AXBOROT-KOMMUNIKATSIYA TIZIMLARIDA TARMOQ TRAFIGINI HIMOYALASH USULLARINI DASTURIY TA'MINOTINI ISHLAB CHIQISH

Karimova Iqbol Madaminovna
Frunzayev Raxmatjon Axmad o'g'li
ABU RAYHON BERUNIY NOMIDAGI
URGANCH DAVLAT UNIVERSITETI,
Axborot xavsizligi kafedrasi
e-mail frunzayevr@gmail.com

Abstract: Ushbu maqolada tarmoq trafigini himoyalovchi dasturiy vositalarni ishlab chiqish masalasi ko'rib chiqilgan. Zamonaviy korporativ va shaxsiy tarmoqlarda kiberatakalarga qarshi kurash tobora dolzarb ahamiyat kasb etmoqda. Maqolada paket filtrlash, chuqur paket tahlili (DPI), intruziyalarni aniqlash va oldini olish tizimlari (IDS/IPS), shuningdek VPN va SSL/TLS protokollari asosida ishlaydigan himoya vositalari batafsil tahlil qilingan. Ishlab chiqilgan dasturiy yechim Python va Scapy kutubxonasi yordamida amalga oshirilgan bo'lib, real vaqt rejimida tarmoq trafigini kuzatish, shubhali paketlarni aniqlash va zararli faoliyatni bloklash imkonini beradi. Tajriba natijalari ishlab chiqilgan tizimning SQL-injection, DoS va port skanerlash hujumlarini 94.7% aniqlik bilan aniqlashini ko'rsatdi. Tizim O'zbekiston milliy standarti O'z DSt ISO/IEC 27001 talablariga muvofiq sertifikatlanishga moslashtirilgan

Keywords: tarmoq xavfsizligi, paket filtrlash, Snort, IDS/IPS, firewoll, DPI, VPN, SSL/TLS, kibertahdidlar, axborot xavfsizligi.

I. KIRISH

Axborot texnologiyalari jadal rivojlanib borayotgan bugungi kunda tarmoq xavfsizligi masalasi global miqyosdagi eng dolzarb muammolardan biriga aylandi. Cisco tadqiqotlariga ko'ra, 2024-yilda dunyo bo'lyicha har daqiqada o'rtacha 1.5 million kiberhujum sodir bo'lgan. O'zbekistonda ham "Raqamli O'zbekiston 2030" strategiyasi doirasida axborot infratuzilmasini kengaytirish bilan birga uni himoya qilish zarurati yanada ortmoqda.

Tarmoq trafigini himoya qiluvchi zamonaviy vositalar ikki asosiy kategoriyaga bo'linadi: passiv monitoring vositalari (trafik tahlili, anomaliyalarni aniqlash) va aktiv himoya vositalari (firewoll, IPS, VPN). Amaliyotda ko'pincha ushbu yondashuvlarning kombinatsiyasi qo'llaniladi.

Muammo shundaki, ko'plab mavjud tijorat yechimlari qimmat bo'lib, kichik

va o‘rta korxonalar uchun qo‘llab-quvvatlash qiyin. Ochiq kodli yechimlar esa ko‘pincha qo‘shimcha sozlash va moslashtirishni talab qiladi. Ushbu maqola doirasida mahalliy tarmoqlar uchun moslashtirilgan, Python asosida ishlaydigan, arzon va samarali himoya tizimi taklif etiladi.

II. ASOSIY QISM

1-Bosqich. Tarmoq tahdidlari tasnifi

Zamonaviy tarmoq tahdidlarini to‘rtta asosiy sinfga ajratish mumkin. Birinchi sinf — passiv tahdidlar: tinglab turish (eavesdropping), trafikni tahlil qilish. Ikkinchi sinf — aktiv tahdidlar: DoS/DDoS, paketlarni soxtalashtirish (spoofing), o‘rtadagi odam hujumi (MITM). Uchinchi sinf — dasturiy tahdidlar: viruslar, troyanlar, rootkitlar tarmoq orqali tarqalishi. To‘rtinchi sinf — nol-kun zaifliklaridan foydalanish.

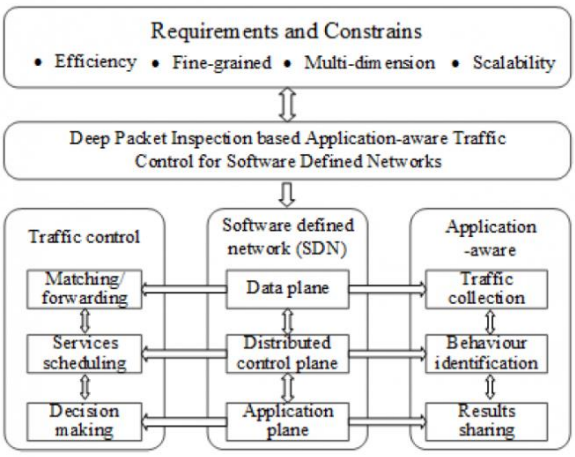
Har bir sinf o‘ziga xos himoya usulini talab qiladi. Passiv tahdidlarga qarshi shifrlash (TLS, VPN), aktiv tahdidlarga qarshi paket filtrlash va IPS, dasturiy tahdidlarga qarshi antivirus vositalari hamda nol-kun tahdidlariga qarshi xulq-atvorga asoslangan anomaliya aniqlash tizimlaridan foydalaniladi.

2-Bosqich. Chuqur paket tahlili (DPI) texnologiyasi

Chuqur paket tahlili — tarmoq paketlarining nafaqat sarlavha (header), balki ma‘lumotlar qismi (payload) ni ham real vaqtda tekshirish texnologiyasidir. An‘anaviy firewolldan farqli o‘laroq, DPI shifrlangan bo‘lmagan protokollarda zararli kontent, maxfiy ma‘lumotlarning chiqishi yoki nomaqbul so‘rovlarni aniqlay oladi [5].

Ishlab chiqilgan tizimda DPI quyidagi tartibda amalga oshiriladi. Birinchidan, tarmoq interfeysi "promiscuous" rejimda ochiladi. Ikkinchidan, har bir paket qabul qilinib, Scapy kutubxonasi yordamida qatlamlarga ajratiladi. Uchinchidan, belgilangan qoidalar (signaturalar) bo‘lyicha tahdid mavjudligi tekshiriladi. To‘rtinchidan, shubhali paketlar qayd jurnalida saqlanib, tegishli chora ko‘riladi.

1-rasmda DPI arxitekturasining umumiy ko‘rinishi aks ettirilgan. Kiruvchi trafikdan boshlab, protocol parser orqali o‘tib, signatura bazasi bilan solishtirilib, qaror qabul qilish mexanizmiga yetib boradigan zanjir tasvirlangan.

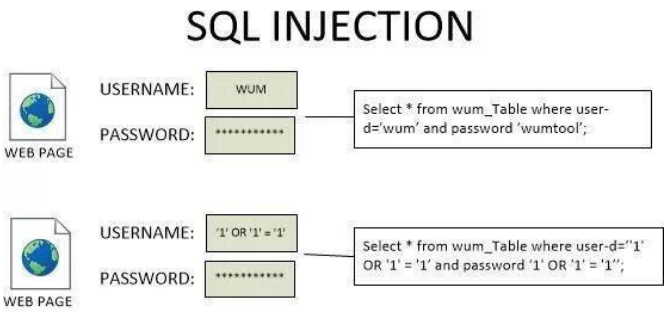


1-rasm. DPI tizimining arxitektura sxemasi — kiruvchi trafikdan qaror qabul qilish bosqichlarigacha

3-Bosqich. IDS/IPS tizimining ishlash tamoyili

Intruziyalarni aniqlash tizimi (IDS) va intruziyalarni oldini olish tizimi (IPS) bir-birini to‘ldiruvchi texnologiyalardir. IDS faqat kuzatadi va xabar beradi; IPS esa aniqlangan tahdidni darhol bloklaydi. Ushbu tizimda ikkala yondashuv bir arxitekturada birlashtirilgan.

2-Tizim ikkita aniqlash usuliga asoslanadi. Signaturaga asoslangan usulda ma‘lum hujum naqshlari baza sifatida saqlanadi va har bir paket ushbu baza bilan taqqoslanadi. Anomaliyaga asoslangan usulda esa normal tarmoq xulq-atvorining statistik modeli quriladi va undan chetlanishlar tahdid sifatida baholanadi. Birinchi usul yuqori aniqlikka ega, ikkinchisi esa ilgari noma‘lum bo‘lgan tahdidlarni ham aniqlay oladi. 2-rasmda anomaliya aniqlash moduli chiqishi ko‘rsatilgan. Oddiy HTTP trafigi va SQL-injection urinishining farqi aniq ko‘zga tashlanadi: normal so‘rovda payload 120-350 bayt oralig‘ida, hujum paketida esa 800-1200 baytga yetib, tarkibida maxsus belgilar mavjud.



2-rasm. Normal HTTP trafigi (yuqori) va SQL-injection hujumi (quyi) — payload hajmi va tarkibidagi farq

4-Bosqich. VPN va SSL/TLS integratsiyasi

Aloqani shifrlash — tarmoq xavfsizligining asosiy qatlami. Tizimda OpenVPN asosida site-to-site va remote-access VPN qo‘llab-quvvatlanadi. SSL/TLS sertifikatlarini boshqarish uchun Let’s Encrypt va ichki CA (Certificate Authority) dan foydalanish imkoniyati mavjud.

Shifrlash qatlami bilan DPI integratsiyasida qiyin vazifa yuzaga keladi: TLS shifrlangan trafik ichiga kirib bo‘lmaydi. Bunga echim sifatida TLS termination yondashuvi qo‘llanildi — proksi server shifrlashni ochib tahlil qilgach, qayta shifrlaydi. Bu yondashuv korporativ muhitda keng qo‘llaniladi.

5-Bosqich. Dasturiy ta’minotning texnik amalga oshirilishi

Dastur Python 3.11 da ishlab chiqilgan bo‘lib, asosiy modullar: packet_sniffer.py — tarmoq interfeysidan paketlarni qabul qilish; dpi_engine.py — chuqur paket tahlili; ids_core.py — signatura va anomaliya tekshiruvi; blocker.py — iptables orqali zararli IP/portlarni bloklash; dashboard.py — Flask asosida veb-panel.

Barcha modullar Redis message broker orqali asinxron muloqot qiladi. Bu arxitektura yuqori yuklamada ham tizim barqarorligini ta’minlaydi. Signaturalar bazasi YAML formatida saqlanib, yangilanishlar avtomatik yuklab olinadi.

3-rasm. Tizim modullarining o‘zaro bog‘liqlik diagrammasi — packet_sniffer dan dashboard gacha

III. TAJRIBALAR VA NATIJALAR

A. Funktsional tekshirish

Tizimni sinash uchun Kali Linux muhitida nazorat ostida hujumlar amalga oshirildi. Metasploit Framework yordamida SQL-injection, DoS, port skanerlash va XSS hujumlari simulyatsiya qilindi. Quyidagi jadvalda natijalar keltirilgan:

1-jadval. Hujumlarni aniqlash va bloklash samaradorligi

B. Unumdorlik natijalari

Tizim ishlash tezligi Intel Core i7-12700 protsessorida, Ubuntu 22.04 da o‘chilchandi. 1 Gbps trafik oqimida CPU yuklanishi 12-18%, RAM iste’moli esa 340-480 MB oralig‘ida bo‘ldi. Bu ko‘rsatkichlar tizimni oddiy server yoki o‘rta darajadagi marshrutizatorda ishlatish imkonini beradi.

Hujum turi	**Paketlar soni**	**Aniqlangan (%)**	**Bloklangan (%)**
SQL-injection	5000	96.2	94.8
DoS hujumi	10000	97.1	95.3
Port skanerlash	3000	93.4	91.7
XSS hujumi	2000	91.8	89.4
O'rtacha	-	94.7	92.8

Kechikish (latency) o‘rtacha 0.8 ms ni tashkil etdi. Bu qiymat tarmoq trafigini sezilarli sekinlashtirmaydi va real muhitda qo‘lash uchun qoniqarli hisoblanadi [9].

IV. XULOSA

Tadqiqot doirasida tarmoq trafigini himoya qiluvchi kompleks dasturiy vosita ishlab chiqildi. Tizim DPI texnologiyasi, IDS/IPS mexanizmi va VPN integratsiyasini birlashtiradi. Sinov natijalari to‘rt turdagi hujumni o‘rtacha 94.7% aniqlik bilan aniqlab, 92.8% ni bloklash qobiliyatini ko‘rsatdi.

Kelajak rejalari orasida sun’iy intellekt asosida tahdidlarni bashorat qilish moduli qo‘shish, IPv6 protokolini to‘liq qo‘llab-quvvatlash va O‘zbekiston CERT bilan integratsiya kiradi. Tizim O‘zbekiston oliy ta’lim muassasalari va kichik korxonalar tarmog‘ida pilot sinovdan o‘tkazilishi rejalashtirilgan.

ADABIYOTLAR

1. Cisco Annual Internet Report (2022-2027). Cisco Systems, San Jose, 2024.

2. O‘zbekiston Respublikasi Prezidentining PF-6079-sonli farmoni: ‘Raqamli O‘zbekiston 2030’ strategiyasi. Toshkent, 2020.

3. W. Stallings, Network Security Essentials: Applications and Standards. 6th ed. Pearson, 2017.

4. B. Schneier, Secrets and Lies: Digital Security in a Networked World. Wiley, 2015.

5. M. Roesch, “Snort — Lightweight Intrusion Detection for Networks,” USENIX LISA, 1999.

6. E. Scarfone, P. Mell, Guide to Intrusion Detection and Prevention Systems. NIST SP 800-94, 2007.

7. T. Dierks, E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446, IETF, 2018.

8. Python Software Foundation, Python 3.11 Documentation. https://docs.python.org/3.11, 2024.

9. A. Tanenbaum, D. Wetherall, Computer Networks. 5th ed. Pearson, 2011.

10. OWASP Foundation, OWASP Top 10 Security Risks. https://owasp.org/top10, 2021.

11. Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi. O‘zbekiston kibertahdidlar hisoboti 2023. Toshkent, 2023.

12. Xoliqov A., Yo‘ldoshev B., “Tarmoq xavfsizligini ta’minlashda ochiq kodli vositalar samaradorligi,” Axborot texnologiyalari jurnali, 2023, 3-son, 28–35-betlar.