# WEB SAYTLARGA BO‘LADIGAN HUJUM TURLARI VA ULARNI BARTARAF ETISH USULLARI

***Tuxtanazarov Dilmurod Solijonovich,*** *O’zXIA ZAKT kafedrasi dotsenti, PhD.*
***Muxammadjonov Xojiakbar Zafarjon o’g’li,*** *O‘zbekiston Respublikasi IIV Akademiyasi Axborot texnologiyalari kafedrasi o‘qituvchisi*

**Annotatsiya**

Ushbu maqolada web saytlarga bo`ladiga hujum turlari keltirilgan. Xozirgi kundagi ko‘p kuzatilayotgan hujum turlari va bunday turdagi hujumlarning sabablari tahlil qilingan. Asosiy hujumlardan DDoS hujumi, SQL-injection, Man-in-the-middle hujumlari, Cross-site scripting (XSS) hujumlari va DNS hujumlari bo`yicha ma’lumotlar keltirib o‘tilgan. Web saytlarga bo‘ladigan hujumlarning sabablari va ularni oldini olish bo‘yicha tavsiyalar keltirilgan.

**Kalit so‘zlar:** Web sayt, Internet, DDoS, SQL-injection, Cross-site scripting, hujum, axborot xavfsizligi, zaifliklar, ma’lumotlar.

Hozirgi kunda kompyuter tarmoqlarini buzishni va boshqa kiberjinoyatlarni amalga oshirishni o‘rganish bo‘yicha axborotga ega bo‘lish juda oson. Kompyuter jinoyatchiligini sodir etish texnologiyasi keltirilgan bosma nashrlar erkin tarqatiladi.

Web-saytlarga hujumlar uning normal ishlashini buzish, maxfiy ma’lumotlarni o‘g‘irlash yoki web-sayt ma’lumotlar bazalariga ruxsatsiz kirish maqsadida web-sayt xavfsizligini buzish uchun ishlatiladigan zararli harakatlar yoki taktikalarni anglatadi. Ushbu hujumlar web-sayt kodlari, arxitekturasi yoki infratuzilmasidagi zaifliklardan foydalanishga intiladigan xakerlar, kiberjinoyatchilar va boshqa zararli shaxslar tomonidan amalga oshirilishi mumkin.

Web-saytlarga hujumlarning keng tarqalgan turlari orasida DDoS hujumlari, SQL in’ektsiya hujumlari, XSS hujumlari, fishing hujumlari, zararli dastur hujumlari, qo‘pol kuch hujumlari, O‘rtadagi odam hujumlari va boshqalar kiradi. Odatda web-sayt egalariga dasturiy ta’minotni muntazam yangilash, xavfsizlik protokollarini joriy etish va foydalanuvchilar o‘rtasida xabardorlikni oshirish kabi hujumlarning oldini olish va yumshatish uchun xavfsizlik choralarini ko‘rish tavsiya etiladi.

Buzg‘unchi tarmoqning biror-bir tashkil etuvchisining ishini buzish orqali butun tarmoqni obro‘sizlantirishi mumkin. Zamonaviy telekommunikatsiya texnologiyalari lokal tarmoqlarni global tarmoqqa – Internetga ulash imkonini berdi. Internetning rivojlanishi xavfsizlikni ta’minlashni dolzarb masalaga aylantirdi va Internetga ulangan tarmoq va tizimlarda, qanday ma’lumotlarga ishlov berilishidan qat’iy nazar, xavfsizlik vositalari bo‘lishini taqozo etadi.

Internetga ulangan kompyuter tajovuz obyekti bo‘lsa, hujumni amalga oshirayotgan shaxsga uning qayerda (qo‘shni xonada yoki boshqa kontinentda) joylashgani katta ahamiyatga ega emas.

Tarmoq texnologiyalari rivojining boshlang‘ich bosqichida viruslar va kompyuter xujumlarining boshqa turlari ta’siridagi zarar kam edi, chunki u davrda dunyo iqtisodining axborot texnologiyalariga bog‘liqligi katta emas edi. Hozirda, xujumlar sonining doimo o‘sishi hamda biznesning axborotdan foydalanish va almashishning elektron vositalariga bog‘liqligi sharoitida mashina vaqtining yo‘qolishiga olib keluvchi hatto ozgina hujumdan kelgan zarar juda katta raqamlar orqali hisoblanadi.

Tarmoqqa noqonuniy kirish, axborotlardan foydalanish va o‘zgartirish, yo‘qotish kabi muammolardan himoya qilish dolzarb masala bo‘lib qoldi. Ish faoliyatini tarmoq bilan bog‘lagan korxona, tashkilotlar hamda davlat idoralari ma’lumot almashish uchun tarmoqqa bog‘lanishidan oldin tarmoq xavfsizligiga jiddiy e’tibor qaratishi kerak.

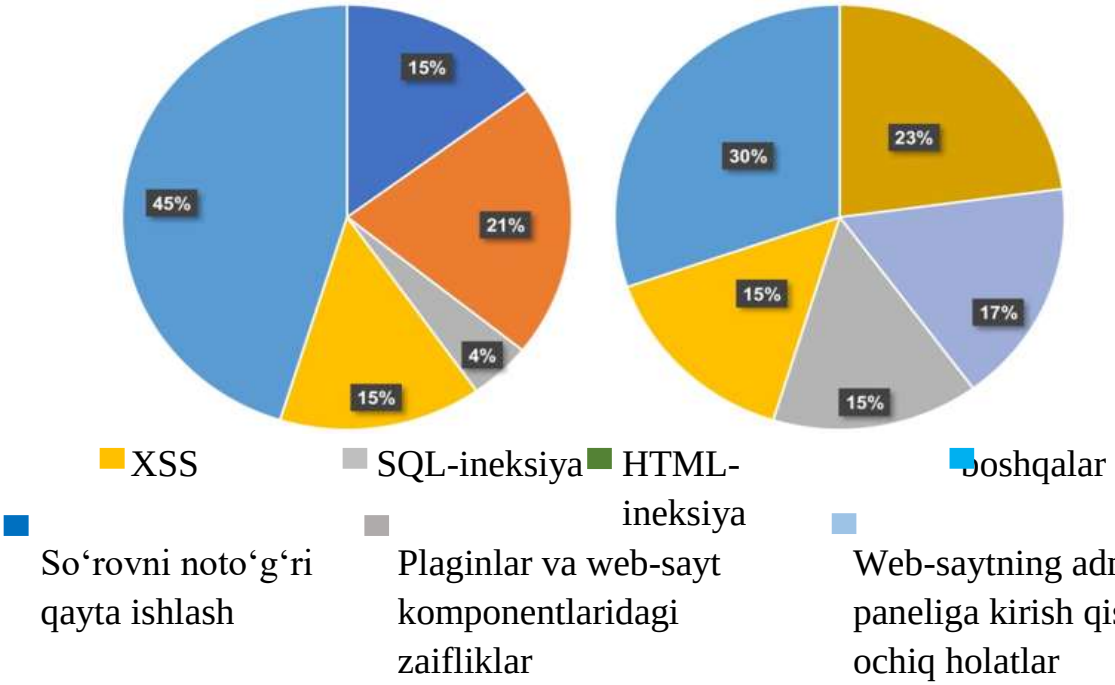
Tarmoq xavfsizligi uzatilayotgan, saqlanayotgan va qayta ishlanayotgan axborotni ishonchli tizimli tarzda ta’minlash maqsadida turli vositalar va usullarni qo‘llash, choralarni ko‘rish va tadbirlarni amalga oshirish orqali amalga oshiriladi. Tarmoq xavsizligini ta’minlash maqsadida qo‘llanilgan vosita xavf-xatarni tezda aniqlashi va unga nisbatan qarshi chora ko‘rishi kerak. Tarmoq xavfsizligiga tahdidlarning ko‘p turlari bor, biroq ular bir necha toifalarga bo‘linadi:[1]

– axborotni uzatish jarayonida hujum qilish orqali, eshitish va o‘zgartirish (Eavesdropping);
– xizmat ko‘rsatishdan voz kechish (Denial-of-service);
– portlarni tekshirish (Port scanning).

Axborotni uzatish jarayonida, eshitish va o‘zgartirish hujumi bilan telefon aloqa liniyalari, Internet orqali tezkor xabar almashish, videokonferensiya va faks jo‘natmalari orqali amalga oshiriladigan axborot almashinuvida foydalanuvchilarga sezdirmagan holatda axborotlarni tinglash, o‘zgartirish hamda to‘sib qo‘yish mumkin. Bir qancha tarmoqni tahlillovchi protokollar orqali bu hujumni amalga oshirish mumkin. Hujumni amalga oshiruvchi dasturiy ta’minotlar orqali CODEC (video yoki ovozli analog signalni raqamli signalga aylantirib berish va aksincha) standartidagi raqamli tovushni osonlik bilan yuqori sifatli, ammo katta hajmni egallaydigan ovozli fayllar (WAV)ga aylantirib beradi.

Axborot tizimlardagi zaifliklar Web-saytlardagi zaifliklar

[11] https://azkurs.org/mavzu-tarmoq-xavfsizligiga-zamonaviy-tahdidlar.html



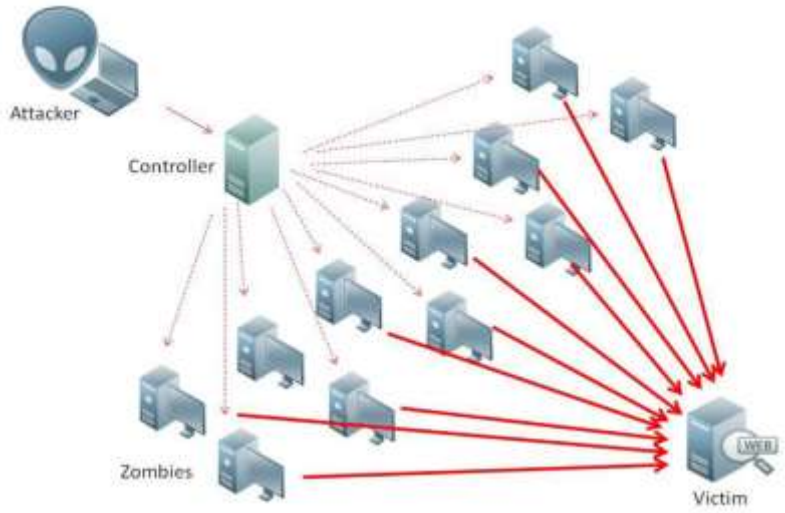

1 – rasm. 2021-yilda milliy Internet segmentida 1,3 milliondan ortiq kiberhujumlar tahlili[2]

Web-saytlarga bo‘ladigan hujum turlari juda ko‘pdir, ulardan ba’zilari katta zarar keltirishi mumkin.

DDoS hujumlari: DDoS (Distributed Denial of Service) hujumida, bir yoki bir nechta hujumchilar ko‘p sonli qurilmalardan foydalanib, maqsadga muvofiq bir vaqtda kompyuter tarmog‘ining ta’mirlash tizimlariga (serverlarga yoki saytlarga) ko‘p muddatli so‘rovlar (trafik) yuborish orqali, tarmoq xizmatlarining ishlashi uchun zaruriy tarmoq resurslarini bo‘shatishga urinib keladi. Bu hujum shaxsiy maqsadlar uchun, yoki korxonalar, siyosiy tomonlar, maishiy xizmatlar yoki siyosiy maqsadlar uchun amalga oshirilishi mumkin.

DDoS hujumida tizimlarda ko`plab xavfsizlik turllari muhimdir. Bu turlar hujumlarni cheklash va doimiy monitoring jarayonlarini o‘z ichiga oluvchi xavfsizlik vositalari, shu jumladan, firewall, Intrusion Detection System (IDS), Intrusion Prevention System (IPS) va DDoS qutqaruvchi (DDoS Mitigation) tizimlarini o‘z ichiga oladi. Ayni vaqtda, tarmoq xizmatlarini amalga oshiruvchi korxonalar va kompaniyalar tarmoqarini xavfsizligini ta’minlash uchun doimiy ravishda xavfsizlik turlarini ko‘paytirishga ham harakat qilishlari zarur bo‘ladi.

[2] https://www.google.com/url?sa=i&url=https%3A%2F%2Fkun.uz%2Fuz%2Fnews%2F2022%2F03%2F02%




2-rasm. DDoS hujumi[3]

DDoS hujumi bo`lishini oldini olish uchun, tarmoqlar faqat to‘g‘ridan-to‘g‘ri saytlarga kirish huquqini o‘zgartirish, filtrlash yoki qo‘shimcha tekshiruvlar orqali hujumlar haqida bildirishlar berish kabi qo‘shimcha chora-tadbirlarini amalga oshirishlari lozim.

Malware hujumlari: Malware, yoki zararli dasturlar, foydalanuvchilarning ruxsati yo‘q ko‘rsatkichsiz kompyuteriga yoki tarmog‘iga yuklanishi mumkin bo‘lgan dasturlar yoki fayllar bo‘lib, bu dasturlarning tizimni buzish, shaxsiy ma’lumotlarni olish, o‘chirish yoki tarmoq xavfsizligini buzish maqsadlari uchun yaratilgan.

Malwareni odatda mutaxassislar qiyinchilik bilan aniqlaydilar, chunki ular avvalo qo‘llashni kutmagan dasturlar yoki fayllar bilan birgalikda yuklanadi. Bundan tashqari, ular odatda foydalanuvchilar tomonidan yukangan fayllar oqali ham amalga oshirilishi mumkin. Bu esa Internetdan yuklab olingan fayllarni tekshirish talab etadi.

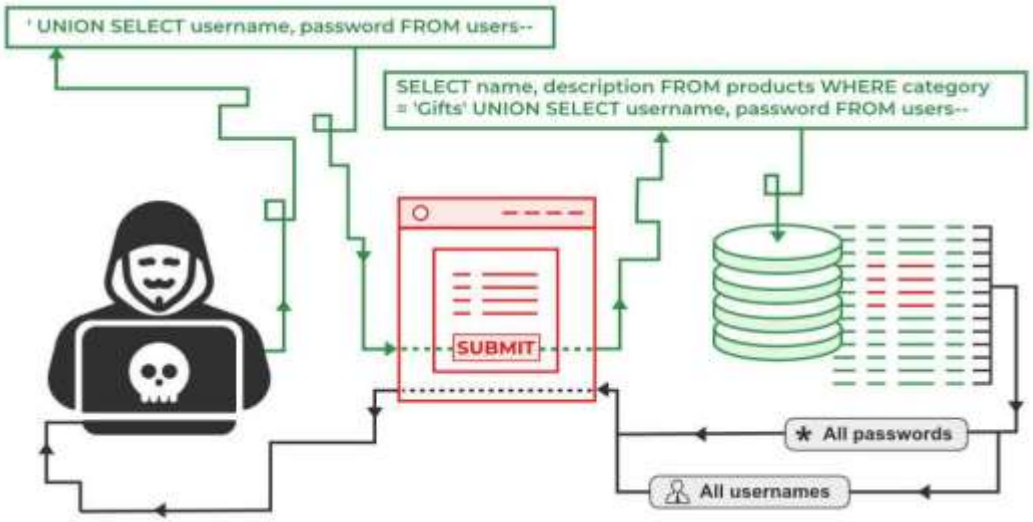
Malware turli shakllarda bo‘ladi, shu jumladan, viruslar, truva atlar, kimyoviy dona (rootkit), spyware va ransomware kabi.


3-rasm. Malware hujumi

[3] https://www.google.com/url?sa=i&url=https%3A%2F%

Ular bir qismini qurilmalarning ochiq operatsion tizimi, brauzer yoki dasturlarning xususiyliklaridan foydalanib, foydalanuvchilarning ma’lumotlari va shaxsiy ma’lumotlarini olish uchun yaratilgan. Malware dan himoyalanish uchun, tizim yoki dasturlar tarkibini yangilash jarayonlari nazorat qilinishi kerak. Shuningdek, foydalanuvchilar keng tarqalgan zararli manbalardan (e-pochta yoki ishonchsiz web resurslardan) saqlanishiga e’tibor berishlari va ularda turli fayllarni yuklab olishni amalga oshirmasligi lozim.

SQL-injection, tarmoq yoki web-saytlar orqali hujum qilishning shakllaridan biri hisoblanadi. Bu hujum turida, hakerlar sayt yoki tarmoqga ma’lum bir dastur orqali kirib, SQL buyruqlarini o‘zgartirish orqali sayt yoki tarmoqdan ma’lumot olishishga harakat qiladi. SQL-Inject hujumi tarmoq yoki saytning ma’lumotlar bazasiga kirish yoki uni o‘zgartirish orqali amaliyotlar bajarish imkoniyatini yaratadi. Hakerlar saytda hujumni amalga oshirish uchun, SQL so‘ro‘vlari ma’lum bir forma yoki sahifada ishlatilgan bo‘lishi kerak. Hakerlar tarmoq yoki saytning SQL bazasiga o‘z SQL buyruqlarini yuborish yoki ma’lumotlarni o‘zgartirish uchun boshqa SQL buyruqlarini boshqa ma’lumotlar bilan birlashtirish imkoniyatiga ega bo‘ladi. SQL-Inject hujumlarining ta’siri ko‘p xil bo‘lishi mumkin masalan, hakerlar foydalanuvchilarning shaxsiy ma’lumotlarini olishi, bular: login va parol, kredit karta ma’lumotlari yoki tijorat yuritish bilan bog‘liq boshqa ma’lumotlarni bo‘lishi mumkin. Bunday jarayonlar orqali foydalanuvchining xavfszizligiga ta’sir o‘tkazishi mumkin.




4 - rasm. SQL-Inject hujumi

SQL-Inject hujumlaridan qutulish uchun, sayt yoki tarmoqda ishlatilgan SQL buyruqlari tekshirilishi, tarmoq yoki sayt ishchi tizimlari va serverlarining yangilash uchun kerakli yopiq ishchi tizimlari hamda dasturlar yuklanishi kerak. Shuningdek, foydalanuvchilar saqlanadigan ma’lumotlarga e’tibor qaratish va ularni muhitni ko‘chirish orqali saqlash, SQL-Inject hujumlaridan qutulish uchun xizmat qiladi.

Cross-site scripting (XSS) hujumlari: Cross-site scripting (XSS) hujumi tarmoq yoki saytda amalga oshiriladigan eng ko‘p ko‘riladigan hujumlardan biridir. XSS

hujumlarida, hakerlar saytga kirib, yozilgan ma’lumotlarni o‘zgartirib, yoki ma’lumotlarga qo‘shimcha skriptlar qo‘shib, saytga kirish yoki foydalanuvchilarning ma’lumotlarini olishga harakat qiladi. Bu hujum, saytga kirish, foydalanuvchilar ma’lumotlarini olish yoki saytni buzish kabi turli xil muammolarni keltirib chiqaradi. XSS hujumining ta’siri turli xil bo‘lishi mumkin, ammo asosiy xususiyati foydalanuvchilarning shaxsiy ma’lumotlarini yoki saytning ish rejalarini buzishga qaratilgan hisoblanadi. XSS hujumlari shu jumladan foydalanuvchining saytga kirish jarayonida, sayt to‘g‘risida ma’lumot olish va shaxsiy ma’lumotlarni yuborish jarayonlarida o‘z ko‘rsatgan skriptlar yoki kodlar orqali hujum qilish mumkin. XSS hujumlari ta’sirini kamaytirish uchun, sayt yoki tarmoqda ma’lumot kiritilishi jarayonlarida ma’lumotlarni tozalash, ma’lumotlarni to‘g‘ri tekshirish va to‘g‘ri formatlash, qo‘shimcha skriptlarni aniqlash va unga aniq tashxislar qo`yish va sayt foydalanuvchilariga bevosita ma’lumot kiritishga ruxsat etilmaganligini tekshirish kabi amallar muhimdir.

Fishing hujumlari: fishing hujum, odatda e-mail, telefon, SMS yoki boshqa kommunikatsiya vositalari yordamida amalga oshiriladigan maxfiy ma’lumotlarni (masalan, bank karta raqamlari, parollar, shaxsiy ma’lumotlar) olishni maqsad qiladi. Hakerlar fishingni e-mail va web-saytlar orqali o‘zlarini bank, tashkilot yoki boshqa shaxslar deb foydalanuvchilarni ishonchiga kirishadi va tuzoqga tushirishadi.

E-mail yoki web-sayt maqbul kelgandan so‘ng, foydalanuvchi ma’lumotlarni kiritib, hakerlarga yuboradi. Fishing hujumlarida, hakerlar ma’lum bir tashkilot yoki bankning rasmiy logo, ismi yoki emblemasini ko‘rsatadigan va ma’lumotlarni to‘plab olish uchun maqbul e’lon yoki e-mail yuborishadi. Foydalanuvchilar, e’lon yoki e-mailga javob berish orqali hujumni amalga oshirishi uchun hakerlarga imkoniyat yaratib beradi.

Fishing hujumlari uchun qo‘llaniladigan boshqa usullar shu jumladan, qo‘shimcha skriptlar yordamida o‘zgartirilgan saytlar yaratish, ko‘p xil xabarlar yuborish yoki qatnashgan tashkilot yoki shaxslarning manzillarini sohtalashtirishlarni kiritish mumkin. Fishing hujumlaridan himoyalanish uchun, e-maillarni va web-saytlarni e’lon qilishda, rasmiy manzil yoki havola (URL) orqali tekshirishga harakat qilinadi. Ma’lum bir bank yoki tashkilotdan e-mail kelganida, e-mail manzilini tekshirib, hujumning ma’lum bir manzil yoki tashkilotga mansub bo‘lmaganligini aniqlanadi. Yana bir usul, ma’lumotlarni to‘plash uchun ko‘rsatilgan havolalar (URL) yoki fayllar yuklash uchun ko‘rsatilgan ssilkalar bosiladi. Bunday havolalar doim shaxsiy ma’lumotlar kiritishga imkon beradigan shaxsiy ma’lumotlar saqlash o‘rnatilmagan yoki xavfsizlik sertifikatlariga ega emas saytlar bilan bog‘liq bo‘lishi mumkin.

Man-in-the-middle (MITM) hujumlari: Man-in-the-middle (MITM) hujum, odatda foydalanuvchining Internet trafikini o‘zgartirish yoki ko‘rib chiqish maqsadida

amalga oshiriladi. Hujum boshqacha bir tarmoq elementi tomonidan amalga oshirilishi mumkin va undan xabardor bo‘lmagan foydalanuvchilarni ta’qib qilish uchun foydalaniladi. MITM hujumi, odatda tarmoqni kuzatish yoki qo‘shimcha muvaffaqiyatli hujumlar olib borilishi mumkin. Hujumda, foydalanuvchining Internet so‘rovlari hujumchi tomonidan o‘zgartiriladi va yopilgan tarmoq elementiga jo‘natiladi. Hujumchi so‘rovlarni ko‘rib chiqib, ularni o‘zgartirib, keyin foydalanuvchiga javob qaytaradi, shuningdek, odatda foydalanuvchi va saytning tarmoq bilan munosabatda bo‘lgan shaxsiy ma’lumotlariga ega bo‘lishi mumkin, masalan, parol, foydalanuvchi nomi, e-pochta manzili, shaxsiy kodi, bank karta raqami va boshqa ma’lumotlar. MITM hujumlaridan himoya qilish uchun, ko‘p foydalanuvchilar saytlar bilan munosabatda yuqori darajali xavfsizlik sertifikatlariga (SSL/TLS) ega bo‘lgan saytlarni tanlashadi. SSL/TLS, foydalanuvchining sayt bilan munosabatda turli tarmoq elementlarini (masalan, hujumchi) aniqlaydi va foydalanuvchini himoya qilishga yordam beradi. Boshqa bir usul, to‘g‘ridan-to‘g‘ri havolani (URL) kiritish orqali saytga kirishni amalga oshirishdir.

DNS hujumi: bu kiber jinoyatchilar serverning domen nomlari tizimida topilgan zaifliklardan foydalanib amalga oshirilgan xujum turlaridir. Domen nomlari tizimining maqsadi foydalanuvchi uchun qulay domen nomlarini DNS-resolver orqali mashina o‘qiy oladigan IP manzillarga tarjima qilishdir.

DNS-resolver birinchi navbatda domen nomi va IP manzili uchun o‘zining mahalliy keshini so‘raydi. Agar u yozuvlarni topa olmasa, u boshqa DNS serverlarini so‘rashda davom etadi. Agar bu bajarilmasa, u domenning kanonik xaritasini o‘z ichiga olgan DNS serverini qidiradi.

Qidiruv muvoffaqqiyatli amalga oshgandan so‘ng, so‘rov yuborgan dastur domen nomini ham, IP manzilini ham mahalliy keshda saqlaydi. Tashkilotlar masofaviy mijozlar va DNS-serverlar o‘rtasidagi trafik oqimini to‘g‘ridan-to‘g‘ri nazorat qila olmaganligi sababli, DNS hujumlari kiber jinoyatchilar uchun tarmoqlarni buzish va nosozliklarini keltirib chiqarishning nisbatan oson usuliga aylandi.

Operatsion tizimning parametrlarining tug‘ri o‘rnatilganligini yoki ularning o‘zgarmaganligini tekshirish uchun «tizim xavfsizligini skanerlash» deb nomlanuvchi 10 ga yaqin maxsus dasturlar ishlab chiqarilgan. Masalan, Solaris operatsion tizimi uchun mo‘ljallangan ASET, Netware va NT uchun KSA, Unix uchun SSS dasturlari mavjud.

SSS (System Security Scanner) dasturi . Ushbu dastur Unix operatsion tizimi urnatilgan kompyuterlarda xavfsizlik xolatini tekshirish va operatsion tizimning tashqi hamda ichki zaif qismlarini aniqlashga yo‘naltirilgan. Bundan tashqari u kirish huqularini, fayllarga egalik qilish huquqlarini, tarmoq zaxiralarini konfiguratsiyalashni, autentafikatsiyalash dasturlarini va boshqalarni tekshirishi mumkin.

Dasturning quyidagi imkoniyatlari mavjud:

– konfiguratsiyani tekshirish, ya’ni ruxsatsiz kirishlarning oldini olish maqsadida konfiguratsiyani tekshirish. Bunga konfiguratsiya fayllari, operatsion tizim versiyasi, kirish huquqlari, foydalanuvchilarning zaxiralari va parollar kiradi;

– tizimdagi xavfli o‘zgarishlarni tekshirish. Ruxsatsiz kirishlar oqibatida tizimda sodir bo‘lgan o‘zgarishlarni qidirishda qo‘llaniladi. Bunday o‘zgarishlarga quyidagi fayllar egallagan xotira xajmining o‘zgarishi, ma’lumotlarga kirish huquqi yoki fayldagi ma’lumotlarning o‘zgarishi, foydalanuvchilarning zaxiralarga kirish parametrlarining o‘zgarishi, shuningdek fayllarni ruxsatsiz boshqa bir tashqi kompyuterlarga uzatishlar kiradi;

– foydalanuvchi interfeysining qulayligi. Bu interfeys yordamida nafaqat dastur bilan qulay ishlash ta’minlanadi, balki bajarilgan ishlar bo‘yicha hisobotlar ham yaratiladi;

– masofadan skanerlash. Tarmoqdagi kompyuterlarni tekshirish va aloqa jarayonida ma’lumotlarni shifrlash imkoniyati ta’minlanadi;

bajarilgan ishlar bo‘yicha to‘liq, hisobotlar yaratiladi.

**Foydalanilgan adabiyotlar**

1. E. Jordan and A. Becker, Princeton officials broke into Yale online admissions http://www.yaledailynews.com/article.asp?AID= 19454, July 25, 2002.
2. Prof. Marwan Dwairy 2010, Journal of Child and Family Studies
3. Suzan Ali, Mounir Elgharabawy, Quentin Duchaussoy, Mohammad Mannan, and Amr Youssef Concordia University, Montreal, Canada
4. https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.geeksforgeeks.org%2Fsql-injection%2F&psig=AOvVaw3aayeeMTmsmkkWe- E
5. https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.alliantcybersecurity.com%2Fdifferent-types-malware-attacks-