TARMOQDAGI ZARARLI TRAFIK TURLARI VA ULARNI ANIQLASH

G‘ulomov Sh.R
Muhammad al-Xorazmiy nomidagi TATU, PhD, dotsent.
sherhisor30@gmail.com,

Annotatsiya: *Ushbu maqolada tarmoqdagi zararli trafiklarga oid asosiy tushunchalari va tarmoq trafigida ularni aniqlash sxemalari keltirilgan. Korporativ tarmoqning ichki segmentida zararli trafik manbalari tasniflangan. Bundan tashqari tarmoq trafigidagi zararli tarfikni aniqlashning statik, signaturali, xatti-harakatlarni tahlil qilish, mashinali o‘qitish va korelatsiya tahlili usullari yoritib berilgan.*

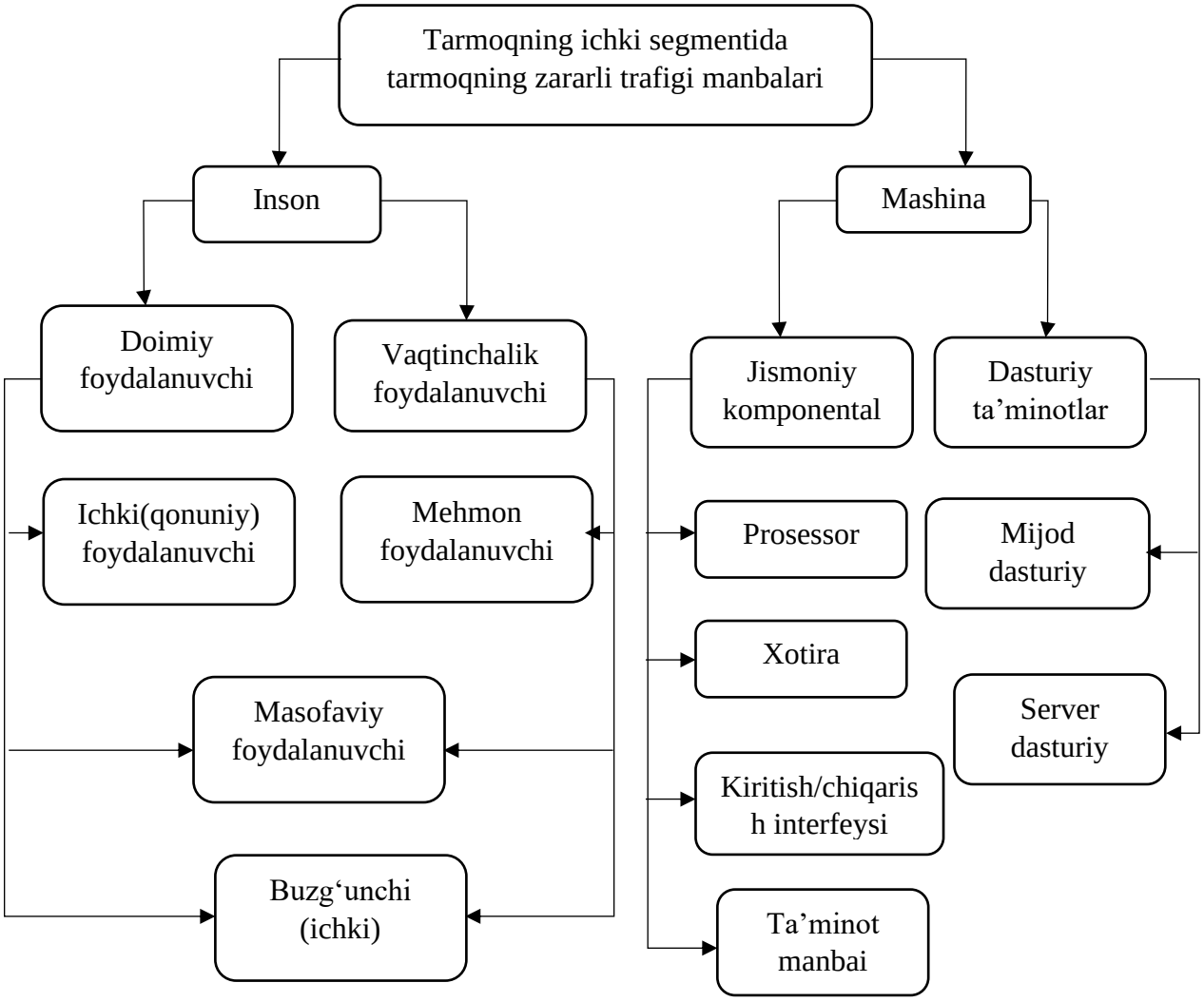
Kalit so‘zlar*: Tarmoq trafigi, zararli trafik, signaturali tahlil, mashinali o‘qitish, korelyatsiya, IDS, Antivirus, Honeypot.*

Kirish

Bugungi kunda aksariyat tashkilotlar uchun yuqori darajadagi axborot xavfsizligini ta’minlash masalasi mahalliy tarmoqning xavfsiz perimetri doirasida amalga oshirilayotgan noqonuniy xatti-harakatlarni aniqlash va bartaraf etish muammosini hal qilishni o‘z ichiga oladi. Check Point Software Technologies kompaniyasining “Cyber Security Report 2022” yillik hisobotiga ko‘ra, statistik ma’lumotlarga ko‘ra, barcha kiberhujumlarning 34 foizi insayderlar tomonidan amalga oshiriladi, bu esa bunday hujumlarni aniqlash va ularga qarshi kurashishga qodir tarmoq xavfsizligi tizimlarini joriy qilish zarurligini ko‘rsatadi [1].

Tashkilot axborot-kommunikatsiya tarmog‘idagi hujumlarni aniqlashning eng istiqbolli usullaridan biri bu tarmoq trafigidagi zararli tarfiklarni aniqlash bo‘lib, bu foydalanuvchilarning yoki mashinalarning zararli harakatlarini, shu jumladan “nolinchi kun hujumlarni” aniqlash imkonini beradi.

Tarmoqdagi zararli trafikni aniqlash masalasini o‘rganish, birinchi navbatda, anomal hodisalarning asosiy manbalarini aniqlashni talab qiladi. Har qanday korporativ tarmoq infratuzilmasi mustaqil ishlaydigan yoki bir-biri bilan o‘zaro ta’sir qiluvchi ko‘plab komponentlarni o‘z ichiga oladi va bu komponentlarning har biri tarmoq anomaliyalarining potensial manbai hisoblanadi. Tarmoq trafigi zararli harakatlarini barcha mumkin bo‘lgan birlamchi manbalarining to‘liq ro‘yxati murakkab vazifadir va shuning uchun korporativ tarmoqning ichki segmentidagi potensial zararli trafik manbalarining umumlashtirilgan tasnifi ishlab chiqilgan. 1-rasmda korporativ tarmoqning ichki segmentida zararli trafik manbalarini tasniflashi keltirilgan. 1-rasmdan ma’lumki, global miqyosda zararli tarmoq trafiklari manbalarini foydalanuvchi va mashina manbalariga bo‘lish mumkin.



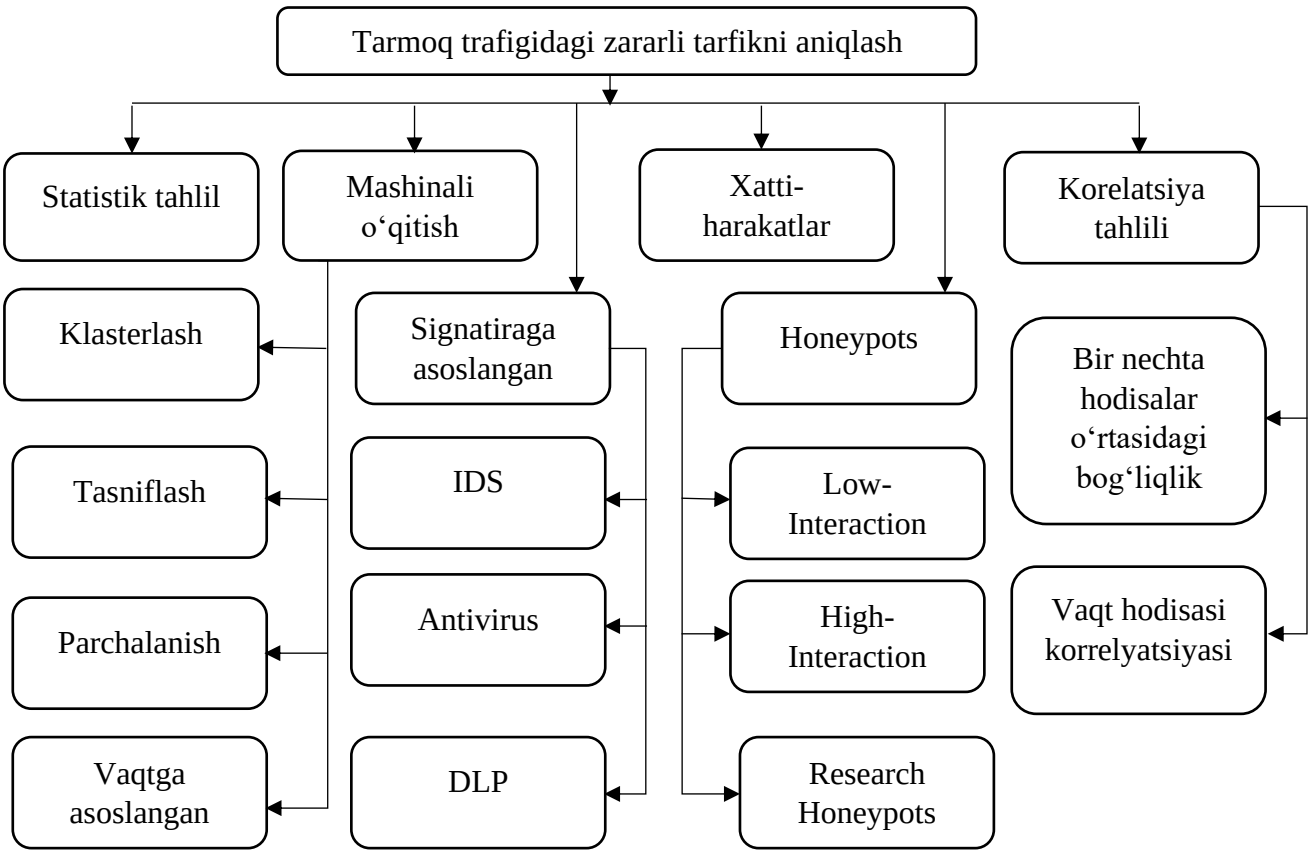
1-rasm. Korporativ tarmoqning ichki segmentida zararli trafik manbalarini tasniflash

Birinchi toifaga tarmoqning ichki segmenti foydalanuvchilari kiradi, ularni doimiylarga bo‘lish mumkin: ular tarmoqqa egalik qiluvchi tashkilot xodimlari va vaqtinchalik - qisqa muddatli muammolarni hal qilish uchun yollanganlar bo‘lishi mumkin. Masofadagi ishchilar va potensial buzg‘unchilar ham doimiy, ham vaqtinchalik foydalanuvchilar bo‘lishi mumkin va zararli tarmoq trafigining potensial manbalarini tavsiflashda hisobga olinishi kerak. Ikkinchi toifaga mashina manbalari kiradi, ular prosessor, xotira, kirish/chiqish interfeyslari va quvvat manbalari va dasturiy ta’minot kabi fizik komponentlar bo‘lib, odatda mijoz va serverga bo‘linadi. Ro‘yxatga olingan fizik komponentlar va dasturiy ta’minot toifalari foydalanuvchi kompyuterlari, serverlar, xavfsizlik va monitoring vositalari kabi kompyuter tarmog‘ining barcha elementlarining asosiy komponentlari hisoblanadi. Shunday qilib, kompyuter tarmog‘idagi har bir qurilma zararli tarmoq trafigining bir nechta potensial manbalarini o‘z ichiga oladi. Shuni ta’kidlash kerakki, manbalar zararli tarmoq trafigini yaratishda mustaqil bo‘lishi mumkin yoki boshqa sanab o‘tilgan manbalardan

anomal trafik paydo bo‘lishiga bevosita ta’sir qilishi mumkin.

Asosiy manbalarni tavsiflashdan tashqari, zararli tarmoq trafigi muammosini o‘rganishning muhim jihati ularning kompyuter tarmog‘ida paydo bo‘lish sabablarini o‘rganishdir[2]. Zararli tarmoq tarfigi sabablarining quyidagi ikkita toifasini ajratib ko‘rsatish mumkin: ishlash bilan bog‘liq zararli trafiklar - bu toifadagi zararli tarmoq tarfigi sabablari tizimlarning apparat va dasturiy ta’minot qismlarini loyihalash xatolari, fizik komponentlarning eskirishi va noto‘g‘ri amalga oshirilishi bo‘lishi mumkin. Kompyuter tarmog‘i komponentlarini konfiguratsiya, foydalanish va boshqarish, shuningdek, dasturiy ta’minot bilan tuzatib bo‘lmaydigan tizimlarining ishlash xususiyatlari. Xavfsizlik bilan bog‘liq zararli tarfiklar - bu turkumda tarmoq anomaliyalarining sabablari apparat yoki dasturiy ta’minot zaifliklaridan foydalanish [3], tarmoq xavfsizligi va monitoring vositalarining yetarli darajada konfiguratsiyasi, foydalanuvchilar va buzg‘unchilarga noqonuniy yoki kutilmagan harakatlar qilish imkonini beruvchi tashkilotning ichki himoyalangan perimetr tarmoqlaridagi xavfsizlik siyosatidagi xatolardir.

Tarmoq trafigida oqimidagi zararli trafikni aniqlash axborot tizimlari xavfsizligini ta’minlashning muhim tarkibiy qismi hisoblanadi. Tarmoq trafigidagi zararli trafikni aniqlashning ko‘plab usullari mavjud. 2-rasmda tarmoq trafigidagi zararli tarfikni aniqlash usullari taqdim etilgan.



2-rasm. Tarmoq trafigidagi zararli tarfikni aniqlash usullari

Statistik tahlil usuli. Ushbu usul tarmoq trafigining normal harakatining statistik profilini yaratishga asoslangan. Bu usulda tarmoq trafigi o‘ziga o‘xshashlik jarayonning ba’zi statistik xarakteristikalari vaqt shkalasi sifatida saqlanib qoladigan hodisani tavsiflaydi [4]. Zararli harakatlar joriy trafik belgilangan profildan sezilarli darajada chetga chiqqanda aniqlanadi. Zararli trafiklarni aniqlash kontekstida statistik tahlil tarmoq trafigining normal harakatining statistik profilini yaratishga tayanadi. Bu usul, oddiy tarmoq sharoitida, trafik xarakteristikalari izchil statistik holatlarga ega bo‘lishini nazarda tutadi va bu holatlardan har qanday sezilarli og‘ish mumkin bo‘lgan zararli trafiklar yoki hujumlarni ko‘rsatishi mumkin.

Tarfik oqimining miqdori*:*

Normal tarfik: O‘rnatilgan statistik profil kunning yoki haftaning ma’lum bir kuni uchun uzatiladigan ma’lumotlarning odatiy miqdorini o‘z ichiga oladi.

Zararli trafik: Ma’lumot uzatish hajmining keskin oshishi yoki kamayishi hujumlar yoki g‘ayritabiiy faoliyatni ko‘rsatishi mumkin.

Seanslar davomiyligi:

Normal tarfik: foydalanuvchi yoki qurilma seanslarining odatiy davomiyligi uchun o‘rnatilgan statistik parametrlar.

Zararli trafik: Juda qisqa yoki aksincha, haddan tashqari uzoq sessiyalar hujum yoki hisob ma’lumotlarining buzilishining ko‘rsatkichi bo‘lishi mumkin.

Statistik tahlilning afzalliklari

– amalga oshirish nisbatan oson;

– oldindan ma’lum bo‘lmagan anomaliyalarni aniqlash qobiliyati.

Statistik tahlilning kamchiliklari:

– o‘zgaruvchan tarmoq muhitiga moslashish uchun statistik profillarni doimiy yangilashni talab qiladi;

– tarmoq tuzilmasidagi o‘zgarishlar, masalan, yangi ilovalarni joriy qilish yoki biznes jarayonlaridagi o‘zgarishlar bo‘lsa, noto‘g‘ri ijobiy natijalar berishi mumkin.

Mashinali o‘qitish usullari. Mashinali o‘qitish algoritmlari, masalan, tasniflash yoki klasterlash usullari, tarmoq trafigidagi zararli tarfikni aniqlay oladigan modellarni yaratish uchun ishlatiladi. Mashinali o‘qitish, tarmoq trafigidagi zararli trafiklarini aniqlash kontekstida, odatdagi ma’lumotlardan avtomatik ravishda o‘rganish va o‘rnatilgan xatti-harakatlar namunalariga mos kelmaydigan harakatlarni aniqlay oladigan algoritmlardan foydalanishni o‘z ichiga oladi. Ushbu usullar tarmoqning [5,6] o‘zgaruvchan tabiatiga moslashish va hatto oldindan ma’lum bo‘lmagan zararli trafiklarni aniqlash qobiliyatiga ega.

Yuqori darajadagi ishonchlilik:

Normal tarfik: Mashinali o‘qitish modeli oddiy ma’lumotlarga o‘qitilgan va

shuning uchun oddiy xatti-harakatlar modellarini aniqlashda yuqori darajadagi ishonchga ega.

Zararli trafik: Model normal deb hisoblagan narsadan sezilarli darajada chetga chiqadigan trafik yoki holatlarning ko‘rinishi zararli tarfik sifatida signal berishi mumkin.

Anomal holatlarni aniqlash:

Normal tarfik: Model tarmoq trafigidagi umumiy xatti-harakatlar modellarini aniqlaydi.

Zararli trafik: Mashinali o‘qitish algoritmi kamdan-kam uchraydigan yoki o‘qitilgan modelga to‘liq mos kelmaydigan holatlarni aniqlashi mumkin, bu zararli tarfiklarni ko‘rsatishi mumkin.

Tarmoq trafigidagi zararli tarfiklarni aniqlash uchun mashinali o‘qitish algoritmlarining turlari:

Klasterlash usullari. K-means, DBSCAN. O‘xshash holatlarni klasterlarga guruhlash, hech qanday klasterga mos kelmaydiganlarini aniqlash.

Tasniflash usullari. Tayanch vektorlar (SVM), qarorlar daraxtlari (Decision Trees). Oddiy va g‘ayritabiiy naqshlar farq qiladigan etiketli ma’lumotlarga modelni o‘rgatiladi.

Parchalanish usullari. One-Class SVM, Autoencoders. Modelni faqat oddiy ma’lumotlarga o‘rgatiladi va zararli trafiklarni o‘qitilgan shablonlarga mos kelmaydigan ob’ektlar sifatida aniqlaydi.

Vaqtga asoslangan usullari. LSTM (Uzoq va qisqa muddatli xotira). Zararli tarfiklarni aniqlash uchun tarmoq trafigidagi vaqtga bog‘liqlikni tahlil qiladi.

Mashinali o‘qitish usullarining afzalliklari:

– ilgari noma’lum bo‘lgan zararli tarifiklarni aniqlash qobiliyati;
– tarmoq tuzilmasi yoki trafik shakllaridagi o‘zgarishlarga moslashish.

Mashinani o‘rganish usullarining kamchiliklari:

– trening uchun katta hajmdagi etiketli ma’lumotlarga ehtiyoj;
– tarmoqdagi o‘zgarishlarni aks ettirish uchun modellar doimiy ravishda yangilanishi kerak;
– noto‘g‘ri pozitivlar ehtimoli, ayniqsa ma’lumotlarning markirovkasi yetarli bo‘lmagan holatlarda.

Signatura usullari. Signaturaga asoslangan usullar joriy tarmoq trafigini ma’lum tahdidlarning ma’lum signaturalari (xususiyatlari) bilan solishtirishga asoslangan. Signaturalar sarlavha maydoni qiymatlarini tekshirishdan tortib, ulanish holatini kuzatishi yoki protokol tahlilini amalga oshirishi mumkin bo‘lgan juda murakkab signaturalargacha o‘zgaradi [7]. Ushbu usul, agar ma’lum signaturalarga

mos keladigan bo‘lsa, ma’lum hujumlarni aniqlash mumkinligini taxmin qiladi.

Moslikni aniqlash:

Normal tarfik: Trafikda ma’lum tahdid signaturalariga mos keladiganlar mavjud emas.

Zararli trafik: Muayyan tahdid yoki hujum turiga xos bo‘lgan signaturalar bilan mos kelishini aniqlash.

Signatura usullarining afzalliklari:

– yuqori aniqlik: Signatura asoslangan usullar ma’lum tahdidlarni aniqlashda yuqori aniqlikni ta’minlaydi;

– kam noto‘g‘ri ijobiy nisbat: Signatura ma’lumotlar bazalarining to‘g‘ri konfiguratsiyasi bilan noto‘g‘ri pozitivlarni minimallashtirish mumkin.

Signatura usullarining kamchiliklari:

– yangi hujumlarga qarshi samarasiz: Signaturaga asoslangan usullar hali signaturalari yaratilmagan yangi hujumlarga nisbatan samarasiz;

– doimiy yangilanishni talab qiladi: Signaturalar yangi tahdidlarni aniqlashi uchun doimiy ravishda yangilanishi kerak;

– noma’lum hujumlarni aniqlab bo‘lmaslik: Signaturaga asoslangan usullar ma’lum tahdidlarga qaratilganligi sababli ular noma’lum hujumlarni o‘tkazib yuborishi mumkin.

Xatti-harakatlarni tahlil qilish usullari. Xatti-harakatlarni tahlil qilish usuli tizimning normal ishlashini kuzatish va ushbu normal xatti-harakatlardan chetlanishlarni aniqlashga asoslangan. Bunday holda, resurslardan foydalanish usullaridagi o‘zgarishlar yoki noodatiy so‘rovlar zararli trafik ko‘rsatkichi bo‘lishi mumkin, chunki ular belgilangan kutilmalarga javob bermaydi. Umuman olganda, tarmoq trafigi Internet bo‘ylab zararli ma’lumotlar paketlarini aniqlash uchun tekshiriladi. Ushbu usullar ko‘pincha trafik monitoringi uchun dasturiy ta’minotga asoslangan usullarni o‘z ichiga oladi. Oddiy trafik paytida ko‘pchilik mashinalar faqat bir nechta boshqa mashinalar bilan o‘zaro ta’sir qiladi. Biroq, viruslarning tarqalishi paytida ko‘plab mashinalar yangi xostlarga ulanishga harakat qilishadi [8]. Tarmoq filtri yordamida yangi xostlarga ulanish tezligini cheklash orqali viruslarning tarqalishini cheklaydi.

Xatti-harakatlarni tahlil qilish usulining afzalliklari:

– yangi hujumlarni aniqlash qobiliyati: signaturaga asoslangan usullardan farqli o‘laroq, xatti-harakatlar tahlili yangi, ilgari noma’lum hujumlarni aniqlashi mumkin;

– noto‘g‘ri pozitivlarni minimallashtirish: tizim noto‘g‘ri pozitivlarni minimallashtirish orqali tarmoq muhitidagi o‘zgarishlarga moslasha oladi.

Xatti-harakatlarni tahlil qilish usulining kamchiliklari:

– “me’yor”ni o‘rnatishda qiyinchilik: Oddiy xatti-harakatni aniqlash qiyin bo‘lishi mumkin, ayniqsa dinamik muhitda;

– keng qamrovli tayyorgarlikni talab qiladi: Usul odatdagi xatti-harakatlar modellarini aniqlash uchun keng qamrovli treningni talab qiladi, bu vaqt talab qilishi mumkin;

– katta hajmdagi ma’lumotlardagi zararli tarafikni aniqlashda qiyinchilik: Katta hajmdagi ma’lumotlarni qayta ishlashda zararli trafiklarni aniqlash shovqin va oddiy xatti-harakatlarning o‘zgarishi tufayli qiyin bo‘lishi mumkin.

Honeypot usullaridan foydalanish. Zararli faoliyatni jalb qilish uchun maxsus tayyorlangan honeypotlar yoki tuzoqlardan foydalaniladi. Honeypot tarmoqdagi zararli trafiklarni, hujumlarni yoki tarmoq skanerlanishini ko‘rsatishi mumkin [9].

Low-Interaction Honeypot: Bu honeypot zaifliklarni taqlid qiladi va ularga resurslarga haqiqiy kirish huquqini bermasdan hujumchilarni jalb qiladi. Mazkur honeypot o‘z ilovasida buzg‘unchi bilan ishlaganda honeypotda o‘rnatilgan operatsion tizimdan foydalanadi va bu buzg‘unchi bilan cheklangan o‘zaro ta’sirga ega [10].

High-Interaction Honeypot: Bu honeypotlar haqiqiy zaifliklarga ega bo‘lgan haqiqiy tizimlarni ifodalaydi va buzg‘unchilarga boshqariladigan resurslarga haqiqiy kirish imkonini beradi.

Research Honeypot: Ma’lumotlarni to‘plash va yangi yoki rivojlanayotgan tahdidlarni tahlil qilish uchun foydalaniladi.

Honeypot monitoringi: Hujum aniqlangandan so‘ng, buzg‘unchilar IP-manzil bloklanadi, keyin honeypot buzg‘unchi haqida ma’lumot to‘playdi [11]. Agar paket mazmuni hujum shabloniga mos kelsa, bu xostdan kelgan paket blokirovkalanadi va honeypotga yo‘naltiriladi. Bir vaqtning o‘zida IP-manzil va hujum turi buzg‘unchi ro‘yxatining ma’lumotlar bazasiga qo‘shiladi.

Honeypotdan foydalanishning afzalliklari:

– yangi tahdidni aniqlash: signaturalari hali yaratilmagan tahdidlarni aniqlay oladi;

– hujum razvedkasi: Tahlil qilish va xavfsizlik bo‘yicha qo‘shimcha treninglar uchun qimmatli ma’lumotlarni taqdim etadi.

Honeypotdan foydalanishning kamchiliklari:

– murosa xavfi: Agar honeypot to‘g‘ri sozlanmagan bo‘lsa, tajovuzkorlar undan haqiqiy tizimlarga hujum qilish uchun foydalanishi mumkin.

– boshqarish va madadlashni talab qiladi: Honeypot samarali bo‘lishi uchun doimiy monitoring va yangilanishni talab qiladi.

Korrelyatsiya tahlili. Zararli trafiklarni ko‘rsatishi mumkin bo‘lgan noodatiy korrelyatsiyalarni aniqlash uchun tarmoqdagi turli hodisalar o‘rtasidagi munosabatni tahlil qiladi [12].

Korrelyatsiya tahlilining afzalliklari:

– murakkab hujumni aniqlash: bir nechta hodisalar yoki hujum bosqichlarida sodir bo‘lgan hujumlarni aniqlay oladi;

– moslashuvchanlik: tarmoq muhitidagi o‘zgarishlarga moslasha oladi, chunki u hodisalar o‘rtasidagi munosabatlarga asoslanadi.

Korrelyatsiya tahlilining zaifliklari:

– “me’yor” ni aniqlashda qiyinchilik: Kutilayotgan korrelyatsiyalarni aniqlash dinamik muhitda qiyin bo‘lishi mumkin;

– noto‘g‘ri pozitivlar: yangi biznes jarayonlarini joriy etish yoki tarmoq tuzilishini o‘zgartirish noto‘g‘ri ijobiy natijalarga olib kelishi mumkin;

– murakkab algoritmlar va hisoblash resurslarini talab qiladi: Korrelyatsiya tahlili, ayniqsa, yirik tarmoqlarda murakkab algoritmlar va katta hisoblash resurslarini talab qilishi mumkin.

Zararli tarmoq trafigini aniqlash muammosini o‘rganish va uning yechish yo‘llari har qanday axborot-kommunikatsiya tarmog‘ining barqaror va xavfsiz ishlashini tashkil etishning muhim elementidir. Zararli tarmoq trafigini tavsiflangan manbalari va sabablari, shuningdek ularni aniqlashning mavjud usullarini tahlil qilish tarmoqdagi zararli trafikni aniqlash nazariyasi bo‘yicha mavjud tadqiqotlarni to‘ldirishga imkon beradi.

Xulosa

Zararli tarmoq trafigini aniqlash muammosini o‘rganish va uning yechish yo‘llari har qanday axborot-kommunikatsiya tarmog‘ining barqaror va xavfsiz ishlashini tashkil etishning muhim elementidir. Zararli tarmoq trafigini tavsiflangan manbalari va sabablari, shuningdek ularni aniqlashning mavjud usullarini tahlil qilish tarmoqdagi zararli trafikni aniqlash nazariyasi bo‘yicha mavjud tadqiqotlarni to‘ldirishga imkon beradi.

ADABIYOTLAR

1. Отчет компании Check Point Software Technologies «Cyber Security Report 2022». — 80 с.
2. Monowar, H. B. Network Traffic Anomaly Detection and Prevention. Concepts, Techniques, and Tools / Monovar H. Bhuyan, Dhruba. K. Bhattacharyya, Jugal K. Kalita // Springer International Publishing, 2017. —285 p.
3. Monowar, H. B. Network Anomaly Detection: Methods, Systems and Tools / Monovar H. Bhuyan, Dhruba. K. Bhattacharyya, Jugal K. Kalita // IEEE Communication Surveys & Tutorials, Vol. 16, No. 1, 2014. —pp. 303–336

4. Татарникова Т. М. Статистические методы исследования сетевого трафика. Информационно-управляющие системы, 2018, № 5, с. 35–43.

5. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей / В. Ф. Шаньгин — М.: ИД «Форум»: ИНФРА-М, 2011. — 416 с.

6. Monowar, H. B. Network Traffic Anomaly Detection and Prevention. Concepts, Techniques, and Tools / Monovar H. Bhuyan, Dhruba. K. Bhattacharyya, Jugal K. Kalita // Springer International Publishing, 2017. — 285 p.

7. Бабенко Герман Валерьевич, Белов Сергей Валерьевич. Анализ поведенческих характеристик трафика Ethernet-TCP/IP на основе сигнатурного метода. Научно-практический журнал. ISSN 1995-5731, Информационная безопасность регионов. 2011. № 2 (9), -С.7-12

8. Miad Faezipour, Mehrdad Nourani, Sateesh Addepalli. A Behavioral Analysis Engine for Network Traffic. IEEE CCNC 2010 proceedings, pp.1-5

9. M.R. Amal, P. Venkadesh. Review of Cyber Attack Detection: Honeypot System. Webology, Volume 19, Number 1, January, 2022, pp. 5497- 5514

10. Abdul Muin Nasution, Muhammad Zarlis, Suherman Suherman. Analysis and Implementation of Honeyd as a Low-Interaction Honeypot in Enhancing Security Systems. Randwick International of Social Science (RISS) Journal Vol. 2, No.1, January 2021| Page: 124-135

11. A. Umamaheswari and B. Kalaavathi, “Honeypot TB-IDS: trace back model based intrusion detection system using knowledge based honeypot construction model,” Cluster Comput., vol. 4, pp. 1–8, 2018.

12. Li, H. Research on intelligent intrusion prevention system based on snort / H. Li, D. Liu // In Proceedings of the 2010 International Conference on Computer, Mechatronics, Control and Electronic Engineering (CMCE), V.-1,— IEEE. 2010. — pp. 251–253.