BANK TIZIMIDA TARMOQ HUJUMLARIDAN HIMOYALASH USUL VA ALGORITMLARI

Jo ‘ramirzayev I.A. Hafizov Sh.F
Toshkent axborot texnologiyalari unversiteti talabalari

Annotatsiya: *Ushbu maqolada bank tizimdagi tarmoq turlari va ularga bo‘ladigan tarmoq hujumlari ko‘rib chiqilgan bo‘lib, shuningdek, bank to‘lov tizimida tarmoq hujumlarini aniqlash usullari va ularni tahlili keltirilgan.*

Kalit so‘zlar: *Tarmoq turlari, tarmoq hujumlar, himoyalash algoritmlari*

BANK TO‘LOV TIZIMIDA TARMOQ HUJUMLARIDAN HIMOYALANISH USULLARI

So‘nggi yillarda banklar va moliyaviy xizmat ko‘rsatuvchi provayderlarga bo‘layotgan kiberhujumlar yanada ommalashdi. Kiberjinoyatchilar zamon bilan rivojlanib, tashkilotlarni nishonga olish uchun yanada murakkab taktikalardan foydalanmoqdalar. Ushbu kiberjinoyatchilar zamon bilan hamnafas bo‘lib rivojlanib borayotgan bir paytda tashkilotlarning hujumlarga qarshi turish va ularga qarshi kurashish uchun xavfsizlik choralarini rivojlantirish talab etiladi.

Bank tizimida tarmoq hujumlaridan himoyalanish uchun bir qancha muhim usullar mavjud, jumladan:

Tarmoqlararo ekran (Firewall). Tarmoqlararo ekranni ikki xil ko‘rinishda qo‘lanilish mumkin: tashqi Firewall va ichki firewall.

– tashqi Firewall: Tarmoqning chetida joylashadi hamda kelayotgan va chiqayotgan trafikni oldindan belgilangan xavfsizlik qoidalari asosida nazorat qiladi.

– ichki Firewall: Tarmoqning ichki qismlarini segmentlash va qo‘shimcha xavfsizlik qatlamini ta’minlash uchun ishlatiladi.

Tarmoqlararo ekran dan foydalanish trafikni filtrash, ya’ni nomaqbul kirishni bloklash hamda qonuniy muloqotni ta’limlash va hujumlardan himoya, ya’ni DDoS, zararli dasturlar va fishing hujumlaridan himoyalanishga yordam berish kabi afzalliklarni beradi.

Tizimga kirishni aniqlash va oldini olish tizimi (Intrusion Detection and Prevention Systems, IDPS). Tizimga kirishni aniqlash va oldini olish tizimi (IDPS) tarmoqqa asoslangan (NIDPS) hamda xostga asoslangan (HIDPS) ko‘rinishlarda bo‘lishi mumkin:

– Tarmoqga asoslangan IDPS (Network-Based IDPS – NIDPS): Tarmoq trafikini shubhali faoliyat uchun kuzatishda qo‘llaniladi.

– Xostga asoslangan IDPS (Host-Based IDPS – HIDPS): Shaxsiy qurilmalar yoki xostlarning noodatiy faoliyatini kuzatish bilan shug‘ullanadi.

Tizimga kirishni aniqlash va oldini olish tizimi (Intrusion Detection and Prevention Systems – IDPS) dan foydalanish real vaqtda xabardorlik, ya’ni potensial kirishlar haqida tezkor xabarnomalar berish va avtomatik javob, ya’ni IP manzillarni

bloklash yoki buzilgan tizimlarni o‘chirish kabi avtomatik choralarni ko‘rish kabi afzalliklarni taqdim etadi.

Tarmoq hujumlaridan himoyalanish usullari tahlili

Himoya usuli	**Qo‘llanilishi**	**Afzalliklari**
Firewall	Perimetr va ichki firewall, trafikni boshqaradi	Trafikni filtrlash, hujumlardan himoyalash
IDPS(IDS/IPS)	Tarmoq va xostga asoslangan, shubhali faoliyatni aniqlaydi va bloklaydi	Real vaqtda xabardorlik, avtomatik javob berish
Shifrlash	Ma’lumotlarni shifrlash, TLS/SSL, tranzitdagi hamda saqlangan ma’lumotlarni himoya qilish	Ma’lumotlarni himoya qilish, xavfsiz aloqani ta’minlash
Ko‘p faktorli autentifikatsiya	Ikki faktorli autentifikatsiya, biometrik autentifikatsiya	Kuchli kirish nazorati, ma’lumotlar o‘g‘irlanishimi kamaytirish
Xavfsiz dasturlash amaliotlari	Penetratsion test, static va dinamik tahlil	Ekpluatatsiyani oldini olish, dastur sifatini kafolatlash
SIEM	Xavfsizlik hodisalari ma’lumotlarini to‘plash, korrelyatsiya va tahlil qilish	Markazlashtirilgan monitoring, proaktiv tahdid boshqaruvi, hodisalarga javob berish
Tarmoq segmentatsiyasi	Tarmoqni segmentlarga ajratish VLAN, DMZ	Hujumlarni cheklash, kirishni nazoratlash
Xavfsizlik auditlari va muvofiqlik	Ichki va tashqi audit	Risklarni identifikatsiya qilish, bo‘lishi mumkin bo‘lgan risklarni kamaytirish
Xodimalrni o‘qitish va xabardorlik	Fishing simulyatsiyalari, xavfsizlik ta’lim dasturlari	Inson xatosini kamaytirish, xavfsizlik xabardorligini oshirish
Anti-Malware va antivirus dasturlari	Endpoint himoyasi, muntazam yangilanishlar	Tahdidlarni aniqlash va yo‘q qilish, tizimning uzviyligini ta’minlash
Tarmoqqa kirishni	Siyosatlarni	Yuqori xavfsizlik,

nazorat qilish (NAC)	amaliyotga tatbiq qilish, endpoint muvofiqlik	risklarni kamaytirish
DLP	Ma’lumotlar oqimini kuzatadi va nazorat qiladi	Ma’lumotlarning yo‘qotilishini oldini oladi, ma’lumotlar yaxlitligini ta’minlaydi

Bank to‘lovi tizimida tarmoq hujumlarini aniqlash usullari va algoritmlari tahlili

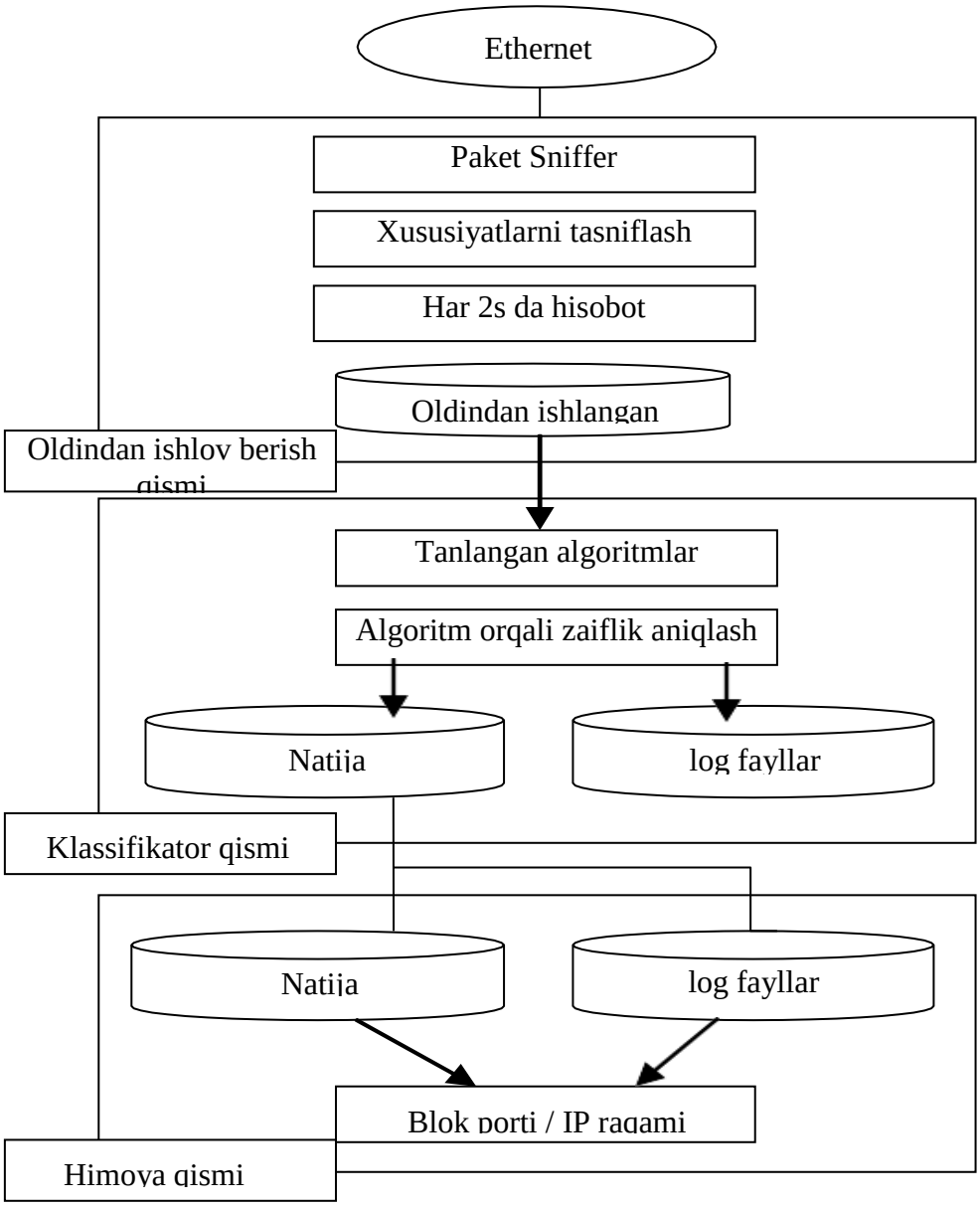
Umuman olganda, tajovuzkorning xatti-harakati qonuniy foydalanuvchinikidan sezilarli darajada farq qiladi va shuning uchun uni aniqlash mumkin [3]. Hujumni aniqlash tizimlari real vaqt rejimida joylashishiga qarab tasniflanishi mumkin.

Xostga asoslangan aniqlash. Xostga asoslangan aniqlash tizimlari tashqi interfeyslarni emas, balki hisoblash tizimining ichki qismlarini kuzatadi va tahlil qiladi [3]. Bunday tizimlar qaysi dastur qaysi manbalarga kirishi va noqonuniy kirishga urinish kabi ichki faoliyatni aniqlashi mumkin.

Tarmoqqa asoslangan aniqlash. Tarmoq Internet orqali dunyoning qolgan qismiga ulangan. Tarmoqqa asoslangan aniqlash tizimi barcha kiruvchi paketlar yoki oqimlarni o‘qiydi va shubhali harakatlarni topishga harakat qiladi. Misol uchun, agar qisqa vaqt ichida juda ko‘p sonli turli portlarga juda ko‘p miqdordagi TCP ulanish so‘rovlari kuzatilsa, kimdir tarmoqdagi ba’zi kompyuter(lar)da “portni skanerlash” ni amalga oshirmoqda deb taxmin qilish mumkin [3].

Aniqlash tizimlari.

Mashinali o‘qitish algoritmlari. Ko‘plab olimlar [4], tarmoq hujumlarini aniqlash va tasniflash uchun mashinali o‘qitish algoritmlaridan foydalangan holda tarmoqqa asoslangan kirishni aniqlash va oldini olish tizimini (IDPS – Intrusion Detection and Prevention System) taqdim etgan. Bunda Decision Tree, Ripple Rule, Random Forest va Bayesian tarmog‘i kabi bir nechta taniqli mashinali o‘qitish algoritmlari qo‘llaniladi(2-rasm).



2-rasm. Hodisalarni aniqlash va oldini olish tizimi jarayoni [4]

Tarmoq trafigi ma’lumotlarining 12 ta xususiyati ko‘rib chiqiladi, ular 17 ta hujum turlarini tekshirish va xizmatlarni rad etish, shuningdek, oddiy tarmoq faolligini aniqlash va tasniflash uchun samarali hisoblanadi. 2.1-rasmdagi algoritmga ko‘ra hodisalarni aniqlash va oldini olish tizimi Oldindan ishlov berish qismi, Tasniflash qismi va Himoya qismidan iborat. Tizim Ethernet-dan paketni aniqlashni boshlaydi va ma’lum vaqt oralig‘ida ma’lumotlar yozuvini shakllantirish orqali muhim xususiyatlarni olish uchun paket ma’lumotlarini oldindan ishlov berish qismiga yuboradi.

Paketli sniffer jarayoni Ethernet interfeysi kartasidan IP, TCP, UDP va ICMP sarlavhasi kabi IP juftligi o‘rtasida paket ma’lumotlarini olish uchun ishlatiladi.

Keyin oldindan ishlangan ma’lumotlar hujum turlarini aniqlash uchun Tasniflash qismiga yuboriladi, aks holda ma’lumotlar oddiy tarmoq faoliyati hisoblanadi. Oldindan qayta ishlangan ma’lumotlar mashinali o‘qitish algoritmlari bo‘yicha tasniflanadi. Tasniflash uchun Ripple Rule, Random Forest, Decision Tree C4.5 va

Bayesian Networkdan iborat mashhur algoritmlardan foydalaniladi. Aniqlash qismidan olingan natija keyin Himoya qismiga yuboriladi. Agar tarmoq hujumlari aniqlansa, tarmoq ma'lumotlar paketlari IP table yordamida bloklanadi. Tarmoq turlarining natijasi shubhali bo'lsa, tizim jo'natuvchining IP-manzilini tajovuzkor IP sifatida qayd qiladi va tajovuzkor IP-ning barcha paketlarini bloklaydi yoki tashlab yuboradi. Agar natija DoS bo'lsa, tizim hujumga uchragan ulanish porti raqamini yozib oladi va keyin hujum qilingan port raqami orqali o'tadigan barcha paketlarni bloklaydi yoki o'chiradi. Eksperimental natijalar shuni ko'rsatadiki, Ripple Rule, Decision tree, Bayesian Network algoritmlari juda yuqori aniqlash tezligiga ega.

XULOSA

Mazkur maqola ishida Bank tizimida tarmoq texnologiyalari turlari va ularga bo'ladigan raqamli hujumlardan himoyalanishda qo'llaniladigan xavfsizlik mexanizmlarining tahlili natijalariga erishildi :

- bank tizimida tarmoq texnologiyalari tavsifi keltirildi;
- bank tizimida tarmoqqa bo'ladigan raqamli hujumlar turlari batafsil yoritildi;
- bank to'lov tizimida tarmoq hujumlarini aniqlash usullari va algoritmlari haqida o'rganildi;
- bank to'lov tizimida tarmoq hujumlaridan himoyalanish uchun yechimlar taklif qilindi;
- bank to'lov tizimida tarmoqqa bo'ladigan hujumlar tasnifi keltirildi;
- bank to'lov tizimlariga bo'ladigan tarmoq hujumlar va ulardan himoyalanish usullari va algoritmlari mexanizmlari batafsil yoritildi.

FOYDALANILGAN ADABIYOTLAR:

1. O'zbekiston Respublikasining "Avtomatlashtirilgan bank tizimida axborotni muhofaza qilish to'g'risida"gi va "O'zbekiston Respublikasining Markaziy banki to'g'risida"gi qonunlari hamda O'zbekiston Respublikasi Prezidentining 2018-yil 8-avgustdagi PF-5505-son "Norma ijodkorligi faoliyatini takomillashtirish konsepsiyasini tasdiqlash to'g'risida"gi Farmoniga muvofiq O'zbekiston Respublikasi Markaziy banki Boshqaruvi qaror.

2. O'zbekiston Respublikasining qonuni "Banklar va bank faoliyati to'g'risida"gi O'zbekiston Respublikasi qonuniga o'zgartirish va qo'shimchalar kiritish haqida Qonunchilik palatasi tomonidan 2019-yil 22-iyulda qabul qilingan Senat tomonidan 2019-yil 11-oktabrda ma'qullangan qarori.

3. Bozorov, Suhrobjon. "DDoS Attack Detection via IDS: Open Challenges and Problems." 2021 International Conference on Information Science and Communications Technologies (ICISCT). IEEE, 2021.

4. Xoliyarov, Farhod, Sherzod Gulomov, and Suhrobjon Bozorov. "The Impact of Artificial Neural Network Architecture on Network Attack Detection." Proceedings of the 7th International Conference on Future Networks and Distributed Systems. 2023.

5. Xie, Y., Tang, S., Huang, X., Tang, C., & Liu, X. (2013). Detecting latent attack behavior from aggregated Web traffic. Computer Communications, 36(8), 895-907.

6. Gyamfi, N. K., & Abdulai, J. D. (2018, November). Bank fraud detection using support vector machine. In 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) (pp. 37-41). IEEE.

7. Bhuyan M. H., Bhattacharyya D. K., Kalita J. K. Network anomaly detection: methods, systems and tools //Ieee communications surveys & tutorials. – 2013. – Т. 16. – №. 1. – С. 303-336.

8. Wattanapongsakorn, N., Srakaew, S., Wonghirunsombat, E., Sribavonmongkol, C., Junhom, T., Jongsubsook, P., & Charnsripinyo, C. (2012, June). A practical network-based intrusion detection and prevention system. In 2012 IEEE 11th international conference on trust, security and privacy in computing and communications (pp. 209-214). IEEE.

16.https://www.flowmon.com/en/solutions/security-operations/network-behavior-analysis-anomaly-detection

17. https://www.zabbix.com/network_monitoring