KOMPYUTER TARMOQLARIDA MAVJUD HUJUM IZLARI VA ULARNING TURLARINING TASNIFI

G‘ulomov Sherzod Radjaboyevich
Muxammad al – Xorazmiy nomidagi TATU “Kiberxavfsizlik” fakulteti dekani, dotsent,
Tel:+998909708464
Email: sherzod.gulomov@tuit.uz
Ramazonova Madina Shavkatovna
Muxammad al – Xorazmiy nomidagi TATU “Kiberxavfsizlik va kriminalistika” kafedrasi assistenti,
Tel:+998997481489
Email: abdujabbor.madina1989@gmail.com
Maxkamova Dildora Begaliyevna
Muxammad al – Xorazmiy nomidagi TATU “Axborot xavfsizligi” kafedrasi stajyor-o‘qituvchisi,
Tel:+998940043840
Email:dildoramahkamova544@gmail.com

Annotatsiya. Ushbu maqolada kompyuter tarmoqlarida uchraydigan hujumlar va ularning turlariga, shuningdek, hujumlarni aniqlash va ularga qarshi kurashish usullariga e’tibor qaratilgan. Maqolada passiv va aktiv hujumlar, jumladan, **tinglash**, **DoS/DDoS hujumlari**, **SQL Injection**, **XSS**, **Phishing** kabi zararli dasturlar va ijtimoiy muhandislik hujumlari keltirilgan. Hujumlardan himoya qilish uchun **firewall**lar, **IDS/IPS tizimlari** va **antivirus dasturlari** kabi texnologiyalar ishlatiladi. Bundan tashqari, zamonaviy texnologiyalar, jumladan **sandboxing**, **mashinani o‘rganish** va **YARA qoidalari** orqali zararli faoliyatlarni aniqlash va tarmoq xavfsizligini ta’minlash usullari muhokama qilingan. **Tarmoq trafigini tahlil qilish** (NTA) esa zararli dasturlarni aniqlashda muhim vosita hisoblanadi.

Kalit so‘zlar: Eavesdropping, MitM, Dos, DDoS, XSS, Trojan Dasturlar, Social Engineering, Phishing, Baiting, Sandboxing, Mashinani o‘rganish, YARA qoidalari, Meta, String, Condition, Network traffic analysis.

Annotation. THIS ARTICLE FOCUSES ON THE ATTACKS AND TYPES OF ATTACKS ENCOUNTERED IN COMPUTER NETWORKS, AS WELL AS METHODS TO IDENTIFY AND COUNTER ATTACKS. THE ARTICLE LISTS PASSIVE AND ACTIVE ATTACKS, INCLUDING EAVESDROPPING, DOS/DDOS ATTACKS, MALWARE SUCH AS SQL INJECTION, **xss**, PHISHING, AND SOCIAL ENGINEERING ATTACKS. TECHNOLOGIES SUCH AS FIREWALLS, **ids/ips** SYSTEMS AND ANTIVIRUS SOFTWARE ARE USED TO PROTECT AGAINST ATTACKS. IN ADDITION, MODERN TECHNOLOGIES, INCLUDING SANDBOXING, MACHINE LEARNING AND METHODS FOR DETECTING MALICIOUS ACTIVITIES AND

ISSN 3030-3907

ENSURING NETWORK SECURITY THROUGH YARA RULES, WERE DISCUSSED. MEANWHILE, NETWORK TRAFFIC ANALYSIS (nta) IS AN IMPORTANT TOOL WHEN IT COMES TO DETECTING MALWARE.

Keywords: Eavesdropping, MitM, Dos, DDoS, XSS, Trojan Programs, Social Engineering, Phishing, Baiting, Sandboxing, Machine Learning, YARA Rules, Meta, String, Condition, Network traffic analysis.

Аннотация. В этой статье рассматриваются атаки, которые встречаются в компьютерных сетях, и их виды, а также методы выявления и противодействия атакам. В статье указаны пассивные и активные атаки, включая прослушивание, DoS/DDoS-атаки, такие как SQL-инъекции, XSS, фишинг и атаки социальной инженерии. Для защиты от атак используются такие технологии, как межсетевые экраны, системы IDS/IPS и антивирусное программное обеспечение. Кроме того, обсуждаются современные технологии, такие как сандбоксы, машинное обучение и правила YARA для обнаружения вредоносной активности и обеспечения сетевой безопасности. Анализ сетевого трафика (NTA) является важным инструментом для обнаружения вредоносных программ.

Ключевые слова: Прослушивание, MitM, Dos, DDoS, XSS, трояны, социальная инженерия, фишинг, приманка, песочница, машинное обучение, правила YARA, метаданные, строка, условие, анализ сетевого трафика.

Kirish

Kompyuter tarmoqlari bugungi kunda dunyo bo‘ylab axborot almashinuvi va internet orqali o‘zaro bog‘lanishning asosiy vositasiga aylandi. Biroq, shu bilan birga, tarmoqdagi ma’lumotlarni kuzatish, o‘g‘irlash yoki zarar yetkazish kabi xavflar ham ortib bormoqda. Bu xavflarning ko‘pchiligi hujumchilarning o‘z maqsadlariga erishish uchun turli xil usullardan foydalanishi bilan bog‘liqdir. Eavesdropping va Man-in-the-Middle (MitM) hujumlari tarmoqda o‘tayotgan ma’lumotlarni yashirincha eshitish va o‘zgartirish orqali amalga oshiriladi. Denial of Service (DoS) va Distributed Denial of Service (DDoS) hujumlari esa tizimning ishlashini to‘xtatish yoki uzilishlarga sabab bo‘lishni maqsad qiladi.

Bundan tashqari, XSS (Cross-Site Scripting) hujumlari veb-saytlarning zaifliklaridan foydalanib, foydalanuvchilarning brauzerlariga zararli kodni kiritishni nazarda tutadi. Troyan dasturlar esa foydalanuvchining xabarini olish yoki kompyuterini boshqarish uchun maxfiy tarzda o‘rnatilgan zararli dasturlardir. Shu bilan birga, Social Engineering va Phishing kabi psixologik manipulyatsiyalar orqali foydalanuvchilarni chalg‘itgan holda maxfiy ma’lumotlarni olish ham keng tarqalgan hujum usullari hisoblanadi.

ISSN 3030-3907

Baiting hujumi foydalanuvchini zararli dasturlarni o‘rnatishga undash uchun turli takliflar yaratadi. Sandboxing texnikasi esa dasturlarni xavfsiz muhitda ishlatish orqali ularning zararli xatti-harakatlarini aniqlashga yordam beradi. Hujumlar bilan kurashish va tarmoq xavfsizligini ta’minlashda mashinani o‘rganish (Machine Learning) texnologiyalari va YARA qoidalari ham yordam beradi. Meta, String va Condition kabi qoidalar yordamida zararli faoliyatlarni aniqlash va tahlil qilish mumkin.

Tarmoq xavfsizligini ta’minlashda Network traffic analysis (tarmoq trafikini tahlil qilish) orqali xavfli xatti-harakatlarni aniqlash, hujumlarni oldini olish va zararni kamaytirish mumkin. Ushbu maqolada kompyuter tarmoqlaridagi turli hujum izlari va ularning tasnifi haqida batafsil so‘z yuritiladi, shuningdek, ularga qarshi kurashish usullari ko‘rib chiqiladi.

Adabiyotlar tahlili va metodologiya.

Maqolada hozirgi kunda kompyuter tarmoqlarida mavjud hujum izlari va ularning turlarining tasnifi, usullari va vositalari yoritilgan adabiyotlar o‘rganib chiqildi. Ushbu sohada bir qancha olimlarning izlanish olib bormoqda. Jumladan A. Perrig, J. Stankovic, and D. Wagner [1], A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum [2], S. Shantharajah, K. Duraiswamy, G. Nawaz[3], Chen, Y., & Liu, Z. [4], Malek, A., & Qian, H.[5], Moustafa, N., & Slay, J.[6], Shankar, S., & Srinivasan, S. [7] va boshqa olimlar izlanishlar olib bormoqdalar.

Kompyuter tarmoqlarida mavjud bo‘lgan hujum izlari va ularning turlari turli xil tahdidlar va hujum metodlarini o‘z ichiga oladi. Ushbu hujumlar tarmoqning xavfsizligini buzishga, ma’lumotlarni o‘g‘irlashga yoki tizim resurslarini suiste’mol qilishga qaratilgan. Quyidagilar eng keng tarqalgan hujum turlari va ularning qisqacha tasnifi hisoblanadi.

Pasiv Hujumlar.

Tinglash (Eavesdropping). Ma’lumotlar tarmoq orqali uzatilganda hujumchi ushbu ma’lumotlarni tinglash orqali o‘zlashtiradi. Ushbu hujum turi ma’lumotlarning maxfiyligini buzadi;

Traffik Tahlili (Traffic Analysis). Hujumchi tarmoq traffigini tahlil qilish orqali tizim haqidagi muhim ma’lumotlarni (masalan, trafik oqimining o‘lchamlari, manzillar va portlar) aniqlaydi.

Aktiv Hujumlar.

- *Man-in-the-Middle (MitM).* Hujumchi ikki taraf o‘rtasidagi aloqaga aralashib, ma’lumot almashinuvini o‘zgartirishi yoki o‘g‘irlashi mumkin.

Denial of Service (DoS) va Distributed Denial of Service (DDoS). Ushbu hujumlar orqali hujumchi maqsadli server yoki tarmoq resurslariga shunchalik ko‘p so‘rov yuboradiki, u ishdan chiqadi yoki javob bera olmay qoladi;

ISSN 3030-3907

SQL Injection. Web ilovalariga zararli SQL kodlarini yuborish orqali ma'lumotlar bazasiga noqonuniy kirish yoki uni buzish;

Cross-Site Scripting (XSS). Foydalanuvchilarning brauzerlarida zararli skriptlarni bajarish orqali foydalanuvchi ma'lumotlarini o'g'irlash.

Viruslar va Wormlar. Ushbu zararli dasturlar tizim fayllariga yopishib, ularni zararlaydi yoki ko'paytiradi[1].

Trojan dasturlar. Foydalanuvchilarni aldov yo'li bilan zararli dasturlarni o'rnatishga undovchi dasturlar.

Ransomware. Fayllarni shifrlab, ularni qaytarib berish uchun to'lov talab qiluvchi zararli dastur.

Ijtimoiy muhandislik (Social Engineering).

Phishing. Foydalanuvchilarni maxfiy ma'lumotlarini (masalan, parollar va bank ma'lumotlari) oshkor qilishga undovchi aldov xabarlar yuborish.

Baiting. Foydalanuvchilarni zararli dasturlarni o'z ichiga olgan jozibali takliflar bilan jalb qilish[2].

Har bir hujum turining oldini olish uchun tarmoq xavfsizligini ta'minlashda turli xil texnologiyalar va yondashuvlar qo'llaniladi, jumladan firewallar, IDS/IPS tizimlari, xavfsizlik devorlari, antivirus dasturlari va foydalanuvchilarni o'qitish.

Kompyuter tarmoqlarida hujum izlarini aniqlash va ularning oldini olish uchun ishlatiladigan usullar va vositalar xilma-xil bo'lib, har biri o'ziga xos vazifalarni bajaradi. Bu vositalar va usullar tarmoqni monitoring qilish, xavfsizlikni ta'minlash va zararli faoliyatni bartaraf etish uchun mo'ljallangan. Quyida eng keng tarqalgan vositalar va ularning ishlatilish tahlili keltirilgan.

Sandboxing. Sandboxing xost tizimiga zarar yetkazmasdan, ularning xatti-harakatlarini kuzatish uchun alohida muhitda dasturlar yoki kodlarni ishga tushirishni o'z ichiga oladi. U odatda shubhali fayllar yoki URL manzillarni boshqariladigan muhitda bajarish va harakatlarini kuzatish orqali tahlil qilish uchun ishlatiladi. An'anaviy sandboxingga muqobil, zamonaviy yondashuv CPU darajasidagi tahlildan foydalanishni o'z ichiga oladi. Ushbu yangi avlod sandboxing usuli fayllarni virtual mashinada dinamik ravishda ishlaydi, lekin asosiy ekspluatatsiya usullarini o'ldirish zanjirida, zararli dasturlardan oldingi versiyada, deterministik, xulq-atvorga bog'liq bo'lmagan tarzda aniqlash uchun tarkibni tahlil qilishga qaratilgan. Ushbu usul potensial zararli artefaktning to'liq bajarilishi oqimiga kirish va uni to'liq «iz» yordamida tahlil qilish uchun Intel PT (Protsessor Trace) afzalliklaridan foydalanadi, shuningdek, bajarish paytida virtual xotiradagi o'zgarishlarni tekshiradi. Fayllar dastur darajasida emas, balki CPU/xotira darajasida tahlil qilinganligi sababli, ushbu yangi avlod sandboxing

ISSN 3030-3907

usuli an’anaviy qum maydonlariga qaraganda ancha tezroq bo‘lib, har bir tarkibni skanerlash uchun bir necha daqiqa vaqt ketishi mumkin.

Mashinani o‘rganish algoritmlari zararli dasturlarni ko‘rsatadigan namunalarni aniqlash uchun katta ma’lumotlar to‘plamini tahlil qilishi mumkin. Ushbu usul zararli dasturlarning o‘tmishdagi misollarini o‘rganish va vaqt o‘tishi bilan yangi tahdidlarga moslashish orqali ma’lum va noma’lum tahdidlarni aniqlashi mumkin. Samarali, mustahkam va kengaytiriladigan zararli dasturlarni aniqlash moduli har bir kompyuter foydalanuvchisi uchun asosiy komponentlar hisoblanadi. Zararli dasturiy ta’minotni aniqlash modullari obyektda to‘plangan ma’lumotlarga asoslanib, tahdid bor yoki yo‘qligini hal qiladi. Zararli dasturlarga qarshi kompaniyalar zararli dasturlarni aniqlash va tasniflashni kuchaytirish uchun tasvirlarni aniqlash, qidirish va qarorlar qabul qilishda muvaffaqiyatli qo‘llanilgan ML sohasiga murojaat qilishdi . Artur Samuel tomonidan berilgan klassik ta’rifga ko‘ra, ML - bu kompyuterlarga «Aniq dasturlashtirilmagan holda o‘rganish qobiliyatini» beradigan usullar to‘plami. Boshqacha qilib aytadigan bo‘lsak, Machine Learning algoritmi o‘zi ko‘rgan ma’lumotlarning asosini tashkil etuvchi tamoyillarni aniqlaydi va rasmiylashtiradi.

Anomaliyani aniqlash. Anomaliyalarni aniqlash usullari tizim yoki tarmoq ichidagi normal xatti-harakatlardan chetlanishlarni aniqlaydi. Bu usul noodatiy harakatlar yoki modellarni belgilash orqali ilgari noma’lum bo‘lgan zararli dasturlar yoki insayder tahdidlarni aniqlashga yordam beradi[3].

YARA qoidalari. YARA – matn yoki ikkilik namunalar asosida zararli dasturlarni aniqlash va tasniflash uchun foydalaniladigan model moslashtirish vositasi. Xavfsizlik bo‘yicha tadqiqotchilar va tahlilchilar zararli dasturlarning muayyan oilalari yoki xatti-harakatlarini aniqlash uchun YARA qoidalarini yaratadilar. YARA dasturiy ta’minotni tahlil qilish va kiberxavfsizlik bo‘yicha mutaxassislar orasida keng qo‘llaniladi. Keling, YARA haqida batafsil ma’lumotlarni ko‘rib chiqaylik.

YARA qoidalarini tushunish (Yet Another Recursive Acronym). YARA qoidalari (rules) - matnli fayllarda yozilgan qoidalar to‘plamidan iborat bo‘lib, ular bir yoki bir nechta shablonlarni qidirish uchun mo‘ljallangan. Har bir qoida quyidagi qismlardan iborat.

Meta. Qoida haqida ma’lumot beruvchi qism (masalan, muallif, tavsif).

Strings. Qidiriladigan satrlar (masalan, faylda mavjud bo‘lgan matnli yoki baytli shablonlar).

Condition. Shartlar (masalan, ma’lum bir satrlar mavjud bo‘lsa, qoida ishlaydi).[4]

ISSN 3030-3907

YARA qoidalari sintaksisi. YARA qoidalari oddiy, lekin kuchli sintaksisga ega. Quyida bir oddiy qoida misoli keltirilgan.

```
rule ExampleRule {
    meta:
        author = "Your Name"
        description = "Example rule to detect a string"
    strings:
        $text_string = "malicious"
    condition:
        $text_string
}
```

1-rasm. YARA qoidalarini kod orqali yozishga misol

Ushbu qoida “malicious” satrini o‘z ichiga olgan fayllarni aniqlaydi.

Murakkab qoidalar. YARA murakkab qoidalarni ham qo‘llab-quvvatlaydi. Masalan, siz bir nechta shartlarni birlashtirishingiz mumkin.

```
rule ComplexRule {
    meta:
        author = "Your Name"
        description = "Complex rule example"
    strings:
        $str1 = "malware"
        $str2 = "virus"
    condition:
        ($str1 and $str2) or filesize > 1MB
}
```

2-rasm. YARA qoidalarini kod orqali yozishda qo‘shimcha shartlarni kiritish

Ushbu qoida «malware» va «virus» satrlarini o‘z ichiga olgan yoki hajmi 1 MB dan katta bo‘lgan fayllarni aniqlaydi.

YARA qo‘llanmalari va uning ilovalari.

zararli dasturlarni aniqlash. Yara qoidalari zararli dasturlarni aniqlash uchun keng qo‘llaniladi. Misol uchun, zararli kod fragmentlarini qidirish uchun maxsus qoidalar yozilishi mumkin;

forensik tahlil. Tizimdagi fayllarni tahlil qilish va potentsial zararli fayllarni aniqlash uchun ishlatiladi;

kibermudofaa. Real vaqt rejimida yoki avtomatlashtirilgan jarayonlar orqali kiberxavfsizlikni mustahkamlash uchun yara qoidalari yordamida zararli faoliyatlarni aniqlash mumkin[5].

ISSN 3030-3907

YARA dasturini ishlatish. YARA ko‘p platformalarda ishlaydi va uni kompyuterda o‘rnatish va ishlatish juda oson. Quyida YARA ni Linux tizimida o‘rnatish va ishlatish ko‘rsatilgan.

```
# YARA ni o'rnatish
sudo apt-get update
sudo apt-get install yara

# YARA qoidasini ishga tushirish
yara rule_file.yar target_file
```

3-rasm. YARA ni o‘rnatish va ishga tushirish.

Bu buyruqlar yordamida YARA ni o‘rnatish va yozilgan qoida faylini maqsad faylga nisbatan ishlatish mumkin. YARA dasturi haqida xulosa qilib aytishimiz mumkinki YARA - zararli dasturiy ta’minotni aniqlash va tahlil qilish uchun kuchli vosita bo‘lib, o‘ziga xos va murakkab qoidalar yozish imkoniyatini beradi. YARA ni bilish va undan foydalanish, kiberxavfsizlik bo‘yicha mutaxassislar uchun zararli dasturlarni aniqlash va oldini olishda juda foydali bo‘lishi mumkin.

Network traffic analysis (Tarmoq trafigini tahlil qilish). Shubhali namunalar yoki imzolar uchun tarmoq trafigini monitoring qilish, buyruq va boshqaruv serverlari yoki boshqa zararli harakatlar bilan zararli dastur aloqasini aniqlashga yordam beradi. NTAni tushunish kiberxavfsizlik bo‘yicha mutaxassislarga zararli dasturlar mavjudligini ko‘rsatishi mumkin bo‘lgan shubhali harakatlarni aniqlash uchun tarmoqlar orqali oqayotgan katta hajmdagi ma’lumotlarni tahlil qilish va sharhlash imkonini beradi. NTA bo‘yicha tajriba zararli dasturlarni aniqlash va tahlil qilishda qanday yordam berishini batafsilroq ko‘rib chiqamiz.

Tarmoq trafigini tahlil qilishning asosiy komponentlari quyidagilar.

Ma’lumotlar yig‘ish. Packet Capture- Wireshark kabi vositalar jonli trafik ma’lumotlarini yozib oladi, bu esa alohida paketlarni anomaliyalar uchun batafsil tekshirish imkonini beradi. Oqim ma’lumotlari, NetFlow, IPFIX va shunga o‘xshash protokollar trafik oqimlarini umumlashtiradi va tarmoq shovqinlarining yuqori darajadagi ko‘rinishini ta’minlaydi.

Trafikni tahlil qilish texnikasi. Imzoga asoslangan aniqlash- zararli trafikni aniqlash va aniqlash uchun ma’lum zararli dastur imzolariga tayanadi. Ma’lum tahdidlar uchun samarali bo‘lsa-da, u muntazam yangilanishlarni talab qiladi va yangi, noma’lum zararli dasturlarga nisbatan samarasiz.

ISSN 3030-3907

Anomaliyalarni aniqlash. Og'ishlarni aniqlash uchun oddiy tarmoq xatti-harakatlarining asoslaridan foydalanadi. Texnikalar potentsial tahdidlarni ko'rsatadigan tartibsiz trafik namunalarini aniqlash uchun statistik tahlil va mashinani o'rganishni o'z ichiga oladi. Xulq-atvor tahlili vaqt o'tishi bilan tarmoq obyektlarining xatti-harakatlariga e'tibor qaratadi, noodatiy kirish urinishlari yoki ma'lumotlarni uzatish kabi zararli harakatlarga mos keladigan namunalarni qidiradi[6].

Zararli dastur ko'pincha buyruqlarni olish yoki ma'lumotlarni chiqarish uchun tashqi serverlar bilan bog'lanadi. Ko'rsatkichlarga quyidagilar kiradi:

- muntazam, bashorat qilinadigan chiquvchi trafik shakllari (mayoq);
- ma'lum zararli IP manzillar yoki domenlarga ulanish;
- chiqish aloqasi uchun ishlatiladigan noodatiy protokollar yoki portlar;
- ma'lumotlarni o'chirish.

Katta, xarakterli bo'lmagan chiquvchi ma'lumotlarni uzatish, ayniqsa notanish yoki shubhali manzillarga ma'lumotlar o'g'irlanishini anglatishi mumkin. Stenografik usullar yoki shifrlangan chiquvchi trafik murakkab eksfiltratsiya urinishlarini ko'rsatishi mumkin.[7]

Razvedka va skanerlash. Hujumni boshlashdan oldin, zararli dastur zaif tizimlarni topish uchun tarmoqni skanerlashi mumkin. Ko'rsatkichlarga quyidagilar kiradi. Portlar va xizmatlarni ketma-ket skanerlash, ICMP trafigining yuqori hajmi yoki noodatiy ARP so'rovlari, anormal foydalanuvchi faoliyati, zararli dasturlar qonuniy foydalanuvchi hisoblarini o'g'irlashi mumkin. Ko'rsatkichlarga quyidagilar kiradi. noodatiy vaqtda yoki kutilmagan joylardan kirish, foydalanuvchi xatti-harakatlaridagi keskin o'zgarishlar, masalan, ushbu foydalanuvchi tomonidan odatda foydalanilmaydigan fayllar yoki tizimlarga kirish.

Hodisaga javob. Real vaqt rejimida trafik monitoringi va tahlili orqali shubhali harakatlarni tezkor aniqlash va javob berish. Tahdid ovlash- hatto maxsus ogohlantirishlar bo'lmasa ham, tarmoq trafigida zararli faoliyat belgilarini faol ravishda qidirish. Sud-tibbiy tahlil- buzilishning ko'lami va ta'sirini tushunish uchun yo'l harakati jurnallarini voqeadan keyingi tekshirish. Uzluksiz monitoring-real vaqt rejimida tahdidlarni aniqlash va kamaytirish uchun tarmoq trafigining uzluksiz monitoringini amalga oshirish.

Tarmoq trafigini tahlil qilish zararli dasturlarni aniqlash va ularga qarshi kurashishni maqsad qilgan kiberxavfsizlik mutaxassislari uchun muhim vazifadir. Tarmoq trafigini sinchkovlik bilan o'rganish uchun turli xil texnika va vositalardan foydalangan holda, tahlilchilar zararli dastur faolligini ko'rsatadigan anomaliyalar va namunalarni aniqlashlari mumkin. Tarmoq ma'lumotlarini samarali talqin qilish

ISSN 3030-3907

qobiliyati kiber tahdidlarni tezkor aniqlash, yumshatish va oldini olish, tashkilot aktivlarini potentsial buzilishlar va ma’lumotlar yo‘qotishlaridan himoya qilish imkonini beradi.

Xulosa

Kompyuter tarmoqlarida hujumlar turli shakllarda va metodlarda amalga oshiriladi, bu esa tarmoq xavfsizligini ta’minlashda ko‘plab muammolarni keltirib chiqaradi. Pasiv va aktiv hujumlar, jumladan Man-in-the-Middle (MitM), DoS/DDoS hujumlari, SQL injection, Cross-Site Scripting (XSS) va boshqa zararli dasturlar, shuningdek, ijtimoiy muhandislik (phishing, baiting) kabi tahdidlar tarmoq tizimlariga jiddiy xavf soladi. Ushbu hujumlarning barchasi ma’lumotlarning maxfiyligi, butunligi va tizimning mavjudligini buzishga qaratilgan. Shu bilan birga, hujum izlarini aniqlash va zararli faoliyatni bartaraf etish uchun tarmoqni monitoring qilishda zamonaviy texnologiyalar, masalan, sandboxing, mashinani o‘rganish (machine learning) algoritmlari, anomaliyani aniqlash, YARA qoidalari va tarmoq trafigini tahlil qilish kabi vositalar keng qo‘llaniladi. Bundan tashqari, zararli dasturlar va tahdidlarni aniqlashning samarali usullaridan biri tarmoq trafigini tahlil qilishdir. Bu jarayon orqali tarmoqdagi anomaliyalar va shubhali faoliyatlar tezda aniqlanib, tahdidlarni bartaraf etish imkonini beradi. Tarmoq trafigini samarali tahlil qilish va vaqtida javob berish tashkilotlarning ma’lumotlar xavfsizligini ta’minlashda muhim rol o'ynaydi.

Umuman olganda, hujum izlarini aniqlash va oldini olish uchun har bir xavf-xatarni chuqur tahlil qilish, turli xil usullarni qo‘llash va xavfsizlik choralari tizimini mukammallashtirish zarur. Kiberxavfsizlikning samaradorligini ta’minlash uchun zamonaviy texnologiyalarni, shu jumladan tarmoq trafigi tahlilini va mashinani o‘rganish algoritmlarini keng joriy etish muhim ahamiyatga ega.

FOYDALANILGAN ADABIYOTLAR:

1. Perrig, J. Stankovic, and D. Wagner, “Security in wireless sensor networks.” Communications of the ACM 47, no. 6 (2004). 53-57.
2. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, “Classification of RFID attacks.” Gen 15693 (2010). 14443.
3. S. Shantharajah, K. Duraiswamy, G. Nawaz, “Key Management and distribution for authenticating group communication”, First international on Industrial and Information System, ISSN. 2164-7011, IEEE.
4. Chen, Y., & Liu, Z. (2021). Machine learning techniques for detecting malicious network activity. International Journal of Computer Networks and Security, 12(2), 45-56

ISSN 3030-3907

5. Malek, A., & Qian, H. (2022). Real-time detection of distributed denial-of-service (DDoS) attacks using network traffic analysis. IEEE Transactions on Information Forensics and Security, 17(2), 222-235.
6. Moustafa, N., & Slay, J. (2019). The role of network traffic analysis in cyberattack detection: A critical review. International Journal of Information Security and Privacy, 13(6), 45-62.
7. Shankar, S., & Srinivasan, S. (2021). Use of deep learning models for network attack detection in real-time traffic. Journal of Artificial Intelligence Research, 60(1), 178-190.

ISSN 3030-3907