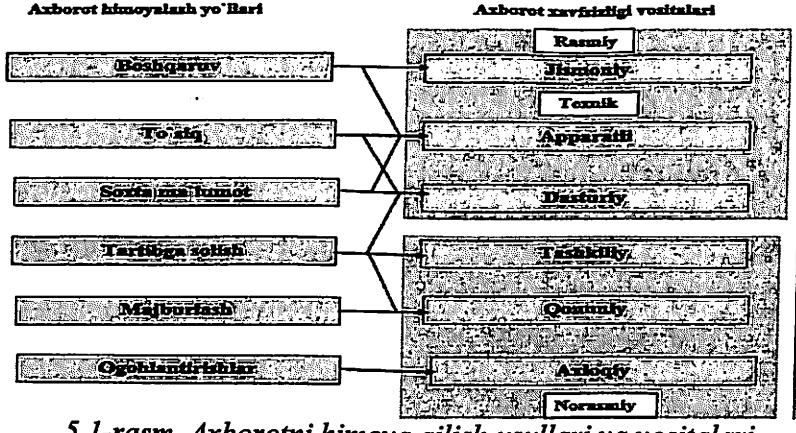
Ogohlantirish-normativ hujjatlar bilan chambarchas bog'liq bo'lgan axborotni himoya qilish usullari, ular xodimlarning belgilangan qoidalarga amal qilishlari shart bo'lgan tadbirlar majmuini joriy etishni nazarda tutadi. Agar axloqiy va shaxsiy sabablarga ko'ra ko'rsatmalarga rioya qiladigan ishchilarga ta'sir ko'rsatish usullari qo'llanilsa, unda bu ogohlantirishga turtki bo'ladi.

5.2. Axborotni himoya qilish vositalari

Axborotni himoya qilish usullari muayyan vositalardan foydalanishni o‘z ichiga oladi (14-rasm). Ma’lumotlarining yo‘qolishi oldini olish va konfidensialligini ta’minlashda quyidagi vositalar qo‘llaniladi:

1) Fizik;
2) Texnik (apparat);
3) Dasturiy ta’minot;
4) Tashkiliy;
5) Qonuniy;
6) Psixologik.

Axborotni muhofaza qilishning ***fizik vositalari*** shaxslarning himoyalangan hududga ruxsatsiz kirishiga yo‘l qo‘ymaydi. Jismoniy to‘siqlarning asosiy an’anaviy usuli-bardoshli eshiklarni o‘rnatish, xavfsizlik qulflari, derazalarga to`siq o`rnatish va boshqalar. Axborot xavfsizligini oshirishda nazorat tekshiruv punktlari, odamlar (qo‘riqchilar) yoki maxsus tizimlar tomonidan amalga oshiriladi. Axborotni yo‘qolishini oldini olish uchun yong‘indan himoya qilish tizimini o‘rnatish tavsiya etiladi. Jismoniy vositalar qog‘oz va elektron tashuvchilardagi ma’lumotlarni himoya qilish uchun ishlatiladi.



5.1-rasm. Axborotni himoya qilish usullari va vositalari o‘rtasidagi o‘zaro bog‘liqlik

Texnik (apparat) vositalari. Bu axborot muhofazasi muammolarini oldini oluvchi turli xil apparatli vositalaridir (mexanik, elektromexanik, elektron va hokazo).

Ular niqob ostida axborotga kirishni oldini oladi. Uskuna quyidagilarni o'z ichiga oladi: shovqin generatorlari, tarmoq filtrlari, radioqurilmalar skanerlari va boshqa ko'plab boshqa qurilmalar, axborot chiqishi mumkin bo'lgan potentsial kanallarini blokirovkalash yoki ularni aniqlash imkonini beradi. Texnik vositalarning afzalliklari ularning ishonchliligi, sub'ektiv omillardan mustaqilligi va modifikatsiyaga nisbatan yuqori barqarorligi bilan bog'liq. Zaifliklari-bir muncha katta sig'im va massa, hamda yo'qori qiymatga egaligidadir.

Dasturiy ta'minot foydalanuvchini identifikatsiya qilish, kirishni boshqarish, axborotni shifrlash, vaqtinchalik fayllarni o'chirib tashlash, himoya tizimini sinovdan o'tkazish va boshqalar kabi dasturlarini o'z ichiga oladi. Dasturiy ta'minotning afzalliklari ko'p qirralilik, moslashuvchan, ishonchlilik, o'rnatish qulayligi, o'zgartirish va rivojlanish qobiliyatidir. Kamchiliklar-kompyuter turlariga (ularning apparaturasiga) bog'liq holda cheklangan tarmoq funksiyalari, fayl serverlari va ishchi stantsiyalar resurslarining bir qismidan foydalanish, tasodifiy yoki ataylab kiritiladigan o'zgarishlarga nisbatan yuqori sezuvchanlik.

Aralash apparat va dasturiy vositalar apparat va dasturiy ta'minot ijro etuvchi bir xil funktsiyalarni bajaradi va umumiylik xususiyatlarga ega.

Tashkiliy vositalar tashkiliy-texnik (kompyuter bilan jihozlangan xonalarni tayyorlash, unga kirishni cheklash talablarini inobatga olgan holda kabel tizimini o'rnatish va hokazo) va tashkiliy-huquqiy (ma'lum bir korxonaning rahbariyati belgilagan milliy qonunlar va ish qoidalari) tarkibdan obirat. Tashkiliy vositalarga lavozimiy ko'rsatmalarni ishlab chiqish, xodimlar bilan suhbat, jazo va imtiyozlar to'plami kiradi. Korxona xodimlarining tashkiliy vositalaridan samarali foydalanishida muhofaza qilinuvchi ma'lumotlar bilan ishlash texnologiyasidan yaxshi xabardor bo'lishi, o'z majburiyatlarini aniq bajarish va yolg'on ma'lumot berish, ma'lumotlarning yo'qolishi yoki sirqib ketmasligini

ta'minlash mas'uliyatini kuchaytiradi. Tashkiliy vositalarning afzalliklari quyidagilardir: ular bir-biridan farq qiladigan turli xil muammolarni yechish, qo'llashdagi qulaylik, tarmoqdagi noxush holatlarga qarshi ta'sirchan javob qaytarish, o'zgartirish va rivojlanish imkoniyatining cheklanmaganligi. Kamchiliklari-sub'ektiv omillarga yuqori qaramlik, jumladan, muayyan birlikda ishni umumiy tashkil qilish.

Qonuniy vositalari-himoyalangan axborotga kirish ruxsati va konfidensial axborotni yo'qotish yoki o'g'irlash bo'yicha javobgarlik chora-tadbirlarini aniqlovchi, hamda shaxslarning faoliyatini tartibga soluvchi normativ-huquqiy hujjatlar to'plamini o'z ichiga oladi.

Psixologik vositalar-axborotni muhofaza qilish va haqiqiyligini saqlab qolishda xodimlarning shaxsiy ishtiyoqini oshirish bo'yicha chora-tadbirlar majmuidan iborat. Xodimlarda shaxsiy qiziqishni yaratishda menejerlar turli xildagi imtiyozlardan foydalanadilar. Psixologik vositalar korporativ madaniyatni shakllantirishni o'z ichiga oladi, unda har bir xodim tizimning muhim qismini sezadi va korxona muvaffaqiyatiga qiziqadi.

Uzatiluvchi elektron ma'lumotlar himoyasi.

Axborot tizimlarining xavfsizligini ta'minlash maqsadida bugungi kunda elektron hujjatlarni ***shifrlash va himoya qilish usullari*** keng qo'llanilmoqda. Ushbu texnologiyalar masofadan ma'lumotlarni uzatish va masofaviy autentifikatsiya qilishning haqiqiyligini ta'minlashga imkon beradi.

Axborotni shifrlash (kriptografik) orqali himoyash usullari maxsus turdagi maxfiy kalitlarni qo'llash natijasida ma'lumotlarni o'zgartirishga asoslangan. Elektron ma'lumotlarning kriptografik texnologiyasi transformatsiyalar algoritmlari, almashtirish usullari, matritsa algebralariga asoslanadi. Shifrlash kuchi ayirboshlash algoritmining murakkabligiga bog'liq. Shifrlangan ma'lumotlar fizik xavflardan tashqari har qanday tahdidlardan himoyalangan.

Elektron raqamli imzo (ERI) elektron hujjatning haqiqiyligini tasdiqlash uchun xizmat qiluvchi parametrdir. Elektron raqamli imzo qog'ozli hujjatdagi rasmiy imzo o'rnini egallaydi va xuddi shu huquqiy

ta'sirga ega. ERI egasini identifikatsiyalash va ruxsat etilmagan o'zgarishlarni yo'qligini tasdiqlash uchun ishlatiladi. Elektron raqamli imzodan foydalanish nafaqat axborotni himoya qilishni ta'minlaydi, balki hujjatlar aylanishi texnologiyasini kamxarajat bo'lishi, hisobotlarni rasmiylashtirish vaqtida hujjatlarning harakatlanish vaqtini qisqartiradi.

Dasturiy ta'minotni ommaviylashuvi va mavjudligi darajasida boshqa vositalar axborotni qo'shimcha ravishda himoya qilish zarur bo'lgan hollarda qo'llaniladi.

Axborotni himoyalashning dasturiy ta'minoti:

Axborotni himoyalashning ichki vositalari

Antivirus dasturlari (antivirus)-kompyuter viruslarini aniqlash va virus bilan zararlangan fayllarni davolash, hamda fayllar yoki operatsion tizimni zararli kod bilan zararlanishini oldini olish, profilaktika qilish uchun mo'ljallangan dastur.

Ma'lumotni ruxsatsiz kirishdan himoya qiluvchi maxsus dasturiy ta'minot ichki himoya vositalaridan ko'ra odatda yaxshi imkoniyatlarga va xususiyatlarga ega. Shifrlash dasturlari va kriptografik tizimlar bilan bir qatorda, boshqa ko'plab axborotni muhofaza qilishning tashqi vositalari mavjud.

Tarmoqlararo ekran (Brandmauer, ing. firewall -"olovli devor" shuningdek, xavfsizlik devori yoki firewall deb ataladi -). Mahalliy va global tarmoqlar o'rtasida maxsus oraliq serverlar yaratiladi, ular orqali barcha transport darajasidagi tarmoq trafiklari filtrlanadi va tekshiriladi. Bu korporativ tarmoqlarga tashqaridan ruxsatsiz kirish xavfini sezilarli darajada pasaytiradi, ammo bu xavfni to'liq bartaraf etmaydi. Mahalliy tarmoqdan chiqqan barcha trafik brandmauer-serveri nomidan yuborilganda, mahalliy tarmoqni deyarli ko'rinmas holga keltiruvchi himoyalash usulning bir turi maskaraddir.

Proksi-serverlar (proxy-ishonchnoma, ishonch egasi). Mahalliy va global tarmoqlar o'rtasidagi barcha tarmoq / transport darajasidagi trafiklar harakati butunlay taqiqlanadi-mahalliy tarmoqdan global tarmoqqa murojaat, marshrutlash maxsus proksi-serverlar orqali amalga oshiriladi. Shubhasiz, bu holatda global tarmoqdan mahalliy tarmoqqa murojaat qilish cheklanadi. Ushbu usul yuqori darajadagi hujumlarga

nisbatan yetarli darajada himoyalashni ta'minlamaydi-masalan, ilova darajasida (viruslar, Java kodi va JavaScript).

VPN (virtual xususiy tarmoq) begona foydalanuvchilarning trafikni tinglashiga imkon beruvchi tarmoq orqali konfidensial ma'lumotlarni uzatish imkonini beradi. Foydalaniluvchi texnologiyalar: PPTP, PPPoE, IPSec.

Axborotni himoyalashning apparat vositalari

Apparat vositalar turli elektron, elektron-mexanik, elektron–optik qurilmalarni o'z ichiga oladi. Bugungi kunga kelib, turli maqsadlar uchun mo'ljallangan apparat vositalari ishlab chiqilgan bo'lib, ular ichida keng ommaviylashganlari quyidagilar:

- himoya rekvizitlarini saqlash uchun maxsus registrlar: parollar, identifikatsion kodlar, maxfiylik darajalari;
- shaxsning o'ziga xos xususiyatlarini identifikatsiya qiluvchi (ovoz, barmoq izlari) asboblar;
- ma'lumotlarni uzatish manzilini vaqti-vaqti bilan tekshirish uchun aloqa liniyasida axborot uzatishni to'xtatish sxemalari.
- ma'lumotlarni shifrlash qurilmalari (kriptografik usullar).
- kompyuterni ishonchli yuklash modullari

Axborotni himoya qilishning texnik vositalari

Axborot tizimining perimetrini himoya qilish uchun:

- xavfsizlik va yong'in signalizatsiya tizimlari;
- raqamli video kuzatuv tizimlari;
- foydalanishni boshqarish tizimlari (ACS).

Axborotni texnik aloqa kanallarida tutib olinishini oldini olishda quyidagi vositalar va chora tadbirlar ta'minlanadi:

- ekranlanuvchi konstruksiyalarda ekranlangan aloqa kabellaridan foydalanish;
- aloqa liniyalarida yuqori chastotali filtrlarni o'rnatish;
- himoyalangan xonalar ("kapsulalar") ni qurish;
- ekranlangan uskunalardan foydalanish;
- faol shovqin tizimlarini o'rnatish;
- nazorat qilinadigan hududlarni yaratish.

5.3. Konfidensial axborotlarni chiqib ketishidan himoyalash

Konfidensial ma'lumotlarni chiqib ketishidan himoya qilish tashkilotning axborot xavfsizligi kompleksining muhim qismidir. DLP-tizimi (ma'lumotlarni chiqib ketishidan himoya qilish tizimi) konfidensial ma'lumotlarning tasodifiy va qasddan chiqib ketishi bilan bog'liq muammolarni hal qiladi.

Axborotlarni chiqib ketishidan himoyalash tizimi (DLP tizimi) konfidensial ma'lumotlarning chiqib ketmasligini ta'minlovchi dastur yoki apparat-dasturiy kompleksdir.

DLP tizimi tomonidan *konfidensial ma'lumotlarni himoya qilishda* quyidagi asosiy funksiyalardan foydalaniladi:

- ma'lumotlarni uzatish kanallaridan o'tuvchi barcha trafikni filtrlash;
- Kontent va konteks darajasida trafikni chuqur tahlil qilish.

DLP tizimida konfidensial axborotni himoya qilish uchta darajada amalga oshiriladi: Data-in-Motion, Data-at-Rest, Data-in-Use.

Data-in-Motion-tarmoq kanallari orqali uzatiladigan ma'lumotlar:

- web (HTTP/HTTPS protokollari);
- internet-messenjerlari (ICQ, QIP, Skype, MSN va boshqalar);
- korporativ va shaxsiy pochta (POP, SMTP, IMAP va boshqalar);
- simsiz tizimlar (WiFi, Bluetooth, 3G va boshqalar);
- FTP-ulanish.

Data-at-Rest-quyidagilarda saqlanuvchi ma'lumotlar:

- serverlar;
- ishchi stantsiyalari;
- noutbuklar;
- ma'lumotlarni saqlash tizimlari (DSS).

Data-in-Use-ishchi stantsiyalarida ishlatiladigan ma'lumotlar. Axborotni chiqib ketishini oldini olishga qaratilgan chora-tadbirlar ikkita asosiy qismdan iborat: tashkiliy va texnik.

Konfidensial axborotni muhofaza qilish kompaniyada mavjud bo'lgan ma'lumotlarni topish va tasniflash bo'yicha tashkiliy choralarni o'z ichiga oladi. Tasniflash jarayonida ma'lumotlar 4 toifaga bo'linadi:

• maxfiy ma'lumotlar;
• konfidensial ma'lumotlar;
• rasmiy xizmat ma'lumotlari;
• ochiq axborot.

DLP tizimlarida konfidensial axborot qanday aniqlanadi? DLP tizimlarida konfidensial axborot qator turli belgilar, shuningdek turli usullar bilan aniqlanishi mumkin, masalan:

• axborotni lingvistik tahlil qilish;
• axborotni statistik tahlil qilish;
• muntazam ifodalar (simvollar);
• raqamli izlar usuli va boshqalar.

Ma'lumot topilgach, guruhlangan va tizimlashtirilgan, ikkinchi texnik tashkiliy qism boshlanadi.

Texnik chora-tadbirlar orqali konfidensial axborotni muhofaza qilish, axborotni chiqib ketishidan himoyalash tizimining funksional imkoniyatlari va texnologiyalaridan foydalanishga asoslangan. DLP tizimi ikkita modulni o'z ichiga oladi: xost modul va tarmoq moduli.

Xost modullari foydalanuvchilarning ishchi stantsiyalarida o'rnatiladi va konfidensial ma'lumotlar (konfidensial ma'lumotlar) bo'yicha foydalanuvchi tomonidan amalga oshiriladigan harakatlar ustidan nazoratni ta'minlaydi. Bundan tashqari, xost modul foydalanuvchi ishlaydigan ilovalar, jarayonlar va ma'lumotlarni ko'chirish yo'llari, Internetda sarflangan vaqt kabi turli parametrlarini kuzatib borishga imkon beradi.

Tarmoq moduli tarmoq orqali uzatiladigan ma'lumotni tahlil qiladi va himoyalangan axborot tizimidan tashqarida chiquvchi trafikni nazorat qiladi. Agar uzatilayotgan trafikda konfidensial ma'lumotlar aniqlansa, tarmoq moduli ma'lumotlarni uzatishni to'xtatadi.

Konfidensial axborotni chiqib ketishidan himoyalash tizimi (*Data Loss Prevention-DLP*) korporativ tarmoqdan tashqarida ruxsatsiz ma'lumotlarni uzatish harakatlarini kuzatib borish va bloklash uchun mo'ljallangan. DLP axborotni chiqib ketishidan himoyalash bilan bir qatorda, tizim foydalanuvchi harakatlarini kuzatish, elektron pochta, ijtimoiy tarmoqlar, chatlar va boshqalar orqali xabarlar almashinuvini

yozish va tahlil qilish funksiyalarni ham bajaradi. DLP tizimining asosiy vazifasi-tashkilotning joriy etgan konfidensiallik siyosatini (axborotni chiqib ketishidan himoyalash) to'liq bajarilishini muvofiqlashtirishdan iborat.

DLP tizimidan konfidensial axborot chiqib ketishi, jiddiy moliyaviy va obro'sizlanish xavfi mavjud bo'lgan, hamda, tashkilotlarda xodimlarning vazifasiga sadoqatini tartibga solishda foydalanish o'ta muhim ahamiyat kasb etadi. DLP klassi yechimlari axborot chiqishini oldini olish uchun savdo shartlari, xizmatlar va yechimlar uchun buyurtma, plastik karta raqamlari, mijozlar hisob ma'lumotlari, xodimlar va mijozlarning shaxsiy ma'lumotlari, moliyaviy ma'lumotlar va hokazo kabi konfidensial ma'lumotlarni himoya qiladi.

Ichki tahdidlardan himoyalanish zaruriyati axborot xavfsizligi vositalari rivojlanishining barcha bosqichlarida mamoyon bo'ldi. Biroq, tashqi tahdidlar boshlanishida yanada xavfliroq hisoblangan. So'nggi yillarda ichki tahdidlarga ko'proq e'tibor qaratilishi bilan DLP tizimlarining mashhurligi ortdi. Ichki tahdidlardan himoyalanish bo'yicha maxsus texnik vositalar 2000 yildan keyin ommaviy ishlab chiqarila boshlandi.

Ma'lumotlarni chiqib ketishidan himoyalash tizimini tatbiq etish, kompaniyaga quyidagilarni kafolatlaydi:

- axborot aktivlarini muhofazasi va muhim strategik axborotni muhofaza qilish;
- tashkilot ma'lumotlarini tizimlashtirish va strukturalash;
- boshqaruv va xavfsizlik xizmatlari uchun biznes va biznes jarayonlarning oshkoraligi;
- kompaniyadagi konfidensial ma'lumotlarning uzatilishini nazorat qilish;
- muhim ma'lumotlarni yo'qotish, o'g'irlash va yo'q qilish bilan bog'liq xatarlarni kamaytirish;
- tashkilotga ichki kiruvchi zararli dasturlardan himoya qilish;
- axborot tizimi tarkibiga kiruvchi barcha ma'lumotlarni saqlash va arxivlashtirish;

DLP tizimining ikkilamchi afzalliklari:

• xodimlarning ish joyida mavjudligini nazorat qilish;

• Internet-trafikni tejash;

• korporativ tarmoqni optimallashtirish;

• foydalanuvchi tomonidan qo'llaniladigan ilovalarni nazorat qilish;

• xodimlarning ish faoliyatini yaxshilash.

DLP tizimlarida konfidensial axborotning aniqlash ikki usulda amalga oshiriladi: formal atributlar tahlili (masalan, hujjatning uzunligi, maxsus kiritilgan teglar, xesh funktsiyasini taqqoslash) va kontent tahlil qilish. Birinchi usul sizga yolg'on pozitsiyalardan (birinchi turdagi xatolar) to'sqinlanishga imkon beradi, lekin hujjatlarni oldindan tasniflash, teglarni kiritishni, signaturalarni to'plash va boshqalarni talab qiladi. Ushbu usulda agar konfidensial hujjat oldingi tasnifga mos kelmagan bo'lsa, konfidensial ma'lumotni o'tkazib yuborish ehtimoli yuqori (ikkinchi turdagi xatolar) bo'lishi mumkin. Ikkinchi usul yolg'on pozitsiyalarni beradi, biroq bu konfidensial axborotni faqatgina muhrlangan hujjatlar orasida o'tkazishni aniqlashga imkon beradi. Yaxshi DLP tizimlarida ikkala usul ham birlashtiriladi.

DLP-tizimlarining tuzilishi tarmoq sathidagi komponentlar (modullari) va xost darajasining tarkibiy qismlarini o'z ichiga oladi. Tarmoqli komponentlari axborot tizimining chegaralarini nazorat qiladi. Odatda ular proksi-serverlar, elektron pochta serverlari va alohida serverlar sifatida namoyon bo'ladi. Xost darajasining tarkibiy qismlari odatda ishchilar shaxsiy kompyuterlarida joylashtiriladi va disklar, flesh-disklar va hokazolarda axborot yozuvchi kanallarni nazorat qiladi. Xost komponentlari tunnellash, steganografiya va nazoratni chetlab o'tishning boshqa mumkin bo'lgan dasturlarini o'rnatish, tarmoq sozlamasi o'zgarishlarini kuzatishga harakat qilmoqda. DLP-tizim markazlashgan boshqaruv uchun qulay modul turidagi har ikkala tarkibiy qismlarni birlashtirishi kerak.

5.4. Korporativ axborotlarni himoya qilish

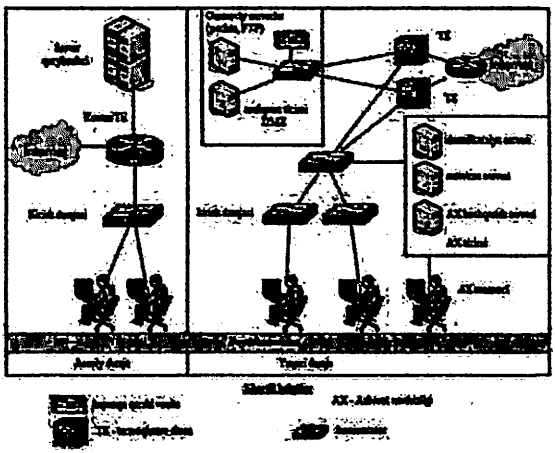
Savdo-sotiq paydo bo'lgandan beri har bir tadbirkor yoki hunarmand, raqobatchilar mijozlarini yo'qotishdan, korporativ, savdo

ma'lumotlari chiqib ketishidan qo'rqib, o'zlarining tovar yoki mahsulot sirini saqlashga harakat qiladilar. Muammolar emas, ularning texnologiyalari, ularsiz zamonaviy biznesni tasavvur qilib bo'lmaydigan korporativ kompyuter tarmoqlari bilan bevosita bog'liq muamomlarni hal qilishning zamonaviy usullari o'zgardi.

Muammo o'zgarmadi, biroq zamonaviy texnologiyalarni tasavvur qila olmaydigan texnologiya va korporativ kompyuter tarmoqlari bilan bevosita bog'liq bo'lgan uni hal qilishning zamonaviy usullari o'zgartirildi.

Kompaniya ichki konfidensial ma'lumotlarini chiqib ketishidan himoya qilish uchun ma'lumotlar muhofazasining kompleks tizimidan foydalaniladi va ular quyidagi hollarda qo'llaniladi:

- kompaniyaning ichki tarmog'i himoyasini yangilash;
- ichki tarmoqni nazoratlash;
- kompaniya axborot chiqib ketishi ehtimolidan shubhalanish;
- korporativ ma'lumotlarini himoyalash.



5.2-rasm. Integratsiyalangan Fortinet korporativ himoya vositalari

Korporativ axborotni himoya qilish Fortinet-xavfsiz korporativ tarmoq arxitekturasini yaratishda ishlatiladigan turli xil konfiguratsiyalarning komponentlaridir. Ular ma'lumot to'plash, trafikni nazorat qilish, Internet va kirish darajalarini o'z ichiga oladi (5.2-rasm).

Fortinet kompaniyasining integratsiyalangan vositalari bir qurilmada barcha xavfsizlik ta'minlash usullarini birlashtirib, tarmoqning infratuzilmasini turli xildagi tahdidlar, zararlardan samarali himoyalash kafolatini ta'minlaydi va kompaniyaning faoliyati va moliyaviy xotirjamligini buzmaydi.

FortitToken ikki faktorli autentifikatsiyalash tizimi yordamida cheklangan amal qilish muddati bilan avtorizatsiya qilish uchun parollarni generatsiyalaydi, tashqi serversiz chetlab o'tishlarni ta'minlaydi.

Ushbu tizim SSL VPN tunnellarini qurishda va ulardan foydalanishda, IPSECda, shuningdek, Wi-Fi tarmog'iga kirishda va FortiGate tizimini boshqarishdagi autentifikatsiyani kuchaytirishga imkon beradi.

FortiGate va FortiToken tizimlaridan foydalanish statsionar va masofali xodimlar uchun ishonchli himoyani ta'minlaydi. Konfidensial korporativ ma'lumotlarga kirish faqat vakolatli xodimlar tomonidan amalga oshiriladi.

FortiGate tarmoqlararo ekrani Fortinet tomonidan ishlab chiqilgan integratsiyalashgan xavfsizlik yechimining asosi hisoblanadi. An'anaviy tarmoqlararo ekrandan farqli o'laroq, FortiGate ma'lumotlar paketlarini OSI modelining yettinchi darajasiga qadar tahlil qilib, ilovalar, kontent va foydalanuvchilarning ishonchli nazoratini ta'minlaydi.

FortiGate kompaniyasi ma'lumotlariga ko'ra, butun dunyoda ikki milliondan ortiq FortiGate qurilmalari o'rnatilgan. Ularning ajralib turadigan xususiyati o'ziga xos FortiASIC tarmoq protsessorlari yordamida erishilgan yuqori ko'rsatkichdir.

Ushbu qurilmalar CPUni yuklamadan xolos qiladi, shuning uchun FortiASIC tarmoq protsessorlari boshqa NGFW qurilmalariga qaraganda besh marta va muntazam tarmoqlararo ekranlaridan o'n marta tezroq ishlashi mumkin.

Fortinet kompaniyasida Forti Sandbox shubhali ob'ektlarning faoliyatini tahlil qiluvchi tizimi katta rol o'ynaydi. Eng real tahdid-noma'lum hujumlar bo'lib, ularning soni oxirgi yillarda bir necha bor oshdi. Ishlab chiqaruvchining fikriga ko'ra, Forti Sandbox foydalanish

aniqlash darajasini ikki yuz ellik kundan bir necha kunga kamaytiradi (statistika ma'lumotlariga ko'ra, tajovuzkorlarning IT buzish qobilatini hisobga olinmasdan o'rtacha vaqtini baholash noo'rin bo'ladi). Fortinet kompaniyasi Forti Gate, Forti Web va Forti Mail kabi boshqa brend yechimlari bilan Forti Sandboxdan foydalanishni tavsiya qiladi. Bu esa, hujumni aniqlash vaqtini bir necha daqiqaga yoki hatto soniyaga qisqartiradi.

Korporativ tarmoqlarning xavfsizligini ta'minlashda xavfsizlik tizimlari qo'llab-quvvatlatlanadi:

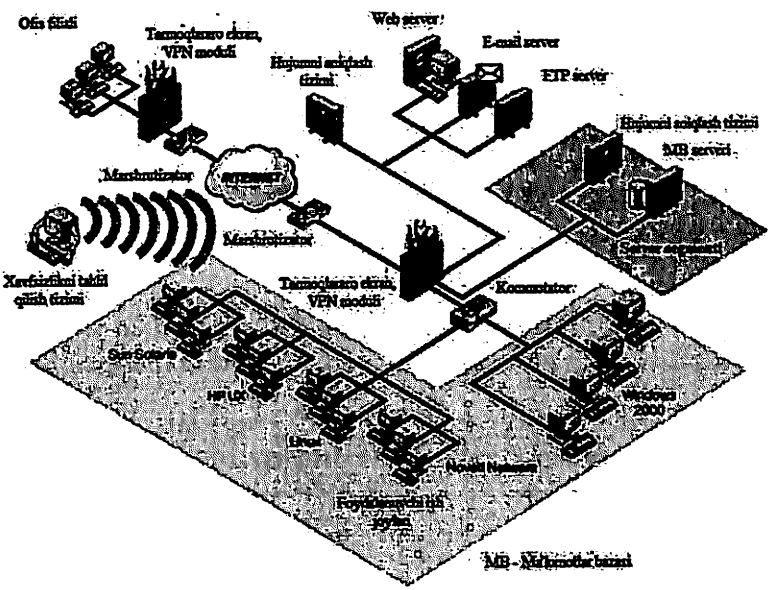
HTTP, HTTPS va FTP protokollari (ya'ni, tezkor messenjerlar, portallar, forumlar, ijtimoiy tarmoqlar va hk) yordamida trafikni boshqarish.

1. Birlashtirilgan tashqi qurilmalarni boshqarish (flesh-disklar, qattiq disklar).

2. Chiquvchi va kiruvchi elektron xabarlarni boshqarish.

3. Yuboriladigan hujjatlar, tasvirlar va boshqa ma'lumotlarni tahlil qilish.

4. Simsiz aloqa xavfsizligini nazorat qilish.



5.3-rasm. DLP tizimi tuzilishi

Ma'lumotlar chqib ketishi oldini olish (*DataLossPrevention-DLP*)-konfidensial ma'lumotlarni axborot tizimidan tashqariga tarqalishiga yo'l qo'ymaydigan texnologiyalar, shuningdek, bunday ma'lumotlarni tarqalishini oldini oluvchi texnik qurilmalardir (dasturiy ta'minot yoki apparat-dasturiy ta'minot) 5.3-*rasm*.

DLP tizimi korporativ tarmoqdan tashqariga konfidensial axborotning tarqalishini oldini olish uchun mo'ljallangan dasturiy mahsulot hisoblanadi. Ushbu tizim korporativ tarmoqdan tashqaridagi axborot oqimlarini tahlil qilishga asoslangan. Muayyan signatura va konfidensial axborotni uzatish aniqlanganda, tizim bunday tranzaktsiyalarni bloklaydi yoki xabarnomalarni xavfsizlik xodimiga yuboradi.

DLP tizimlari himoyalangan axborot tizimining perimetri orqali o'tadigan axborot oqimlarining tahliliga asoslangan. Ushbu oqimdagi konfidensial ma'lumotlarni aniqlaganda, tizimning faol komponenti ishga tushiriladi va xabarni (paket, oqim, sessiya) uzatish bloklanadi.

5.5. MB xavfsizlik xususiyatlari

Ma'lumot omborlari ikkita komponentni o'z ichiga oladi: saqlangan ma'lumotlar (asl ma'lumotlar bazasi) va nazorat qilish dasturlari (MBBT).

Xususan, saqlangan ma'lumotlarning xavfsizligini ta'minlashda avvalo ma'lumotlarni xavfsiz boshqarishni ta'minlanilishi zarur. Bunga asoslanib, barcha zaifliklar va MBBT xavfsizligi masalalarini ikki toifaga bo'lish mumkin: ma'lumotga bog'liq va bog'liq bo'lmagan ma'lumotlar.

Mustaqil ma'lumotlar zaifliklari boshqa dasturiy ta'minot turlariga ham xosdir. Ularning sabablari, masalan, dasturiy ta'minotni o'z vaqtida yangilanmasligi, mavjud funktsiyalardan to'liq foydalana olmaslik yoki dasturiy ta'minot boshqaruvchilarining yetarli darajada malakaga ega emasligi bo'lishi mumkin.

MBBT xavfsizligining ko'p jihatlari ma'lumotga bog'liq hisoblanadi. Shu bilan birga, ko'p zaifliklar ma'lumotlarga bevosita bog'liqdir. Misol uchun, ko'pchilik MBBT foydalanuvchilarni ruxsat

etilgan foydalanuvchi funksiyalari (o‘z navbatida, so‘rovlar tilining operatorlari deb hisoblash mumkin) yoki dasturlash tilidagi tasodifiy funksiyalar majmualarini o‘z ichiga olgan, muayyan so‘rovlar tili yordamida ma’lumotlarga so‘rovlarni qo‘llab-quvvatlaydi.

Qo‘llaniladigan tillarning arxitekturasi, hech bo‘lmaganda maxsus tillar va funksiyalar majmui, ma’lumotni saqlash uchun ishlatiladigan ma’lumotlar modeli bilan bevosita bog‘liq. Shunday qilib, model tilning o‘ziga xos xususiyatlarini va u yerda ba’zi zaifliklarning mavjudligini aniqlaydi. Bunday zaifliklar, masalan inyeksiyalar tilning sintaksisiga qarab farqli ravishda amalga oshiriladi (sql-inyektsiya, java-inyektsiya).

Ma’lumotlar bazasi xavfsizligi talablari

Zaifliklarni ajratish asosida ma’lumotni saqlash uchun ma’lumotlarga bog‘liq va ma’lumotlardan mustaqil xavfsizlik choralarini farqlashimiz mumkin.

Ma’lumotlardan mustaqil bo‘lgan xavfsiz ma’lumotlar bazasi tizimiga qo‘yiladigan talablar quyidagilardan iborat:

Ishonchli muhitda ishlash. Ishonchli muhit deb, xavfsizlik siyosati negizidagi korxona infratuzilmasi va uning himoya mexanizmlarini tushunishimiz zarur. Shunday qilib, barcha boshqa korporativ tizimlar uchun qo‘llaniladigan xavfsizlik qoidalariga muvofiq, MBBT ning ishlashi haqida so‘z yuritiladi.

Ma’lumotlar fayllarining jismoniy xavfsizligini tashkil etish.

Umuman olganda, MBBT ma’lumotlar fayllarining jismoniy xavfsizligiga bo‘lgan talablar boshqa foydalanuvchilar va ilovalarga qo‘llaniladigan talablardan farq qilmaydi.

Xavfsiz va MBBT aktual sozlamalarini tashkil qilish.

Ushbu talab yangilanishlarni o‘z vaqtida o‘rnatish, foydalanilmagan xususiyatlarni o‘chirib qo‘yish yoki ishonchli parol siyosatini qo‘llash kabi umumiy xavfsizlik vazifalarini o‘z ichiga oladi.

Quyidagi talablarni ma’lumotga bog‘liq deyishimiz mumkin:

– foydalanuvchi dasturiy ta’minoti xavfsizligi;

– bunda xavfsiz interfeyslarni va ma’lumotlarga kirish ruxsati mexanizmlarini yaratish vazifalari qamrab olinadi;

– xavfsiz tashkilot va ma’lumotlar bilan ishlash.

Axborotni tashkil qilish va boshqarish masalasi axborot saqlash tizimining kalitidir. Bu sohada ma'lumotlar xavfsizligini boshqarish va ma'lumotlar bazasiga xos bo'lgan xavfsizlik muammolari bilan ma'lumotlar yig'ish vazifasi mavjud. Aslida, bu vazifa ma'lumotlarga bog'liq bo'lgan zaifliklarning asosiy qismini va ulardan himoya qilishni o'z ichiga oladi.

Xavfsiz ma'lumotlar bazalarini yaratishning asosiy jihatlari

MBBT ning axborot xavfsizligini ta'minlash bo'yicha aniqlangan muammolarni hal qilish uchun xavfsizlikning zaifliklarini yopish usulidan axborot omborlari xavfsizligini ta'minlash kompleks yondashuviga o'tish zarur. Ushbu o'tishning asosiy bosqichida quyidagi holatlat bo'lishi lozim.

Murakkab usullarni yaratish ularni ma'lumotlar omborlari va foydalanuvchi dasturiy ta'minotini ishlab chiqishda va joriy etishda foydalanish imkonini beradi. To'liq metodologiyadan so'ng, MBBT boshqaruvining ko'pgina xatolarini oldini olishga va hozirgi kunga kelib eng keng tarqalgan zaifliklardan himoya qilishga imkon beradi.

MBBTning zaifliklarini, tahdidlari baholash va tasniflash. MBBTning zaifliklarini va tahdidlari tasniflash keyinchalik ulardan tahlil va himoya qilishni tartibga solish, hamda, xavfsizlik mutaxassislarini zaiflik va ularning sabablari o'rtasidagi munosabatlarni o'rnatishga imkon beradi. Natijada, MBBT da muayyan mexanizmni joriy qilish bilan administratorlar va ishlab chiquvchilar u bilan bog'liq bo'lgan tahdidlarni aniqlab, ularni oldindan aniqlab olishlari va tegishli xavfsizlik vositalarini tayyorlashlari mumkin.

Standart xavfsizlik mexanizmlarini ishlab chiqish. Ma'lumotni qo'llashning yondashuvlari va tillarini standartlashtirish turli MBBTlarga nisbatan qo'llaniladigan xavfsizlik vositalarini yaratishga imkon beradi. Ayni paytda ular faqat metodik yoki nazariy bo'lishi mumkin, chunki afsuski tayyor dasturiy ta'minot kompleksi xavfsizligi vositalarining paydo bo'lishi asosan ishlab chiqaruvchilarning standartlarni yaratish va ularga rioya qilish istagiga bog'liq.

Turli xil MBBT larida ma'lumotlar bazasini himoyalash vositalari bir-biridan farq qiladi. Zamonaviy Borland va Microsoft MBBT

tahlillari asosida ma'lumotlar bazasini himoya qilish vositalari an'anaviy ravishda asosiy va ikkinchi darajali ikkita guruhga bo'linadi.

Axborotni himoya qilishning vositalari asosida quyidagilarni o'z ichiga oladi:

- parolli himoyalash;
- ma'lumotlar va dasturiy ta'minotni shifrlash;
- ma'lumotlar bazasi ob'ektlariga kirish huquqini yaratish;
- ma'lumotlar bazasi jadvallari maydonlarini va yozuvlarini muhofaza qilish.

Parolli himoya qilish-ma'lumotlar bazasini ruxsatsiz foydalanishdan himoya qilishning oddiy va samarali usulidir. Parollar oxirgi foydalanuvchilar yoki MB administratorlari tomonidan o'rnatiladi. Parollarni hisobga olish va saqlash MBBT ning o'zi tomonidan amalga oshiriladi. Odatda parollar shifrlangan shaklda muayyan tizimdagi MBBT fayllarida saqlanadi. Shuning uchun, parolni topish va aniqlashning imkoni mavjud emas. Parol kiritilgandan so'ng MBBT foydalanuvchisi himoyalangan ma'lumotlar bazasi bilan ishlash uchun barcha imkoniyatlarga ega bo'ladi.

Ma'lumotlarni shifrlash (butun ma'lumotlar bazasi yoki alohida jadvallar) boshqa dasturlarni ma'lumotlarni o'qiy olmasligi uchun ishlatiladi. Dasturlarning manba matnini ma'lum algoritm asosida shifrlash uning ruxsatsiz foydalanuvchiga ayon bo'lishini oldini oladi.

Asosiy MBBT resurslaridan foydalanishni nazorat qilish uchun, ko'pgina tizimlar ma'lumotlar bazasi obyektlariga kirish huquqlarini o'rnatish vositalariga ega. Kirish huquqlari obyektlardagi mumkin bo'lgan harakatlarini belgilaydi. Ob'ektning egasi (obyektni yaratgan foydalanuvchi), shuningdek, ma'lumotlar bazasi ma'muri barcha huquqlarga ega. Qolgan foydalanuvchilar turli xil obyektlar uchun turlicha kirish darajalariga ega bo'lishlari mumkin.

Odatda, jadvalga nisbatan quyidagi kirish huquqi berilishi mumkin.

- ma'lumotlarni o'qish (o'qish);
- ma'lumotlarni o'zgartirish (tahrir qilish);
- yangi yozuvlar qo'shish;

• ma'lumotlarni qo'shish va o'chirish;

• barcha operatsiyalar, shu jumladan jadvalni tuzilishini o'zgartirish.

Jadvaldagi ma'lumotlarda o'rnatilgan chora – tadbirlar alohida maydonlar va alohida yozuvlar o'rtasidagi munosabat bo'yicha farqli bo'lishi mumkin. Relyatsion MBBTda alohida yozuvlar maxsus muhofaza qilinmaydi.

Jadvallar maydonidagi o'rnatilgan ma'lumotni muhofaza qilish huquqlarini quyidagilarga ajratish mumkin:

• kirishni to'liq rad etish;

• faqat o'qish;

• barcha amallarga ruxsat etish (ko'rish, yangi qiymatlarni kiritish, o'chirish va o'zgartirish).

Shakllarga nisbatan ikkita asosiy operatsiya ko'zda tutilishi mumkin: ish uchun chaqiriq va ishlab chiqish (Dizaynerning vazifasi). Tayyorlangan ilovalarning ekranli shakllari uchun dizaynerga murojaat qilishni bekor qilish maqsadga muvofiq, chunki oxirgi foydalanuvchi dasturni buzishga sabab bo'lmasligi kerak. Ekranda shakllanadigan alohida elementlar ham himoyalangan bo'lishi mumkin. Misol uchun, manba jadvalining ba'zi maydonlari foydalanuvchi uchun ko'rinmasligi yoki yashirilgan bo'lishi mumkin va ayrim maydonlar faqat ko'rish uchun mavjud bo'ladi.

Hisobotlar ekrandagi shakllarga juda o'xshaydi. Quyidagilar bundan mustasno. Birinchidan, ular jadvaldagi ma'lumotlarni o'zgartirishga ruxsat bermaydi va ikkinchidan, ularning asosiy maqsadi axborotni chop etishdir. Hisobotlar, shuningdek, ekran shakllari, o'zlarining ishlab chiqish vositalaridan foydalanishga taqiqlangan bo'lishi ham mumkin.

MBBT dasturlarida ishlatiladigan dastur matnlarini ko'rish va o'zgartirishda (tasodifiy yoki ataylab) shifrlashdan tashqari, ularni parolli muhofaza qilish mumkin.

Qo'shimcha ma'lumotlar bazasi xavfsizligi vositalari xavfsizlik vositalariga bevosita aloqador bo'lmagan, lekin ma'lumotlar

xavfsizligiga to‘g‘ridan-to‘g‘ri ta’sir qiladigan narsalarni o‘z ichiga oladi. Bu quyidagi vositalardan iborat:

- turlari bo‘yicha ma’lumotlarning qiymatlarini nazoratlash vositalari;
- kiritiluvchi ma’lumotlarining ishonchliligini oshirish;
- jadvallar aloqasining yaxlitligini ta’minlash;
- tarmoqdagi ma’lumotlar bazasi obyektlaridan umumiy foydalanishni tashkil qilish.

Ma’lumotlar bazasi strukturasini aniqlash vaqtida foydalanuvchi ushbu qiymat kiritilgan maydon turiga mos kelmaydigan qiymatlarni kiritishi mumkin (masalan, matnli ma’lumotlarni raqamli maydonga kiritish). Bunday holda, MBBT qiymatlarni boshqarish vositalaridan foydalanib, kirishni bloklaydi va foydalanuvchiga xatolik haqida xabar beradi.

MBBT ga kiritiluvchi qiymatlarning ishonchliligini oshirish vositalari, qayta ishlanuvchi ma’lumotlarning semantikasi bilan bog‘liq chuqurlashtirilgan nazoratda ishlatiladi. Ular, odatda, jadval yaratish vaqtida quyidagi cheklashlarni belgilash qobiliyatini taqdim etadi: minimal va maksimal qiymatlar, qiymat (kiritish bo‘lmasa), majburiy kiritish talabi; kirish maskasini (shablonni) sozlash va h.k.

Ma’lumotlar bazasidagi ma’lumotlar ishonchli nazoratini tashkil qilishning etishning yanada rivojlangan shakli, saqlash protseduralarini ishlab chiqishdir. Xotirada saqlanadigan protseduralar serverda joylashtirilgan ma’lumotlar bazalarida ishlatiladi. Saqlangan protseduralar algoritmlari ma’lum funktsiyalarni (shu jumladan nazorat funktsiyalarini) ma’lumotlar bo‘yicha bajarilishini ta’minlaydigan dasturlar hisoblanadi. Protseduralar ma’lumotlar bilan saqlanadi va kerak bo‘lganda, ilovalardan yoki ma’lumotlar bazasida ba’zi hodisalar sodir bo‘lganda chaqiriladi.

Amaliy muammolar yechimi, odatda, bir nechta jadvallardan ma’lumotlarni tanlashni talab qiladi. Ma’lumotlar bazasidagi jadvallar bog‘lanishi mumkin. MBBT tegishli jadvallarning mantiqiy yaxlitligini ta’minlash vazifalarini o‘z zimmasiga oladi. Agar MBBT bu

funktsiyalarni bajarmasa, ulanishning to‘g‘riligi uchun mas‘uliyat dastur zimmasida bo‘ladi.

Jadvallar bilan bog‘lanishning butunligini nazorat qilishda MBBT ta’sir ko‘rsatishi mumkin bo‘lgan harakatlarga misol keltiramiz. Ikkala jadval o‘rtasidagi oraliqda 1.M shaklining bog‘lovchisi mavjud va shuning uchun yordamchi jadvalning bir nechta yozuvlari asosiy jadvalning bitta yozuviga mos kelishi mumkin.

Yordamchi jadvalga yozuvlar qo‘yilganda, tizim asosiy jadvalning ulanish sohasidagi mos keladigan qiymatlarning mavjudligini nazorat qiladi. Agar kiritilgan qiymat asosiy jadvalda bo‘lmasa, MBBT vaqtincha yangi yozuv bilan ishni bloklaydi va qiymatni o‘zgartirish yoki butun yozuvni o‘chirishni taklif qiladi.

Qo‘shimcha jadvallardan yozuvlarni o‘chirishni nazoratlab bo‘lmaydi. Yozuvni asosiy jadvaldan o‘chirishda tekshirish amalga oshiriladi. Asosiy jadvaldagi yozuvlar qo‘shimcha jadvalning bir nechta yozuvlari bilan bog‘liq bo‘lgan hollarda, ikkita ehtimoliy xatti-harakat mavjud. Asosiy yozuv hech bo‘lmaganda bitta bo‘ysinuvchi yozuvga (foydalanuvchi yozuvni o‘chirish kerak) yoki asosiy yozuvni va barcha bo‘ysinuvchi yozuvlarni (kaskadni yo‘q qilish) o‘chirib yubormaguncha asosiy yozuvni o‘chirib tashlamaslik zarur.

Ma’lumotlar bazalari bilan ishlovchi taqsimlangan axborot tizimlarida bir xil obyektlar (ma’lumotlar bazasi ob‘ektlarini bo‘lishish) bo‘yicha turli harakatlar o‘rtasidagi nizolarni hal qilish muammosi mavjud. Misol uchun, mahalliy tarmoq foydalanuvchilardan biri ma’lumotlar bazasini tahrirlaganda, ikkinchisi esa baza tuzilishini o‘zgartirmoqchi bo‘lsa, nima qilish kerak? Bunday holatlarda MBBT nizolarni hal qilish mexanizmlarini taqdim etishi kerak.

Odatda, bir nechta foydalanuvchi bir vaqtning o‘zida tarmoqda ishlayotganida, cheklashdan foydalaniladi. Cheklash turli ma’lumotlar bazasi obyektlarida va obyektlarning alohida elementlarida harakat qilishlari mumkin. Ob’ektni cheklash obyektni ishlatish bilan parallel ravishda bir obyektning ishlab chiqarish rejimiga kirishga urinish bo‘lganida amalga oshiriladi. Ma’lumotlar bazasi jadvallari uchun

alohida yozuvlar yoki maydonlar bilan ishlashda qo'shimcha cheklovlar paydo bo'lishi mumkin.

5.6 Kompyuter viruslaridan himoyalanish

Zamonaviy shaxsiy kompyuter bilan ishlashda foydalanuvchi (va ayniqsa yangi boshlovchilar) ko'plab muammolarga duch kelishi mumkin: ma'lumotlarni yo'qotish, tizimni osilib qolishi, kompyuterning ba'zi qismlarining ishdan chiqishi va boshqalar. Ushbu muammolarning sabablaridan biri (dasturiy ta'minotdagi xatolar bilan birga) va foydalanuvchining o'zi tomonidan amalga oshirilmagan harakatlar tizimga kirgan kompyuter viruslari bo'lishi mumkin. Ushbu dasturlar, biologik viruslar kabi, ko'payadi, tizimning disk maydonlariga yoki fayllarga o'zini yozadi, ko'pincha noxush oqibatlarga olib keladigan turli xil nomaqbul harakatlarni keltirib chiqaradi. Ushbu kod qurboni bo'lmaslik uchun har bir foydalanuvchi kompyuter viruslaridan himoya qilish tamoyillarini yaxshi bilishi kerak.

Kompyuter viruslarini aniqlash, yo'q qilish va ulardan himoya qilish uchun viruslarni aniqlash va yo'q qilishga imkon beradigan bir necha turdagi maxsus dasturlar ishlab chiqilgan. Bunday dasturlarga *antivirus* dasturlari deyiladi. Antivirus dasturlari quyidagi turlarga ajratiladi:

- detektor dasturlari;
- tuzatuvchi dasturlari yoki faglar;
- revizor dasturlari;
- filtr dasturi;
- vaksinalash dasturlari yoki immunizatsiya vositalari.

Detektor dasturlari RAM va fayllarda ma'lum bir virusga xos bo'lgan signaturani qidiradi va aniqlangandan so'ng tegishli xabarni chiqaradi. Bunday antivirus dasturlarining kamchiliklari shundaki, ular faqat shu turdagi dasturlarni ishlab chiquvchilarga ma'lum bo'lgan viruslarni topishlari mumkin.

Tuzatuvchi dasturlari yoki ***faglari,*** shuningdek, ***emlash dasturlari*** nafaqat virus bilan yuqtirilgan fayllarni topadi, balki ularni "davolaydi", ya'ni fayllarni asl holatiga qaytarib, virus dasturining tanasini fayldan

olib tashlaydi. Ishlarining boshida faglar tezkor xotiradan viruslarni qidirib topadi, ularni yo'q qiladi va shundan keyingina fayllarni "davolash" ga o'tadi. Faglar orasida polifaglar ajralib turadi. Tuzatuvchi dasturlari ko'plab viruslarni qidirish va yo'q qilish uchun mo'ljallangan . Ularning eng mashhurlari: Aidstest, Scan, Norton antivirus, Doktor Web.

Yangi viruslar doimiy ravishda paydo bo'lishini hisobga olsak, detektor dasturlari va doktor dasturlari tezda eskiradi va muntazam ravishda yangilanishlarni talab qiladi.

Revizor dasturlari eng ishonchli viruslardan himoya qilish vositalaridan biridir. Revizorlar kompyuterda virus yuqmasdan oldin dasturlar, kataloglar va tizimli disk sohalarining dastlabki holatini saqlab qo'yadi, so'ngra vaqti-vaqti bilan yoki foydalanuvchining ko'rsatmasiga binoan hozirgi holatni asl holati bilan taqqoslaydi. Aniqlangan o'zgarishlar monitor ekranida aks etadi. Qoida ko'ra, vaziyatni taqqoslash operatsion tizim yuklanishi bilanoq amalga oshiriladi. Taqqoslashda faylning uzunligi, siklni boshqarish kodi (faylni tekshirish miqdori), o'zgartirish sanasi va vaqti hamda boshqa parametrlar tekshiriladi. Revizor dasturlarida yashirin viruslarni aniqlaydigan algoritmlar mavjud va hatto dasturning versiyasida kiritilgan o'zgarishlarni virus tomonidan kiritilgan o'zgarishlardan tozalash mumkin. Revizor dasturlari orasida Rossiyada keng tarqalgan Adinf dasturi mavjud.

Filtr dasturlari-bu kompyuterda shubhali virusga qarshi harakatlarni aniqlash uchun mo'ljallangan kichik dasturlardir. Bunday harakatlar quyidagilarni o'z ichiga olishi mumkin:

- com, exe kengaytmali fayllarni tuzatishga urinishlar;
- fayl xususiyatlarini o'zgartirish;
- diskning aniq manziliga to'g'ridan-to'g'ri yozish;
- diskning yuklanish bo'limlariga yozish;
- rezident dasturni yuklash.

Ilova ko'rsatilgan harakatlarni bajarishga harakat qilganda, "qo'riqchi" foydalanuvchiga xabar yuboradi va tegishli harakatni taqiqlash yoki ruxsat berishni taklif qiladi. Filtr dasturlari juda

foydalidir, chunki ular virusni ko'payishdan oldin uning mavjudligining erta bosqichida aniqlay oladi. Biroq, ular fayllarni va disklarni "davolamaydi". Viruslarni yo'q qilish uchun siz boshqa dasturlardan, masalan, faglardan foydalanishingiz kerak. Qo'riqchi dasturlarining kamchiliklari ularning "darakchiligi" (masalan, ular bajariladigan faylni nusxalashga bo'lgan har qanday urinish to'g'risida doimiy ravishda ogohlantirishi) va boshqa dasturlar bilan mumkin bo'lgan mojarolarni o'z ichiga oladi. Filtr dasturiga misol sifatida MS-DOS yordamchi paketining bir qismi bo'lgan Vsafe dasturini keltirish mumkin.

Vaktsinalar yoki ***immunizatorlar*** bu fayllarni zararlanishiga to'sqinlik qiluvchi rezident dasturlardir. Vaktsinalar ushbu virusni "davolaydigan" tuzatuvchi dasturlari bo'lmagan hollarda qo'llaniladi. Vaktsinalar faqat ma'lum viruslarga nisbatan bo'ladi. Vaktsina dasturni yoki diskni ularning ishiga ta'sir qilmasligi uchun o'zgartiradi va virus ularni yuqtirganligini sezadi va shuning uchun unga kirmaydi. Hozirgi vaqtda emlash dasturlari cheklangan.

Viruslar va viruslarni yuqtirgan fayllarni o'z vaqtida aniqlash, aniqlangan viruslarning har bir kompyuterda to'liq yo'q qilinishi virus epidemiyasining boshqa kompyuterlarga tarqalishining oldini olishi mumkin.

Asosiy xulosalar

Kompyuter ma'lumotlarini muhofaza qilish axborotning yaxlitligini tekshirish masalalarini hal etuvchi usullar va vositalar, kompyuter resurslariga unda saqlanadigan dasturlar va ma'lumotlarga, shuningdek, dasturiy ta'minot mahsulotlaridan ruxsatsiz foydalanishni istisno qiluvchi chora tadbirlar majmui tushuniladi.

Axborot xavfsizligini ta'minlashning asosiy tamoyillari quyidagilardan iborat: tizimlilik, murakkablik, himoyalashning uzluksizligi, yetarlilik, boshqaruv va qo'llashdagi moslashuvchanlik, himoyalash mexanizmlari va algoritmlarining ochiqligi, himoyalash choralari va vositalarini qo'llash qulayligi.

Himoya qilishning oltita asosiy usuli mavjud: to‘siq, niqoblash, tartibga solish, boshqarish, majburlash, ogohlantirish.

Ma’lumotlarining yo‘qolishi oldini olish va konfidensialligini ta’minlashda quyidagi vositalar qo‘llaniladi: Fizik, Texnik (apparat), Dasturiy ta’minot, Tashkiliy, Qonuniy, Psixologik.

Axborotlarni chiqib ketishidan himoyalash tizimi (DLP tizimi) konfidensial ma’lumotlarning chiqib ketmasligini ta’minlovchi dastur yoki apparat-dasturiy kompleksdir.

Axborotni himoyalovchi hech bir kompyuter tizimi mutlaq xavfsiz deb qaralmaydi. Ushbu choralarning barchasi buzg‘unchini axborotlarga kirish ruxsatini ma’lum darajada cheklaydi xolos.

Konfidensial axborotni chiqib ketishidan himoyalash tizimi (*Data Loss Prevention-DLP*) korporativ tarmoqdan tashqarida ruxsatsiz ma’lumotlarni uzatish harakatlarini kuzatib borish va bloklash uchun mo‘ljallangan.

Axborotni himoya qilishning vositalari asosida quyidagilarni o‘z ichiga oladi: parolli himoyalash, ma’lumotlar va dasturiy ta’minotni shifrlash, ma’lumotlar bazasi ob‘ektlariga kirish huquqini yaratish, ma’lumotlar bazasi jadvallari maydonlarini va yozuvlarini muhofaza qilish.

Axborotni shifrlash (kriptografik) orqali himoyash usullari maxsus turdagi maxfiy kalitlarni qo‘llash natijasida ma’lumotlarni o‘zgartirishga asoslangan. Elektron ma’lumotlarning kriptografik texnologiyasi transformatsiyalar algoritmlari, almashtirish usullari, matritsa algebralariga asoslanadi.

Kompyuter viruslarini aniqlash, yo‘q qilish va ulardan himoya qilish uchun viruslarni aniqlash va yo‘q qilishga imkon beradigan bir necha turdagi maxsus dasturlar ishlab chiqilgan. Bunday dasturlarga *antivirus* dasturlari deyiladi.

Antivirus dasturlari quyidagi turlarga ajratiladi: detektor dasturlari, tuzatuvchi dasturlari yoki faglar, revizor dasturlari, filtr dasturi, vaksinalash dasturlari yoki immunizatsiya vositalari.

Nazorat savollari

1. Kompyuter ma'lumotlarini himoyalash deb nimani tushunamzi?

2. Axborot xavfsizligini ta'minlashning asosiy tamoyillarini ayting.

3. Axborot xavfsizligini ta'minlashning asosiy usullarini ayting.

4. Axborotni himoyalash vositalarini keltiring.

5. Axborotni himoyalashning apparatli vositalarini izohlang.

6. Konfidensial axborotlarni chiqib ketishidan himoyalashda qanday vositalardan foydalaniladi?

7. Qanday holatda axborotlar chiqib ketishidan kompleks himoyalangan deb tushuniladi?

8. MB ni yaratish xususiyatlarini keltiring.

VI-BOB. BUZISH VA HUJUMDAN HIMOYALANISH

6.1. Hujumlarni aniqlash

Hujumlarni aniqlash tizimi texnologiyalari odatiy ravishda ikki toifaga bo'linadi: anomaliyani aniqlash (anomaly detection) va noto'g'ri foydalanishni aniqlash (misuse detection). Biroq ushbu tizimlarning amaliyotga tatbiq etilish prinsiplarini hisobga olgan holda boshqa tasniflash qo'llaniladi: tarmoq darajasida (network-based) va xost darajasida (xost-based) hujumlarni aniqlash. Birinchisi tizim tarmoq trafigini tahlil qiladi, ikkinchisi-operatsion tizim yoki dasturning jurnallarini tahlil qiladi. Sinflarning har biri o'zining afzalliklari va kamchiliklariga ega. Shuni takidlash kerakki, ba'zi hujumlarni aniqlash tizimlari aynan qaysidir nomlangan sinflarning biriga olib borishi mumkin. Odatda, ular bir nechta toifalarning imkoniyatlarini o'z ichiga oladi. Ammo, bu tasnif bir hujumni aniqlash tizimini boshqasidan ajratib turadigan asosiy imkoniyatlarni aks ettiradi.

Hozirgi vaqtda anomaliyani aniqlash texnologiyasi keng ommaviylashmagan bo'lib, u hech qanday tijorat tizimida ishlatilmaydi. Ushbu texnologiya nazariy jihatdan mukammal ko'rinsada, ammo amalga uning tadbiqi juda murakkabdir.

Hujumlarni aniqlashga qaratilgan yana bir yondashuv-bu namuna (pattern) yoki signatura (signature) bo'yicha hujumni tariflash va nazoratlanuvchi hududda (tarmoq trafigi yoki log) ma'lum bir namunani qidirishdir. Antivirus tizimlari ushbu texnologiya asosidagi hujumlarni aniqlashning yaqqol namunasidir.

Yuqorida aytib o'tilganidek, tarmoqli va operatsion darajadagi hujumlarni aniqlash tizimining ikkita sinfi mavjud. Tarmoqli (network-based) hujumlarni aniqlash tizimining asosiy afzalligi, tajovuzni tugunga yetib bormasidan oldin identifikatsiya qilishdan iborat. Ushbu tizimlar katta tarmoqlarda o'rnashishni osonlashtiradi, chunki ular tashkilotda ishlatiladigan turli platformalarda o'rnatishni talab qilmaydi.

Xost darajadagi hujumlarni aniqlash tizimlari muayyan operatsion tizim ostida ishlash uchun yaratilgan bo'lib, ularga muayyan cheklovlar qo'yiladi. Operatsion tizim o'zini qanday tutish kerakligi haqidagi bilimlardan foydalangan holda, ushbu yondashuv asosida qurilgan vositalar ba'zan tarmoq hujumlarini aniqlash vositalari tomonidan o'tkazib yuborilgan bosqinchilikni aniqlashi mumkin. Tashkilot tarmoq tugunlarining kata qismini himoya qilishda, tarmoq darajasidagi hujumlarni aniqlash tizimlaridan foydalanish, ehtimol, eng yaxshi tanlov bo'lishi mumkin, chunki tarmoqdagi tugunlar sonining ko'payishi hujumni aniqlash tizimidan foydalanadigan xavfsizlik darajasiga ta'sir qilmaydi.

Hujumni aniqlash tizimi (HAT) (ing. Intrusion Detection System (IDS))-kompyuter tizimi yoki tarmog'iga ruxsatsiz kirishni (buzib kirish yoki tarmoq hujumi) aniqlash uchun mo'ljallangan dasturiy yoki apparat ta'minot.

Bunday tizimlarni qo'llashning asosiy maqsadi-korporativ tarmoqqa ruxsatsiz kirishlarni aniqlash va ularga qarshi choralar ko'rish: axborot xavfsizligi bo'yicha mutaxassislarga hujumni amalga oshirishi, aloqani uzish va hujumchilarning keyingi hatti-harakatlarini cheklash uchun xavfsizlik brandmauerini qayta konfiguratsiyalash, ya'ni xaker hujumlaridan va zararli dasturlardan himoya qilishdir.

IDS tarmoq xavfsizligi infratuzilmasining zaruriy tayanchiga aylanib bormoqda. Tarmoqlararo ekrandan (firewall)dan tashqari, xavfsizlik siyosati asosida ishlovchi, IDS shubhali faoliyatni kuzatish va monitoring qilish mexanizmi sifatida xizmat qiladi. IDS hujumkor Firewallni chetlab o'tganida bu haqda administratorga xabar beradi, bu esa, o'z navbatida, hujumni oldini olish uchun qo'shimcha choralar ko'rishni ta'minlaydi. Hujumni aniqlash texnologiyalari tizimni to'liq xavfsizligini kafolatlamaydi. Shunga qaramay, amaliyotda IDS ning ko'plab foydalari jihatlari mavjud.

IDS dan foydalanish bir nechta maqsadlarga erishishga yordam beradi:

– bostirib kelish yoki tarmoq hujumlarini aniqlash;

– ehtimoliy hujumlarni bashoratlash va uning rivojini oldini olishda zaifliklarni aniqlash. Tajovuz qiluvchi odatda maqsadli tizimning zaifliklarini aniqlashda tarmoqni zondlash (skanerlash) yoki boshqa testlash kabi bir qator dastlabki ishlarni amalga oshiradi;

– mavjud tahdidlarni hujjatlashtirish;

– xavfsizlik nuqtai-nazaridan, ayniqsa yirik va murakkab tarmoqlarda ma'muriy boshqaruvning sifatini nazorat qilish;

– paydo bo'lgan zaifliklar haqida foydali ma'lumotlar olish, zaifliklarga olib keladigan omillarni qayta tiklash va rostlash;

– tarmoqdagi resurslarning joylashuvi to'g'risida qaror qabul qilishda muhim ahamiyatga ega mahalliy tarmoqqa (tashqi yoki ichki hujumlarga) nisbatan hujum manbaini aniqlash;

– hodisalar haqidagi ma'lumotlarni yozib borish. Odatda, axborot mahalliy holatda saqlanadi, biroq ushbu ma'lumotlar ixtiyoriy markazlashtirilgan log to'plovchi yoki SIEM-tizimiga yuborilishi mumkin;

– axborot xavfsizlik ma'murini xavfsizlik intsidentlari haqida ogohlantirish. Xabarnomaning bu turi alert deb nomlanib, u bir nechta kanallarda mavjud bo'lishi mumkin: elektron pochta, SNMP-tuzoqlari, tizim jurnali xabarlari va IDS tizimi boshqaruv konsoli. Shuningdek, skriptlardan foydalanilgan dasturlashtiriluvchi reaktsiya ham bo'lishi mumkin;

– hisobotni generatsiyalash, ya'ni hisobotlar talab qilinadigan hodisalar bo'yicha barcha ma'lumotlarni umumlashtirish uchun yaratiladi.

Har qanday holatda, ushbu mahsulotlar *hujumga oid signaturalarni*, odatda g'arazli yoki shubhali xatti-harakatlarni ko'rsatadigan o'ziga xos namunalarni qidiradi. IDS tarmoq trafikidan ushbu namunalarni qidirishda *tarmoq darajasida* ishlaydi. IDS hujum signaturalarini operatsion tizim yoki dastur qayd jurnallaridan izlayotganda, bu *tizim darajasida* deyiladi. Har bir yondashuv o'zining afzalliklari va kamchiliklariga ega, biroq ikkovi ham bir-birini to'ldiradi. Hujumlarni aniqlash tizimining eng samarali yondashuvi bu ikkita texnologiyadan birgalikda foydalanishdir.

1) Tarmoq sathida hujumlarni aniqlash

Tarmoq sathida hujumni aniqlash tizimlari qayta ishlanmagan tarmoq paketlarini tahlil qilish maqsadida, ma'lumot manbai sifatida ishlatadi. Qoida tariqasida, IDS tarmoqni tinglash rejimida ishlaydigan tarmoq adapteridan foydalanadi va tarmoq segmentidan o'tayotgan har bir trafikni real tahlil qiladi.

Hujum aniqlangandan so'ng, javob moduli ogohlantirish variantlarining keng doirasini ta'minlaydi, signalni chiqaradi va hujumga qarshi choralarni qo'llaydi. Ushbu variantlar tizimdan tizimgacha o'zgaradi, lekin odatda u quyidagilarni o'z ichiga oladi: administratorni konsul yoki elektron pochta orqali xabardor qilish, hujum qilingan uzel bilan aloqani bekor qilish va / yoki keyinchalik tahlil ishlarini olib borish va dalillarni to'plash uchun sessiyalarni qayd etish.

2) tizim sathida hujumlarni aniqlash

80-yillarning boshlarida, hatto tarmoqlar rivojlanmasdan oldin, hujumlarni aniqlashning eng keng tarqalgan amaliyoti shubhali faoliyat to'g'risida ma'lumot beruvchi qayd jurnallarni ko'rish bilan chegaralangan edi. Zamonaviy tizim darajasida hujumlarni aniqlash tizimlari amalga mavjud hujumlarni anglash va kelajakda ulardan foydalanish imkoniyatlarini yo'qotish uchun tegishli usullarni aniqlashda kuchli vosita bo'lib qolmoqda. Zamonaviy tizim darajasidagi IDSlar avvaldan qayd jurnallarni ishlatadilar, ammo ular yanada avtomatlashtirilgan bo'lib, eng so'nggi matematik tadqiqotlar asosida murakkab aniqlash usullarini o'z ichiga oladi. Odatda, tizim darajasida IDS Windows NT yoki Unix boshqaruvi ostida ishlovchi tarmoqlarda tizimni boshqarish, hodisalar va xavfsizlik hodisalari jurnallarini (security log yoki syslog) kuzatib boradi. Ushbu fayllardan birortasi o'zgarganda, IDS muvofiqlikni aniqlash uchun yangi yozuvlarni hujum signaturasi bilan taqqoslaydi. Shunday muvofiqlik aniqlanganda, tizim administratorga ogohlantirish signali yuboradi yoki boshqa javob berish mexanizmlarini ishga tushiradi.

Tarmoq sathida hujumlarni aniqlash tizimining afzalliklari. Tarmoq sathidagi IDSlar tizim darajasida hujumlarni aniqlash

tizimlariga mavjud bo'lmagan ko'plab afzalliklari mavjud. Darhaqiqat, ko'plab mijozlar arzon narxlardagi hozirgi kun talabiga javob beradigan tarmoqli sathida hujumlarini aniqlash tizimidan foydalanadilar. Tarmoq sathida hujumlarni aniqlash tizimining xavfsizlik siyosatini samarali amalga oshirishda eng muhim tarkibiy qism hisoblangan asosiy sabablar quyida keltirilgan.

Ekspluatatsiya narxining pastligi. Tarmoq darajasidagi IDS bir nechta tizimlar o'rtasidagi trafiklar aylanishini nazorat qilish uchun tarmoqning eng muhim nuqtalarida o'rnatilishi lozim. Tarmoq sathidagi tizimlar har bir xostda, alohida hujumlarni aniqlash tizimining dasturiy ta'minotini o'rnatishni talab etmaydi. IDS tarmoqning barcha qismini to'liq nazorat qilish imkoniga ega emas, biroq korxona tarmoqlarida undan foydalanish tizim sathidagi hujumlarni aniqlash tizimiga nisbatan amalda tadbiq etish bilan bog'liq xarajatlarini kamaytiradi.

Tizim darajasida o'tkazib yuborilgan hujumlarni aniqlash. Tarmoq darajasidagi IDS tarmoq paketlari sarlavhalarini shubhali yoki buzg'unchilik nuqtai nazaridan o'rganadi. Tizim darajasidagi IDS paket sarlavhalari bilan ishlamasligi sababli, ular ushbu turdagi hujumlarni aniqlay olmaydi. Misol uchun, ko'pgina "xizmatni rad etish" ("denial-of-service") va "fragmentlangan paketlar" (TearDrop) tarmoq hujumlari faqat tarmoq orqali o'tayotgan paket sarlavhalarini tahlil qilish orqali aniqlanishi mumkin. Hujumning bunday turi trafikni real vaqtda tekshiradigan tarmoq darajasidagi IDS yordamida tezda aniqlanishi mumkin. Yuqorida aytilganidek, tizim darajasidagi tizimlar tarmoq darajasida ishlamaydi va shuning uchun ular bunday hujumlarni tanib olish xususiyatiga ega emas.

Xaker o'z faoliyati izlarini yashirishi ancha murakkab. Tarmoq darajasidagi IDS real vaqtda hujumlarni aniqlanganda jonli trafikni ishlatadi. Shunday qilib, xaker uning mavjudligini izlarini yo'q qila olmaydi. Tahlil qilinayotgan ma'lumotlar nafaqat hujum usullari haqida ma'lumot, balki tajovuzkorni sudda va dalillarni aniqlashda yordam beradigan ma'lumotlarni ham o'z ichiga oladi. Ko'pgina xakerlarga qayd jurnallari bilan ishlash tanish bo'lganligi sababli, ular ushbu fayllarni o'zlarining faoliyat izlarini yashirishda qanday qilib

manipulyatsiya qilishni biladilar, natijada hujumni aniqlash uchun zarur bo‘lgan ushbu ma’lumotni tizim darajasidagi tizimlarning ish samaradorligini kamaytiradi.

Real vaqtda aniqlash va javob qaytarish. Tarmoq darajasidagi IDS shubhali va buzg‘unchilik hujumlarini qo‘llanilgan usullari, ro‘y berishi bo‘yicha aniqlaydi, shuningdek, tizim darajasidagi IDSga qaraganda tezroq xabar berish va javob qaytarishni ta’minlaydi. Tizim darajasidagi IDS, qoida tariqasida, hujumlarni tegishli jurnalga yozilish vaqtiga qadar sezmaydi va ro‘yxatga olinganidan so‘ng javob choralarini ko‘radi. Ushbu nuqtada, eng muhim tizimlar yoki resurslar allaqachon buzilgan bo‘lishi yoki tizim darajasidagi IDS ishlaydigan tizimning ishlashi buzilishi mumkin.

5. Muvaffaqiyatsiz hujumlar yoki shubhali xatarlarni aniqlash. Tarmoqlararo ekran (Firewall) dan tashqarida o‘rnatilgan IDS tarmoqlararo ekran resurslariga yo‘naltiruvchi hujumlarni aniqlay oladi va ularni yo‘qqa chiqarishi ham mumkin. Tizim darajasidagi tizimlar tarmoqlararo ekranga yetib bormaydigan xost hujumlarini ko‘rmaydi. Ushbu yo‘qolgan ma’lumotlar xavfsizlik siyosatini baholash va takomillashtirishda muhim ahamiyatga ega bo‘lishi mumkin.

6. OTdan mustaqillik. Tarmoq darajasidagi IDS korporativ tarmoqda o‘rnatilgan operatsion tizimlardan mustaqildir. Tizim darajasidagi hujumlarni aniqlash tizimlari to‘g‘ri ishlashi va kerakli natijalarni generatasiya qilishda muayyan operatsion tizimlarni talab etadi.

6.2. Kompyuter hujumlarini aniqlash vositalari

Hujumlarni aniqlash texnologiyasi quyidagi vazifalarni hal qilish lozim:

- ma’lum hujumlarni tanib olish va mas‘ul xodimni ogohlantirish.
- hujumlarni haqidagi ma’lumot manbalarini “tushunish”.
- korxona tarmog‘i tarkibiy qismlari bo‘lgan foydalanuvchilar, tizimlar va tarmoqlar operatsiyalarini nazorat qiluvchi xavfsizlikga mas‘ul personal yuklamasini kamaytirish yoki xalos etish.

Xavfsizlik doirasida ekspert bo'lmaganlar tomonidan xavfsizlik vositalarini boshqarish imkoniyati.

Korporativ tarmoq sub'ektlari (foydalanuvchilar, dasturlar, jarayonlar va boshqalar) ning barcha harakatlarini nazorat qilish.

Ko'pincha hujumlarni aniqlash tizimlari o'zlarining dasturlarini kengaytiradigan vazifalarni bajarishi mumkin. Misol uchun,

Xavfsizlik devorlarining samaradorligini nazoratlash. Misol uchun, hujumlarni aniqlash tizimini (korporativ tarmoq ichidagi) tarmoqlararo ekrandan (TE) so'ng o'rnatish, TE tomonidan o'tkazib yuborilgan hujumlarni va TE nuqsonlarni aniqlash imkonini beradi.

O'rnatilmagan yangilanishlar yoki eskirgan dasturiy ta'minotli tugunlarini boshqarish.

Muayyan Internet uzellariga kirishni bloklash va nazorat qilish. Hujumlarni aniqlash tizimlari xavfsizlik devorlarigacha bo'lgan va turli xil URL-larga kirishni boshqarish tizimiga ega bo'lmagan holda, masalan, WEBsweeper, korporativ tarmoq foydalanuvchilari ayrim internet resurslariga, masalan, pornografik kontent web-serverlariga kirishini qisman nazorat qilishlari va bloklashlari mumkin. Tashkilotning tarmoqlararo ekran va hujumni aniqlash tizimini sotib olishga moliyaviy imkoniyati yetmagan hollarda va TE funktsiyalari, hujumni aniqlash tizimi, router va proksi-server o'rtasida vazifalar bo'linishi zarur. Bundan tashqari, hujumlarni aniqlash tizimlari kalit so'zlar asosida xodimlarning serverlarga kirishini nazorat qilishlari mumkin. Masalan, sex, job, crack va h.k.

- Elektron pochta nazorati. Hujumlarni aniqlash tizimlari elektron pochta orqali ishonchsiz xodimlarni funksional vakolatlariga kirmaydigan vazifalarni bajarishini nazoratlashda ishlatilishi mumkin, masalan, rezyume yuborish. Ba'zi tizimlar elektron pochta xabarlari virusini aniqlab olishlari mumkin, garchi ular haqiqiy virusga qarshi tizimlardan yiroq bo'lsa-da, bu vazifani ancha samarali bajaradi.

Axborot xavfsizligi sohasida mutaxassislarning vaqt va tajribasidan yaxshi foydalanib hujum sabablarini aniqlash va uni bartaraf etish hujumni o'zini aniqlashdan ko'ra maqbul yechim sanaladi. Hujumlarning sabablarini bartaraf etish, ya'ni, zaifliklarni aniqlash va

yo‘qotish, administrator hujumlarni potentsial amalga oshirish faktini bartaraf etadi. Aks holda, hujum vaqti-vaqti bilan takrorlanadi va doimiy ravishda boshqaruvchining harakati va e’tiborini talab qiladi.

Hujumlarni aniqlash tizimlarining turli xil tasniflari mavjud, eng keng tarqalgan tasnif, bu tadbiq etish tamoyiliga muvofiq tasniflashdir:

1. xost-based, ya’ni ma’lum bir tarmoq tuguniga yo‘naltirilgan hujumlarni aniqlash.

2. network-based, ya’ni butun tarmoq yoki tarmoq segmentiga yo‘naltirilgan hujumlarni aniqlash.

Bitta kompyuterni boshqaradigan hujumlarni aniqlash tizimlari, qoida tariqasida, operatsion tizim jurnallaridan va turli ilovalardan (web-server, DBMS, va hokazo) ma’lumotlarni to‘playdi va tahlil qiladi. Ushbu tamoyil bilan RealSecure OS Sensor ishlaydi. Biroq yaqinda operatsion tizimining yadrosi bilan yaqindan integratsiyalashgan tizimlar tarqatilib, xavfsizlik siyosati buzilishlarini aniqlashning yanada samarali usuli ta’minlandi. Bundan tashqari, bunday integratsiya ikkita yo‘l bilan amalga oshirilishi mumkin. Birinchidan, barcha OS tizimidagi chaqiruvlarni (shu jumladan, Entercept ishi) yoki barcha kirish / chiqish tarmoq trafigini kuzatib borish mumkin (RealSecure Server Sensor ishlaydi). Ikkinchidan, hujumni aniqlash tizimi operatsion tizimni chetlab o‘tgan barcha tarmoq trafigini to‘g‘ridan-to‘g‘ri tarmoq kartasidan ushlab, OTga bog‘liqlikni kamaytiradi va shu bilan birga hujumlarni aniqlash tizimining xavfsizligini oshiradi.

Tarmoq darajasidagi hujumlarni aniqlash tizimlari tarmoqdagi ma’lumotlarni, ya’ni tarmoq trafigidan ma’lumotlarni to‘playdi. Ushbu tizimlar an’anaviy kompyuterlarda (masalan, RealSecure Network Sensor), ixtisoslashgan (masalan, RealSecure for Nokia yoki Cisco Secure IDS 4210 and 4230) yoki router yoki kommutatorga integratsiyalangan kompyuterlarda (masalan, CiscoSecure IOS o‘rnatilgan dasturiy ta’minot yoki Cisco Catalyst 6000 IDS Module) bajarilishi mumkin. Dastlabki ikkala holatda tahlil qilinadigan ma’lumot tarmoq interfeyslaridan foydalanishni buzuvchi rejimda to‘plash va tahlil qilish yo‘li bilan to‘planadi. Keyingi holatda, trafik tarmoq uskunalari shinasidan ushlab qolinadi. Hujumlarni aniqlash uchun ikkita

shartdan biri-tizimdagi nazorat qilinadigan ob'ektning keyingi hatti-harakatlarini tushunish yoki barcha mumkin bo'lgan hujumlar va ularning modifikatsiyasini bilish talab etiladi. Birinchi holda, anomaliyani aniqlash texnologiyasi va ikkinchi holatda-zararli hatti-harakat yoki zo'ravonlikni aniqlash texnologiyasidan foydalaniladi. Ikkinchi texnologiya namuna yoki signatura shaklida hujumni tariflash va boshqariladigan maydonda (masalan, tarmoq trafigi yoki qayd jurnali) ma'lum bir namunani qidirishdan iborat. Ushbu texnologiya viruslarni aniqlashga juda o'xshaydi (antivirus tizimlari hujumni aniqlash tizimining eng yaxshi namunasidir), ya'ni, tizim ma'lum bo'lgan barcha hujumlarni aniqlashi mumkin, ammo yangi, hali noma'lum bo'lgan hujumlarni aniqlashga qodir emas. Bunday tizimlarda qo'llaniladigan yondashuv juda sodda va bugungi kunda bozorda deyarli barcha hujumlarni aniqlash tizimlariga asoslanadi. Deyarli barcha hujumlarni aniqlash tizimlari signatura yondashuviga asoslanadi.

Hujumlarni aniqlash tizimining afzalliklari:

1) Kommutatsiya sizga bir necha kichik tarmoq segmentlari kabi yirik tarmoqlarni boshqarish imkonini beradi. Natijada, tarmoq trafiki hujumlarini aniqlaydigan tizimni o'rnatish uchun eng yaxshi joyni aniqlash murakkablashadi. Ba'zan kommutatorlarda maxsus portlar (span portlar) yordam berishi mumkin, lekin har doim emas. Muayyan tugunlar darajasida hujumlarni aniqlash aniqlash tizimlari faqat kerak bo'ladigan tugunlarga joylashtirishi sababli kommutatsiya qiluvchi tarmoqlar ishini samarali bo'lishi imkonini ta'minlaydi.

2) Tarmoq darajasidagi tizimlar har bir xostga hujumni aniqlash tizimining dasturiy ta'minotini o'rnatishni talab qilmaydi. IDS tarmoqning barcha qismini to'liq nazorat qilish imkoniga ega emas, biroq korxona tarmoqlarida undan foydalanish tizim sathidagi hujumlarni aniqlash tizimiga nisbatan amalda tadbiq etish bilan bog'liq xarajatlarini kamaytiradi. Bundan tashqari, tarmoq segmentini nazoratlash uchun segmentdagi tugunlar sonidan qat'iy nazar faqat bitta sensor talab etiladi.

3) Jinoyatchining kompyuteridan chiqib ketgan tarmoq paketini qaytarib bo'lmaydi. Tarmoq darajasida ishlaydigan tizimlar real vaqtda

hujumlarni aniqlashda jonli trafikni ishlatadi. Shunday qilib, tajovuzkor o'zining ruxsat etilmagan faoliyati izlarini yo'q qila olmaydi. Tahlil qilinayotgan ma'lumotlarga nafaqat hujum usullari, balki tajovuzkorni sudda va dalillarni aniqlashga yordam beradigan ma'lumotlar ham kiradi. Ko'pgina xakerlarga qayd jurnallari bilan ishlash tanish bo'lganligi sababli, ular ushbu fayllarni o'zlarining faoliyat izlarini yashirishda qanday qilib manipulyatsiya qilishni biladilar, natijada hujumni aniqlash uchun zarur bo'lgan ushbu ma'lumotni tizim darajasidagi tizimlarning ish samaradorligini kamaytiradi.

4) Tarmoq darajasida ishlovchi tizimlar shubhali voqealar va ular orqali yuzaga kelgan hujumlarga aniqlik kiritadi, shuningdek qayd jurnallarini tahlil qiluvchi tizimlarga nisbatan tezkor xabar berish va javob qayratishni ta'minlaydi. Misol uchun, xaker TCP protokoli asosida "xizmat ko'rsatishdan voz kechish" hujumi ko'rinishidagi tarmoq hujumini tarmoq darajasidagi hujumni aniqlash tizimi tomonidan, hujum qilinuvchi uzelga ulanishni yakunlash uchun, sarlavhada Reset bayrog'i o'rnatish bilan TCP paketini yuborishi mumkin. Qayd etish jurnallarini tahlil qilish tizimi hujumlarni tegishli jurnalga yozilish vaqtiga qadar sezmaydi va ro'yxatga olinganidan so'ng javob choralarini ko'radi. Ushbu nuqtada, eng muhim tizimlar yoki resurslar allaqachon zararlangan bo'lishi yoki uzel darajasida yuklanuvchi hujumlarni aniqlash tizimining ishlash qobiliyati buzilishi mumkin. Real vaqt miqyosida xabar qilish oldindan belgilangan parametrlarga tezkor javob berishga imkon beradi. Ushbu reaktsiyalar oralig'i hujum va tajovuzkor haqida ma'lumot to'plash uchun nazorat rejimida ruxsatlar kengayishidan tortib, toki hujumni darhol to'xtatishga qadar o'zgaradi.

Xullas, tarmoq darajasida ishlaydigan hujumni aniqlash tizimlari korporativ tarmoqqa o'rnatilgan operatsion tizimlarga bog'liq emas, chunki ular korporativ tarmoqning barcha tugunlaridan o'tuvchi tarmoq trafigini tekshiradi. Hujumlarni aniqlash tizimi, u yoki bu paketni qaysi OT generatsiya qilishidan qat'iy nazar aniqlash tizimi tomonidan qo'llab-quvvatlanadigan standartlarga mos keladigan bo'lsa, u haqida qayg'urishi shart emas. Misol uchun, tarmoq Windows 98, Windows NT, Windows 2000 va XP, NetWare, Linux, MacOS, Solaris va boshqa

tizimlar ostida ishlatishi mumkin, lekin agar ular IP orqali bir-birlari bilan aloqa o'rnatadigan bo'lsa, ushbu protokollarni qo'llab-quvvatlovchi ixtiyoriy hujumni aniqlash tizimlari, ushbu operatsion tizimlarga qaratilgan hujumlarni aniqlay oladi. Tarmoq va tugun darajasida hujumlarni aniqlash tizimlaridan birgalikda foydalanish tarmog'ingiz xavfsizligini oshiradi.

Ko'plab kompyuter hujumlaridan qanday himoyalanish kerak. Tarmoqni kompyuter hujumlaridan himoya qilish-doimiy va noan'anaviy vazifa bo'lib, biroq qator oddiy himoya vositalarini qo'llash tarmoqqa suqilib kirishga urinishlarni to'xtatishi mumkin. Misol uchun, barcha ish stantsiyalarida o'rnatiladigan yaxshi konfiguratsiya qilingan tarmoqlararo ekran va antivirus dasturlari aksariyat kompyuter hujumlarini amalga oshirilishiga to'sqinlik qiladi. Quyida sizning tarmog'ingizni himoya qilishga yordam beruvchi 14 ta turli himoya choralari haqida qisqacha bayon qilamiz.

1) Dasturlar uchun tuzatmalarni tezkor o'rnatish (Patching). Kompaniyalar dasturlarda yuzaga kelgan xatolar oqibatlarini bartaraf etish uchun tuzatishlarni tez-tez ishlab chiqadilar. Agar siz dasturga tuzatishlarni o'z vaqtida kiritmasangiz, tajovuzkor bu xatolardan foydalanib kompyuteringizga bostirib kirishi mumkin.

2) Virus va troyan otlarini aniqlash. Yaxshi antivirus dasturlari har qanday tarmoqdagi xavfsizlikni oshirishning ajralmas vositasidir. Ular kompyuterlarning ishlashini kuzatadilar va ulardagi zararli dasturlarni topadilar. Ulardan kelib chiqadigan yagona muammo shundaki, ular maksimal darajada ishlashi uchun tarmoqdagi barcha kompyuterlarga o'rnatilishi kerak.

3) Tarmoqlararo ekran. Tarmoqlararo ekran (firewalls) tashkilot tarmog'ini himoya qilishning eng muhim vositasidir. Ular tarmoqdagi kiruvchi va chiquvchi trafikni kuzatadilar. Tarmoqlararo ekran tarmoqda uzatiluvchi har qanday turdagi trafikni cheklashi yoki boshqa turdagi trafik tekshiruvlarini bajarishi mumkin.

4) Parolni fosh etish (Password Crackers). Odatda xakerlar kompyuterlardagi shifrlangan parollarni saqlovchi fayllarni qo'lga kiritishda kam ma'lum bo'lgan zaifliklardan foydalanadilar.

Keyinchalik, bu shifrlangan fayllardagi zaif parollarni aniqlaydigan parollarni ochuvchi maxsus dasturlardan foydalanadilar.

5) Shifrlash. Hujumkor ko'pincha tarmoq trafigining eng muhim nuqtalarini tinglashi natijasida, ulardan foydalanuvchi nomlari va parollarini qo'lga kiritish orqali tarmoqlarga suqilib kiradilar.

6) Zaif nuqtalar skanerlari. Bu muayyan turdagi hujumlarga qo'l keluvchi tarmoqlardagi zaifliklarni kompyuterlarda qidirish uchun mo'ljallangan dasturdir. Skanerlar zaifliklarning katta ma'lumotlar bazasiga ega bo'lib, ulardan kompyuterlardagi u yoki bu zaifliklarni tekshirishda foydalanadilar.

7) Xavfsizlik nuqtai nazaridan kompyuterlarning to'g'ri konfiguratsiyasi. Yangitdan o'rnatilgan operatsion tizimlarga ega kompyuterlar, odatda, hujumlarga qarshi himoyasizdir.

8) Hujumkor dialer (war dialer). Foydalanuvchilar ko'pincha tashkilot tarmog'ining himoya vositalari chegaralarini aylanib o'tib, kompyuterlariga kiruvchi qo'ng'iroqlarni qabul qilishga ruxsat beradilar. Foydalanuvchi modem orqali ulanishni qo'llab chaqiruvni amalga oshiradi va so'ngra, uydan turib korporativ tarmoqdan foydalanishi mumkin bo'ladi.

9) Xavfsizlik bo'yicha tavsiyalar (security advisories). Xavfsizlik bo'yicha tavsiyalar-kompyuter jinoyatlariga qarshi kurashuvchi guruhlar va dastur ishlab chiqaruvchilar tomonidan so'nggi paytlarda topilgan zaifliklar to'g'risidagi ogohlantirishlardir.

10) Hujumlarni aniqlash vositalari (Intrusion Detection). Hujumlarni aniqlash tizimlari kompyuter hujumlarini darhol aniqlaydilar. Ular tarmoq ichidan tashkil qilingan hujumlarni aniqlashda brandmauerlardan keyin o'rnatilishi mumkin.

11) Tarmoq topologiyasini aniqlash vositalari va port skanerlari. Ushbu dasturlar tarmoqning qanday tashkil etilganligi va unda ishlovchi kompyuterlar hamda har bir mashina ko'rsatuvchi barcha xizmatlarning to'liq tasvirini yaratishga imkon beradi.

12) Xavfsizlik intsidentlarini tergov qilish guruhi. Har bir tarmoq qanchalik xavfsiz bo'lishidan qat'iy nazar, xavfsizlik bilan bog'liq qandaydir hodisaga duch keladi (hatto noto'g'ri signallar ham bo'lishi

mumkin). Ushbu holatda tashkilot xodimlari qanday harakatlarni amalga oshirishini oldindan bilishi kerak.

13) Xavfsizlik siyosati. Tarmoq xavfsizligi tizimi zaif joy himoyalangani kabi kuchlidir. Agar bir tashkilot doirasida turli xil xavfsizlik siyosati o'rnatilgan tarmoqlar mavjud bo'lsa, unda ma'lum bir tarmoqning zaif xavfsizligi tufayli bir tarmoq obro'sizlanishi mumkin.

14) Xavfsizlik devori va WWW-serverlarni blokirovka qilishga urinish barqarorligini testlash. Kompyuterni blokirovka qilishga qaratilgan hujumlar Internetda keng tarqalgan. Tajovuzkorlar doimo WWW saytlarini ishdan chiqaradi, kompyuterlarni qayta yuklaydi yoki tarmoqlarni haddan tashqari bema'ni paketlar bilan to'ldirib tashlaydi.

6.3. Hujumlarni aniqlovchi tarmoq tizimlari

Tarmoq hujumlarini aniqlash tizimlari ko'pincha xavfsizlik devorlarini (firewall) almashtirishga urinib, xavfsizlikning yuqori darajasini ta'minlashga harakat qilishadi. Biroq shuni unutmaslik lozimki, xavfsizlik devorlari (firewall) oddiy tizim bo'lib, ular asosan u orqali o'tuvchi trafiklarni o'tishiga yo'l qo'yish yoki taqiqlashga qaratilgan qoidalarga asoslanadi. Texnologiyadan foydalangan holda qurilgan xavfsizlik devorlari, nazorat qilinayotgan yoki qilinmayotgan vaqtda trafikda hujumning mavjudligini ishonch bilan aytishga imkon bermaydi. Ular faqat trafiklarning qoidaga muvofiq yoki muvofiq emasligini aniqlab beradi xolos. Masalan, xavfsizlik devorlari (ya'ni, HTTP-trafik) TCP ulanishlaridan tashqari 80-portdagi barcha ulanishlarni bloklash uchun konfiguratsiyalangan. Shunday qilib, 80-portdagi har qanday trafik xavfsizlik devorlari nuqtai nazaridan qonuniydir. Boshqa tomondan, hujumni aniqlash tizimi ham trafiklarni nazorat qiladi, lekin ularda hujum belgilarini izlaydi. Trafikning qaysi portiga mo'ljallanganligi ularga unchalik muhim emas. Odatiy holatda hujumlarni aniqlash tizimining barcha trafiklari shubhali hisoblanadi. Ya'ni, hujumni aniqlash tizimi TE bilan bir xil ma'lumot manbalari asosida ishlaydi, ya'ni tarmoq trafigi bilan ular qo'shimcha funktsiyalarni bajaradilar. Misol uchun, HTTP so'rovi "Get/../../../etc/passwd HTTP/1.0" dir. Haqiqatan ham har qanday TE

ushbu so'rovni o'zidan o'tkazishi mumkin. Biroq, hujumni aniqlash tizimi ushbu hujumni osongina aniqlab, uni blokirovka qiladi. Hujumni aniqlashning o'zi yetarli emas, shunga mos ravishda bunga munosabat bildirish kerak. Ko'pchilik hujumlarni aniqlash tizimining samaradorligini belgilashda qo'llaniladigan javob qaytarish varianlari asos hisoblanadi. Bugungi kunga kelib, quyidagi javob qaytarish variantlari taklif etiladi:

- hujumlarni aniqlash tizimining konsoli (shu jumladan, zaxiralash) yoki integratsiya tizimi konsoliga xabar berish (masalan, xavfsizlik devori);
- hujum haqida ovozli ogohlantirish;
- tarmoq boshqaruv tizimlari uchun SNMP nazorat seanslarini ishlab chiqarish;
- hujum haqidagi E-pochta xabarini generatsiyalash;
- smartfon yoki kompyuterga qo'shimcha xabarlar berish.

Kamdan-kam qo'llanilsada juda qiziqarli. Ruxsatsiz faoliyat aniqlanganligi to'g'risidagi xabar administratorga emas, balki tajovuzkorga yuboriladi. Ushbu javob variantini qo'llab-quvvatlovchilarning fikriga ko'ra, huquqbuzar o'zining aniqlanganini bilib, o'z harakatlarini to'xtatishga majbur bo'ladi.

Aniqlangan hodisalarni majburiy ro'yxatga olish. Qayd etish jurnali sifatida bo'lishi mumkin: matnli fayl, tizim yozuvlari (masalan, Cisco Secure Integrated Software). Xavfsiz Telefonga o'rnatilgan dasturiy ta'minot), maxsus formatdagi matnli fayl (masalan, Snort tizimida), mahalliy MS Access ma'lumotlar bazasi, SQL ma'lumotlar bazasi (masalan, RealSecure tizimida). Qayd qilingan ma'lumotlarning miqdori, odatda, SQL ma'lumotlar bazasi-MS SQL yoki Oracle talabiga binoan bo'lishini hisobga olish kerak.

Hodisalar trassirovkasi (event trace) ya'ni, ularni ketma-ketlikda va tajovuzkor tomonidan amalga oshiriladigan tezlikda yozish. Keyin administrator har qanday vaqtda tajovuzkorning faoliyatini tahlil qilish uchun kerakli hodisalar ketma-ketligini (real vaqtda, tezlashtirish yoki sekinlashtiruvchi) aylantirib ko'rishi (takrorlash yoki qayta tinglash)

mumkin. Bu uning malakalarini, ishlatilgan hujum usullarini va boshqalarni tushunishga imkon beradi.

Buzg'ichning hatti-harakatlarini to'xtatish, ya'ni, ulanishni tugatish. Buni quyidagicha amalga oshirish mumkin:

- ulanishni to'xtatish (session hijacking) va har ikkala nom uchun tarmoq ulanishining har bir ishtirokchisiga o'rnatilgan RST bayrog'i bilan paketni yuborish (tarmoq darajasida ishlaydigan hujumni aniqlash tizimida);

- buzg'unchi foydalanuvchi hisobini blokirovkalash (tugun darajasida hujumni aniqlash tizimida). Bunday blokirovkalash muayyan vaqt davomida yoki administrator tomonidan qayd yozuvni cheklamasdan amalga oshirilishi mumkin. Hujumlarni aniqlash tizimi ishga tushirilgan imtiyozlarga bog'liq holda, bloklash kompyuterning o'zi ham, hujumga yo'naltirilgan va tarmoqning butun doirasi ichida harakat qilishi mumkin;

- tarmoq vositalari yoki xavfsizlik devorini qayta konfiguratsiyalash. Hujum router yoki xavfsizlik devorida aniqlanganda, kirishni boshqarish ro'yxatini o'zgartirish uchun buyruq yuboriladi. Keyin, hujum qiluvchi tugunga ulanishga bo'lgan barcha urinishlar rad etiladi. Buzg'unchining hisobini to'sib qo'yish bilan bir qatorda kirishni nazorat qilish ro'yxatini ma'lum bir vaqt oralig'ida yoki o'zgarish administrator tomonidan qayta tiklanadigan tarmoq uskunalari tomonidan bekor qilinmaguncha o'zgartirilishi mumkin;

- xavfsizlik devorlari yordamida tarmoq trafikni bloklash. Ushbu parametr, shaxsiy xavfsizlik devorlarida mavjud funktsiyalarni bajarishga imkon beruvchi, himoyalangan kompyuterning resurslariga kiradigan trafikni hamda oluvchini cheklash imkonini beradi.

Masofadan qo'llaniladigan hujumlarga qarshi vositalar. Ayni paytda, masofadan turib hujumlarni oldini oluvchi quyidagi tizimlar keng tarqalgan:

– TE, dasturiy va apparat ta'minot asosida amalga oshiriladi;

– kriptoprotokollar;

– apparat va dasturiy tarmoq trafigi analizatorlari.

Tarmoqlararo ekran (Firewall)

Umumiy holda, TE quyidagi uch asosiy funktsiyani amalga oshiradi:

1. Tarmoq trafigini ko'p bosqichli filtrlash.

Filtrlash odatda uchta darajada amalga oshiriladi:

– tarmoq (IP);

– transport (TCP, UDP);

– amaliy (FTP, TELNET, HTTP, SMTP, va h.k.).

Tarmoq trafigini filtrlash TE tizimlarining asosiy funksiyalaridan biri sanaladi va tarmoq xavfsizligi ma'muri IP tarmog'ining maxsus segmentida tarmoq xavfsizligi siyosatini markazlashtirilgan tarzda amalga oshirishga imkon beradi, ya'ni shunga mos ravishda TElarni o'rnatish orqali siz foydalanuvchilarni tashqi tarmoqdan mos keladigan xost-xizmatlarga kirishga ruxsat etishingiz yoki uni taqiqlashingiz mumkin. Himoyalangan segmentda joylashtirilgan xostlar va foydalanuvchilar ichki tarmoqdan tashqi tarmoqning tegishli resurslariga kirishlari mumkin. Tizimdagi xavfsizlik siyosatini amalga oshirish uchun tizim sub'ektlari o'zlarining ob'ektlariga ma'mur tomonidan belgilanadigan erkin foydalanish huquqlariga muvofiq taqsimlanishiga imkon beradigan sub'ektlar (foydalanuvchilar) va tizim ob'ektlari (masalan, fayllar) o'rtasida tegishli munosabatlarni to'g'ri belgilaydigan mahalliy OT ma'muri bilan taqqoslash mumkin. Xuddi shu qarashlar xavfsizlik devori filtrlashida ham qo'llaniladi: subyekt bilan o'zaro aloqadorlik sifatida xost foydalanuvchilarning IP-manzillari, oby'ekt sifatida esa transport protokollari va masofaviy kirish xizmatlari taqdim qilinuvchi kerakli ruxsat chegaralari-IP-manzil xostlarini ajratish lozim.

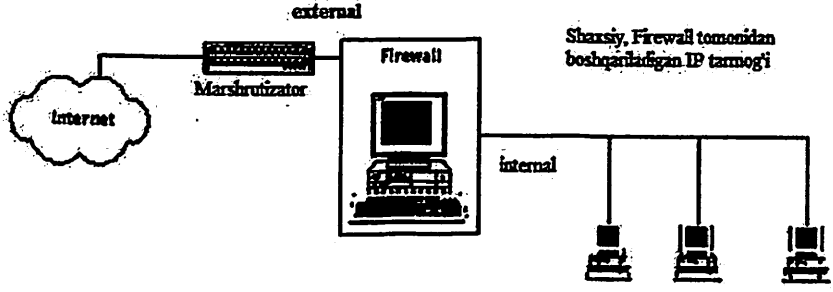
2. TE-xostda foydalanuvchini Proxy-sxema yordamida qo'shimcha identifikatsiya va autentifikatsiya qilish.

Proxy-sxemasi, birinchi navbatda, tarmoqning himoyalangan TE segmentiga kirishda, masofaviy foydalanuvchilarni qo'shimcha identifikatsiya va autentifikatsiya qilishni amalga oshirishga imkon beradi va ikkinchidan, bu virtual IP-adreslar bilan xususiy tarmoqlarni yaratish uchun asos bo'lib xizmat qiladi. Proksi-sxemaning ma'nosi TE-xostida oraliq proxy server (proxy ing. vakolat) orqali yakuniy manzilga

ulanishni yaratishdir. Ushbu proksi-serverda abonentni qo'shimcha identifikatsiyasini amalga oshirilishi mumkin.

3. "Virtual" IP manzillariga ega xususiy tarmoqlarni yaratish (Virtual Private Network-VPN).

Tarmoq xavfsizligi ma'muri ichki IP-tarmoqning asl topologiyasini yashirishni ma'qul ko'rganda, unga xususiy tarmoq (VPN tarmog'i) yaratish uchun TE tizimlaridan foydalanish tavsiya qilinadi. VPN-tarmoq xostlariga ixtiyoriy "virtual" IP-manzil tayinlanadi. Tashqi tarmoqqa (TE orqali) murojaat qilish uchun yuqorida tavsiflangan proksi-serverlarni TE xostida ishlatish yoki tashqi adreslash imkoni mavjud maxsus marshrutlash tizimlarini (marshrutlash) qo'llash kerak. Bu shuni anglatadiki, ichki VPN tarmog'ida ishlatiladigan virtual IP manzil tashqi manzillashda qo'l kelmaydi (tashqi manzil VPN tarmog'idan tashqaridagi abonentlarga qaratilgan). Shuning uchun, proksi-server yoki marshrutlash vositasida tashqi tarmoq abonentlari o'zining asl IP-manzili bilan o'zaro aloqa qilish imkoniyatiga ega bo'lishi lozim. Shuningdek, IP-tarmoqni yaratish uchun yetarlicha IP-manzillar ajratilmagan hollar uchun ushbu sxema qulaydir (IPv4 standartida, bu yoppasiga va hamohang sodir bo'ladi, shuning uchun proxy- sxema yordamida qiymatga ega IP-tarmoqni yaratishda proxy-server uchun faqat belgilangan IP-manzil yetarlidir).



6.1-rasm. To'liq xususiyatli Firewall xostining umumiy sxemasi

Shunday qilib, Firewall-metodikasining kamida bitta funksiyasini amalga oshiriluvchi har qanday qurilma Firewall-qurilmasi hisoblanadi. Misol uchun, FreeBSD yoki Linux operatsion tizimli kompyuterdan Firewall xosti sifatida foydalanishga hech nima to'sqinlik qilmaydi va

mos ravishda OT yadrosini shunga moslash kerak bo'ladi. Ushbu turdagi tarmoqlararo ekran IP-trafikni ko'p darajali filtrlashni ta'minlaydi. Bozorda taklif etilayotgan kuchli Firewall-komplekslar odatda, barcha Firewall vazifalairni amalga oshiruvchi metodika kompyuter yoki mini kompyuter bazasida yaratiladi va ular to'liq funksional Firewall hisoblanadi. Quyidagi rasmda tashqi tarmoqdan ajratilgan to'liq funksional Firewall-xost tarmoq segmenti tasvirlangan.

Tarmoq xavfsizligini ta'minlashda Firewall usulidan foydalanish maqsadga muvofiq, lekin bu *yetarli* shart *emas,* shuni nazarda tutish kerakki, Firewall o'rnatilganda, siz barcha tarmoq xavfsizligi muammolarini birdan hal qilasiz va Internetdagi barcha mumkin bo'lgan masofaviy hujumlardan xalos bo'lasiz. Internet tarmog'i xavfsizligi nuqtai nazaridan hech bir Firewall himoya jihatidan yagona yechim bo'la olmaydi.

Dasturiy himoyalash usullari.

Internet tarmog'ida dasturiy himoya usullaridan foydalanib ulanishni himoyalash imkoniyatini beruvchi kripto-protokollarni o'z ichiga oladi.

Masofaviy hujumlardan saqlanishdagi dasturiy ta'minotning yana bir sinflari bu tarmoq trafigini oldindan ma'lum masofaviy faollik va aniqlangan ta'sirlarga qarshi turish uchun tahlil qilishdir.

Taqsimlangan hisoblash tizimlaridagi masofaviy hujumlar muvaffaqiyatining asosiy sabablaridan biri, tarmoq almashuv protokollaridan foydalanishdir, ular masofaviy ob'ektlarni aniqlashning ishonchliligini, ulanish va uning asosida uzatiluvchi ma'lumot himoyasini ta'minlay olmaydi. Shu sababli, internetni ishga tushirish vaqtida, yopiq va ochiq kalitli kriptografiyadan foydalangan holda, turli xil xavfsiz tarmoq protokollarining yaratilishi tabiiy holdir. Simmetrik kriptoalgoritmli klassik kriptografiya jo'natuvchi uchun mo'ljallangan va qabul qiluvchi tomonlar xabarlarni shifrlash va deshifrlash uchun nosimmetrik (bir xil) kalitlarga ega ekanligini ko'rsatadi. Ushbu kalitlar kriptografiyada statik kalitlarni taqsimlashning standart muammosi deb ataladi va ular cheklangan sonli abonentlar o'rtasida oldindan taqsimlanishi kerak. Shubhasiz, simmetrik kalitlarga ega klassik

kriptografiyani qo'llash faqat cheklangan sonli ob'ektlar to'plamida bo'lishi mumkin.

Internet tarmog'ida barcha foydalanuvchilar uchun statik kalitlarni tarqatish muammosini hal qilishni tasavvur etish mumkin emas. Internetda ilk himoyalangan almashinuv protokoli Kerberos bo'lib, u so'nggi abonent uchun statik kalitlarni tarqatishga asoslangan edi. Xuddi shu tarzda, maxsus xizmat xodimlari klassik simmetrik kriptografiyadan foydalanib Internet tarmog'i uchun himoyalangan kriptoprotokollarni ishlab chiqishga majbur. Bu shuni anglatadiki, ba'zi sabablarga ko'ra tasdiqlangan ochiq kalitli kriptoalgoritmlar mavjud emas. Dunyoning har bir nuqtasida mazkur shifrlash standartlari qabul qilingan va tasdiqlangan.

Shunday qilib, internet-foydalanuvchilari himoya imkoniyatini cheklanmasligini ta'minlash uchun virtual ulanish kalitlarini dinamik ravishda ochiq kalitli kriptografiyadan foydalanib yaratish maqsadga muvofiq. Ulanishni himoyalashda foydalaniladigan asosiy yondashuvlar va protokollar haqida keyinchalik to'xtalib o'tamiz.

SKIP protokoli.

SKIP protokoli (Secure Key Internet Protocol) IP-paketlar inkapsulyatsiyasi standartini belgilaydi, bu tarmoq darajasidagi mavjud IPv4 standartida foydalaniladigan ulanish va u orqali uzatiladigan ma'lumotlarni himoya qilishga imkon beradi. Bunga quyidagicha erishiladi: SKIP-paket-ma'lum formatdagi spetsifikatsiyaning SKIP sarlavha va kriptogram (shifrlangan ma'lumotlar) ma'lumotlar maydoni bo'lgan normal IP-paketdir. SKIP-paketining bunday tarkibi Internetdagi ixtiyoriy xostga mone'liklarsiz yo'naltiriladi (tarmoqlararo manzillash odatdagidek SKIP-paketida IP-sarlavhasi orqali amalga oshiriladi). SKIP paketining oxirgi qabul qiluvchisi kriptogram ishlab chiquvchilar tomonidan oldindan aniqlangan algoritmga ko'ra shifri yechiladi va operatsion tizimning yadrosiga mos keladigan oddiy modulga (TCP yoki UDP) yuboriladi, oddiy TCP yoki UDP paketini ishlab chiqaradi. Aslida, tamoyilga ko'ra, ishlab chiquvchi o'zining ma'lumotlar sxemasi bo'yicha SKIP sarlavhasidan farqli ravishda o'z asl sarlavhasini yaratishga hech narsa to'sqinlik qilmaydi.

S-HTTP protokoli. S-HTTP (Secure HTTP) protokoli-Enterprise Integration Technologies (EIT) kompaniyasi tomonidan ishlab chiqilgan bo'lib, xususan, veb-himoya HTTP protokolidir. S-HTTP protokoli faqat veb- serverning HTTP hujjatlarini ishonchli shifrlashni ta'minlaydi va OSI modelining amaliy sathida ishlaydi. S-HTTP protokolining bu xususiyati uni mutlaqo ixtisoslashtirilgan aloqa himoyasini ta'minlaydi va uni boshqa barcha amaliy protokollar (FTP, TELNET, SMTP, va hokazo) himoya tizimi sifatida tadbiq etib bo'lmaydi. Bundan tashqari, bugungi kunda ommaviy foydalaniluvchi veb-brauzerlarning hech biri (na Netscape Navigator 3.0 na Microsoft Explorer 3.0) ushbu protokolni qo'llab-quvvatlamaydi.

SSL protokoli. SSL protokoli (Secure Socket Layer)-Netscape tomonidan ishlab chiqilgan OSI seansli darajada ishlaydigan universal ulanish protokolidir. Ochiq kalitli kriptografiyadan foydalangan holda ushbu protokol sizning istalgan amaliy protokol (DNS, FTP, TELNET, SMTP, va boshqalar) yordamida har qanday aloqani dinamik ravishda himoya qilishga imkon beruvchi universal vositadir. Buning sababi shundaki, SSL, S-HTTP dan farqli o'laroq, OSI ning oraliq darajasida (transport-TCP, UDP, va amaliy-FTP, TELNET, va boshqalar) ishlaydi. Shu bilan birga, virtual SSL ulanishni yaratish jarayoni Diffie va Hellman sxemasiga muvofiq amalga oshiriladi, bu kriptografik seansli kalitini yaratishga imkon beradi, bu SSL aloqasi abonentlari uzatilgan xabarlarni shifrlash uchun foydalanadi. Bugungi kunda SSL protokoli deyarli HTTP ulanishlari uchun rasmiy xavfsizlik standarti, ya'ni web-serverlarni himoya qilish uchun shakllandi. Albatta, biror web-server bilan SSL-ulanishni o'rnatish uchun SSL qo'llab-quvvatlaydi vebserver talab etiladi. Veb- serverlarning bunday versiyalari allaqachon mavjud (masalan, SSL-Apache).

Shunday qilib, bu xavfsiz almashinuv protokollari, ayniqsa SSL (asosan, 40 bitdan ortiq kalit) bilan keng foydalanish, uzoq masofali hujumlarning oldini olish yo'lida ishonchli to'siq qo'yadi va butun dunyo bo'ylab krakerlarning hayotini jiddiy ravishda murakkablashtiradi. *Biroq Internetdagi hozirgi xavfsizlik vaziyatining barcha fojiasishundan iboratki, mavjud kripto-protokollarning hech biri*

(va ularning ko'pchiligi) barcha tarmoq operatsion tizimining ishlab chiqaruvchilari tomonidan qo'llab-quvvatlanadigan yagona aloqa standarti sifatida shakllantirilgan! Bugungi SSL protokoli ushbu rolga mos keladi. Agar u barcha tarmoq operatsion tizimlari tomonidan qo'llab-quvvatlansa, maxsus dastur SSL-mos keluvchi serverlar (DNS, FTP, TELNET, WWW, va boshqalar) yaratilishini talab qilmagan bo'lar edi . Xavfsiz sessiya darajasidagi protokol uchun yagona standartni qabul qilsangiz, har bir alohida xizmatni himoya qilish uchun ko'plab standartlarni qabul qilishingiz kerak bo'ladi. Masalan, empirik, qo'llab-quvvatlanmaydigan Xavfli DNS protokoli ishlab chiqilgan. Sinxronlashtiruvchi SSL bilan birgalikda xavfsiz FTP va TELNET serverlari mavjud. Bularning barchasi, barcha ishlab chiqaruvchilar tomonidan himoyalangan protokol uchun yagona standartni qabul qilmasdan, hech qanday mantiqqa olib kelmaydi. Bugungi kunda tarmoq operatsion tizimining sotuvchilari ushbu mavzu bo'yicha yagona pozitsiyani qabul qila olmaydilar va shuning uchun bu muammolarning echimini to'g'ridan-to'g'ri Internet-foydalanuvchilarga o'tkazadilar va ***o'zlarining*** axborot xavfsizligi muammolarini hal qilishni taklif qiladilar!

Internetdan foydalanuvchilarning tezkor miqdoriy o'sishi va foydalanuvchilarga taqdim etilayotgan imkoniyatlarning kengayishi uzoqdan hujumlarni xavf ostiga qo'yadi. Hujumlar katta ma'naviy va moddiy zarar bilan shug'ullanadigan, shaxslar va tashkilot ham amalga oshiriladi. Bu hujumlarni aniqlaydigan va ularni amalga oshirishga yo'l qo'yadigan vositalarni ishlab chiqishni talab qiladi.

6.4. Internet tarmog'ida masofadan amalga oshiriladigan hujumlardan himoyalash

Bugungi kunda Internetning o'ziga xos xususiyati-tarmoq axborot resurslarining 99% ommaviyligidadir. Ushbu manbalarga masofadan ulanish tarmoqning har qanday ruxsatsiz foydalanuvchisi tomonidan anonim tarzda amalga oshirilishi mumkin. Davlat resurslariga bunday ruxsatsiz kirishning namunasi WWW yoki FTP serverlariga ulanish imkonini beradi.

Foydalanuvchilar qaysi internet- resurslarga kirishni rejalashtirganligi haqida siz quyidagi savolga javob berishingiz kerak: foydalanuvchi tarmoqdan masofadan foydalanishga ruxsat beradimi? Agar yo'q bo'lsa, unda tarmoq operatsion tizimi, masofaviy kirish imkoniyatini beruvchi server-dasturlarsiz "sof mijoz" operatsion tizimi sifatida foydalanish imkonini beradi (masalan, Windows 95 yoki NT Workstation) shunday qilib ushbu tizimga masofaviy kirish imkoniyati *tamoyilga binoan, mumkin emas*, chunki u dasturiy ta'minot bilan ta'minlanmagan Mijoz operatsion tizimini tanlab olish, odatda ma'lum bir foydalanuvchi xavfsizlik muammosini hal etadi(faqat mavjud bo'lmagan obyektga kira olmaydi!). Biroq, bu holda tizimning funksionalligi yomonlashadi. Bu yerda, bizning fikrimizcha, xavfsizlikning asosiy aksiomasi o'z vaqtida shakllantiriladi:

Xavfsizlik aksiomasi. Kompyuter tizimining imkoniyati, qulayligi, tezligi va funksionalligi tamoyillari xavfsizlikning tamoyillariga zid keladi.

Ushbu aksioma tamoyil jihatidan shaffofdir: qulaylik foydalanuvchanllik imkoniyatining kengligi hisoblash tizimining xavfsizlik darajasini keskin pasaytiradi. Qator misollar keltirish mumkin. Masalan, DNS xizmati: qulay, lekin xavfli.

Shunday qilib, Internet foydalanuvchisi tarmoqqa kirish uchun faqat mijoz tarmoq operatsion tizimidan foydalanishga qaror qilganda va uning yordamida faqat ruxsatsiz kirish amalga oshiriladi. Xavfsizlik masalalari hal qilinganmi? Bir oz emas! Barchasi yaxshi bo'lganda edi, bunchalar yomon bo'lmasdi. "Xizmatdan voz kechish hujumi"da na foydalanuvchi tomonidan o'rnatilgan foydalanish ruxsati va na OT turi ahamiyatga ega emas (xususan mijoz OT hujumlardan himoyalanganlik nuqtai nazaridan birmuncha afzaldir). Ushbu hujum Internet protokollarida va infratuzilmada asosiy xavfsizlik kamchiliklarini qo'llaydi, foydalanuvchi xostdagi operatsion tizimga zarar yetkazishning yagona maqsadi-uning ish faoliyatini izdan chiqarishdan iborat. ICMP protokoli yordamida soxta marshrutdan foydalanishni nazarda tutadigan hujum maqsadi-Windows 98 yoki Windows NT xizmatdan voz kechishga olib kelish hisoblanadi. Bu holatda foydalanuvchi o'zining

kamtarona xosti buzg'unchiga qiziqish uyg'otmasligiga umid qiladi, aks holda bu uning ish samaradorligini buzishi mumkin.

Himoyalashning ma'muriy usullari. Ushbu yo'nalishdagi to'g'ri qadam siz bilan birgalikda kerakli xavfsizlik darajasini ta'minlash uchun barcha vazifalarni hal etishga harakat qiladigan axborot xavfsizligi bo'yicha mutaxassisga taklif qilish bo'ladi. Bu nimani (murakkab ob'ektlar ro'yxati va RVS resurslari) nimadan (ma'lum bir RVSga mumkin bo'lgan tahdidlarning tahlili) va qanday (talablarni ishlab chiqish, xavfsizlik siyosatini aniqlash va ma'muriy va dasturiy-apparatiy choralarni ishlab chiqish) himoyalash kerakliligini aniqlash uchun hal etilishi lozim bo'lgan murakkab kompleks vazifadir.

Ehtimol, axborotni buzg'unchi ta'sirlardan himoya qilishning eng oddiy va eng arzon usuli bu –ma'muriy usul bo'lishi mumkin.

Tarmoq trafigini tahlil qilishdan qanday himoyalash mumkin?

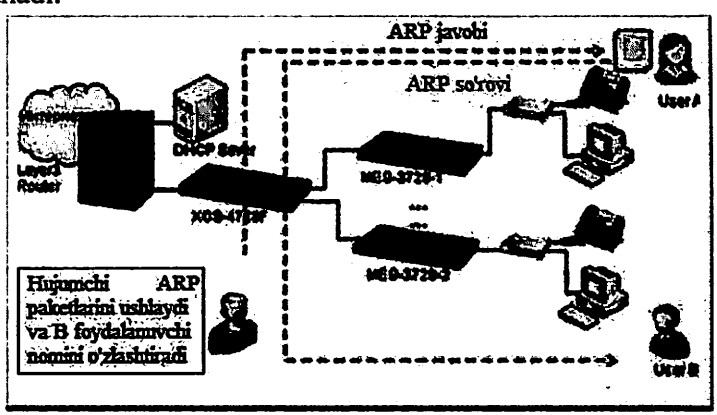
Foydalanuvchilar masofadan uzatadigan barcha xabarlarni aloqa kanali bo'ylab shifrlanmagan ko'rinishda uzatadigan bo'lsa, ular krakerlar tomonidan eshitish dasturlaridan ixtiyoriy ma'lumotni tutib olishi mumkin. Bundan tashqari, asosiy TELNET va FTP masofaviy erkin foydalanish dastur protokollari tarmoq orqali uzatiladigan foydalanuvchilarning identifikatorlari (nomlari) va autentifikator (parol) larning asosiy kripto muhofazasini ta'minlamasligini ko'rsatishi mumkin. Shu sababli, tarmoq administratori, ushbu asosiy protokollarning uzoqdan *ruxsat berilganligini* ta'minlashga yo'l qo'ymasliklari kerakligi haqida aniq ma'lumot berishi mumkin, ularning tizimlarining resurslariga kirish va tarmoq trafigini tahlilini doimiy ravishda mavjud tahdid deb hisoblashni hisobga olmaysiz, ammo siz ularni doimiy IP-trafikni muhofaza qilish kripto algoritmlarini qo'llash orqali uning xavfini sezilarli darajada pasaytira qila olasiz.

Qanday qilib soxta ARP-serverdan himoyalanish kerak?

Internet tarmog'ida IP-paketlarni manzillashda xostning IP-adresiga qo'shimcha ravishda, tarmoq adapteri Ethernet manzili (manzillash bir tarmoq ostida bo'lganda) yoki router Ethernet- manzili (tarmoqlararo manzillashda) talab qilinadi. Dastlab, xost u bilan birga bitta segmentga kiradigan boshqa xostlar Ethernet-manzillari hamda,

router Ethernet-manzili haqida ma'lumotga ega bo'lmasligi mumkin. Shunday qilib, xost masofaviy qidirish algoritmi yordamida hal qilinishi lozim bo'lgan standart muammo bilan duch keladi.

Internet tarmog'ida ushbu muammoni bartaraf etish uchun ARP protokolidan (Address Resolution Protocol) foydalaniladi. ARP bir segmentda joylashgan xostlar uchun IP va Ethernet manzillari o'rtasida bir-biriga mos keladigan bog'liqlikni qabul qilishga imkon beradi (19-rasm). Ushbu protokol quyidagicha ishlaydi: tarmoq resursiga birinchi bor kirganingizda, xost siz istagan resursning (router yoki xost) IP manzilini ko'rsatadigan va Ethernet manzilidan so'ragan ARP so'rovini yuboradi. Ushbu so'rov, tarmoq segmentidagi barcha stantsiyalar, jumladan, izlangan manzilni qabul qiladi. Ushbu so'rovni qabul qilganidan so'ng, xost so'rovlarni ARP-jadvaliga qayd etadi va keyin uning so'rovini so'ragan xostga o'zining Ethernet-manzili bilan ARP javobini yuboradi. Qabul qilingan ARP javobi Ethernet-manzili so'ralgan kompyuterning OT xotirasiga kiradigan ARP –jadvalida saqlanadi.



6.2-rasm. ARP protokoli ish sxemasi

Tarmoq operatsion tizimida IP-tarmog'ining bir segmenti ichida IP va Ethernet manzili haqidagi ma'lumot mavjud bo'lmasa, ushbu protokol tajovuzkorning kerakli Ethernet manzilini qidirish uchun soxta javob yuborishi mumkin bo'lgan ARP so'rovini yuborishga imkon beradi, natijada kanal darajasidagi barcha trafik tajovuzkor tomonidan

ushlanib qolinadi va soxta ARP serveridan o'tadi. Shubhasiz, bu hujumni bartaraf etish uchun uni amalga oshirish mumkin bo'lgan sababni yo'q qilish kerak. Ushbu masofadan qilinadigan hujum muvaffaqiyatining asosiy sababi, har bir xost kompyuterning OT da qolgan barcha bir segmentdagi xostlar IP va Ethernet-manzillari haqidagi zaruriy ma'lumotlarning yo'qligidir. Shunday qilib tarmoq administrator uchun eng oson yechim bu-statik Apr-jadvalni ma'lum fayl sifatida yaratish va uni manzil haqida ma'lumot so'raladigan o'rinlarda kiritish hisoblanadi (odatda UNIX OTda /etc/ethers). Ushbu fayl segmentdagi har bir xostga o'rnatiladi va shuning uchun tarmoq operatsion tizimi masofali ARP qidirishdan foydalanish oldi olinadi.

Qanday qilib soxta DNS-serverdan himoyalanish kerak?

Internet tarmog'ida DNS xizmatidan foydalangan holda krakerlar soxta DNS-server xost soxta marshrutni ulash orqali global nazoratni qo'lga kiritishi mumkin. Potentsial DNS zaifliklariga asoslangan ushbu masofaviy hujumni amalga oshirish juda ko'p Internet foydalanuvchilari uchun fojiali oqibatlarga olib kelishi va bu global tarmoqning axborot xavfsizligini buzilishiga olib kelishi mumkin. Keyingi ikki xatboshi, administratorlar va tarmoq foydalanuvchilari va DNS serverlari administratorlari uchun bu masofaviy hujumni oldini olish yoki murakkablashtirish uchun mumkin bo'lgan ma'muriy usullarni taklif qiladi.

Tarmoq administratori soxta DNS serverlardan qanday himoyalanishi mumkin?

Agar siz bu savolga qisqacha javob bersangiz, unda hech ma'no yo'q. DNS-ning mavjud versiyalarida hujumdan na ma'muriy, na dasturiy jihatdan himoyalanish imkonsiz. Xavfsizlik nuqtai nazaridan maqbul yechim, bu sizning himoyalangan segmentingizda DNSdan foydalanishdan bosh tortishdir! Albatta xostlarga murojaat qilishda nomlardan butunlay voz kechish foydalanuvchilarga juda noqulay bo'ladi. Shuning uchun quyidagi kelishuv yechimini taklif qilamiz: ismlardan foydalaning, ammo masofaviy DNS qidirish mexanizmidan voz keching. Siz DNS xizmatining maxsus DNS-serverlari bilan kelishidan oldin ishlatilgan sxemaga qaytish ekanini to'g'ri deb bilasiz.

So‘ngra, tarmoqdagi har bir mashinada tarmoqdagi barcha xostlarning tegishli nomlari va IP-manzillari to‘g‘risidagi ma’lumotlarni o‘z ichiga olgan *xosts* fayl bor. Ma’lumki, bugungi kunda administrator ushbu faylga faqat shu segmentdagi foydalanuvchilar tomonidan tez-tez tashrif buyuradigan serverlar haqidagi o‘xshash ma’lumotlarga kirishishi mumkin. Shuning uchun, ushbu yechimning amaliyotda ishlatilishi o‘ta murakkab va, ehtimol, aniq emas (masalan, ismlar bilan URLni ishlatadigan brauzerlar bilan nima qilish kerak).

Umumiy umidsiz xulosa quyidagicha: internetda *DNSning mavjud* versiyasidan foydalanilganda noto‘g‘ri DNS serveridan himoya qilish uchun qabul qilinadigan yechim *yo‘q* (ARP holatida bo‘lgani kabi, siz uni rad qilmaysiz va ulardan foydalanish xavfli)!

DNS server administratori soxta DNS serveridan qanday himoyalanishi mumkin?

Agar siz bu savolga qisqacha javob bersangiz, yana, hech qanday ma’no yo‘q. Ushbu masofadan turib qilinadigan hujumni amalga oshirishni murakkablashtirishning yagona yo‘li-UDP emas, balki xostlar va boshqa DNS-serverlar bilan muloqot qilish uchun faqat TCP protokolidan foydalanishdir. Biroq, bu faqat hujumni amalga oshirishni qiyinlashtiradi-DNS so‘rovining oldini olish va TCP identifikatori ISN ning boshlang‘ich qiymatining matematik prognozi ehtimoli haqida unutmaslik lozim.

Xulosa qilib aytganda, barcha Internet tarmoqlarida tezda yangi, xavfsizroq DNS versiyasiga o‘tish yoki xavfsiz protokol uchun bitta standartni qabul qilishi tavsiya etiladi. Ushbu o‘tishni amalga oshirish uchun barcha katta xarajatlarga qaramasdan, sodda zaruriy, Internet tarmog‘i ushbu xizmat yordamida o‘z xavfsizliklarini buzish uchun muvaffaqiyatli urinishlar ortib borishidan oldin oddiygina kerakli qadamlar solinishi mumkin!

Xizmatdan voz kechishdan qanday saqlanish kerak?

Internetning mavjud bo‘lgan IPv4 standartida xizmat ko‘rsatishdan voz kechishdan himoyalanishning maqbul usullari mavjud emas. Buning sababi shundaki, ushbu standartda xabarlar marshrutini nazorat qilish imkonsiz. Shu sababli, tarmoq ulanishlari ustidan ishonchli nazoratni

amalga oshirish imkoniyati mavjud emas, chunki tarmoq sub'yektiga aloqador masofaviy ob'ekt bilan cheklanmagan miqdordagi aloqa kanallarini band qilish imkoniyati mavjud va shuning uchun ham bu yashirin qolishi mumkin. Internet tarmog'idagi ixtiyoriy server masofali hujum asosida to'laqonli tahlil qilinishi mumkin.

Hujum nigohida bo'lgan tizim ishonchliligini oshirishda qilinishi mumkin bo'lgan yagona taklif, imkon qadar kuchli kompyuterlardan foydalanishdir. Protsessorlarning soni va chastotasi qanchalik yo'qori bo'lsa, RAM hajmi qanchalik ko'p bo'lsa, aloqa o'rnatishga urinayotganlar tomonidan soxta so'rovlar "bo'ron"i yuborilganida tarmoq operatsion tizimining ishlashi yanada ishonchli bo'ladi. Bunga qo'shimcha ravishda, hisoblash kuchi uchun mos bo'lgan va ko'plab ulanish so'rovlarini joylashtiradigan ichki navbatli operatsion tizimlardan foydalanish kerak. Aytaylik, masalan, siz super kompyuterda Linux yoki Windows NT operatsion tizimini o'rnatdingiz bir vaqtning o'zida qayta ishlanadigan so'rovlar uchun navbatning uzunligi taxminan 10 ga teng va navbatni tozalash vaqti bir necha daqiqa bo'lsin, unda kompyuterning barcha hisoblash kuchiga qaramasdan OT buzg'unchilar tomonidan butunlay nosoz holga keltiriladi.

6.5. Saytni buzishdan qanday himoyalash mumkin

Saytni buzishdan himoya qilish bugungi kunda ko'plab sayt egalari uchun muhim vazifadir. Ko'plab boshlangich xakerlik bilimlarini o'zida mujassamlashtirgan qo'llanmalarning paydo bo'lishi sababli, hatto sizning saytingiz haqida ilgari umuman qiziqmagan Internet foydalanuvchilari ham to'satdan o'zlarini sinab ko'rishi va yangi olingan bilimlarni tajribada sinashni istashadi. Saytingizni buzishdan himoya qilish uchun nima qilish kerak?

Boshlash holda biz saytni buzishdan himoya qilishning nodasturiy usullarini sanab o'tamiz. Albatta, siz ham ular haqida bir necha marta eshitgansiz, lekin ehtimol e'tibor bermagandirsiz.

1-usul. Murakkab parollarni tanlang. Amaliyot shuni ko'rsatadiki, parolni tanlashda ishlatiluvchi eng aqlli dasturlar hatto bir yildan kam vaqtda sakkizta belgili parolni osonlik bilan yengishi mumkin. Holbuki,

sakkiz xonali sonning kombinatsiyasi $2x10^{12}$, sakkizta noma'lum belgili buzg'unchi kombinatsiyani esa undanda ortiq.

2-usul. Administrator paneliga tasdiqlanmagan shaxslarga kirish huquqini bermang. Aks holda, sayt buzilganidan so'ng hayron bo'lmang. Bundan tashqari, ixtiyoriy shaxslarga saytga HTML kodini kiritish huquqini bermaslik kerak, chunki tajovuzkor foydalanuvchilar saytga zararli kod qo'shishi mumkin.

3-usul. Yangi ma'lumotlar bazasiga ega antivirusdan foydalaning.

4-usul. Parolni FTP mijozlarida saqlamang. Parolni o'z ichiga olgan fayl, hatto shifrlangan bo'lsa ham, uni buzish xaker uchun bu oddiy o'g'rilik-to'pni uloqtirishday gap.

5-usul. Parolni saqlash uchun siz xotirangizga tayanmasangiz, maxsus parol saqlash menejerlaridan foydalanganingiz yaxshiroq. Parol menedjer shifrlangan faylda parollaringizni saqlash va tartibga solish imkonini beruvchi maxsus dasturdir. Parol menejeriga kirish uchun sizga alohida parol kerak-kalit. Aytgancha, bir parolni eslab qolish, ular o'nlab turli xillardan ko'ra osonroq emasmi?

6-usul. Shubhali havolalarga kirmang. Bunga sharx berib o'tirishga hojat yo'q.

Biroq, har doim ham sayt buzmasligi sayt egasining beparvoligi yoki e'tiborsizligi tufayli yuzaga keladi. Ba'zan saytning zaifligi professional xakerlar tezda k nashf etadigan manba kodlaridir. Agar saytingiz kontentni boshqarish tizimlaridan biriga (CMS) asoslangan bo'lsa , unda bu tizimlar ishlab chiquvchilari sizning xavfsizligingiz haqida qayg'urgani va manba kodidagi zarur xavfsizlik elementlarini kiritilganligini aniqlashtiring.

Saytingizda tayyor skriptlardan foydalangan bo'lsangiz, ular har doim zaif bo'lishi mumkinligini esda tuting. Aslida,skriptlar bir necha veb-dasturlash ekspertlari ishtirokida yoziladi, bu esa xakerlarning keyinchalik o'z hujumlari uchun foydalanishi mumkin bo'lgan xatolar, ehtimolini oshiradi. Shuning uchun maxsus forumlarda, masalan, antichat.ru da skript haqida fikrlarni bilish ortiqcha bo'lmaydi. Tayyorlangan skriptning ishonchliligining yaxshi ko'rsatkichi ham

uning mavjudligi va ko'plab boshqa saytlarda uzoq muddatli ishlashi bo'ladi.

Agar siz ssenariylarni mustaqil o'zingiz yozayotgan bo'lsangiz, ularning xavfsizligini ta'minlashga e'tibor bering. Misol uchun, formalardan ma'lumotlarni yuborish va qabul qilish bilan ishlaydigan buyruq fayllarida (POST usuli va GET usuli qo'llaniladi) har doim foydalanuvchi tomonidan kiritilgan ma'lumotlarni filtrlash. Bu ish bajarilmaganda, xaker forma orqali zararli javascript kodni yuborishi mumkin. Shunday qilib, xaker sizning cookie fayllaringizga kira oladi yoki sahifani ishlamaydigan holga keltiradi. Bunday hujum XSS deb ataladi.

Ayniqsa, foydalanuvchi ma'lumotlariga asoslangan ma'lumotlar bazasi bilan bog'langan skriptni diqqat bilan tekshirib ko'rishingiz kerak. Xaker sizning web-saytingiz serveriga biron-bir faylni yuklash imkoniyatini qo'lga kiritsa, unda o'zi xohlagan amalni qila oladi.

Afsuski gap DDoS-hujumlari haqida ketganda, mustahkam saytlar deyarli mavjud emasdir. DDoS hujum-saytingizga ko'p sonli kompyuter bilan bir vaqtning o'zida ko'plab so'rovlarni jo'natishni boshlaydi. Server bunday so'rovlarni bajarolmaydi va sayt ishlamay qoladi. Bundan tashqari, skript juda "beso'naqay" bo'lsa, saytni juda ko'p so'rovlarsiz "to'xtatib qo'yish" mumkin.

Veb-serverlar xavfsizligi darajasi

Tarmoq himoyasini murakkabligi bo'yicha olti darajaga bo'lish mumkin:

Birinchi daraja-eng elementar va majburiydir. Bu yerda asosiy xavfsizlik vositasi - firewall hisoblanadi. Firewall foydalanuvchilarga taqdim etilgan xizmatlardan foydalanishni cheklashi kerak. Shuningdek, firewall barcha, biridan boshqasiga ulanishlarni nazorat qilishi lozim. Bu yerda kelib chiqishi noaniq bo'lgan DT o'rniga, litsenziyalangan dasturiy ta'minotlardan foydalanish maqsadga muvofiq. Bu sizning ma'lumotlaringizni himoya qilishning eng zamonaviy "qal'asi"dir. Ushbu bosqichda ko'pgina xavflarni yo'q qilish mumkin.

Ikkinchi daraja-web-server ishlaydigan operatsion tizim konfiguratsiyasini nazarda tutadi. Har bir operatsion tizim xavfsizlik

nazorat ro'yxatlarini yaratishga imkon beradi. Ushbu o'rnatishlar kompaniya bilan hamkorlik qiladigan ishlab chiqaruvchilarning operatsion tizimlari bilan muvofiqlashtirilgan bo'lishi kerak.

Uchinchi daraja-tarmoqqa yo'naltirilgandir. Xosting ta'minoti provayderlari tarmoq uskunalarini hujum datchiklarini va DT bilan jihozlash zarur. Eng muhimi, xavf haqida olingan signal to'g'ri qayta ishlanishi va zararsizlantirilishi kerak.

To'rtinchi daraja-xosting darajasidagi DT larni o'rnatish. Bu juda murakkab vazifa. Birinchidan, o'z xosting kompaniyangiz bilan qarshiliklarga duch kelishingiz mumkin. Ikkinchidan, bunday dasturiy ta'minot oddiy datchiklardan ko'ra ancha murakkab. Shuning uchun xavfsizlik darajasi ham yuqori.

Beshinchi daraja-ikki A va B daraja ostiga ega. 5A darajasi-web-server operatsion tizimi va barcha ilovalar o'rtasida qatlamlash rolini bajaradigan maxsus dasturiy ta'minot o'rnatishga yo'naltirilgan. Bunday bufer xakerlarga barcha operatsion tizimni bajarilishi vaqtida ilova zaifliklariga qilinadigan hujumlarni oldini oladi. Bu avvalgi darajadagi web-server ustunligini ta'minlovchi DT qo'llashi lozim bo'lgan ancha serxarajat variantidir. 5B darajasi-muayyan ilovaga firewall yoki proksi serverlarni o'rnatishga yo'naltirilgan. Ular HTTP protokoli haqida qayg'uradi va potentsial tajovuzkorlarning web-serverda o'rnatilgan ilovalarni ishga tushirishga muvaffaq bo'lishidan oldin hujumlarni oldini olishga imkon beradi. Biroq proksi-server bu operatsiyaning muhim cheklovidir. Proksi konfiguratsiyasi va sozlamalari ham bir san'atdir.

Oltinchi daraja-xavfsizlikning o'ziga xos yuqori turidir. Bu yerda faqat ishonchli operatsion tizimlar va ularning nazorati ostida ishlaydigan ilovalarga ruxsat beriladi. Boshqacha qilib aytadigan bo'lsak, barcha amaldagi ilovalar va operatsion tizimlar kompaniyaning muayyan ehtiyojlari uchun maksimal ravishda moslashtirilishi yoki ishlab chiqilishi kerak. Bu eng qimmat, lekin ayni paytda himoya qilishning eng samarali usulidir. Bundan tashqari, tarmoq boshqaruvchisidan maxsus tayyorgarlik va ko'pincha foydalanuvchilardan qo'shimcha sarf xarajatlarni talab qiladi. Har

qanday dasturiy yangilanish ishonchli tizimga integratsiyalashuvni talab qiladi.

6.6. DoS va DDoS hujumlariga qarshi kurashish usullari

Quyidagi sabablarga ko'ra DDoS hujumlaridan himoyalanish murakkabdir:

Tabiiy tarmoq zaifliklari. Birinchidan, bu holda jinoyatchilar tomonidan ishlatiladigan tarmoq zaifliklari mavjud emas. Hujum muvaffaqiyatli bo'ladi, chunki barcha kompyuter platformalarining tabiatida yetkazib berishning aniq chegarasi mavjud. Kompyuterlar, klasterlar yoki bulutli tizimlar, muayyan vaqt ichida ishlashi mumkin bo'lgan so'rovlar soni bo'yicha jismoniy cheklovlarga ega. Muvaffaqiyatli DDoS hujumi faqat shu bo'shliqni to'ldirish uchun yetarlicha trafikni yaratishi kerak. Boshqa hujumlarning aksariyati maxsus patchlar, xavfsizlik tizimlarining konfiguratsiyasi yoki siyosatdagi o'zgarishlardan foydalanishi mumkin. Ammo ushbu yondashuvlarning hech biri DDoSga qarshi bardosh bera olmaydi. Xizmatlar har doim mavjud bo'lishi lozim, demak, ular hujumga qarshi himoyasizdir.

Tartibsizlikni cheklashdagi imkonsizlik. Hujum manbaining ko'pligi bois DDoS hujumini to'sish juda qiyin. Son jihatidan bir nechta bo'lgan IP-adreslar hujumini bloklashni ta'minlash juda murakkab. Hujumni to'xtatish uchun minglab manzillar vaqtincha qora ro'yxatga qo'shilishi kerak. Tajovuzkor qonuniy xostlarni butunlay hujumga qamrab oladigan usulini (spoofing) qo'llagan holda, aybsiz xostlar ham qora ro'yxatga kiritilishi mumkin.

Aybdorni qidirish. Bu yerda biz uchinchi muammoga duch kelamiz: qaysi foydalanuvchilarning qonuniy so'rovlarni amalga oshirishi va qaysilari DDOSda ishtirok etayotganini aniqlash juda qiyin. Ushbu xizmatlardan foydalanuvchi barcha kompyuterlar serverga yuklamani oshiradi, chunki ularning hammasi bilmagan holda hujumga ishtirok etadi. Qaysi mijozlar xostlarining "yaxshi" va "yomon" ekanligini aniqlash uchun juda ehtiyotkorlik bilan tekshirish kerak. Har

qanday qaror qabul qilinishidan oldin siz ko‘p hisob-kitoblarni amalga oshirishingiz va ularni tezda bajarishingiz kerak.

Kuchli DDoS hujumi qurbon Internet-kanalining barcha imkoniyatlarini ishga solishi mumkin, shuning uchun bu muammo buzg‘unchilar tomonida hal etilmaydi: samarali himoya qilish faqat operator aloqa darajasida ta’minlanishi mumkin. Internet Umbrella doimo himoyalangan tarmoq uchun turli xil trafik profillarining ortiqcha zichlik darajasini kuzatib boradi va uni standart trafik qiymatlari bilan taqqoslaydi.

DDoS hujumiga duch kelganda qo‘llanilishi lozim bo‘lgan, chora-tadbirlar ro‘yxati.

1.Hujum sodir bo‘lganligiga ishonch hosil qiling.

2.DNS noto‘g‘ri konfiguratsiyasi, marshrutlash muammolari va inson faktori kabi umumiy sabablarga ko‘ra to‘xtab qolishining oldini olish.

3.Texnik mutaxassislarga murojaat qiling. Texniklar yordamida qanday resurslarga hujum qilinganligini aniqlang.

Ilovalarning ahamiyatini belgilash. Eng ustuvor dasturlarni saqlab qolish uchun ustuvorlikni belgilang. Yuqori DDoS-hujumlar va cheklangan resurslar sharoitida asosiy daromad manbalarini ta’minlaydigan ilovalarga e’tibor qaratish lozim.

Masofaviy foydalanuvchilarni muhofaza qiling. Biznesingiz faoliyatini ta’minlang: oq ro‘yxatga ishonchli masofali foydalanuvchilarning IP-manzillarini kiritish va ushbu ro‘yxatni asosiy qilish. Ushbu ro‘yxatni onlayn tarzda tarqating va xizmat ko‘rsatuvchi provayderlarga kirish uchun uni yuboring.

Hujum sinfini aniqlang. Siz qanday hujumga duch keldingiz: Keng? Past kuchli va sekin? Sizga xizmat ko‘rsatuvchi provayderingiz hujumning miqyosi haqida xabardor qiladi.

Hujum manbalarining manzillari bilan bog‘liq variantlarni ko‘rib chiqing. Murakkab hujumlar bo‘lsa, sizning xizmat ko‘rsatuvchi provayderingiz manbalar sonini aniqlay olmaydi. Tarmoqlararo ekran yordamida IP-manzillarning kichik ro‘yxatlarini bloklang. Katta hujumlar geolokatsiya ma’lumotlari asosida bloklanishi mumkin.

Dastur darajasida hujumlarni bloklash. Zararli trafikni aniqlang va ma'lum vosita tomonidan yaratilganligini tekshiring. Sizning mavjud yechimlaringiz bilan ta'minlanishi mumkin bo'lgan qarshi chora-tadbirlar yordamida har bir alohida holat uchun dastur darajasida ma'lum hujumlar bloklanishi mumkin.

Himiya perimetrini kuchaytirish. 7-darajali assimetrik DDoS hujumiga duch kelgan bo'lishingiz mumkin. Dastur darajasida himoyaga e'tibor bering: login tizimlari, shaxsni aniqlash tizimi yoki haqiqiy Real Browser Enforcement texnologiyalaridan foydalaning.

Tarmoq resurslarini cheklash. Agar avvalgi chora-tadbirlar yordam bermagan bo'lsa, unda resurslarni cheklash kerak-bu bilan "yomon" va "yaxshi" trafik cheklangan bo'ladi.

Jamoatchilik bilan aloqalarni boshqarish. Agar hujum ommaviylashgan bo'lsa, rasmiy bayonot tayyorlang va xodimlarni xabardor qiling. Siyosat darajasida ko'rib chiqiladigan hujum bo'lganda zarur bo'lsa, hujumni tasdiqlang. Agar bo'lmasa, texnik murakkabliklarga murojaat qiling va barcha masalalarni jamoatchilik bilan aloqalar boshlig'iga yo'naltirish uchun xodimga maslahat bering.

DoS hujumi ko'rinishidagi tahdidlarni uch tarzda kamaytirish mumkin:

Anti-spoofing xususiyatlari-Router va tarmoqlararo ekran anti-spoofing xususiyatlari to'g'ri konfiguratsiyalash DoS hujumi xavfini kamaytirishga yordam beradi. Ushbu funktsiyalar, hech bo'lmaganda, RFC 2827 filtrlashni o'z ichiga olishi kerak. Agar xaker o'zining haqiqiy identifikatsiyasini yashira olmasa, u hujum qilishga qaror qilishi mumkin emas.

Anti-DoS funktsiyalari-Router va tarmoqlararo ekran Anti-DoS funktsiyalarini to'g'ri konfiguratsiyalash hujumlarning samaradorligini cheklashi mumkin. Ushbu funktsiyalar vaqtning ixtiyoriy onida yarim ochiq kanallarning sonini cheklaydi.

Trafik hajmining chegaralanganligi (traffic rate limiting)-tashkilot trafik miqdorini cheklash uchun provayderga murojaat qilishi mumkin. Ushbu turdagi filtrlash tarmog'ingiz orqali o'tadigan zararsiz trafik miqdorini cheklash imkonini beradi. Misol tariqasida faqat tashxislash

maqsadida ICMP trafigi miqdorini cheklash mumkin. DoS hujumlari odatda ICMP dan foydalanadi.

Afsuski, DDoS hujumlaridan himoyalanishning universal choralari hamon mavjud emas. Bu apparat, dasturiy ta'minot va hatto tashkiliy xarakterga ega bo'lgan kompleks yondashuvni talab qiladi.

Tarmoqdagi ulkan Cisco kompaniyasining dasturiy va apparat tizimlari eng samarali hisoblanadi, ammo ular siz uchun kerakli narsalarni yaratishi kerak.

IIS serverlarini himoya qilish uchun siz Microsoft (dasturiy ta'minot) yechimlardan foydalanishingiz mumkin, ammo bu kompaniyaning saxiyligini bilgan holda, ular ham bepul emasligini taxmin qilishingiz mumkin.

Ayni paytda maxsus DDoS hujumlari daromadli va faol rivojlanayotgan tarmoqdagi jinoyatchilikka aylandi. Google-da qidirish asosida siz "mutaxassislar" tomonidan yaratilgan raqobatchilar saytini yo'q qilishda yordam beruvchi o'nlab dasturlarni topishingiz mumkin.

DDoS dan himoya qilishning asosiy tamoyillari qanday?

1) Avvalo, ortiqcha (saytingizga) jamoatchilik e'tiborini radikal jalb qilmaslik, har qanday odamlarning irqiy, milliy va diniy e'tiqodlariga putur yetkazadigan kontentni e'lon qilmaslik lozim.

2) Agar siz "buyurtma" yoki oldindan e'tirof etilgan ko'rsatmalarni e'tiborsiz qoldirgan bo'lsangiz, unda web-serverning apparat-resurslaridan bir necha bor rezervlashni amalga oshirish hamda, taqsimlangan va ikkilamchi tizimlarni qurish maksimal samarali bo'lishini ta'minlaydi. DDoS hujumlarini amalga oshirish uchun zararli kod bilan zararlangan juda ko'p sonli kompyuterlar ishlatiladi. Ushbu kompyuterlar botnetlarda (zombi mashinalarining tarmoqlari) birlashtiriladi, bu esa odatda kompyuter egalari bexabar bo'lgan tajovuzkorning buyrug'i ostidagi DDoS-hujumlarini amalga oshirilishiga olib keladi.

3) DDoS hujumidan dasturiy ta'minot sathida himoyalanish mumkin. Buning uchun sizga bepul DDoS Deflate skripti yordam beradi. Shu bilan siz kichik bosqin va DDoS dan osongina xalos bo'lishingiz mumkin. Skript DDoS va bosqinni aniqlash uchun "netstat" buyrug'idan foydalanadi va so'ngra iptables yoki apf xavfsizlik firewalli yordamida zararkunandalarning IP manzillarini bloklaydi. Shuni unutmaslik kerakki, har qanday zaif DDoS hujumi server faoliyatiga raxna solishga qodir. Misol tariqasida, faraz qilaylik, hujum qiladigan zombi mashinalari 10-50 tani tashkil etib, ularning barchasi keng kanallarga ega, siz komandirovkada yoki o'nlab (yoki hatto yuzlab) serverlar bilan ishlayotganingizda, bularning barchasini himoya tizimini rostlash uchun sizda jismonan quvvat yetishmaydi. Bunday holatda, hatto kam sonli mashinalar ham aloqa kanalini "band qilishi" yoki Apache, mysql va boshqa web-serverlarni ishdan chiqarishi mumkin. Boshqacha qilib aytganda, ma'mur serverni uzluksiz "kuzatib borish" asosida hujumlarni osongina aniqlay oladi. Ammo, bu signalizatsiya tizimini va hujum qiluvchi zombi mashinalarini blokirovka qilish jarayonini avtomatlashtirishni talab etiladi.

Savol tug'iladi, himoyalanish qanday amalga oshiriladi?

1) Agar sizda server mavjud bo'lsa, unda sizga nisbatan qilingan hujumni aniqlash vositalariga ega bo'lishingiz lozim. Saytingiz bilan bog'liq muammolar mavjudligini oldindan aniqlash, sodir bo'lishi mumkin bo'lgan, DDoS hujumini qisqa muddatda bartaraf etish choralarini ko'rishni ta'minlaydi.

2) DDoS kiruvchi trafikning profil mexanizmini qo'llash orqali aniqlanishi mumkin. Agar siz serveringizdagi trafik o'zgarishlarining o'rtacha miqdori va dinamikasini bilsangiz, xarakteristik bo'lmagan o'zgarishlarni tezda aniqlab olishingiz mumkin. Ko'pgina DDoS hujumlari olingan trafik miqdori keskin oshishi bilan tavsiflanadi va profil mexanizmi bu o'tishning hujum yoki yo'qligini aniqlashga yordam beradi.

3) O'tkazuvchanlik qobiliyatini oshiruvchi qo'shimcha aloqa kanallari. Qo'shimcha aloqa kanallarini qo'llash, hatto tarmoq kengligi hisob-kitoblari sizni qoniqtirmagan holda ham foydadan xoli bo'lmaydi. Bunday holatda, masalan, reklama kampaniyasining natijalari, maxsus takliflar yoki ommaviy axborot vositalarida kompaniyangiz haqida tilga olinishi mumkin bo'lgan yoki kutilmagan trafik yuklamalarini bartaraf etishingiz mumkin. DDoS hujumi amalga oshirilganda tarmoq kengligining zaxirasi 500% ni tashkil etishi, muammolarni bartaraf etmasa-da, sizning zaruriy choralarni ko'rishingiz uchun bir necha qo'shimcha daqiqalarni beradi.

4) Tarmoq perimetri muhofazasi (xususiy serveringiz bo'lganda).

Hujum samaradorligini qisman qisqartirish, ayniqsa, uning boshlanishida bir nechta oddiy texnik chora-tadbirlar mavjud:

• serverning ortiqcha yuklanishini oldini olish uchun router o'tkazish qobiliyatini cheklang;

• marshrutizator ayni hujumkor manzillaridan kelayotgan paketlarni rad qilishi uchun qo'shimcha filtrlarni qo'llang;

• yarim ochiq ulanishlar uchun taym-autni yanada qat'iy qilib sozlang.

• soxta va buzilgan paketlarni rad eting;

• SYN, ICMP va UDP ni ishlov berishning xato chegarasini pastroq bo'lishini belgilang.

Ammo haqiqat shundaki, agar ilgari bu qadamlar yetarlicha samarali bo'lgan bo'lsa, endilikda DDoS hujumlarini ushbu usullar bo'yicha tenglashtirish o'ta globaldir.

Birinchi qadam internet-provayderingizga (yoki sizning resursingiz uchinchi tomonning serverida joylashgan bo'lsa, xosting provayderiga qo'ng'iroq qilish) va hujum bilan bog'liq darhol yordam so'rash. Provayderingiz kontakt ma'lumotlari favqulodda holatlarda uni qidirish vaqtini yo'qotmaslik uchun har doim qo'l ostida bo'lishi lozim. Hujum miqyosiga qarab ular allaqachon xabardor bo'lishi mumkin.

Siz foydalanadigan server kompaniyangizda emas balki, xost-markazda joylashgan joylashgan bo'lsa, DDoS hujumiga qarshi turish imkoniyati oshib boradi, chunki ma'lumotlar markazlari juda yaxshi jihozlar va aloqa kanallari, shuningdek, bunday hujumlarni ko'proq biladigan tajribali xodimlarga ega. Bundan tashqari, agar sizning serveringiz ma'lumotlari qayta ishlash markazida joylashgan bo'lsa, sizga hujum qilganda korporativ tarmoq zarar ko'rmaydi, shuning uchun hech bo'lmaganda biznesingizning bir qismi, masalan, elektron pochta va VoIP xizmati an'anaviy tarzda ishlashi kerak.

Hujum yetarlicha kuchli bo'lganda, birinchi navbatda sizning Internet provayderingiz web-serveringizga yo'naltirilgan trafiklarni cheklab qo'yadi.

"Ichki korporativ DDoS-hujumlari provayderlar uchun ortiqcha noqulayliklar keltirib chiqaradi, chunki DDoS tarmoq kengligining ko'p qismini band qilishi va boshqa mijozlarning dasturlari faoliyatiga salbiy ta'sir ko'rsatishi mumkin.

6.1-jadval

OSI 7-sathi: Amaliy

Ma'lumot turi	Ma'lumotlar
Saht tavsifi	Ma'lumot paketlarini yaratish boshlanadi. Ma'lumotlarga kirish va ulanish. FTP, SMTP, Telnet, RAS foydalanuvchi protokollari
Protokollar	FTP, HTTP, POP3, SMTP va ulardan foydalanadigan shlyuzlar
DoS texnologiyasi misollari	PDF GET so'rovlari, HTTP GET, HTTP POST (web-sayt shakllari: login, foto / video yuklash, qayta aloqani tasdiqlash)
DDoS hujumlarining oqibatlari	Resurs yetishmovchiliklari. Hujumkor serverda xizmatlarning tizim resurslaridan ortiqcha sarflanishi.

Internet OSI modelidan foydalanadi. Umuman olganda, ushbu model barcha aloqa vositalarini qamrab oluvchi 7 sathga ega: jismoniy

muhitdan boshlanib (1-sath), ilovalarning bir-biri bilan "muloqot qilish" sathi (7-sath) bilan yakunlanadi.

DDoS hujumlari yetti sathning har birida kuzatilishi mumkin. Quyida ularni batafsilroq ko'rib chiqamiz.

Nima qilish kerak: DTni tizimli monitoring qilish oday dastur zaifliklarini aniqlash uchun o'ziga xos algoritmlar, texnologiyalar va yondashuvlar to'plamini (ushbu dastur ishlatilgan platformaga bog'liq holda) ishlatadigan dasturiy ta'minotni muntazam ravishda monitoring qilish zarur. Bunday hujumlarni aniqlash orqali, ularni bir marta va doimiy ravishda to'xtatish va ularning manbasini izlab topish mumkin. Bu ushbu qatlamda o'ta sodda tarzda amalga oshiriladi.

6.2-jadval

OSI 6-sathi: Ijrochi

Ma'lumot turi	**Ma'lumotlar**
Saht tavsifi	Resursdan qabul qiluvchiga ma'lumotlarni translyatsiyalash
Protokollar	Ma'lumotlarni siqish va kodlash protokollari (ASCII, EBCDIC)
DoS texnologiyasi misollari	SSL spoof so'rovlari: shifrlangan SSL paketlarini skanerlash, tajovuzkorlar SSL dan qurbonning serverida HTTP hujumlar uchun foydalanadi
DDoS hujumlarining oqibatlari	Tajovuzkor tizimlar SSL ulanishlarini qabul qilishni to'xtatishi yoki avtomatik ravishda qayta ishga tushishi mumkin

Nima qilish kerak: Zararni kamaytirishda, taqsimlangan SSL shifrlash infratuzilmasi (masalan, imkon qadar katta serverda SSL-ni joylashtirish) va dastur platformasida hujumlar yoki qoidalar buzilganligi dastur trafigini tekshirish kabi vositalarga e'tibor berish kerak. Yaxshi platformalar trafik shifrlanganligini va xavfsiz bastion tugunning himoyalangan xotirasida saqlangan deshifrlangan kontent bilan dastlabki infratuzilmaga qaytarilishini kafolatlaydi.

6.3-jadval

OSI 5-sathi: Seansli

Ma'lumot turi	Ma'lumotlar
Saht tavsifi	Ulanishni o'rnatish va bekor qilishni boshqarish, operatsion tizimda tarmoq orqali aloqa sessiyalarini sinxronlash (masalan, kirish/chiqishni amalga oshirganda)
Protokollar	Kirish/chiqish protokollari (RPC, PAP)
DoS texnologiyasi misollari	Telnet protokoli hujumi serverdagi Telnet server dasturining zaif nuqtalaridan foydalanadi, bu esa serverga kirish imkoniyatini bermaydi
DDoS hujumlarining oqibatlari	Administratorning svitchni boshqarishini imkonsiz qiladi

Nima qilish kerak: Tahdid xavfini kamaytirish uchun dasturiy ta'minotni yangilanishini qo'llash kerak.

6.4-jadval

OSI 4-bosqich: Transport

Ma'lumot turi	Segmentlar
Saht tavsifi	1dan 3 darajagacha bo'lgan xabarlarni uzatishni boshqaruvchi, tugunlar orasidagi ma'lumotlarni uzatishda xatolikka yo'l qo'ymaslik
Protokollar	TCP, UDP protokollari
DoS texnologiyasi misollari	SYN-flood, Smurf-hujum (o'zgartirilgan manzillar bilan ICMP-so'rovlariga hujum)
DDoS hujumlarining oqibatlari	Kanal kengligi yoki ruxsat etilgan ulanishlar soni chegaralariga erishish, tarmoq uskunalari uzilishi

Nimani qilish kerak: DDoS-trafikni filtrlash, blackholing sifatida tanilgan-mijozlarni himoya qilish uchun ko'pincha provayderlar tomonidan ishlatiladigan usul (biz o'zimiz bu usulni ishlatamiz). Ammo, bu yondashuv, mijozning saytini tajovuzkor va ruxsat etilgan

foydalanuvchi trafiklari uchun ham cheklaydi. Biroq, DDoS hujumlariga qarshi kurashishda provayderlar iste'molchilarni tarmoq uskunalari ishini susaytirish va xizmatlarni inkor etish orqali kirishga cheklovlar o'rnatish bilan tahdidlardan himoya qilishda foydalanadi.

6.5-jadval

OSI 3-bosqich: Tarmoq

Ma'lumot turi	**Paketlar**
Saht tavsifi	Turli tarmoqlar aro ma'lumotni boshqarish va uzatish
Protokollar	Protokollar IP, ICMP, ARP, RIP va ularni ishlatadigan router
DoS texnologiyasi misollari	ICMP flood-DDos maqsadli tarmoq to'la o'tkazuvchanligini qayta yuklash uchun ICMP xabarlaridan foydalangan, OSI modeli uchinchi sathi hujumlari
DDoS hujumlarining oqibatlari	Tajovuz qilingan tarmoq o'tkazuvchanlik qobiliyatining pasayishi va xavfsizlik brandmauerining qayta yuklanish ehtimolligi

Nima qilish kerak: ICMP protokoli orqali ishlov beriladigan so'rovlar sonini cheklash va trafikning Firewallning ish tezligi va Internet polosasi o'tkazuvchanlik qobiliyatiga ta'sir etuvchi trafikni kamaytirish lozim.

6.6-jadval

OSI 2-bosqich: Kanal

Ma'lumot turi	**Kadrlar**
Saht tavsifi	Xabarlarni jismoniy darajada uzatilishini o'rnatish va kuzatish
Protokollar	802.3, 802.5 protokollari, shuningdek, ularni ishlatadigan nazorat qurilmalari, kirish nuqtalari va ko'priklar mavjud
DoS texnologiyasi misollari	MAC Flood-Tarmoq Switchlari ma'lumot paketlarini to'ldirish
DDoS hujumlarining oqibatlari	Yuboruvchidan qabul qilinuvchi barcha ma'lumot oqimlari portlarning ishlashini bloklaydi.

Nima qilish kerak: Ko'pgina zamonaviy switchlar MAC manzillari sonini serverda autentifikatsiya, avtorizatsiya va hisoblash (AAA protokoli) bilan tasdiqlangan va keyinchalik filtrlangan ishonchli bo'lganlar bilan cheklangan tarzda tuzilishi mumkin.

Nima qilish kerak: Jismoniy tarmoq qurilmalarining ishlashini monitoring qilish uchun tizimli yondashuvdan foydalaniladi.

6.7-jadval

OSI 1-bosqich: Jismoniy

Ma'lumot turi	**Bitlar**
Saht tavsifi	Ikkilik ma'lumotlarni uzatish
Protokollar	Protokollar 100BaseT, 1000 Base-X, shuningdek, ularni ishlatadigan uyalar, soket va patch paneli
DoS texnologiyasi misollari	Jismoniy zararlanish, jismoniy ishga to'siq yoki jismoniy tarmoq aktivlarini boshqarilish
DDoS hujumlarining oqibatlari	Tarmoq uskunalari yaroqsiz holga keladi va ishni davom ettirish uchun ularni tamirlash kerak bo'ladi

Shunday qilib, hujumlardan himoyalanishda, asosiy himoya mexanizmlari tadbiq etilgan va quyidagi komponentlardan tarkib topgan kompleks himoya vositalaridan foydalanish lozim:

• himoya perimetri deb ataluvchi, mudofaaning birinchi chizig'i bo'lgan, tarmoqlar aro ekran va tadbiq etiluvchi kompleks himoya vositalari.

• himoya vositasi samaradorligini baholash va uzellar, protikollar, xizmarlar himoyalanganligini tahlil qilishda foydalaniluvchi vositalar.

• real vaqt rejimida monitoring qiluvchi, hujumni aniqlash vositalari.

6.7. Simsiz tarmoqlarni himoya qilish usullari

Simsiz tarmoqlarni himoya qilishning quyidagi usullari mavjud:

1. MAC-manzilni filtrlash.

Filtrlash uch usulda amalga oshiriladi:

- kirish nuqtasi istalgan MAC manzilli stansiyalarga kirish imkonini beradi;

- kirish nuqtasi faqat MAC manzillari oq ro'yxatga kiritilgan stansiyalarga kirishni ta'minlaydi;

- kirish nuqtasi faqat MAC manzillari "qora ro'yxat"ga joylashgan stansiyalarga kirishni rad etadi.

2. SSID yashirin identifikator tartibi (ingl. Service Set IDentifier):

O'zini aniqlash uchun kirish nuqtasi muntazam ravishda mayoq kadrlarini yuboradi. Har bir kadr aloqaning xizmat ko'rsatish ma'lumotlarini, xususan, SSIDni o'z ichiga oladi (simsiz tarmoq identifikatori). Yashirin SSID holida ushbu maydon bo'sh, ya'ni simsiz tarmoqni aniqlab bo'lmaydi va SSID qiymatini bilmasdan unga ulanib bo'lmaydi. Biroq, kirish nuqtasiga ulangan barcha stansiyalar ulanish pfofillari o'z ichiga olgan tarmoqdagi identifikatorlarni ko'rsatuvchi Probed Request so'rovlarini yuborib SSID ni bilib olishlari mumkin. Ishchi trafikni tinglab, kerakli kirish nuqtasiga ulanish uchun SSID qiymatini osonlik bilan qo'lga kiritish mumkin.

3. Wired Equivalent Privacy (WEP)-Wi-Fi tarmoqlari xavfsizligini ta'minlash algoritmi.

U simsiz tarmoqda avtorizatsiyalangan foydalanuvchilarga uzatiladigan ma'lumotni konfidensialligi va tinglashdan himoyalashni ta'minlashda foydalaniladi. WEPning ikkita turi mavjud: WEP-40 va WEP-104, ular faqat kalit uzunligi bilan farq qiladi. Hozirgi kunda ushbu texnologiya eskirgan, chunki uni bir necha daqiqada buzish mumkin. Biroq, shunga qaramasdan undan keng qo'llanilmoqda. Wi-Fi tarmoqlari xavfsizlik masalalari uchun WPA tavsiya etiladi.

4. WPA va WPA2 (Wi-Fi Protected Access)-bu simsiz aloqa qurilmalari uchun yangilangan sertifikatlash dasturi. WPA texnologiyasi WEP tarmog'ining simsiz Wi-Fi xavfsizlik texnologiyasining o'rnini bosdi. WPA afzalliklariga ma'lumotlar xavfsizligi va simsiz tarmoqlarga kirish nazoratini mukammalligi kiradi. Muhim xususiyati, ham apparat, ham dasturiy ta'minot sathida bir nechta simsiz qurilmalar o'rtasidagi moslik hisoblanadi.

5. Autentifikatsiya.

WPA va WPA2 parolini buzish, ayniqsa, AES shifrlashdan foydalanganda ancha murakkab va ko'p sarf-xarajatni talab etadi, lekin buni mumkinligini inkor etib bo'lmaydi. Ushbu tahdiddan himoyalanish uchun autentifikatsiyalash kerak. Autentifikatsiyalash mijoz kompyuterini tarmoqda ro'yxatga olinishini talab qiladigan yana bir xavfsizlik darajasini qo'shadi. An'anaga ko'ra, bu sertifikatlar, nishonlar yoki parollar (PreShared-Key sifatida ham tanilgan) yordamida amalga oshiriladi, ular autentifikatsiya serverida tekshiriladi.

6. O'zi-o'zini himoya qilish.

Tarmoqni ishlatmayotgan paytda o'chiring! Kirish nuqtasini o'chirib qo'yish- ko'pincha, foydalanuvchilar himoyalanishning eng qulay usullarini e'tiborsiz qoldiradilar. Hech qanday simsiz tarmoq yo'q ekan, demak, hech qanday muammo ham yo'q.

12345678, 11111111 va shunga o'xshash parollarni hech qachon qo'ymasligingiz kerak, masalan, shaxsiy ma'lumotlaringizni yoki oila a'zolaringizni, masalan, telefon raqamini, pasportlarning seriya raqamlarini, tug'ilgan kunini, xonadon raqamini va boshqalarni parol sifatida foydalanmang. Parolni kamida oyiga bir marta o'zgartirganingizga ishonch hosil qiling.

Bundan tashqari, ruxsatsiz kiruvchi foydalanuvchilarni cho'chitish uchun tarmog'ingiz nomini o'zgartirish, masalan, virus.exe, mvd-bo'lim_24 kabi qo'shimchalar himoya darajasini oshirishi mumkin.

Albatta, siz professional xakerlarga qarshi o'zingizni himoya qila olasiz, ammo u oddiy o'g'rilar va havaskorlarga qarshi shaffof ishlaydi.

Asosiy xulosalar

Hujumlarni aniqlash tizimlari qurilish texnologiyalari bo'yicha ikkita toifaga bo'linadi: anomaliyani aniqlash va jinoyatni aniqlash.

Hujumlarni aniqlashga qaratilgan yana bir yondashuv – bu namuna (pattern) yoki signatura (signature) bo'yicha hujumni tariflash va nazoratlanuvchi hududda (tarmoq trafigi yoki log) ma'lum bir namunani qidirishdir.

Intrusion Detection System (IDS) - kompyuter tizimi yoki tarmog'iga ruxsatsiz kirishni (buzib kirish yoki tarmoq hujumi) aniqlash uchun mo'ljallangan dasturiy yoki apparat ta'minotdir.

Tarmoq darajasidagi hujumlarni aniqlash tizimining afzalliklari: ekspluatatsiya narxining pastligi, tizim darajasida o'tkazib yuborilgan hujumlarni aniqlash, xaker o'z faoliyati izlarini yashirishi ancha murakkab, real vaqtda aniqlash va javob qaytarish, muvaffaqiyatsiz hujumlar yoki shubhali xatarlarni aniqlash, OTdan mustaqilligi.

Tarmoqni himoya qilishga yordam beradigan turli himoya vositalari:

Dasturlar uchun tuzatmalarni tezkor o'rnatish, virus va troyan otlarini aniqlash, tarmoqlararo ekran, kriptoparollar, shifrlash, zaif nuqtalar skanerlari, xavfsizlik nuqtai nazaridan kompyuterlarning to'g'ri konfiguratsiyasi, hujumkor dialer, xavfsizlik intsidentlarini tergov qilish guruhi, xavfsizlik bo'yicha tavsiyalar, hujumlarni aniqlash vositalari, tarmoq topologiyasini aniqlash vositalari va port skanerlari, xavfsizlik siyosati, xavfsizlik devori va WWW-serverlarni blokirovka qilishga urinish barqarorligini testlash.

Ayni paytda, masofadan turib hujumlarni oldini oluvchi quyidagi tizimlar keng tarqalgan:

TE, dasturiy va apparat ta'minot asosida amalga oshiriladi;

kriptoprotokollar;

apparat va dasturiy tarmoq trafiki analizatorlari;

Kompyuter tizimining imkoniyati, qulayligi, tezligi va funksionalligi tamoyillari xavfsizlikning tamoyillariga zid keladi.

Tarmoq himoyasini murakkabligi bo'yicha olti darajaga bo'lish mumkin.

Afsuski, DDoS hujumlaridan himoyalanishning universal choralari hamon mavjud emas. Bu apparat, dasturiy ta'minot va hatto tashkiliy xarakterga ega bo'lgan kompleks yondashuvni talab qiladi.

Nazorat savollari

1. Hujumlarni aniqlash tizimlari qurilish texnologiyalari bo'yicha qanday turlarga bo'linadi?

2. *Hujumlarni aniqlash tizimi nima?*

3. *Tarmoq sathida hujumlarni aniqlash tizimi afzalliklari nimada?*

4. *Ko'p sonli kompyuter hujumlaridan qanday himoyalanish mumkin?*

5. *Tarmoq trafigini tahlil qilishdan qanday himoyalanish mumkin?*

6. *Soxta ARP-serverdan qanday himoyalanish mumkin?*

7. *Soxta DNS-serverdan qanday himoyalanish mumkin?*

8. *Tarmoq ma'muri soxta DNS- serverdan qanday himoyalanishi mumkin?*

9. *Xizmatdan voz kechishdan qanday himoyalanishi mumkin?*

10. *Saytni buzishdan qanday himoyalanishi mumkin?*

11. *DDoS hujumidan himoyalanishning qanday asosiy tamoyillari mavjud?*

12. *DDoS- hujumiga duch kelgandagi chora-tadbirlar ro'yxati.*

13. *Simsiz tarmoqning asosiy himoya usullarini sanab bering.*

FOYDALANILGAN ADABIYOTLAR

1. Mirziyoyev Sh.M. Tanqidiy tahlil, qat'iy intizom va shaxsiy javobgarlik har bir rahbar faoliyatida kunlik normaga aylanishi kerak. Vazirlar Mahkamasining 2016 yilda mamlakatni ijtimoiy-iqtisodiy rivojlantirish yakunlari va 2017 yilga mo'ljallangan iqtisodiy dasturning eng muhim ustuvor yo'nalishlariga bag'ishlangan kengaytirilgan majlisidagi ma'ruzasi. Sh.M. Mirziyoyev. –Toshkent: O'zbekiston, 2017. -104 b.

2. O'zbekiston Respublikasi Prezidentining 2017 yil 27 iyundagi PF-1989-sonli "O'zbekiston Respublikasining Milliy axborot-kommunikatsiya tizimini yanada rivojlantirish chora-tadbirlari to'g'risida" gi qarori.

3. O'zbekiston Respublikasi Prezidentining 2018 yil 14 martdagi PF-5379-sonli "O'zbekiston Respublikasining davlat xavfsizligi tizimini takomillashtirish chora-tadbirlari to'g'risida" gi qarori.

4. Бирюков А.А. Информационная безопасность: защита и нападение. 2-е издание, перераб. доп. – М.: ДМК Пресс, 2017, -434 с.

5. Бирюков А.А. Информационная безопасность: защита и нападение. М.: ДМК Пресс, 2016, -474 с.

6. Внуков А.А. Защита информации: учебное пособие для бакалавриата и магистратуры. –М.: Издательство Юрайт, 2017.

7. Герасименко В.А., Малюк А.А., "Основы защиты информации". М.: МИФИ, 2015 г.

8. Гордейчик С.В., Дубровин В.В. Безопасность беспроводных сетей. –М.: Горячая линия-Телеком, 2018.

9. Гордон Я. Компьютерные вирусы без секретов. - М.: Новый издательский дом, 2008 г.

10. Джей Бил. и др. Обнаружение вторжений. — М.: ООО «Бином- Пресс», 2006 г. — 656 с.

11. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации: Учебник для вузов / – М.: ООО «Издательство Машиностроение», 2009 – 508 с.

12. Казарин О.В., Забабурин А.С. Программно-аппаратные средства защиты информации: учебник и практикум для вузов. – М.: Издательство Юрайт, 2018. – 312 с.

13. Касперски К. Записки исследователя компьютерных вирусов. - СПб.: Питер, 2007 г..

14. Касперски К. Компьютерные вирусы изнутри и снаружи. - СПб.: Питер, 2008 г.

15. Масалков А.С. Особенности киберпреступлений: инструметы нападения и защиты информации. – М.: ДМК Пресс, 2018. – 226 с.

16. Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака на Internet 2-е изд., перераб. и доп. –М.: ДМК, 2013 г.

17. Нестеров С.А. Информационная безопасность и защита информации: Учебное пособие. – СПб.: Изд-во Политехнического университета, 2009. –126 с.

18. Парандовский А.А. Энциклопедия компьютерных вирусов. - М.: Солон-Р, 2010 г..

19. Петров В.П., Петров С.В. «Информационная безопасность человека и общества», издательство «Энас», 2007 г., 336 с.

20. Петраков А.В. Основы практической защиты информации. 3-е изд. Учебное пособие - М.: Радио и связь, 2001г.-368с.

21. Прохоров А. Защита присутствия в Интернете от вирусов, Компьютер Пресс 6'2005 г.

22. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 2014.

23. Сёмкин С.Н, Э. В. Беляков, С. В. Гребенев, В. И. Козачок. Основы организованного обеспечения информационной безопасности объектов информатизации. М.: Изд-во «Гелиос АРВ», 2005 г.

24. Семененко В.А., Федоров Н.В. Программно-аппаратная защита информации. – М.: МГИУ, 2007.

25. Сердюк В. А. Новое в защите от взлома корпоративных систем. –Москва: Техносфера, 2007. - 360 с.

26. Столингс В. Основы защиты сетей. Приложения и стандарты. – М.: Вильямс, 2002.

27. Хорев П.Б. Программно-аппаратная защита информации: учеб. пособие. –2-е изд., М.: ФОРУМ: ИНФРА-М, 2019. - 352 с.

28. Хорев П.Б. Методы и средства защиты информации в компьютерных системах.- М.: Академия, 2008.

29. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации (под редакцией Ковтанюка) К.: Издательство Юниор, 2003г.-504с.

30. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. Краткий курс. — Ростов-на-Дону: Феникс, 2008. -253 с.

31. Шаньгин В.Ф. «Информационная безопасность», М: ДМК Пресс, 2014 г., 702 стр.

32. Шаньгин В. Ф. информационная безопасность компьютерных систем и сетей: учеб. пособие. – М.: ИД «Форум»: Инфра-М, 2008 –416 с.

33. Щеглов А.Ю., Щеглов К.А. Защита информации: основы теории: учебник для бакалавриата и магистратуры. – М.: Издательство Юрайт, 2019. – 309 с.

34. Deborah Radcliff. Ответный удар, «Сети/network world», № 09, 2000г.

35. Himanen P., Torvalds L., Castells M. Xaker Ethic and the Spirit of the Information Age. – Random house trade paperbacks / New York, 2001.

36. Himanen Pekka. The Xaker Ethic and the Spirit of the Information Age (Prologue by Linus Torvalds and epilogue by Manuel Castells). New York: Random House, 2001.

37. Yusupov S.Yu., Medetov S.K. Application of Biometric Methods in Cryptography. 4th International Conference on Application

of Information and Communication Technologies, Tashkent, Uzbekistan, 12-14 October 2010. 107-109.

38. Юсупов С.Ю., Мухамедшина А.С. Исследование принципов и методов построения компьютерной стеганографии. Вестник ТУИТ. №4, 2011, стр.36-39.

39. Yusupov S.Yu., Abduraxmanov A.A., Qurbonov E.I. The complex Analysis of the Project of Ensuring Information Security in Communication Systems. Information Security from the Point of View of the State and the Right. International Conference in central Asia on Internet ICI 2013 "The Next Generation of Mobile, Wireless and Optical Communications Networks with Application to Information and Communication Technologies", Tashkent, Uzbekistan, 8-10 October, 2013, 110-114.

40. Yusupov S.Yu., Gulomov Sh. R., Yusupov B.K. The analysis models Formation infrastructure of information protection system. International Conference ITPA 2014 "Perspectives for the Development of Information Technologies", November 4-5, 2014, Tashkent, Uzbekistan.

41. Yusupov S.Yu., Karimova N.O. Building intrusion detection systems on cloud computing system. International Scientific Conference ITPA 2015 "Perspectives for the Development of Information Technologies", November 4-5, 2015, Tashkent, Uzbekistan.

42. Юсупов С.Ю., Самаров Х.К. Некоторые вопросы укрепления кибербезопасности в Республике Узбекистан. "Развитеие информационных технологий в Республике Таджикистан: приоритетные и инновационные направления", 29 сентября 2018 года, Душанбе, Таджикистан, стр. 177-182.

43. Юсупов С.Ю., Гуломов Ш.Р. Цифровая криминалистика: учебное пособие. –Ташкент, «Aloqachi», 2018, 284 стр.

44. Юсупов С.Ю., Ганиев А.А. Взлом и защита компьютерных систем и сетей: учебное пособие. –Ташкент, «Aloqachi», 2019, 228 стр.

SHARTLI BELGILAR VA QISQARTMALAR

APT - Advanced Persistent Threat
ARP - Address Resolution Protocol
BGP – Border Gateway Protocol
BIOS - Basic Input-Output system
CMS - Content Management System
CPE - Customer Premises Equipment
CVE - Common Vulnerabilities and Exposures
DAS - Directly Attached Storage
DLP - Data Leak Prevention
DMCA - Digital Millennium Copyright Act
DMZ - Demilitarized Zone
DNS - Domain Name System
DOS - Denial of Service
DDOS - Distributed Denial of Service
FTP - File Transfer Protocol
ICMP - Internet Control Message Protocol
IDS - Intrusion Detection System
IMEI - International Mobile Equipment Identity
ISN - International Security Network
IP - Internet Protocol Address
LAN - Local Area Network
MAC - Media Access Contro
MSIL - Microsoft Intermediate Language
NAT - Network Address Translation
OSI - Open Systems Interconnection
OSPF – Open Shortest Path First
OTP - One-Time Passwords
RIP - Routing Information Protocol
RFC - Request for Comments
RTKF - Registry Trash Keys Finder

SEAK - Social Engineering Automation Kit
SKIP - Secure Key Internet Protocol
S-HTTP - Secure HTTP
SNMP - Simple Network Management Protocol
SSID - Service Set IDentifier
SSL - Secure Socket Layer
SQL - Structured Query Language
TCP - Transmission Control Protocol
TTL - Time to live
UCITA - Uniform Computer Information Transactions Act
UDP - User Datagram Protocol
VPN - Virtual Private Network
XSS - Cross-Site Scripting
WAV- ichki vosita fayllari
WEP - Wired Equivalent Privacy
WLAN - Wireless Local Area Network
WPA - Wi-Fi Protected Access
AT – Avtomatlashtirilgan tizimlar
TE – Tarmoqlararo ekran
RK - Ruxsatsiz kirish
OT – Operatsion tizim
SHK – Shaxsiy kompyuter
DT – Dasturiy ta'minot
THT - Taqsimlangan hisoblash tizimi
AXT – Axborot xavfsizligi vositalari
KNBT - Kirishni nazoratlash va boshqarish tizimlari
TDT – Tarmoq dasturiy tamonoti
MBBT – Ma'lumotlar bazasini boshqarish tizimi
MST - Ma'lumotni saqlash tizimi
BAT - Buzilishni aniqlash tizimi
ERI - Elektron raqamli imzo

ATAMALAR LUG'ATI

Autentifikatsiya (Authentication)-bu biror narsaning haqiqiyligini tekshirish jarayoni. Ushbu atama ko'pincha axborot texnologiyalari muhitida qo'llaniladi. Foydalanuvchi kiritgan parolni server ma'lumotlar bazasida saqlanadigan parol bilan taqqoslash autentifikatsiya misoli bo'lishi mumkin.

Avtorizatsiya (Authorization)-ma'lum bir shaxsga yoki shaxslar guruhiga muayyan harakatlarni amalga oshirish huquqini berish; shuningdek, ushbu harakatlarni bajarishda ushbu huquqlarni tekshirish (tasdiqlash) jarayoni. Ko'pincha siz ushbu operatsiyani amalga oshirish uchun biron bir shaxsning "vakolati bor" degan iborani eshitishingiz mumkin bu uning bunga huquqi borligini anglatadi.

Android-bu smartfonlar, planshetlar, elektron kitoblar, raqamli pleerlar, soatlar, fitness bilakuzuklari, o'yin pristavkalari, noutbuklar, netbuklar, smartfonlar, televizorlar va boshqa qurilmalar, avtomobil ko'ngilochar tizimlari va uy robotlari uchun mo'ljallangan operatsion tizim.

Asosiy kirish-chiqish tizimi (BIOS-Basic Input-Output system) bu kompyuterning ona platasidagi chipda saqlanadigan past darajadagi dastur.

Simsiz mahalliy tarmoqlar (WLAN-Wireless LAN)-ko'plab kompyuterlarni ulanishini ta'minlaydigan va cheklangan o'rinlarda joylashgan simsiz tarmoq.

Botnet-Ma'lum sondagi xostlardan iborat va botlar (avtonom dasturiy ta'minot) ishlayotgan kompyuter tarmog'i.

Bruteforce-bu avtomatik rejimda elektron pochta xizmatidagi qayd yozuv uchun parollarni tanlaydigan maxsus dastur. Himoya usuli bu taxmin qilinadigan yoki mantiqiy hisoblab bo'lmaydigan murakkab paroldan foydalanish.

Disassembler-mashina kodini assembler til kodiga aylantirish imkonini beradi. Assembler kodi bu mashina kodining o'qilishi mumkin

bo'lgan shakli (bit satriga qaraganda o'qilishi oson). Disassemblerdan foydalanib, mashina kodida qaysi ko'rsatmalar ishlatilishini bilib olishingiz mumkin.

Dekompilyator - bu assembler yoki mashina kodini yuqori darajadagi tilda, masalan, C manba kodiga aylantirish imkonini beradigan vositadir.

DLP-tizimi (Data Leak Prevention)-ma'lumotlarning noqonuniy tarqalishidan himoya qilish tizimi-maxfiy axborotning sirqib tizimidan tarqalishini oldini olish shuningdek, bunday sirqishning oldini olish uchun texnik qurilmalar texnologiyalarini o'z ichiga oladi (dasturiy ta'minot yoki dasturiy ta'minot va apparat vositalari).

DoS (Denial of Service) hujumi kompyuter tarmog'iga, alohida kompyuterga yoki axborot tizimiga xizmat ko'rsatishni rad etish hujumi.

DDoS (Distributed Denial of Service)-xizmat ko'rsatishdan voz kechish hujumining keng tarqatilgan ko'rinishi. Turli nuqtalardan yuborilgan ko'plab so'rovlar natijasida tarmoq manbai ishdan chiqariladi.

Internet Spyware-bu turdagi dasturiy ta'minot ulanishlar, barcha tashrif buyurilgan resurslar, elektron pochta xabarlarini yuborish va qabul qilish, onlayn-do'konlardan qilingan xaridlar haqidagi ma'lumotlarni to'playdigan dastur.

ICMP (Internet Control Message Protocol)-xatolar haqida xabar beruvchi va tarmoq uzellari o'rtasida aloqani ta'minlovchi TCP/IP protokollari to'plamidagi majburiy nazorat protokoli. Aynan ICMP protokoli TCP/IP muammolarini topish va tuzatish uchun Ping vositasidan foydalanadi).

IP_ manzil (Internet Protocol Address)-TCP/IP protokoli steki asosida qurilgan kompyuter tarmog'idagi tugunning noyob tarmoq manzili.

IP-spoofing-xakerning o'zini korporatsiya ichida yoki tashqarisida joylashgan vakolatli foydalanuvchi sifatida ko'rsatishi.

Immunizator (Vaktsinalar)-fayllarni yuqtirishni oldini oluvchi rezident dasturlar.

HDD Spyware-ushbu turdagi dasturlar foydalanuvchining qattiq diskida saqlangan ma'lumotlarni skanerlaydi.

Keylogger (*key-tugma* va *logger- qurilmani ro'yxatdan o'tkazuvchi*) - jabrlanuvchining kompyuteridagi har bir bosilgan tugmani tadqiq qiluvchi kichik dasturdir. Ushbu usulni qo'llash uchun siz murakkab narsalarni qilishingiz yoki maxfiy ma'lumotlarga ega bo'lishingiz shart emas.

Keylogget-ilovaning ishlash paytida foydalanilgan tugmachalar haqida ma'lumot saqlash uchun mo'ljallangan. Ushbu turdagi dasturlardan foydalangan holda siz parollar, loginlar va h.k. kiritishlarni kuzatib borishingiz mumkin.

Kirishni boshqarish-bu kirishni boshqarishni to'g'ri sozlash orqali IP spoofing oldini olish usuli.

Crack-dasturiy ta'minotni buzish imkonini beruvchi dastur. Qoidaga ko'ra, krek ommaviy foydalanishga mo'ljallangan. Darhaqiqat, krek bu buzish ko'rinishlaridan biri bo'lib, ko'pincha muntazam tuzatishlar.

Cracker-krek yaratish bilan shug'ullanuvchi kishi.

Lokal tarmoq (LAN-Local Area Network)-lokal tarmoq. O'zaro axborot almashish muhiti orqali bog'langan, bir biriga yaqin binolardagi (chegaralangan hududdagi) ko'plab kompyuterlar to'plamidan hosil bo'lgan tarmoq.

Saytlararo skriptlar (XSS-Cross-Site Scripting)-saytlararo skriptlar (XSS- Cross-Site Scriptin)-veb-tizim tomonidan chiqarilgan sahifaga zararli kodni kiritish va ushbu kodni tajovuzkorning web-serveri bilan o'zaro ta'sir qilishdan iborat veb-tizimlarga qilingan hujum.

Shlyuz chegara protokoli yoki dinamik marshrutlash protokoli (BGP- Border Gateway Protocol)-tashqi shlyuzlarni marshrutlash protokollari sinfiga (EGP-External Gateway Protocol) tegishli va Internetdagi asosiy dinamik marshrutlash protokoli.

Tarmoqlarni boshqarishning sodda protokoli (SNMP-Simple Network Management Protocol)-bu TCP/UDP arxitekturalariga

asoslangan IP tarmoqlarida qurilmalarni boshqarish uchun standart Internet protokoli.

Uzatishni boshqarish protokoli (TCP-Transmission Control Protocol)–ma'lumotlarning uzatilishini boshqarish uchun mo'ljallangan Internet uzatishning asosiy protokollaridan biri. TCP va IP-ni almashadigan tarmoqlar va pastki tarmoqlarga TCP/IP tarmoqlari deyiladi.

Ma'lumotlari marshrutlash protokoli (RIP-Routing Information Protocol)-eng oddiy marshrutlash protokollaridan biridir. Kichik kompyuter tarmoqlarida ishlatiladi, u qo'shni marshrutizatorlarga yo'riqnoma orqali ma'lumotni dinamik ravishda yangilashga imkon beradi.

Reverse engineering Reverse engineering (teskari ishlab chiqarish,teskari loyihalash, teskari injiniring, revers-injiniring) uning ishlash prinsipini tushunish uchun ba'zi bir tugallangan qurilma yoki dasturni, shuningdek uning hujjatlarini o'rganish lozim. Odatda, asl ob'ektni yaratuvchisi ob'ektni tuzilishi (ishlab chiqarish) va usuli to'g'risida ma'lumot bermagan holda ishlatiladi.

Domen nomlari tizimi (DNS-Domain Name System)–domen nomlari tizimi, shuningdek domen nomlarini ruxsatini beruvchi serverlar tizimi (DNS_servers).

SMS troyanlari-qisqa raqamlarga pullik xabarlarni yuborish.

Sniffer paket (trafik analizatori deb ham ataladi)-bu tarmoq trafigini tutib olib va tahlil qiladigan dastur yoki boshqa apparat vositasi. Hozirgi vaqtda ushbu dasturlar huquqiy asosga ega, shuning uchun ular tarmoqda keng qo'llaniladi, ammo ulardan ham foyda, ham zarar uchun foydalanish mumkin.

CVE (Common Vulnerabilities and Exposures)-bu ma'lum bo'lgan xavfsizlik zaifliklarining ma'lumotlar bazasi. Har bir zaiflik uchun CVE-yil shaklining identifikatsiya raqami, tavsifi va tarifi bilan umumiy kirish havolalari beriladi.

Hujumni aniqlash tizimi (IDS-Intrusion Detection System)-kompyuter tizimi yoki tarmog'iga ruxsatsiz kirishni (buzib kirish yoki

tarmoq hujumi) aniqlash uchun mo'ljallangan dasturiy yoki apparat ta'minot.

Cookie Spyware-kuki-fayllar haqida ma'lumot to'playdi.

Yuqorida sanab o'tilgan josus vositalardan foydalanib, ayg'oqchilar, osonlik bilan parollarni va kodlarni o'qib oladi, masalan, Internet orqali plastik karta vositasida tovarlar yoki xizmatlar haqini to'lashda, WebMoney yoki boshqa to'lov tizimlariga kirish parollarini o'g'irlashni amalga oshiradi.

Outpost Firewall-bu kompyuterni Rossiyaning Agnitum kompaniyasi tomonidan xakerlik hujumlaridan himoya qilish uchun chiqarilgan shaxsiy xavfsizlik devori. Outpost shuningdek web-sahifalarga reklama va faol tarkibni yuklashga to'sqinlik qiladi.

TTL-bu qisqartirish. Bu quyidagilarni anglatishi mumkin: Time to live-IP protokolidagi ma'lumot paketining ishlash muddati (tizimda ruxsat etilgan maksimal vaqt), DNS yozuvlari.

Fishing (ing. fishing -baliq ovlash)-bu Internet-firibgarlikning bir turi, uning maqsadi foydalanuvchining identifikatsiya ma'lumotlarini olishdir. Bunga parollar o'g'irlanishi, kredit karta raqamlari, bank hisoblari va boshqa maxfiy ma'lumotlar kiradi.

FTP-mijoz (File Transfer Protocol) "faylni uzatish protokoli" - FTP serveriga kirishni soddalashtirish uchun kompyuter dasturi. Maqsadga qarab, u foydalanuvchiga masofaviy FTP serveriga matnli konsol rejimida oson kirishni ta'minlaydi, faqat foydalanuvchi buyruqlari va fayllarini yuborish vazifasini o'z zimmasiga oladi yoki masofaviy serverda fayllarni foydalanuvchi kompyuterining fayl tizimini bir qismi kabi ko'rsatishi mumkin.

Elektron raqamli imzo (ERI) elektron hujjatning haqiqiyligini tasdiqlash uchun xizmat qiluvchi parametrdir. Elektron raqamli imzo qog'ozli hujjatdagi rasmiy imzo o'rnini egallaydi va xuddi shu huquqiy ta'sirga ega. ERI egasini identifikatsiyalash va ruxsat etilmagan o'zgarishlarni yo'qligini tasdiqlash uchun ishlatiladi. Elektron raqamli imzodan foydalanish nafaqat axborotni himoya qilishni ta'minlaydi, balki hujjatlar aylanishi texnologiyasini kamxarajat bo'lishi, hisobotlarni rasmiylashtirish vaqtida hujjatlarning harakatlanish vaqtini qisqartiradi.

Eksployitlar-axborot resursi zaifliklaridan foydalanishga imkon beradigan dastur, harakatlar ketma-ketligi yoki buyruqlar to'plami. Eksploitlar hatto tajribasi ko'p bo'lmagan foydalanuvchiga dastur, web-sayt yoki eksploit mo'ljallagan boshqa resursni buzishga imkon beradi.

SQL in'ektsiyasi-saytni buzishning eng osonusullaridan biridir. Bunday in'ektsiyalarning mohiyati ma'lumotlarga o'zboshimchalik bilan SQL kodini kiritish (GET, POST so'rovlari yoki Cookie qiymatlari orqali uzatiladi). Agar sayt himoyasiz bo'lsa va bunday in'ektsiyalarni istalgancha amalga oshirish mumkin.

Wi-Fi-bu IEEE 802.11 standartlariga asoslangan qurilmalar bilan simsiz mahalliy ulanish texnologiyasidir. Wi-Fi qisqartmasi ostida (ing. Wireless Fidelity "simsiz ulanish") hozirgi kunda radiokanallar orqali raqamli oqim va ma'lumotlarni uzatish uchun standartlar to'plami ishlab chiqilmoqda.

Valgrind-bu bepul tuzatuvchi dastur bo'lib, dasturni Linux muhitida uni bajarish paytida tahlil qilishni ta'minlaydi.

ILOVALAR

Ilova 1.

Ba'zi hujumlar turlarining ro'yxati

Portni tekshirish (Port Scanning)	O'z-o'zidan hujum emas, balki tizimning TCP va UDP kabi ochiq portlarni (masalan, kompyuterning nazoratini qo'lga kiritish uchun hujumkor ulanishi mumkin bo'lgan portlar) asosida potentsial zaifliklarni aniqlash maqsadidagi harakatlar, tizimning turli xil so'rovlarga bo'lgan munosabati va hk. Katta tarmoqlarda, bu tizimni mavjud tarmoq manbalarini ("Network scan" kabi utilitalar) skanerlaydigan dasturlardan foydalanganda ro'y berishi mumkin.
Xizmatdan voz kechish (Denial Of Service)	Tizimning ishdan chiqishiga yoki ishlashning yomonlashishiga olib keladigan har qanday harakatdir. Barcha tizim manbalarining to'liq safarbar etish orqali xato yoki ishdan chiqishdan oldin turli xil manzillardan katta miqdordagi ma'lumotlarni tizimingiz portlariga yuborishga urinishlar bo'lishi mumkin. Bunday vaziyatning tasodifiy yuzaga kelishi ehtimoli juda past, bo'lib, ushbu holda Outpost Firewall-ning konfiguratsiyasiga alohida e'tibor qaratish lozim.
Fragmentlangan ICMP paketlari (Fragmented ICMP)	Ushbu hujum Microsoft TCP/IP dasturiy ta'minotidagi zaifliklardan foydalanadi. Ushbu hujum Microsoft TCP/IP-ni tadbiq etishdagi zaiflikdan foydalanadi. Windows 95, 98, NT yoki 2000 tizimi ostida ishlaydigan kompyuterda paket hajmi 1472 baytdan oshadigan tarzda o'zgartirilgan bo'laklar shaklida ICMP paketlarini yuborib,

	kompyuterning normal ishlashini buzishiga va hatto OTning ish samadorligini pasayishiga olib keladi. Parchalanib ketgan ICMP paketlari oxir oqibatda hujum qilingan tizimning TCP/IP steki kompyuter xotirasining noto‘g‘ri manziliga ruxsatsiz kirishga olib keladi. Bu ba’zi xizmatlarning rad etilishiga (xizmatni rad etish) yoki OTni ishdan chiqishiga olib keladi.
	Bugungi kunda ushbu hujumlar o‘z dolzarbligini yo‘qotib, ammo ushbu paketlarni qabul qilish tizimingizni umumiy zaif nuqtalarga nisbatan tekshirilayotganligini anglatishi mumkin. Odatda ma’murlar tarmoq ishlashi va katta paketlarni o‘tkazuvchanlik qobiliyatini tetslashda qisman ICMP paketlarini ishlatadi. Masalan, quyidagi buyruqni bajarish hujumni aniqlashga olib kelishi mumkin: ping IPaddress -l 65500. Masalan, ushbu turdagi hujumning bir nechta variantlari mavjud: Ushbu turdagi hujumlarning bir nechta turlari mavjud, masalan: JOLT2, protsessor quvvatining kattagina hajmini sarflash maqsadida fragmentlangan bir xil IP-paketlarning uzluksiz oqimi foydalanib xizmatni rad etish hujumidir. Ko‘pgina Windows operatsion tizimlari IP-paketlarni yaratish usullaridagi xatolar tufayli ushbu hujumga duch keladi. TARGA3 tasodifiy noto‘g‘ri IP-paketlarni yuboradi, bu esa ba’zi IP-steklarning ishdan chiqishi yoki kutilmagan holatlarning paydo bo‘lishiga olib keladi. Noto‘g‘ri IP-paketlar noto‘g‘ri ma’lumotlar (protokol, paket

	o‘lchami, nom, parametrlar, ofset, TCP segmentlari va marshrutlash bayroqlari) va noto‘g‘ri fragmentlarga bo‘linadi. TCP to‘plami noto‘g‘ri paketni qabul qilganida, yadro uni qayta ishlash uchun resurslarni ajratadi. Tizim yetarlicha kattalikdagi noto‘g‘ri shakllangan paketlarni qabul qilganda, barcha resurslarning safarbar etilishi uning ishdan chiqishiga olib kelishi mumkin.
Fragmentlangan IGMP paketlari (Fragmented IGMP)	Fragmented ICMP faqat IGMP paketlarni ishlatiladi. Bunday hujumga misol sifatida IGMPSYN–xizmat ko‘rsatishdan voz kechish, qurbonning kompyuterini foydalanuvchanligini yo‘qotishga qaratilgan hujumni keltirish mumkin. IGMPSYN, birinchi turdagi IGMP so‘rovlarini tasodifiy manba manzillari bilan yuboradi.
Qisqa fragmentlar (Short Fragments)	Ushbu hujum ko‘plab qismlarga bo‘linadigan juda katta IP-paketlarni qayta ishlash xususiyatlaridan foydalanadi va keyin yadro asl paketni olish uchun barcha qismlarni to‘playdi. Hujum paketning juda qisqa qismini yuboradi, unda hatto sarlavha ham bo‘lmaydi, bu esa tizim yig‘ilgandan so‘ng ishdan chiqishiga olib keladi.
“My Address” hujumi	Mahalliy kompyuterning IP-manzilini belgilash, tarmoqdagi mavjudligini o‘zgartirish va barcha ulanishlarini masofali tarzda kompyuterlardan o‘z maqsadlari uchun ishlatishni ko‘zlagan umumiy hujum. Ushbu muammo noto‘g‘ri yozilgan dasturiy ta’minot natijasi yoki e’tiborsizlik oqibati bo‘lishi mumkin. Ushbu turdagi hujumga Snork hujumini

	keltirish mumkin.
Bir-biriga bog'langan fragmentlar (Overlapped Fragments)	IP protokoli spetsifikatsiyasi bu oldingi qabul qilingan fragmentlarning yangisini qayta yozishga olib keladigan to'plash algoritmini tavsiflaydi. Ushbu turdagi realizatsiyada, tajovuzkor birinchi qismda zararsiz ma'lumotlar mavjud bo'lgan paketlar ketma-ketligini yaratishi mumkin va so'ngraTCP sarlavhasidan (masalan, maqsad portidan) olingan ma'lumotni qisman jamlaydi va shu bilan uning o'zgarishiga olib keladi, bu esa tizim qobiliyatini pasayishiga olib keladi.
"Winnuke" hujumi	Ushbu hujumlar Windows 95, NT va 3.11 tizimlariga qaratilgan va TCP Out-of-band (OOB) xususiyatidan foydalanadi. Tajovuzkor jabrlanuvchi kompyuterning 139 portiga OOB ma'lumotli paket yuboradi. Port 139, OOB bayrog'i o'rnatilmagan holda kiruvchi paketlarni qabul qilmaydigan NetBIOS portidir. Kompyuter ushbu paketni qayta ishlashga qodir emas, bu esa Internetga ulanishning yo'qolishiga va hatto xizmatni tark etishiga va tizimning buzilishiga olib kelishi mumkin.
"Teardrop"hujumi	Teardrop TCP/IP-da amalga oshirilgan jamlash algoritmi yordamida "IP fragmentlar xatosini jamlash" deb nomlangan usuldan foydalanib fragmentlarni noto'g'ri qayta ishlanishiga olib keladi. Ushbu hujum fragmentning boshi va uzunligi uchun noto'g'ri o'rnatilgan qiymatlari bo'lgan datagramni yuborishdan iborat. Paketning qiymati o'enini o'zgartirib, ushbu parametrlar

	ma'lumotlar kompyuter xotirasida yig'gandan so'ng, ularning o'rnini o'zgartiradi, bu esa xizmatni rad etish yoki Windows 3.1, 95, NT ishlaydigan tizimlarning ishdan chiqishiga olib keladigan xotira xatolariga olib keladi.
"Nestea" hujumi	Nestea-Teardrop kabi fragmentlardan foydalanuvchi hujumning bir turi. Ba'zi TCP/IP steki fragmentlarning maxsus ketma-ketliklarini noto'g'ri qayta ishlash natijasida tizimning ishdan chiqishiga olib keladi. Nestea hujumi Linux operatsion tizimlarida keng tarqalgan va Linuxni qayta fragmentlangan kodidan (ortiqcha hajmdagi qabul qilingan paketlarni qayta formatlaydigan va to'playdigan kod) foydalaniladi. Ushbu hujum ta'siri ostidagi tizimlar: Win 3.1, 95, NT va Linuxning ba'zi versiyalari.
"Iceping" hujumi	ICMP protokolini qo'llashda SPing zaifligidan foydalanadi. Ushbu zaiflik, bir necha kilobaytdan kichik o'lchamli fragmentlarga bo'lingan katta hajmli ICMP paketlarini noto'g'ri qayta ishlashga olib keladi (64 kilobaytdan ortiq), bu esa paketni tuzishda tizimni osilib qolishi yoki to'xtalishiga sabab bo'ladi. Hujum ta'siri nafaqat Windows tizimlari, balki Mac OS va ba'zi Unix versiyalariga ham tegishlidir.
ICMP - hujumi	ICMP hujumlari ICMP zaifliklaridan foydalanadi. ICMP IP qatlami tomonidan xostlarga bir tomonlama ma'lumotli xabarlarni yuborish uchun ishlatiladi. ICMP-da autentifikatsiya mavjud emasligi sababli, ushbu protokoldan foydalanilgan hujumlar

	xizmat ko'rsatishni rad etishga olib keladi va buzg'unchilarga paketlarni ushlab olishga imkon beradi. Bu sinfning hujumlari orasida 1234 va MOYARI13 mavjud. Ikkala hujumning mazmuni - bu har xil noto'g'ri ICMP paketlarini jabrlanuvchining kompyuteriga yuborish, bu esa OT ishdan chiqishiga olib keladi (tarmoq steki javob bermayapti). Hujum Windows 95/98 ga qarshi ishlatilgan.
"Opentear" hujumi	Opentear tasodifiy ravishda o'zgartirilgan manba manzilidan foydalanadi va tasodifiy fragmentlangan UDP paketlarini tasodifiy portlarga yuboradi. Ushbu paketlar Windows 95, 98, NT, 2000 va OpenBSD ning ayrim versiyalarida CPU vaqtining 100% ni oladi va tizimning qayta yuklanishiga olib kelishi mumkin.
"Nuke" hujumi	Ushbu hujum TCP/IP protokolining xususiyatlaridan foydalanadi va Windows 95, 98, NT va 2000 larda tarmoqni qo'llab-quvvatlashning noto'g'ri qo'llanilishi natijasidir. TCP/IP tarmoqlarida tugunlarning ishlashini tekshirish uchun ICMP protokoli ishlatiladi. Faoliyatdagi xatoliklar, masalan, ulanishning yo'qolishi yoki aloqa liniyasidagi yetishmovchilik kabi, ICMP xabari yaratiladi, undan keyin yo'nalishni marshrut stolidan chiqarib tashlash yo'li bilan marshrutni qayta tashkil etish kabi muayyan harakatlar paydo bo'ladi. Shu bilan birga, kirish mumkin bo'lmagan tugundan barcha ulanishlar uzilib qoladi. Nuke hujumi ICMP paketini (odatda

	139 port orqali) B kompyuterga ulangan A kompyuteriga "manzillash ruxsat etilmagan" xabari bilan uzatadi.
IGMP-hujumlari	IGMP hujumlari IGMP protokolining zaifliklari yoki uning realizatsiyasidagi xatoliklardan foydalanadi. Bu sinf hujumlari: FAWX, FAWX2, KOX, SYN. FAX, KOX IGMP kabi, xizmatining rad etish hujumidir. FAWX va KOX jabrlanuvchi tizimiga tushishga olib keluvchi yirik o'lchamdagi IGMP paketlaridan foydalanadi. Ushbu hujum ta'siridaga tizimlar: Win 95, 98, NT. FAWX2 Windows 95, 98, 2000 da ko'k ekran paydo bo'lishiga sabab bo'luvchi fragmentlangan chiqindilarni 139 portiga yuboradi.
139 Portiga hujum qilish	Bo'sh (NULL) nomli maydoni bilan SMB freymni yuboradi va quyidagi tizimlarning beqarorligi va osilishiga sabab bo'ladi: Windows 95, 98, NT.
"RST" hujumi	Ushbu zaiflik buzg'unchiga o'rnatilgan TCP ulanishlarini rad etish uchun shartlarni yaratishga imkon berishi mumkin, bu esa muddatidan oldin sessiyani yakunlanishiga olib keladi. Hujum manbai sifatida tasodifiy IP-manzildan foydalanganligi sababli manba (agar mavjud bo'lsa) serverga qayta ulanish paketini (RST/ACK) yuboradi va ulanish so'rovini yubormaganligini bildiradi. Ehtimol, IP-manzili faol ulanishlarning hech biriga mos kelmasligi mumkin (bu tasodifiy sondir); server ulanishni qaytadan boshlashga urinib, SYN/ACK paketlarini soxta IP-manzili manbaga va keyin RST/ACK

	(qaytarib olish uchun ACK paketlarini qabul qilmagani uchun) so‘rovini yuboradi. Bularning barchasi tugatilmagan yoki yarimochiq ulanishlarni hosil qiladi. RST hujumlari marshrutni muntazam ravishda o‘zgartirishi mumkin, bu esa uning resurslarini oladi.
“TIDCMP” hujumi	TIDCMP- bu qurbonning routeriga ICMP 4 turidagi soxta xabarni yuboradigan ICMP manbaga nisbatan bostirish hujumidir. Manbani bostirishning maqsadi qabul qiluvchi tugunining hozirgi vaqtda ma’lumotni qayta ishlashga qodir emasligi va u davom etishi mumkin bo‘lgan vaqtgacha ishni to‘xtatishi kerakligi haqida manba kompyuterini ogohlantirishdir.
“RFPOISON” hujumi	Maxsus tayyorlangan paket bo‘lib, NT 4.0 tizimi ostida ishlaydigan tarmoq ulanishlarini rad etishga va yaroqsiz holga keltirishga sabab bo‘ladi. Ushbu hujum, services.exe deb ataladigan xizmatlarning buzilishiga olib keladi, bu esa, o‘z navbatida, nomlangan kanallar orqali xatti-harakatlarni bajarishga imkon bermaydi. Natijada, foydalanuvchilar tizimga masofadan kirish, ro‘yxatga olish kitobini boshqarish, umumiy foydalaniluvchi fayl papkalariga yangi ulanishlarni yaratish yoki masofaviy boshqaruvni amalga oshirish imkoniyatidan judo bo‘ladi. Internet Information Server kabi xizmatlar ham to‘g‘ri ishlamasligi mumkin. Muammoni manbai srvsvc.dll xizmatlariga services.exe chaqiriqlarini amalga oshiradi. Ba’zi MSRPC chaqiriqlari bloklashga olib kelishi mumkin

	bo‘lgan services.exe jarayonini noto‘g‘ri interpretatsiya qiluvchi NULL qiymatini qaytaradi. Ushbu xavfsizlik zaifliklari boshqalarda ham kuzatiladigan bo‘lsa, bunday hujum kompyuterda xato tuzatuvchisini ishga tushurishi mumkin (masalan, Dr Watson). Agar xato tuzatuvchisi troyanchi bilan oldindan almashtirilgan bo‘lsa, unda zararli kod jabrlanuvchi kompyuterida ishga tushiradi.
“RFPARALYZE” hujumi	NetBIOS tadbiqida (Network Basic Input/Output System, Microsoft Windows 95/98 dasturlarining mahalliy tarmoq ichida ishlashga imkon beruvchi asosiy tarmoq kirish/chiqish tizimi - Asosiy Tarmoq Kirish/Chiqish tizimi - Asosiy Tarmoq Kirish/Chiqish tizimi-), masofaviy ulanish zaifliklari mavjud. NetBIOS sessiyasiga NULL nomli maxsus paketga so‘rov berish yordamida, tajovuzkor masofaviy xizmat ko‘rsatishni rad etilishiga sabab bo‘ladi. RFParalyze bu zaiflikni NetBIOS-da ishlatadi va NetBIOS-ga asoslangan Windows Messenger Service xizmatini maqsad qilib qo‘yadi va ilovalarga kelgan xabarning hodisasi haqida foydalanuvchini xabardor qilish imkonini beradi. Taziq ostidagi tizim tarmoq ulanishlari bloklanadi, qayta ishga tushadi yoki tarmoqga ulanish qobiliyatini yo‘qotadi.
Noto‘g‘ri IP opsiyasi (Malformed IP Options)	IP Options maydoni o‘lchamidagi 38 baytdan katta paketni yuboradi, bu TCP/IP-paketidagi buferlarni to‘ldirishga olib keladi, bu esa hujum qilingan tizimdagi har qanday

	zararli kodni ishlatish yoki Windows 2000, XP SP1da xizmat ko'rsatishni rad etishga olib keladi. Bunga qo'shimcha ravishda, Windows har bir ICMP xabari paketga javob beradi, bu tarmoq trafigini ortiqcha sarflanishi va butun tarmoqni sekinlashishiga olib keladi.
RPC DCOM zaifliklari	Microsoft Windows-dagi bufer toshqinlari zaifligi 135-chi TCP/UDP portini tinglaydigan DCOM RPC interfeysi orqali masofadan ishlatilishi mumkin. Muammo DCOM ob'ektini faollashtirish so'rovlarini tekshirishdagi chegaralanganlikdir. Ushbu xatolikdan foydalanib tizimga masofadan kira olish va mahalliy tizimning imtiyozlari bilan zararli kodni bajartirish va tizimning ishdan chiqishiga sabab bo'lishi mumkin. Ushbu zaiflik turli qurtlar (masalan, MSBlast) va ba'zi xaker vositalari tomonidan ishlatiladi. Ushbu hujum ostidagi tizimlar: Windows 2000 Professional SP4, Windows 2000 Server SP4, Windows XP Professional SP 1, Windows NT 4.0, Windows 2003.
Noto'g'ri IP-paket	Jabrlanuvchi kompyuterga hujum paytida noto'g'ri sarlavha uzunligidagi IP, TCP yoki UDP paketlari yuboriladi. Bunday paketlar tizim tomonidan qabul qilinmaydi va ularning ortiqcha miqdori cho'kishlar va boshqa tizim xatolariga olib keladi.
Ethernet-hujumlar	Tarmoq orqali ma'lumotlar bir kompyuterdan boshqasiga yuborilganda, manba kompyuter MAC-manzilini maqsadli kompyuterning IP-manzilidan aniqlash uchun ARP so'rovini yuboradi. Xabar yuborilgan vaqt va Ethernet manzili bilan javob vaqtida

	ma'lumotlar uchinchi shaxs tomonidan almashtirilishi, o'g'irlanishi yoki ruxsatsiz qayta yo'naltirilishi mumkin. Bu sinf quyidagi hujumlarni namoyon etadi: IP-manzili o'zgarishi (IP-spoofing)-Buzg'unchi IP-adresini o'zgartiradi va xizmatni rad etishga olib keladigan tarmoqni ortiqcha ma'lumot bilan band qilishga urinadi. Shlyuz manzilni almashtirish (Gateway sniffing)-Xaker o'z MAC manzilini o'z o'rniga qo'yishi va ARP javoblarini nazorat qiluvchi kompyuterga trafikni yo'naltirishi mumkin. Bu unga paketlarni va barcha uzatiluvchi ma'lumotlarni ko'rish imkonini beradi. Shuningdek, trafikni mavjud bo'lmagan kompyuterlarga yo'naltirishga imkon beradi, bu ma'lumotni uzatishda kechikishlar yoki xizmatni rad etishga olib keladi. IP-manzil to'qnashuvi-tajovuzkor kompyuterning tarmoqqa kirishini bloklashi, noto'g'ri ARPning javoblarini ishlab chiqarishi va tarmoqdagi har bir IP-adresini takrorlashi, IP-manzildagi nizolarga sabab bo'lishi mumkin.

Xaker hujumlarining apparat vositalari

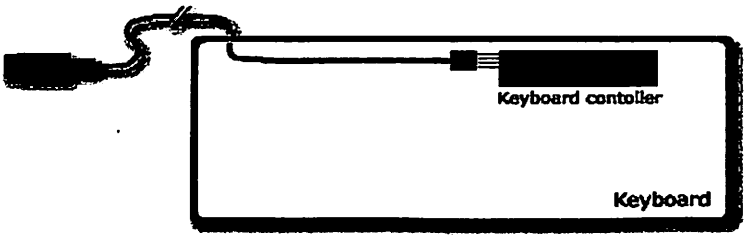
1. KeyGrabber Module o'rnatilishi

KeyGrabber modulini USB yoki PS/2 klaviaturasiga joylashtirish bu foydalanuvchi tomonidan bajarilishi kerak bo'lgan bir martalik jarayon. Klaviaturadan kiritilgan ma'lumotlar modul tomonidan klaviatura quvvat manbaiga ulanishi bilan ushlanib qolinadi. Keyinchalik ma'lumotni yuklab olish uchun xuddi shu klaviaturadan foydalanish kerak. Quyida qisqacha o'rnatish qo'llanmasi mavjud, ammo batafsil ma'lumot uchun foydalanuvchi yo'riqnomasiga murojaat qilish maqsadga muvofiq.

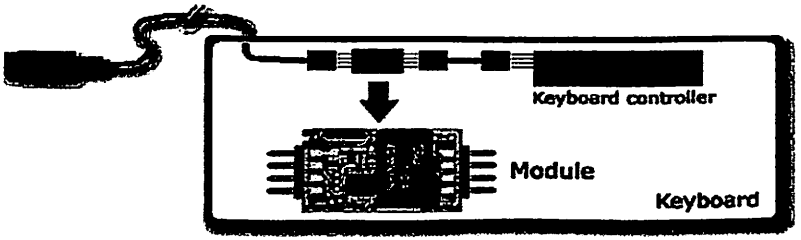
KeyGrabber Module-ni to'g'ri ulash va o'rnatilishiga foydalanuvchi javobgar hisoblanadi.

KeyGrabber moduli klaviatura boshqaruvchisi (klaviatura ichida) va klaviatura simlari o'rtasida joylashtirilishi kerak. Buning uchun PS / 2 kabelining to'rtta asosiy simlarini (VCC, GND, CLK, DATA) yoki USB simini (VCC, GND, D +, D-) kesib oling va ularni ikkala tomondan modulga ulang. Ba'zi klaviaturalarda qo'shimcha foydalanilmagan simlar (NC) va ekran mavjud.

O'rnatishdan oldin



O'rnatishdan keyin



Standart PS/2 va USB klaviaturasi kompyuterga 2 quvvat liniyasi va 2 ma'lumot liniyalari orqali ulanadi. KeyGrabber Moduli ushbu qatorda kompyuter va klaviatura o'rtasida joylashtirilgan bo'lishi kerak. Ba'zi hollarda, yana ikkita foydalanilmagan chiziqlar va siz e'tibor bermaydigan ekran mavjud.

2. Raspberry Pi

Raspberry Pi-bu bank kartasi o'lchamidagi yagona to'lov kompyuteri bo'lib, dastlab informatika fanini o'qitish uchun byudjet tizimi sifatida ishlab chiqilgan bo'lib, keyinchalik mualliflar kutganidan ancha kengroq ommalashib ketgan. Raspberry Pi Foundation tomonidan ishlab chiqilgan. Faqat uch yil ichida 4,5 milliondan ortiq Raspberry Pi qurilmalari sotildi.

Raspberry Pi bir nechta to'plam darajalari mavjud: "A" modeli, "B", "B +" modeli, "2B", "Nol" va "3B" modellari. Dastlabki uchta versiya soatiga 700 MGts chastotali Broadcom BCM2835 ARM11 protsessor va 256MB/512MB RAM moduliga ega, paket-on-pack texnologiyasidan foydalangan holda to'g'ridan-to'g'ri protsessorga joylashtirilgan. "2 B" modeli 1 Gigagerts chastotasi va 1 Gb tezkor xotiraga ega 4 ta Cortex-A7 protsessor bilan jihozlangan. "A" rusumli bitta USB 2.0 porti, ikkitasi "B" va to'rtta "B +" va "2 B" modellari mavjud. Shuningdek, "B", "B +" va "2 B" modellarida Ethernet port mavjud. Asosiy yadro qo'shimcha ravishda, BCM2835 OpenGL ES 2.0, apparat tezlashishi va FullHD-video va DSP-yadrolarni qo'llab-quvvatlaydigan grafik yadroni o'z ichiga oladi. Asosiy xususiyatlardan biri bu real vaqt soatlarining yetishmasligidir.

Raspberry Pi-ning eng qiziqarli xususiyatlaridan biri bu GPIO (umumiy maqsadlar uchun kirish/chiqish) portlarining mavjudligi. Buning yordamida turli xil qurilmalarni boshqarish uchun "malina" kompyuteridan foydalanish mumkin. "B" modelida 26 pinli taxtali, "B +" va "2B" modellarida 40 pinli GPIO ulagichi mavjud.

Raspberry Pi asosan Linux operatsion tizimlarida ishlaydi. Windows 10 IOT-ni o'rnatish ham mumkin. Bundan tashqari, siz Raspberry litsenziyalangan Windows 10 IOT-ni 50 dollarga sotib olishingiz mumkin. ARM11 Linux-ning barcha versiyalarini qo'llab-

quvvatlamaydigan ARM-ning 6-versiyasiga asoslangan. Operatsion tizimlarni o'rnatish uchun NOOBS vositasi mavjud.

3. KeyLogger

Keylogger (ing: keylogger) Kompyuter klaviaturasidagi klavishlarning har bir bosilishini qayd etuvchi dasturiy mahsulot (modul) yoki apparat vositasi. Tugmachalar ro'yxatdan o'tkazilgandan so'ng, ular haqidagi ma'lumotlar keyinchalik olish maqsadida kompyuterda dastur tomonidan yashiriladi yoki tajovuzkor elektron pochta manziliga yuboriladi.

Turlari bo'yicha

Dasturiy keyloggerlar shaxsiy kompyuter foydalanuvchisi faoliyatini kuzatuvchi dasturiy mahsulotlar guruhiga kiradi. Dastlab, ushbu turdagi dasturiy mahsulotlar faqat klaviaturadagi tugmachalar, shu jumladan tizimdagi tugmachalar haqidagi ma'lumotlarni maxsus dastur jurnalida (jurnal faylida) qayd etish uchun mo'ljallangan edi, keyinchalik ushbu dasturni o'rnatgan shaxs tomonidan o'rganib chiqilgan. Jurnal faylini tarmoq orqali tarmoq drayveriga, Internetdagi FTP-serverga, elektron pochta va boshqalarga yuborish mumkin.

Hozirgi vaqtda ushbu nomni "eski uslubda" saqlab qolgan dasturiy mahsulotlar ko'plab qo'shimcha funktsiyalarni bajaradi-bu Windows-dan ma'lumotni olish, sichqonchani bosish, clipboardni ushlab turish, ekran rasmlari va faol oynalarni "suratga olish", barcha olingan va yuborilgan elektron xabarlarni qayd etish, pochta, fayllarning ishlashini kuzatish va tizim registri bilan ishlash, printerga yuborilgan vazifalarni yozish, mikrofondan ovozni va kompyuterga ulangan veb-kameradan olingan rasmlarni ushlash va boshqalar.

Apparatli keyloggerlari-bu klaviatura va kompyuter o'rtasida ulanadigan yoki klaviaturaning o'zida birlashtiriladigan miniatyurali qurilmalar. Ular klaviaturada bajarilgan barcha tugmachalarni qayd etishadi. Ro'yxatdan o'tish jarayoni oxirgi foydalanuvchi uchun mutlaqo ko'rinmasdir. Uskuna klaviaturalari barcha tugmalarni muvaffaqiyatli ushlash uchun biron bir dasturni kompyuterga o'rnatishni talab qilmaydi. Uskuna klaviatura biriktirilganda, kompyuterning yoqilgan

yoki o'chirilgan holati muhim emas. Uning ish vaqti cheklanmagan, chunki u ishlashi uchun qo'shimcha quvvat manbaini talab qilmaydi.

Ushbu qurilmalarning ichki quvvatga bog'liq bo'lmagan xotirasi hajmi 20 milliongacha tugmachalarni Unicode yordamida yozib olishga imkon beradi. Ushbu qurilmalar har qanday shaklda bajarilishi mumkin, shunda hatto mutaxassis ba'zida axborotni tekshirish paytida ularning mavjudligini aniqlay olmaydi. O'rnatish o'rniga qarab, apparat keylogger tashqi va ichki turlarga bo'linadi.

Akustik keylogger-bu kompyuter tomonidan klaviaturadagi tugmachalarni bosib foydalanuvchi tomonidan yaratilgan tovushlarni birinchi bo'lib yozib oladigan, so'ngra ushbu tovushlarni tahlil qilib, matn formatiga o'tkazadigan apparat qurilmalaridir.

Qo'llanilish usuli bo'yicha

Faqat keyloggerlardan foydalanish usuli (keyloggerni modul sifatida o'z ichiga olgan apparat yoki dasturiy mahsulotlar) xavfsizlikni boshqarish va xavfsizlikni buzish o'rtasidagi chiziqni ko'rishga imkon beradi.

Ruxsat etilmagan foydalanish-klaviatura o'rnatilishi (modul sifatida keylogger-ni o'z ichiga olgan apparat yoki dasturiy mahsulotlar) avtomatlashtirilgan tizim egasining (xavfsizlik ma'murining) ma'lumotisiz yoki ma'lum bir shaxsiy kompyuter egasining xabarisiz amalga oshiriladi. Vakolatsiz shaxslar tomonidan ishlatiladigan klaviaturalar (dasturiy yoki apparat vositalari) josuslarga qarshi mahsulotlar yoki josuslarga qarshi dasturlar deb nomlanadi. Ruxsatsiz foydalanish, qoida tariqasida, noqonuniy harakatlar bilan bog'liq va "biriktirilgan" bajariladigan faylni sozlash va qabul qilish qobiliyatiga ega, u o'rnatishda hech qanday xabar ko'rsatmaydi va ekranda darchalarni yaratmaydi, shuningdek foydalanuvchi kompyuterida o'rnatilgan modul uchun o'rnatilgan yetkazib berish va masofadan o'rnatish vositalariga ega, ya'ni o'rnatish jarayoni foydalanuvchining kompyuteriga to'g'ridan-to'g'ri jismoniy kirishsiz amalga oshiriladi va ko'pincha administrator huquqlarini talab qilmaydi.

4. Ar Drone

Ushbu qurilma boshqalardan juda farq qiladi. undan foydalanib, siz trafikka to'sqinlik qilmasligingiz, tugmalarni bosmasligingiz va ish stolidagi rasmlarni saqlashingiz mumkin emas! Zamonaviy pentesting tobora ko'proq josuslikka o'xshaydi, shuning uchun mutaxassislar bu imkoniyatni e'tiborsiz qoldirmaydilar. Bu toza suvning o'yinchoqidir: uning ichiga kamera o'rnatilgan oddiy kvadrokopter. Ar Drone-ning ikkinchi versiyasi yuqori aniqlikdagi kamera bilan jihozlangan, shuning uchun u qanchalik ajoyib va josuslik filmi filmiga o'xshamasin, xonada nimalar bo'layotganini, qanday jihozlardan foydalanilayotganini va xodimlarning o'zini qanday tutishini deraza orqali ko'rishingiz mumkin. Ko'zni ochish va fotografik xotiraga ega bo'lish shart emas: video yoziladigan kameraga USB flesh-diskni ulashingiz mumkin. Qurilmani boshqarish imkon qadar sodda: siz maxsus dasturni o'rnatganingizdan so'ng iPhone, iPad va Android-ni masofadan boshqarish pulti sifatida ishlatishingiz mumkin. Qurilma tinch maqsadlarda ham ishlatilishi, hamda qushlar parvozi balandligidagi go'zal tasvirlarni olish mumkin.

Ilova 3.

Xaker hujumlarining dasturiy vositalari

1. Burp Suite - xakerga yordam beradigan bir qator xususiyatlarga ega. Ushbu moslamada ishlatiladigan ikkita mos dastur "Burp Suite o'rgimchak" ni o'z ichiga oladi, siz cookie fayllarini ko'rib chiqish orqali turli xil sahifalar va web-sayt sozlamalarini o'rganishingiz va belgilashingiz mumkin. Ushbu web-ilovalarga, shuningdek, maqsadli web-ilovalarga bir qator avtomatlashtirilgan hujumlarni amalga oshiradigan Intruder-ga ulanishni amalga oshiradi.

Burp Suite - bu ko'plab web-saytlar web-saytlarning zaifliklari va maqsadli web-ilovalarni tekshirish uchun foydalanishi mumkin bo'lgan ajoyib veb-xakerlik vositasidir. Burp Suite dastur haqida batafsil ma'lumotdan foydalangan holda ishlaydi, HTTP-ga yo'naltirilgan protokoldan o'chirildi. Ushbu vosita sozlanadigan va zararli hujum qiluvchi HTTP so'rovini keltirib chiqaradigan algoritm orqali ishlaydi, bu xakerlar ko'pincha foydalanadilar. Burp Suite SQL in'ektsiyasi va

saytlararo skriptlash (a) uchun zaifliklarni aniqlash uchun juda foydalidir.

2. Angry IP-Scanner (shuningdek, ipscan nomi bilan ham tanilgan) bu tezkor va ishlatish uchun qulay bo'lgan tarmoqni buzadigan skaner. IP-manzillarni va portlarni skanerlash uchun ushbu xakerlik vositasining asosiy maqsadi boshqa odamlarning tizimlarida ochiq kirish nuqtalar va portlarni topishdir. Shuni takidlash kerakki, Angry IP-Scannerda xakerlik qilishning boshqa usullari ham bor, siz ulardan qanday foydalanishni bilishingiz kerak. Ushbu buzg'unchilik vositasining keng tarqalgan foydalanuvchilari tarmoq ma'murlari va tizim muhandislari sanaladi.

Imkoniyatlari:

xostlarni faolligi bo'yicha tarmoqda tekshirish

berilgan IP manzillar oralig'ini tekshirish

UDP va TCP so'rovlarini qo'llab-quvvatlash

topilgan har bir kompyuter uchun siz tarmoqdagi kompyuter nomini, uning ishchi guruhini va tarmoq kartasining MAC manzilini aniqlashingiz mumkin

mahalliy tarmoqdagi kompyuterlardagi ochiq portlarni ko'rish

telnet, ssh, ftp, web-server va boshqalarga tezkor kirish.

3. Kali Linux.

Kali Linux-bu testlashni o'tkazish va xavfsizlikni auditlash uchun mo'ljallangan Linux-ning rivojlangan distributori.

Kali-bu Debian rivojlanish standartlariga to'liq mos keladigan BackTrack Linux-ning to'liq qayta yig'ilishidir. Kali barcha Linux foydalanuvchilariga bajarilishi mumkin bo'lgan fayllarni, qo'llab-quvvatlanadigan fayllarni, kutubxonalarni va boshqalarni osongina topishga imkon beradigan Filesystem Hierarchy Standartiga rioya qilish uchun yaratilgan.

Kali maxsus testlash uchun mo'ljallangan va shuning uchun ushbu saytdagi barcha hujjatlar Linux operatsion tizimi haqida oldindan ma'lumot talab qiladi.

4. Nmap dasturi

Tarmoq ma'muriyatining majburiyatlari ko'p narsalarni o'z ichiga oladi va tarmoq auditi eng asosiylaridan biridir. Agar uning o'lchamlari kichik bo'lsa, tarmoq auditi qiyin emas. Ammo siz boshqarayotgan tarmoqning kattaligi har bir qurilmani yoki xostni ishlamasligini yoki ishlamayotganligini, unga qaysi OS o'rnatilganligini, qaysi portlari ochiq va qaysi biri yo'qligini aniqlash uchun qo'lda chetlab o'tishning iloji bo'lmasa nima bo'ladi? Agar siz shunday vaziyatga tushib qolsangiz, unda OpenSource tarmoq audit dasturlari dunyosida deyarli standart bo'lgan dastur - **Zenmap** sizga yordam beradi.

Zenmap - mashhur Nmap yordam dasturi uchun grafik qobiq. **Nmap** - bu xavfsizlikni tahlil qilish va tarmoqni tekshirish uchun OpenSouce konsol vositasi. Nmap o'zi juda kuchli yordamchi dastur bo'lishiga qaramasdan, katta tarmoqlarda ishlayotganda, ko'pgina ma'murlar konsol vositalarini yolg'iz ishlatishni istashmaydi. Ba'zilar aytganidek: "Rasm ming qatlamdan iborat". Zenmap-da, ular shubhasiz to'g'ri, chunki uning yordamida siz o'zingizning tarmog'ingizning interfaol grafik xaritasini olishingiz mumkin.

Zenmap - bu juda katta yordamchi dastur bo'lib, u tarmoq ma'murlariga deyarli har qanday hajmdagi tarmoqlarni tekshirish imkoniyatini beradi. Ajoyib vosita, ulardan foydalanish oson va qo'shimcha ravishda - OpenSource. Profil muharririni sinchkovlik bilan tekshirib ko'ring va o'zingiz uchun hamma narsani eng yaxshi tarzda sozlang, shunda siz ushbu vositaning to'liq kuchini to'liq bilib olasiz.

Ilova 4.

Xakerlik hujumlari va guruhlariga misollar

Ashley Madisonga nisbatan hujum

Internet tarixidagi eng epik mojarolardan biri. Ashley Madison– tanishuv, turmush quruvchilarga mo'ljallangan Kanada ijtimoiy tanishish xizmati 2002 yilda "Hayot qisqa. Romanni yoningiz tomon boshlang" shiori ostida ish boshlangan. 2015 yilga kelib, xizmat butun dunyo bo'ylab 40 milliondan ortiq foydalanuvchilarga ega bo'ldi. O'zini Impact Team deb atagan xakerlar guruhi bu saytning mijozi bo'lgan,

biroq vaqt o'tib o'zi haqidagi ma'lumotni o'chirib tashlashni talab qilgan odamlarga taalluqli axborotni ham qo'lga kiritganini e'lon qilgandi. Ko'p vaqt o'tmay, foydalanuvchi ma'lumotlari internet orqali turli web-saytlar va forumlarda "fosh etildi".

Bu axborot sirqib chiqishi oqibatida ajralishlarning sonini hisoblash qiyin. Eng achinarlisi, ba'zi holatlarda odamlar o'zlarining qayd yozuvlari va xat-xabarlari ommaga oshkor qilingach, o'z joniga qasd qilishdi.

Stuxnet qurtlari

G'arb Eronning yadroviy dasturini bir necha yil avval Stuxnet kompyuter viruslari yordamida zararsizlantirishga muvaffaq bo'ldi. Bu mashhur virus 2010 yilda kashf etilgan bo'lib, uning yordamida Eronning yadroviy dasturi to'xtatilgan edi. Eron dunyoning qolgan barcha nasihat va tahdidlariga qaramasdan, Eron ushbu yadroviy dasturini qisqartirishdan bosh tortdi.

Amerika ommaviy axborot vositalarining ma'lum qilishicha, Stuxnet Qo'shma Shtatlar va Isroilning razvedka xizmatlari tomonidan birgalikda ishlab chiqilgan. Ular birgalikda uni Isroil cho'lidagi ma'lumot markazida sinab ko'rishdi va keyinchalik uni Eronning yadroviy dasturida ishtirok etgan Eron olimlari tomonidan qo'llaniladigan kompyuter tarmog'iga olib kirishdi.

"Qurt" uranni sinash uchun ishlatilgan sentrifuglarning uchdan ikki qismini nazorat qilib, ularning ishlariga kichik o'zgarishlar kiritdi. Shuning uchun eronliklar o'zgarishlarni deyarli payqashmagan. Buning o'rniga, ular o'zlarini adashgan deb hisobladi va tadqiqotlari noto'g'ri yo'nalishda degan xulosaga kelishdi. Ushbu xakerlar hujumi tufayli Eron yadroviy dasturi bir necha yilga kechiktirilgan.

Melissa virusi

1999-yili, Nyu-Jersidagi dasturchi Devid Smit Windows tizimi boshqaruvi ostida ishlaydigan kompyuterlarga internet orqali virusni tarqatdi. Virus "Microsoft Word" dagi "Muhim xabar ..." elektron-xatcho'piga biriktirib qo'yilgan. Virusga maxsus joziba qo'shildi, chunki maktub ilovasida nomaqbul pulli saytlar uchun to'lovlar qilishda

ishlatiluvchi parollar bo‘lgan matnli faylni o‘z ichiga olgan. Hisoblash muvaffaqiyatli bo‘ldi.

Foydalanuvchi ilovani bosgandan so‘ng, Melissa faollashdi va kompyuterni birinchi ellik kishi uchun ommaviy pochta sifatida ko‘chirishni buyuradi. Foydalanuvchilar faylni faol ravishda ochdilar. Biroq to‘g‘ri, parollar yo‘q edi. Aksincha, foydalanuvchilarning kompyuterlarini zararlovchi makros bor edi. Virus tizimning juda muhim fayllarini o‘zgartirdi.

Ba’zi ma’lumotlarga ko‘ra, dunyodagi kompyuterlarning 20 foizi ushbu virus bilan zararlangan. Tabiiyki, biz Windows-ning kompyuterlari haqida gapiramiz. Melissa virusi nafaqat butun avlodga taqlid qilardi, balki parazitlar sonini ko‘paytirdi. Mutaxassislarning fikriga ko‘ra, virusning nusxalari Internet orqali Windowsni yangilashni yoqtirmaydigan foydalanuvchilarning kompyuterini zararlashni davom ettirmoqda.

Sony Playstation bazasi

Sony Playstation tarmog‘ini buzilishi so‘nggi yillardagi eng mashhur voqealardan biriga aylandi. 2011-yilda o‘zlarini Lulzsec deb nomlagan bir guruh xakerlar Sony Playstation tarmog‘idagi Sony ma’lumotlar bazasini yorib, 77 milliondan ortiq o‘yinchilar login va parollari, kontakt ma’lumotlarini ochiqladi. Sony vakillari, o‘yinchilar kredit karta ma’lumotlarining o‘g‘irlanmaganligini e’tirof etishdi.

Mojaro epik tus oldi. Sony xavfsizlik tizimini takomillashtirish va zaifliklarni yaxshilash maqsadida bir necha kun davomida o‘yin xizmatini to‘xtatishga majbur bo‘ldi. Xakerlar tomonidan o‘g‘irlangan ma’lumotlar sotilmaganligi yoki hech kimning zarariga ishlatilmagani aniq bo‘lganidan so‘ng ham, mojaroning o‘lchamlari va Sony-ning obro‘siga putur etkazish to‘xtab qolmadi.

Shuningdek, 2014-yilda Sony serverlari takror hujumga uchragan. Bu safar xakerlar kompaniyaning kino biznesiga qiziqish bildirishdi. Filmlarning nashr etilmagan nusxalari, ishlab chiqaruvchilarning ichki qiyofasi o‘g‘irlangan. Ushbu hujum Shimoliy Koreya bilan bog‘liq. Aftidan, Koreyalik xakerlar Sony Pictures kompaniyasini o‘zlarining

mamlakat rahbariyatiga suiqasdga urinishi haqidagi filmni chiqarishni taqiqlab qo'ymoqchi bo'lishgan.

Home Depot buzg'unchiligi

2014 yilning yozida xakerlar Amerikaning yirik «Home Depot» savdo tarmog'ining serveriga kirishdi. Buzg'unchilik, Microsoft Windows operatsion tizimidagi zaiflik sababli amalga oshirildi. Home Depotga qilingan hujum haqida ma'lumotga ega bo'lgan Microsoft, "tuynukni" qoplagan "patch" ni chiqardi, ammo bu juda kech edi. Xakerlar bir muncha vaqt tizimda bo'lgan va 56 milliondan ortiq to'lov kartalari ma'lumotlarini o'g'irlashgan.

Xaker hujumidan keyingi zararni hisoblash qiyin, ammo haqiqat muhim - bu tarixdagi foydalanuvchi ma'lumotlarining eng katta o'g'irlanishi bo'lib, bunga birgina operatsion tizimdagi zaiflik kifoya qildi.

eBay buzg'unchiligi

Dunyoning eng mashhur onlayn bozori bo'lgan EBay, 2014-yilning yozida, katta xakerlik hujumi ta'sirida qoldi, natijada 145 milliondan ortiq foydalanuvchilar shaxsiy ma'lumotlari o'g'irlangan. To'g'ri, ma'lumotlar sirqib chiqishi moliyaviy ma'lumotlarga, to'lov kartalari haqidagi ma'lumotlarga ta'sir ko'rsatmadi.

EBayga yetkazilgan zarar miqdori juda katta edi. Milliondan ortiq onlayn xaridorlar parol bilan himoyalangan ma'lumotlarni yo'qotdi. Ushbu xaker hujumi Internet tarixidagi eng ommaboplardan biri bo'lgan. Shuningdek, eBay hamon "tuynuk"larni kiber xavfsizlik asosida yo'q qilishga harakat qilmoqda.

Spamhaus: tarixdagi eng katta DDOS hujumi

Spamhaus xizmatida spamerlar va xakerlar qora ro'yxati kiritilgan bo'lib, Internet tarixidagi eng kuchli DDOS hujumlarining maqsadiga aylandi. DDOS hujumi asosan katta hajmdagi ma'lumotlar oqimidir. Minglab kompyuterlar, ba'zan butun dunyo bo'ylab, xakerlar kompyuter tizimlarini so'rov toshqini, ortiqcha yuklanishiga majburlaydi.

2013 yil mart oyida ushbu DDOS hujumi juda keng tarqalgan bo'lib, butun sayyoramizdagi Internet ishini sekinlashtirdi va aksariyat mamlakatlarda soatlab internetni butunlay o'chirib qo'ydi. Jinoyatchilar

signallarni kuchaytirib qayta jo'natish uchun yuzlab DNS serverlarini ishlatishdi va uni tarmoqdagi har bir serverga soniyasiga 300 gigabit tezlikgacha uzatdilar.

Hujum, qasoskorlik harakati bo'ldi, Spamhaus faoliyati tufayli Internet-serverlarning qora ro'yxatlari mavjud bo'lib, ulardan katta miqdordagi istalmagan pochta jo'natmalari amalga oshirilmoqda. Dunyo bo'ylab internet-provayderlar ushbu ro'yxatlarni spam manbalarini bloklash uchun foydalanishi va o'z foydalanuvchilarini "Nigeriyalik baxt maktublari" dan ozod qilish va " enlarge your pencil " kabi qiziqarli takliflarni taklif qilishi mumkin.

Mashhur xaker guruhlari

Lizard Squad

Lizard Squad haqidagi ma'lumotlar ommaviy axborot vositalarida birinchi marta "League of Legends" va "Call of Duty" o'yinlarini taqdim etganlaridan so'ng paydo bo'ldi. Keyinchalik Sony Playstation Network va Microsoft Xbox Live kabi jiddiy hujumga duch keldik. Ko'rinishidan, ushbu guruh vakillari Sony personallariga yoqmasdi. 2014 yil avgust oyida ular Twitter-da Sony Online Entertainment prezidenti uchib kelgan samolyotni portlatish bilan tahdid qilishdi.Yaxshiyamki, samolyot favqulodda qo'nishni amalga oshirdi va hamma narsa qurbonlarsiz amalga oshirildi.

Bundan tashqari, Lizard Squad Islomiy Davlat bilan aloqasini e'lon qiladi. Misol uchun, Malaysia Airlines kompaniyasiga qilingan hujumdan so'ng, hacktivistlar kompaniyaning web-saytida "Lizard Squad-rasmiy Kiber-Xalifalikka qarshi" nomli xabarni e'lon qilishdi. ISIS g'alaba qozonadi". Bir necha oy oldin, ular Sony serverlarida ISIS bayroqlarini joylashtirishdi. Biroq, guruhning faoliyati siyosiy sabablarga ko'ra emas, balki, ommaviy axborot vositalarining diqqatini jalb qilish uchun ISISga murojaat qilish kerak.

2. Anonymous

Anonymous-ehtimol, barcha zamonning eng mashhur xakerlik guruhidir. Bu kompyuter hujumlari ijtimoiy va siyosiy hodisalar yuzaga kelishiga sabab bo'lgan o'n minglab hacktivistlarning markazsizlashtirilgan onlayn jamiyati. Guruh hukumat, diniy va

korporativ web-saytlarga ko'p sonli hujumlardan keyin mashhur bo'ldi. U Pentagonga hujum qilib, Facebookni ezib tashlash, Los Zetasni, Meksikadagi giyohvand kartelini yo'q qilish va Scientologiyaga qarshi urush e'lon qilish bilan tahdid qildi.

2010 yilda Anonymous Visa, MasterCard va PayPal tizimlariga hujumlarni kamaytirishga qaratilgan katta miqyosli aksiyalarni qaytarish operatsiyasi (Operation Payback) ni tashkil qildi. WikiLeaks asoschisi Julian Assanj asos solgan. 2011 yilda hacktivistlar Nyu-York fond birjasining web-saytiga hujum qilib, ijtimoiy-iqtisodiy tengsizlikka qarshi "Захвати Уолл-стрит" (Occupy Wall Street) harakatini qo'llab-quvvatlashdi.

2010-yilda, Anonymous Visa, MasterCard va PayPalga qarshi hujumlarni boshladi.

2009 yildan beri AQSh, Buyuk Britaniya, Avstraliya, Niderlandiya, Ispaniya va Turkiyadagi o'nlab odamlar Anonim faoliyati bilan shug'ullangani uchun hibsga olingan. Guruh vakillari bunday taqiblarni qoralaydilar va o'zlarini asirga oladigan shahidlar deb atashmoqda. Xaktivist shiori: "Biz Anonimmiz. Biz legionmiz. Biz kechirmaymiz. Bizni kuting».

3. LulzSec

LulzSec (Lulz Security qisqartmasi) - bu eng xavfsiz deb hisoblangan kompaniyalar serverlariga "kulgi uchun" hujum qiladigan tashkilot. Dastlab, u "2011 yildan buyon sizning xavfsizligingiz ustidan kulish" shiori ostida ishlagan yetti nafar ishtirokchidan iborat edi. Sana tasodifan tanlanmagan: 2011 yilda Anonymous nomi allaqachon mashhur bo'lgan va u HBGary federalga katta zarba bergan. Keyinchalik bu hodisa Forbes jurnali uchun eng yuqori darajali kiber jinoyatlar ro'yxatiga kiritilgan. Xaker guruhining nomi "Lulz" - LOL (Laughing Out Loud)dir.

LulzSecning birinchi hujumlari asosida Fox.com, LinkedIn va 73,000 X Factor ishtirokchilari parollari o'g'rilangan. 2011-yilda ular Sony Pictures-ning foydalanuvchisi hisoblarini buzgan va rasmiy CIA web-saytini o'chirib qo'yishgan.

Muvaffaqiyatli hujumlardan so‘ng, LulzSec an’anaviy ravishda manbalarga bostirib kirishni qoldirdi, natijada ba’zi mutaxassislar ularni jiddiy cybermovers emas, balki Internet jokerlari deb hisoblashga moyil. Biroq, guruhning vakillari o‘zlarini ko‘proq qobiliyatga ega deb hisoblashgan.

2011 yil iyun oyida LulzSec o‘zini-o‘zi tarqatish to‘g‘risida xabarni yubordi. Biroq, bir oy o‘tgach, xakerlar News Corporation gazetasiga yangi hujumni boshladilar. Ular The Sun web-saytiga kirib, uning bosh sahifasida uning avtori Rupert Merdokning o‘limi haqidagi xabarni joylashtirdilar.

LulzSecning asosiy ishtirokchilari 2012 yilda hibsga olingan. FBI axborot xodimi 28 yoshli guruhning boshlig‘i edi. Xete Xavier Monsegur, Sabu nomi bilan atalgan. Prokuror Sandip Patel o‘z nutqida xakerlar “Anonymous” kabi siyosiy g‘oyalar bilan bog‘liq emasligini bildirdi va ularni “bugungi kun qaroqchilari” deb atadi.

4. Syrian Electronic Army

Suriya Elektron Armiyasi (SEA) xakerlik guruhining maqsadi Suriya Prezidenti Bashar Asadni qo‘llab-quvvatlashdir. Hujumchilarning maqsadi-ko‘pincha siyosiy muxolifat guruhlari, inson huquqlari tashkilotlari va G‘arbning yangiliklar saytlaridir. Guruhning Suriya hukumati bilan aloqalari mantiqsiz. Veb-saytida SEA o‘zini “Suriyadagi qo‘zg‘olonga oid dalillarni keng tarqalib ketishiga befarq bo‘lmaydigan yosh suriyalik qo‘shiqchilar guruhi” deb tariflaydi. Ayni paytda, bir qator ekspertlar tashkilot o‘z faoliyatini Suriya hukumati nazorati ostida olib borayotganini takidlamoqda.

SEA tomonidan qo‘llaniladigan usullar qatorida an’anaviy DDoS hujumlari, spam, fishing va viruslarni tarqatish hisoblanadi. Hujum qilingan saytning asosiy sahifasida ular odatda siyosiy xabarlar va Suriya bayrog‘ini joylashtiradilar. Suriya kompyuterlari qurbonlari The Independent, The Daily Telegraph, Evening Standard, The Daily Express, Forbes, Chicago Tribune, CBC, La Repubblica va boshqa nashrlar bo‘lishdi. Syrian Electronic Army a‘zolari Barak Obama va Nikolya Sarkozining Facebookdagi qayd yozuvlariga ham hujum qilishdi.

Ilova 5.

DDoS hujumiga qarshilik namunalari

Jadvalda tipik hujumlar va ta'sir, manbalar cheklanganida qilinadigan harakatlar haqidagi odatiy tushunchalar va kengroq bilim bazasi va chuqur tahlilga asoslangan boshqa ta'sirlar bilan taqqoslanadi.

Tex./bosh direktor savollar	Bugungi javoblar qanday	Qanday javoblar bo'lishi kerak
Hujumga qanday qarshi kurashamiz?	Dos-hujumlar aks ettirish tizimi ma'lum trafikni blokirovka qiladi, o'tkazuvchanlikni 60 foizga kamaytiradi, ammo trafikning 40 foizi hanuzgacha tarmoqqa kiradi va xavfsizlik devoriga salbiy ta'sir qiladi. Biz xavfsizlik devori sessiyalari jadvalini kengaytirish ustida ishlamoqdamiz; ammo buni amalga oshirish uchun siz uni qayta yoqishingiz kerak bo'ladi.	SYN flood hujumi DOS hujumlariga qarshi kurashish tizimi yordamida muvaffaqiyatli bloklandi. HTTP - flood hujumi yanada murakkabroq edi, uni so'rovlarga javob berish texnologiyasi bilan to'xtatib bo'lmadi. Buning o'rniga, xulq-atvorni tahlil qilish texnologiyasi faollashtirildi va u samarali bo'ldi. Ishlatilgan hujum turi R.U.D.Y. Bu yangi versiya va mavjud xavfsizlik xususiyatlari tomonidan samarali ravishda to'xtatilmagan. Uni blokirovka qilish uchun biz maxsus signatura yaratdik.
Bunga kim javobgar?	Uni bilib bo'lmaydi. Ammo, trafik dunyoning turli burchaklaridan kelganligi ma'lum bo'ldi. Biz Evropa xaridorlarini yo'qotmaslik uchun geo-himoyadan foydalanishni istamaymiz.	Hujum qilganlarning IP-manzillari Sharqiy Evropa kibertashkiloti tomonidan boshqariladigan taniqli botnetga tegishli. Ushbu tashkilot "buyurtma berish uchun DDoS" ni taklif qiladi; hujumning narxi, ehtimol, 1000 dollarni tashkil qiladi. Buyurtmachilarning

		hujumiga sabab odatda tijorat raqobatidir.
Biz uni to‘xtata olamizmi?	Yo‘q, nima qilish lozim?	Xo‘sh? Biz hujumni to‘xtatish uchun qarshi hujum texnikasini qo‘llaymiz. Biz TCP RST paketlarini yuborish orqali ularning vositalaridan birini sekinlashtira oldik, shuningdek, oyna hajmi maydoniga nol qiymati bo‘lgan paketdan foydalanib, boshqa vositani to‘liq ishlatmay qo‘ydik.
Boshqa risklar mavjudmi?	Bizdagi ma’lumotlarga binoan, yo‘q.	Ushbu guruhda bizning tashkilotimizning ichki tarmog‘iga kirishga harakat qiladigan xakerlar borligini bilamiz, shuning uchun biz nafaqat DDoS hujum qaydlarini, balki boshqa barcha xavfsizlik voqealarini ham kuzatib boramiz. Xavfsizlik devori, IPS va WAF-ga kirish imkoniyati mavjud va ular doimo ishlaydi.
Hujum to‘liq bartaraf etilganmi?	Ha, hujum qilganlarning faolligi biz ertalab kuzatgan trafiklarga nisbatan pasaygan. Biz tajovuzkorlarning 70% harakatlariga to‘sqinlik qildik. Sayt hali ham sekin ishlaydi, lekin hech bo‘lmaganda ishlaydi.	Ha. Sayt normal kechikish bilan juda yaxshi ishlaydi. Tizimga ruxsatsiz kirish ro‘yxatdan o‘tkazilmagan.

S.Y. YUSUPOV, A.A. GANIYEV, O.N. BEKMIRZAYEV

KOMPYUTER TIZIMLARI VA TARMOQLARINI BUZISH VA HIMOYALASH

O'quv qo'llanma

Muharrir **Sh. Bazarova**
Badiiy muharrir **K. Boyxo'jayev**
Kompyuterda sahifalovchi **Z. Ulug'bekova**

Nashr. lits. AI № 305.
Bosishga ruxsat 10.03.2023-yilda berildi.
Bichimi 60x84 1/16. Ofset qog'ozi №2.
"Times New Roman" garniturasi.
Shartli b.t. 13,4. Nashr hisob t. 13,8.
Adadi 100 dona. 5-buyurtma.

«IQTISOD-MOLIYA» nashriyoti
100000, Toshkent, Amir Temur, 60 «A».

«DAVR MATBUOT SAVDO» MCHJ
bosmaxonasida chop etildi.
100198, Toshkent, Qo'yliq, 4-mavze, 46.