FIREWALL VA IDS/IPS TIZIMLARI: HIMOYA VA VOSITALARI

Qodirov Farrux Ergash o‘g‘li
Matematika va ta’limda axborot texnologiyasi kafedrasi mudiri, Ilmiy rahbar
Mardonov Zuhriddin Asatullo o‘g‘li
Shahrisabz davlat pedagogika instituti matematika va informatika yo’nalishi 2-bosqich talabasi
https://doi.org/10.5281/zenodo.15117551

Annotatsiya: Ushbu maqolada axborot xavfsizligini ta’minlashda muhim rol o‘ynovchi himoya vositalari – firewall (tarmoqlararo ekran), IDS (hujumlarni aniqlash tizimi) va IPS (hujumlarning oldini olish tizimi) haqida so‘z boradi. Firewall tarmoq xavfsizligining birinchi darajali himoya chizig‘i bo‘lib, ma’lum qoidalarga asosan kiruvchi va chiquvchi trafikni nazorat qiladi. IDS tizimlari esa tarmoq yoki tizimdagi shubhali faoliyatni aniqlab, administratorni xabardor qiladi, IPS esa bunday tahdidlarni avtomatik ravishda bloklaydi. Maqolada ushbu himoya vositalarining ishlash tamoyillari, farqlari va afzalliklari tahlil qilinadi hamda ularni axborot xavfsizligi strategiyasida samarali qo‘llash bo‘yicha tavsiyalar beriladi.

Kalit so‘zlar: firewall, IDS, IPS, tarmoqlararo ekran, kiberxavfsizlik, axborot xavfsizligi, tarmoq xavfsizligi, hujumlarni aniqlash, hujumlarning oldini olish, xavfsizlik devori, tarmoq monitoringi, tahdidlarga qarshi himoya.

Kirish: Zamonaviy axborot texnologiyalari jadal rivojlanishi bilan birga, kiberxavfsizlik tahdidlari ham ortib bormoqda. Kompaniyalar, tashkilotlar va individual foydalanuvchilar uchun ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlash muhim masalalardan biriga aylandi. Xususan, turli xil zararli dasturlar, kiberhujumlar va tarmoqdagi noqonuniy harakatlar natijasida jiddiy xavflar yuzaga kelishi mumkin.Bunday tahdidlarga qarshi samarali himoya choralaridan biri firewall, IDS (Intrusion Detection System – hujumlarni aniqlash tizimi) va IPS (Intrusion Prevention System – hujumlarning oldini olish tizimi) texnologiyalaridan foydalanishdir. Ushbu tizimlar tarmoq xavfsizligini ta’minlashda muhim rol o‘ynaydi va turli xildagi kiberhujumlarning oldini olish, shuningdek, zararli trafikni nazorat qilish imkonini beradi. Firewall tizimi tarmoq xavfsizligining asosiy himoya vositalaridan biri bo‘lib, ma’lum qoidalarga asosan trafikni boshqaradi va ruxsat etilmagan ulanishlarni bloklaydi. IDS va IPS tizimlari esa tarmoq yoki tizimga nisbatan sodir etilayotgan hujumlarni aniqlash va ularning oldini olishga qaratilgan. IDS hujum haqida xabar beruvchi monitoring tizimi bo‘lsa, IPS esa hujumlarni avtomatik ravishda to‘xtatish imkoniyatiga ega. Ushbu maqolada firewall va IDS/IPS tizimlarining ishlash tamoyillari, farqlari hamda ularning afzallik va kamchiliklari tahlil qilinadi. Shuningdek, axborot xavfsizligini ta’minlashda ushbu vositalarni qanday samarali qo‘llash mumkinligi bo‘yicha tavsiyalar beriladi.

IDS (Intrusion Detection System) tizimlari tarmoq yoki tizimga kirish urinishlarini aniqlash va kuzatish uchun mo‘ljallangan xavfsizlik mexanizmlaridir. IDS tizimlari quyidagi turlarga bo‘linadi:

IDS tizimlari qaysi darajada ishlashiga qarab ikkiga bo‘linadi:

- HIDS (Host-based IDS) – Faqat bitta kompyuter yoki serverga o‘rnatiladi va ushbu tizimdagi zararli faoliyatni kuzatadi.

- NIDS (Network-based IDS) – Tarmoqdagi trafikni kuzatib, hujumlarni aniqlaydi.

IDS tizimlari ishlash uslubiga qarab quyidagi guruhlarga bo‘linadi:

- Signature-based IDS – Oldindan ma’lum bo‘lgan hujum namunalariga (imzolariga) asoslanib, tahdidlarni aniqlaydi.

- Anomaly-based IDS – Oddiy (normal) tarmoq faoliyatidan chetga chiqqan harakatlarni kuzatib, noma’lum hujumlarni aniqlaydi.

- Hybrid IDS – Signature va anomaly metodlarini birlashtirib ishlaydi, bu esa aniqroq natija beradi.

IDS va IPS farqlari:

- IDS (Intrusion Detection System) – Faqat hujumlarni aniqlaydi va ogohlantiradi.

- IPS (Intrusion Prevention System) – Hujumni aniqlabgina qolmay, uni bloklaydi ham.

Mashhur IDS tizimlari:

- Snort (ochiq kodli, NIDS)

- Suricata (NIDS, yuqori samaradorlik)

- OSSEC (HIDS, loglarni tahlil qiladi)

- Bro (Zeek) (tarmoq trafigini chuqur tahlil qiladi)

IDS turlariga quyidagilar kiradi:

Tarmoqqa asoslangan: tarmoqqa asoslangan IDS (NIDS) kompyuter tarmog'ining strategik nuqtalarida kiruvchi va chiquvchi trafikni tekshirib o‘rnatiladi. U tarmoq protokollarini, trafik naqshlarini va paket sarlavhalarini kuzatishga qaratilgan.

Xostga asoslangan: Xostga asoslangan IDS (HIDS) IT muhitidagi alohida mashinalar yoki serverlarga o‘rnatiladi. U ruxsatsiz kirish urinishlari va tizimdagi g'ayritabiiy o‘zgarishlar kabi hodisalarni aniqlash uchun tizim jurnallari va fayllarini kuzatishga qaratilgan.

Gibrid: Gibrid IDS ham tarmoqqa, ham xostga asoslangan yondashuvlarni birlashtiradi. Ushbu turdagi IDS IT ekotizimidagi voqealarning to‘liqroq ko‘rinishini ta'minlaydi.

IDS vositalari tarmoq paketlarini tahlil qilish va ularni ma'lum hujum imzolari yoki xatti-harakatlar naqshlari bilan solishtirish orqali ishlaydi. Agar IDS buzg'unchini aniqlagan deb hisoblasa, u tizim ma'murlari yoki xavfsizlik guruhlariga ogohlantirish yuboradi. Ushbu ogohlantirishlar aniqlangan faoliyat haqida batafsil ma'lumotni o‘z ichiga oladi, bu esa xodimlarga tezda tekshirish va javob berish imkonini beradi. IDS kompyuter tarmoqlari va tizimlarining xavfsizligi va yaxlitligini ta'minlashda muhim rol o‘ynaydi.

Mavzuga doir adabiyotlar tahlili

Axborot xavfsizligi va tarmoq himoyasi sohasida ko‘plab tadqiqotchilar firewall, IDS va IPS tizimlarining samaradorligi hamda ularning tahdidlarga qarshi kurashishdagi o‘rnini chuqur o‘rgangan. Ushbu bo‘limda mavzuga oid ilmiy maqolalar, darsliklar va texnik hujjatlar asosida ushbu himoya vositalarining nazariy va amaliy jihatlari tahlil qilinadi.

1. Firewall texnologiyalari bo‘yicha adabiyotlar

Firewall’lar tarmoq xavfsizligining asosiy komponenti sifatida ko‘riladi. Stalling W. tomonidan yozilgan “Network Security Essentials” kitobida firewallning ishlash tamoyillari, turlar va tarmoqlarni himoya qilish strategiyalari batafsil yoritilgan. Shuningdek, Tanenbaum A.S. va Wetherall D. ning “Computer Networks” kitobida firewall’larning paket filtrlash, holatni tekshirish va ilovalar darajasidagi nazorat funksiyalari tahlil qilinadi.

Ilmiy maqolalar orasida firewall texnologiyalarining samaradorligi va ularning zamonaviy tahdidlarga moslashuvi bo‘yicha bir qator tadqiqotlar olib borilgan. Masalan, Z. Fu va boshqalar tomonidan yozilgan "A Survey on Firewall Technologies" maqolasida zamonaviy

firewall'larning rivojlanishi va yangi xavf-xatarlarga moslashish imkoniyatlari muhokama qilingan.

2. IDS va IPS tizimlari bo'yicha adabiyotlar

Hujumlarni aniqlash va oldini olish tizimlari bo'yicha ilmiy adabiyotlarda IDS va IPS'ning ishlash mexanizmlari, signatura va anomaliya asosidagi yondashuvlar haqida ko'plab tadqiqotlar mavjud. Kevin Scarfone va Peter Mell tomonidan tayyorlangan "Guide to Intrusion Detection and Prevention Systems (IDPS)" hujjatida IDS/IPS tizimlarining umumiy ishlash tamoyillari va ularning xavfsizlik strategiyalaridagi roli batafsil tushuntirilgan.

Bundan tashqari, Bace R. va Mell P. tomonidan yozilgan "Intrusion Detection Systems" asari IDS'larning arxitekturasi, signatura va statistik tahlil asosida ishlash usullarini ko'rib chiqadi. Bu manbalar IDS va IPS tizimlarining hujumlarni aniqlash, tahdidlarni tahlil qilish va ularga munosabat bildirishdagi samaradorligini tushunish uchun muhim ahamiyat kasb etadi.

3. Zamonaviy tahdidlar va ularni bartaraf etish strategiyalari

Kiberxavfsizlik sohasida doimiy ravishda yangi tahdidlar paydo bo'lib, firewall, IDS va IPS tizimlarini takomillashtirish zarurati tug'iladi. Stouffer K., Lightman S. va boshqalar tomonidan tayyorlangan "NIST Guide to Industrial Control System Security"qo'llanmasida sanoat tarmoqlari uchun xavfsizlik choralarini belgilash bo'yicha tavsiyalar berilgan. Shuningdek, "Cybersecurity and Cyberwar: What Everyone Needs to Know" asarida zamonaviy kiberhujumlar va ularga qarshi himoya usullari muhokama qilingan.

Ushbu adabiyotlar firewall, IDS va IPS tizimlarining afzalliklari va cheklovlarini tushunishda hamda ularni zamonaviy tahdidlarga qarshi samarali ishlatish strategiyalarini ishlab chiqishda muhim ilmiy asos beradi.

Natija va muhokama

Tadqiqot natijalari shuni ko'rsatadiki, firewall, IDS va IPS tizimlari tarmoq xavfsizligini ta'minlashda muhim rol o'ynaydi, ammo ularning har biri o'ziga xos xususiyat va cheklovlarga ega. Ushbu bo'limda har bir himoya vositasining samaradorligi, ularning afzallik va kamchiliklari hamda real hayotda qo'llanilishi tahlil qilinadi.

1. Firewall'larning samaradorligi

Tahlillar shuni ko'rsatadiki, firewall tizimlari tarmoqni tashqi tahdidlardan himoya qilishda samarali vosita hisoblanadi. Ular paket filtrlash, NAT (Network Address Translation) va DPI (Deep Packet Inspection) kabi texnologiyalar yordamida zararli trafikni bloklash imkonini beradi. Biroq, firewall faqat ruxsat etilgan yoki taqiqlangan trafikni nazorat qiladi, bu esa murakkab kiberhujumlarni aniqlash va ularning oldini olishda yetarli bo'lmasligi mumkin.

2. IDS va IPS tizimlarining afzalliklari va cheklovlari

IDS tizimlari tarmoq yoki tizimga qilingan hujumlarni aniqlashda samarali bo'lsa-da, ular faqat ogohlantirish berish bilan cheklanadi. IPS esa avtomatik ravishda tahdidlarni bartaraf etish imkoniyatiga ega, bu esa tarmoq xavfsizligini yanada mustahkamlashga yordam beradi. Biroq, IDS va IPS tizimlarining samaradorligi ularning signatura va anomaliya asosidagi hujumlarni aniqlash qobiliyatiga bog'liq. Yangi turdagi hujumlarni aniqlash uchun doimiy yangilanish va tahlil talab etiladi.

Bundan tashqari, IPS tizimlari noto'g'ri musbat (false positive) va noto'g'ri manfiy (false negative) natijalarga olib kelishi mumkin. Ya'ni, xavfsiz trafikni xatolik bilan hujum sifatida

aniqlashi yoki haqiqiy tahdidlarni o‘tkazib yuborishi ehtimoli mavjud. Shu sababli, IDS/IPS tizimlarini samarali ishlatish uchun ular sun’iy intellekt va mashinaviy o‘rganish texnologiyalari bilan boyitilishi lozim.

3. Zamonaviy tahdidlarga qarshi kurashish strategiyalari

Tahlillar shuni ko‘rsatadiki, faqat bitta xavfsizlik vositasidan foydalanish yetarli emas. Firewall, IDS va IPS tizimlarini birgalikda qo‘llash orqali yanada mustahkam himoya mexanizmini yaratish mumkin. Masalan:

- Ko‘p qatlamli himoya (Defense in Depth) – Firewall, IDS va IPS tizimlari birgalikda ishlatilsa, tarmoqning turli darajalarida xavfsizlikni ta’minlash mumkin.

- Sun’iy intellekt asosidagi monitoring – IDS/IPS tizimlariga mashinaviy o‘rganish algoritmlarini qo‘llash orqali yangi turdagi hujumlarni oldindan aniqlash imkoniyati ortadi.

- Doimiy yangilanish va audit – Tizimlarning doimiy ravishda yangilanishi va tahlil qilinishi kiberhujumlarning oldini olishda muhim ahamiyatga ega.

Xulosa va takliflar

Tadqiqot natijalariga ko‘ra, firewall, IDS va IPS tizimlari tarmoq xavfsizligini ta’minlashda muhim rol o‘ynaydi, biroq ularning har biri o‘ziga xos afzallik va cheklovlarga ega. Firewall tarmoqdagi trafikni nazorat qilib, ruxsat etilmagan ulanishlarni bloklasa, IDS tizimi hujumlarni aniqlash va administratorni ogohlantirish bilan shug‘ullanadi. IPS esa avtomatik tarzda tahdidlarni bartaraf qilish imkoniyatiga ega. Shuningdek, zamonaviy kiberxavfsizlik tahdidlari shuni ko‘rsatadiki, faqat bitta himoya vositasidan foydalanish yetarli emas. Ularning kombinatsiyalangan ishlashi – ko‘p qatlamli himoya strategiyasi (Defense in Depth) samaradorligini oshiradi. IDS/IPS tizimlarining samaradorligi esa doimiy yangilanish va sun’iy intellekt asosida tahlil qilish orqali oshirilishi mumkin.

Takliflar

Tarmoq xavfsizligini yanada mustahkamlash maqsadida quyidagi takliflarni ilgari surish mumkin:

- 1. Ko‘p qatlamli himoya modelini joriy etish – Firewall, IDS va IPS tizimlarini birgalikda ishlatish orqali tarmoq xavfsizligini kompleks tarzda ta’minlash lozim.
- 2. Sun’iy intellekt va mashinaviy o‘rganish texnologiyalarini tatbiq etish – IDS/IPS tizimlarining tahdidlarni avtomatik ravishda aniqlash va bartaraf etish qobiliyatini oshirish uchun ularni AI algoritmlari bilan takomillashtirish zarur.
- 3. Doimiy yangilanish va monitoring tizimini tashkil etish – Hujumlarning oldini olish uchun himoya vositalarini muntazam yangilash, tarmoq trafikini real vaqt rejimida kuzatib borish va tahlil qilish kerak.
- 4. Noto‘g‘ri musbat va noto‘g‘ri manfiy natijalarni kamaytirish – IDS va IPS tizimlarining ishlash samaradorligini oshirish uchun ularda noto‘g‘ri signal berish ehtimolini kamaytirishga e’tibor qaratish lozim.
- 5. Xodimlarning kiberxavfsizlik bo‘yicha malakasini oshirish – Himoya tizimlaridan maksimal darajada samarali foydalanish uchun IT mutaxassislarini muntazam ravishda o‘qitish va ularga yangi tahdidlar haqida ma’lumot berish muhimdir.

Yuqoridagi takliflarni amalga oshirish orqali tashkilotlar va tarmoq administratorlari axborot xavfsizligini sezilarli darajada mustahkamlashlari va zamonaviy kiberhujumlarga qarshi samarali himoya choralarini ishlab chiqishlari mumkin.

Foydalanilgan adabiyotlar/Используемая литература/References:

1. Кодиров, Ф. Э., and О. Д. Дониёров. "ЭФФЕКТИВНЫЕ МОДЕЛИ РАЗВИТИЯ МЕДИЦИНСКОГО ОБСЛУЖИВАНИЯ НАСЕЛЕНИЯ КАШАКАДЬИНСКОЙ ОБЛАСТИ." Символ науки 7-2 (2022): 15-17.

2. Zoxidov, J. B., F. E. Qodirov, and I. J. Bozorova. "QUARTUS II PROJECT CONCEPT AND ITS OPPORTUNITIES AND PROBLEMS." АКТУАЛЬНЫЕ ПРОБЛЕМЫ ТЕХНИЧЕСКОГО И ТЕХНОЛОГИЧЕСКОГО ОБЕСПЕЧЕНИЯ ИННОВАЦИОННОГО РАЗВИТИЯ. 2019.

3. Uzakov, Gulom, et al. "Simulation of a tubular pyrolysis reactor using comsol multiphysics software." International Scientific and Practical Conference Digital and Information Technologies in Economics and Management. Cham: Springer Nature Switzerland, 2023.

4. Қодиров, Ф. "ҲУДУДЛАРДА ТИББИЙ ХИЗМАТЛАРНИ ДАСТУРИЙ ПАКЕТЛАР ЁРДАМИДА ЭЛЕКТРОН ТИББИЙ БАЗАСИНИ ЯРАТИШ." O'zbekiston Respublikasi Oliy Va o'rta Maxsus ta'lim Vazirligi Namangan Muhandislik-Qurilish Instituti (2022).

5. Qodirov, F. E., O. D. Doniyorov, and H. Shokirov Sh. "Basic concepts of information security in information systems. Wide threats and their consequences." концепции устойчивого развития науки в современных условиях (2021): 153-155.

6. Bozorova, Irina Jumanazarovna, and Dilfuzaxon Mamasharipovna Karayeva. "Modern programming technologies and their role." интеллектуальный капитал xxi века. 2020.

7. Ergash o'g'li, Qodirov Farrux. "Hududlarni ijtimoiy-iqtisodiy rivojlantirishda har bir hududning o 'ziga xos xususiyatlari." Scientific Journal of Actuarial Finance and Accounting 4.09 (2024): 178-183.

8. Qodirov, Farrux, and Muxlisa Mavlonova. "O'ZBEKISTONDA ZIYORATGOH VA QADAMJOLAR, TURIZM XIZMATLARINI JADAL RIVOJLANTIRISH ISTIQBOLLARI." YANGI O'ZBEKISTONDA MILLIY TURIZM ISTIQBOLLARI 1.01 (2024).

9. Qodirov, F., N. Sirojev, and S. Negmatova. "FEATURES OF THE ANDROID STUDIO SOFTWARE PACKAGE." Академические исследования в современной науке 2.17 (2023): 130-146.

10. Қодиров, Ф. Э., et al. "ДЛЯ ПРОВЕРКИ МОДЕЛЕЙ АДЕКВАТНОСТИ, ЧУВСТВИТЕЛЬНОСТЬ И СОПРОТИВЛЕНИЯ." ИНТЕГРАЦИЯ НАУКИ, ОБЩЕСТВА, ПРОИЗВОДСТВА И ПРОМЫШЛЕННОСТИ. 2019.11. Qodirov, F. E., D. A. Akbarova, and S. H. Shokirov. "SOFTWARE FOR WORKING WITH COMPUTER GRAPHICS AND THEIR TASKS. APPLICATION OF DIGITAL IMAGE PROCESSING FIELDS." (2021): 57-58.

11. Jumanazarovna, Bozorova Irina, and Kodirov Farruh Ergash O'G'Li. "Principle of electrocardiographic work and its role in modern medicine." Вопросы науки и образования 15 (99) (2020): 31-36.

12. Kodirov, F. E., and J. E. Nematov. "BASIC TECHNOLOGY AND SERVICE MANAGEMENTMULTISERVICE NETWORKS." Инновации в технологиях и образовании: сб. ст. участников XII Между (2019): 214.

13. Қодиров, Ф. Э., and Ж. Э. Нематов. "РАЗВИТИЕ ЛОКАЛЬНОЙ СЕТИ НА ОСНОВЕ

ТЕХНОЛОГИИ GPON." Инновации в технологиях и образовании: сб. ст. участников XII Между (2019): 288.

14. Кодиров, Ф. Э., and М. У. Маматмурадова. "РАЗРАБОТКА ЦИФРОВОЙ ПРОГРАММЫ ШИФРОВАНИЯ И ВНЕДРЕНИЕ В ПРАКТИКУ." Инновации в технологиях и образовании: сб. ст. участников XII Между (2019): 275.

15. Абдирасулов, Ж. У., and Ф. Э. Кодиров. "ЭФФЕКТИВНОСТЬ ANGULAR JS ДЛЯ СОЗДАНИЯ ДИНАМИЧЕСКИХ ВЕБ-САЙТОВ И ОПТИМИЗАЦИИ ИХ ПРОИЗВОДИТЕЛЬНОСТИ." Инновации в технологиях и образовании: сб. ст. участников XII Между (2019): 228.

16. Qodirov, F. E., J. B. Zohidov, and H. I. Karamatova. "ADVANTAGES OF PROGRAMMING LANGUAGES JAVASCRIPT, JAVA AND PYTHON." МОДЕЛИРОВАНИЕ И АНАЛИЗ СЛОЖНЫХ ТЕХНИЧЕСКИХ И ТЕХНОЛОГИЧЕСКИХ СИСТЕМ. 2019.

17. Qodirov, F. E., J. U. Abdirasulov, and J. E. Nematov. "FORMING GOVERNMENT AGENCY WEBSITES WITH WORDPRESS CONTENT MANAGEMENT SYSTEM." Инновации в технологиях и образовании: сб. ст. участников XII Между (2019): 219.

18. Турдиев, У. К., and Ф. Э. Кодиров. "Задача Коши Для Одномерной Системы Уравнений Типа Бюргерса Возникающей В Двухскоростной Гидродинамике." Инновации в технологиях и образовании: сб. ст. участников XI Между (2018): 349.

19. Qodirov, F. E. "Methodological aspects and importance of development of medical services through econometric modeling and forecasting options." academy. uz/index. php/yo.