IDS/IPS TIZIMLARINING ISHLASH PRINSIPI VA ULARNI CHETLAB O‘TISH USULLARI

O‘ktamova Fotimaxon Rustamjon qizi
Farg‘ona davlat universiteti talabasi
fotimaoktamova5@gmail.com
Sobirjonov Behzodbek Qahramon o‘g‘li
Farg‘ona davlat universiteti o‘qituvchisi.
behzodbekqahramonovich@gmail.com

Annotatsiya

Ushbu maqolada zamonaviy axborot tizimlari va kompyuter tarmoqlarida keng qo‘llaniladigan IDS (Intrusion Detection System) hamda IPS (Intrusion Prevention System) tizimlarining ishlash prinsiplari, asosiy turlari va ularning amaliy qo‘llanilishi tahlil qilinadi. Maqolada IDS/IPS tizimlarining signatura asosidagi, anomaliya asosidagi va stateful protocol analysis metodlari ilmiy manbalar asosida yoritilgan. Shuningdek, kiberhujumchilar tomonidan ushbu tizimlarni chetlab o‘tishda qo‘llaniladigan fragmentatsiya, payload obfuscation, timing attack va protocol ambiguity kabi aldash usullari keng tahlil qilingan. Zamonaviy himoya yondashuvlari sifatida deep packet inspection, traffic normalization hamda mashinaviy o‘rganish asosidagi aniqlash metodlarining samaradorligi ko‘rib chiqilgan. Tadqiqot natijalari IDS/IPS tizimlarining axborot xavfsizligini ta’minlashdagi muhim rolini hamda ularni muntazam takomillashtirish zarurligini ko‘rsatadi.

Kalit so‘zlar: *IDS, IPS, kiberxavfsizlik, tarmoq xavfsizligi, intrusion detection, intrusion prevention, signatura asosidagi aniqlash, anomaliya asosidagi aniqlash, packet fragmentation, payload obfuscation, timing attack, deep packet inspection, machine learning, axborot xavfsizligi.*

Аннотация

В данной статье будут проанализированы принципы работы, основные виды и практическое применение систем IDS (система обнаружения вторжений) и IPS (система предотвращения вторжений), широко применяемых в современных информационных системах и компьютерных сетях. В статье рассматриваются методы анализа сигнатур, аномалий и протоколов состояния систем IDS / IPS, основанные на научных источниках. Также был проведен обширный анализ методов обмана, используемых киберпреступниками для обхода этих систем, таких как фрагментация, обфускация загрузки платежей, timing Attack и protocol ambiguity. В качестве современных защитных подходов были рассмотрены эффективность

глубокой инспекции пакетов, нормализации трафика, а также методов обнаружения на основе машинного обучения. Результаты исследования показывают важную роль систем IDS/IPS в обеспечении информационной безопасности, а также необходимость их систематического совершенствования.

Ключевые слова: *IDS, IPS, кибербезопасность, сетевая безопасность, обнаружение вторжений, предотвращение вторжений, обнаружение на основе сигнатур, обнаружение на основе аномалий, фрагментация пакетов, обфускация загрузки, Атака времени, глубокая проверка пакетов, машинное обучение, информационная безопасность.*

Annotation

This article analyzes the operating principles, basic types and practical applications of IDs (Intrusion Detection System) and IPS (Intrusion Prevention System) Systems, which are widely used in modern information systems and computer networks. The article covers the signature-based, anomaly-based and stateful protocol analysis methods of IDS/IPS systems based on scientific sources. Deception techniques such as fragmentation, payload obfuscation, timing attack, and protocol ambiguity used by cyberattacks to circumvent these systems have also been extensively analyzed. The effectiveness of deep packet inspection, traffic normalization, and machine learning-based detection techniques have been considered as modern protection approaches. The results of the study show the important role of IDS/IPS systems in ensuring information security as well as the need for regular improvement.

Keywords: *IDS, IPS, cybersecurity, network security, intrusion detection, intrusion prevention, signature-based detection, anomaly-based detection, packet fragmentation, payload obfuscation, timing attack, deep packet inspection, machine learning, information security.*

Kirish

Hozirgi raqamli texnologiyalar jadal rivojlanayotgan davrda axborot xavfsizligini ta’minlash eng muhim masalalardan biriga aylandi. Internet tarmoqlari, korporativ serverlar, bulutli xizmatlar va IoT qurilmalarining keng qo‘llanilishi bilan bir qatorda kiberhujumlar soni va murakkabligi ham ortib bormoqda. Xususan, ruxsatsiz kirishlar, zararli dasturlar, DDoS hujumlari, port scanning va ma’lumotlar o‘g‘irlanishi kabi tahdidlar zamonaviy axborot tizimlari uchun jiddiy xavf tug‘diradi. Shu sababli tarmoq va tizim xavfsizligini monitoring qilish, hujumlarni erta bosqichda aniqlash hamda oldini olishga qaratilgan vositalar muhim ahamiyat kasb etadi. Bunday himoya vositalarining eng samaralilaridan biri IDS (Intrusion Detection System) va IPS (Intrusion Prevention System) tizimlaridir. NIST tomonidan chop etilgan Guide to Intrusion Detection and Prevention Systems (IDPS)

hujjatiga ko‘ra, IDS va IPS tizimlari tarmoq trafigi hamda tizim faoliyatini doimiy kuzatib, shubhali yoki ruxsatsiz harakatlarni aniqlash uchun xizmat qiladi. IDS tizimi asosan ogohlantirish va monitoring vazifasini bajaradi, IPS esa aniqlangan tahdidni real vaqt rejimida bloklash yoki bartaraf etish imkoniyatiga ega.

Ilmiy adabiyotlarda IDS tizimlari asosan ikki asosiy yondashuv asosida ishlashi ko‘rsatib o‘tiladi: **signatura (signature-based)** va **anomaliya (anomaly-based)** usullari. Signatura asosidagi usul oldindan ma’lum hujum namunalarini aniqlashga xizmat qilsa, anomaliya asosidagi usul tizimning normal ishlash holatini o‘rganib, undan chetga chiqishlarni topishga qaratilgan. Zamonaviy tadqiqotlarda esa sun’iy intellekt va mashinaviy o‘rganish algoritmlari yordamida yangi turdagi hujumlarni aniqlash bo‘yicha samarali yondashuvlar taklif etilmoqda. Shu bilan birga, zamonaviy kiberhujumlar faqat oddiy usullar bilan cheklanib qolmay, IDS/IPS tizimlarini aldashga qaratilgan evasion techniques — ya’ni fragmentatsiya, payload obfuscation, timing attack va protocol ambiguity kabi usullar orqali ham amalga oshiriladi. Bu esa mazkur tizimlarning ishlash samaradorligini chuqur o‘rganish va ularni takomillashtirish zaruratini yuzaga keltiradi.

Mazkur maqolaning maqsadi IDS/IPS tizimlarining ishlash prinsiplari, asosiy aniqlash metodlari hamda ularni aldash usullarini ilmiy manbalar va amaliy misollar asosida tahlil qilishdan iborat.

IDS/IPS tizimlarining umumiy tavsifi. Axborot tizimlari va kompyuter tarmoqlarining keng rivojlanishi bilan bir qatorda kiberxavfsizlik masalalari ham dolzarb ahamiyat kasb etmoqda. Xususan, ruxsatsiz kirishlar, zararli dasturlar, tarmoq skanerlari, DDoS hujumlari va ma’lumotlar o‘g‘irlanishi kabi tahdidlar tashkilotlar faoliyatiga jiddiy zarar yetkazishi mumkin. Shu sababli, tarmoq va tizim xavfsizligini ta’minlashda IDS (Intrusion Detection System) va IPS (Intrusion Prevention System) tizimlari muhim himoya vositasi sifatida qo‘llaniladi. NIST SP 800-94 rasmiy standartiga ko‘ra, IDS – bu kompyuter tizimi yoki tarmoqda sodir bo‘layotgan voqealarni kuzatib, ehtimoliy xavf va ruxsatsiz kirishlarni aniqlashga xizmat qiluvchi dasturiy yoki apparat tizimidir. IPS esa IDS imkoniyatlariga qo‘shimcha ravishda aniqlangan tahdidni avtomatik tarzda bloklash, trafikni to‘xtatish yoki sessiyani uzish imkoniyatiga ega.

IDS/IPS tizimlari ishlash joyiga qarab bir necha turlarga bo‘linadi. **Tarmoq asosidagi IDS (NIDS)** tarmoq orqali uzatilayotgan barcha paketlarni monitoring qiladi va paket tarkibini tekshiradi. **Host asosidagi IDS (HIDS)** esa ma’lum bir server yoki kompyuter ichidagi log fayllar, tizim chaqiriqlari, fayl o‘zgarishlari va foydalanuvchi faoliyatini nazorat qiladi. Bundan tashqari, **wireless IDS** va **network behavior analysis** tizimlari ham mavjud bo‘lib, ular simsiz tarmoqlar va trafik xulq-atvorini tahlil qilishga mo‘ljallangan.

IDS/IPS tizimlarining ishlash prinsipi IDS/IPS tizimlarining ishlash prinsipi asosan uchta asosiy metodga tayanadi.

- Birinchisi, signatura asosidagi aniqlash (signature-based detection) usuli hisoblanadi. Bu yondashuv oldindan ma’lum bo‘lgan hujum namunalarini bazada saqlangan qoidalar bilan solishtiradi. Masalan, SQL injection, malware signaturalari yoki port scan paketlari uchun oldindan yozilgan qoidalar orqali trafik tahlil qilinadi. Ushbu metod juda tez va aniq ishlaydi, biroq uning asosiy kamchiligi – yangi yoki oldin uchramagan zero-day hujumlarni aniqlashdagi cheklovidir.
- Ikkinchi usul, anomaliya asosidagi aniqlash (anomaly-based detection) bo‘lib, tizim normal trafik va foydalanuvchi xatti-harakatlarini o‘rganadi. Keyinchalik ushbu normal modeldan chetga chiqish holatlari tahdid sifatida qayd etiladi. Masalan, serverga odatda sekundiga 100 ta so‘rov keladigan bo‘lsa, birdaniga 10 000 ta so‘rov kelishi DDoS hujum belgisi sifatida aniqlanishi mumkin. Zamonaviy ilmiy tadqiqotlarda ushbu usulda mashinaviy o‘rganish va sun’iy intellekt algoritmlari keng qo‘llanilmoqda.
- Uchinchi yondashuv, stateful protocol analysis usuli bo‘lib, paketlarni TCP/IP, HTTP, DNS kabi protokollarning standart qoidalari asosida tekshiradi. Agar paket tarkibi yoki session holati RFC standartlariga mos kelmasa, tizim buni shubhali holat sifatida belgilaydi. Amaliy jihatdan qaralganda, eng mashhur ochiq kodli IDS/IPS tizimlari sifatida Snort, Suricata va Zeek keng qo‘llaniladi.

IDS/IPS tizimlarini aldash usullari. Shunga qaramay, zamonaviy kiberhujumlar IDS/IPS tizimlarini chetlab o‘tish uchun turli evasion (aldash) usullaridan foydalanadi. Ilmiy maqolalarda bu usullar tizimlarning eng muhim zaif tomonlaridan biri sifatida ko‘rib chiqiladi. Eng keng tarqalgan usullardan biri packet fragmentation hisoblanadi. Bunda zararli trafik bir nechta kichik segmentlarga bo‘lib yuboriladi. Agar IDS ushbu fragmentlarni to‘liq va to‘g‘ri yig‘a olmasa, hujum signaturasini aniqlay olmaydi. Tadqiqotlar shuni ko‘rsatadiki, ayrim IPS qurilmalarida aynan fragmentatsiya hujumlari yuqori bypass natijalarini bergan.

- Ikkinchi muhim usul – payload obfuscation, ya’ni zararli kodni yashirish

hisoblanadi. Bu usulda hujumchi payloadni URL encoding, Base64 yoki Unicode formatlarida kodlaydi. Masalan, oddiy SQL injection ifodasi turli kodlash usullari yordamida IDS qoidalaridan yashirilishi mumkin.

- Uchinchi usul sifatida timing attack ko‘rsatiladi. Bu holatda hujumchi paketlarni juda sekin va vaqt oralig‘ida yuboradi, natijada anomaly-based IDS tizimi uni normal trafik sifatida qabul qilishi mumkin. Ayniqsa threshold asosida ishlovchi tizimlar bunday usulga sezgir bo‘ladi.

Bundan tashqari, protocol ambiguity usuli ham muhim o‘rin tutadi. Bu usulda IDS va target host protokolni turlicha interpretatsiya qiladigan holatlardan foydalaniladi. Masalan,

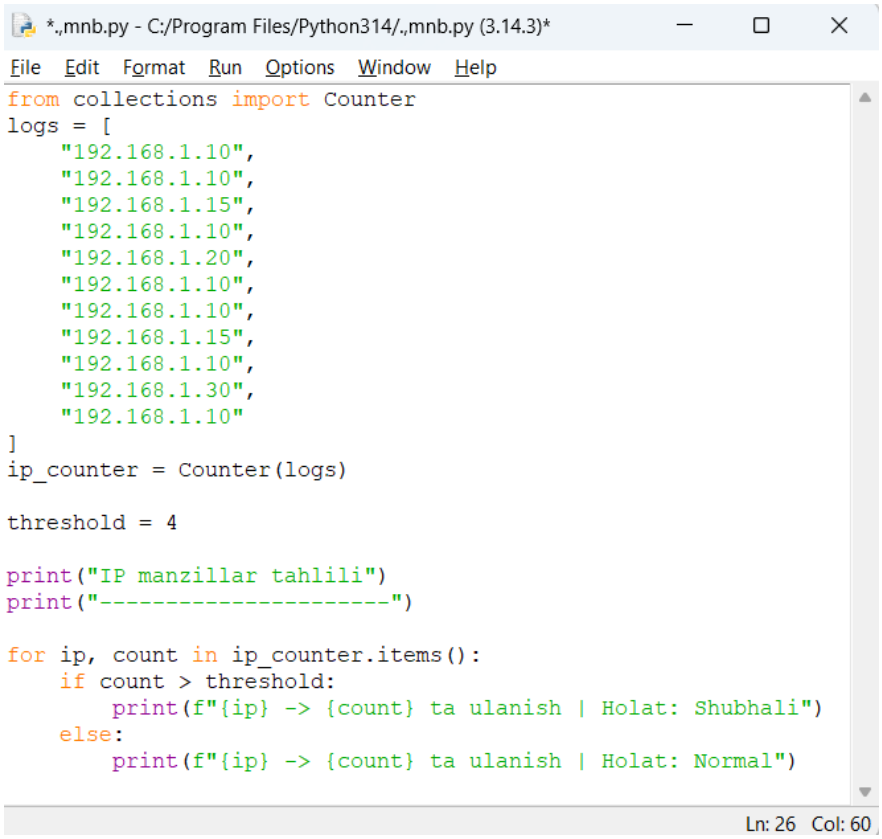
overlapping fragments yoki noto‘g‘ri TCP flag kombinatsiyalari orqali IDS va serverning paketni qayta yig‘ish jarayoni farqlanadi. Natijada zararli trafik tizim tomonidan aniqlanmasligi mumkin.

Zamonaviy himoya usullari. Ilmiy tadqiqotlar shuni ko‘rsatadiki, bir nechta evasion usullarini kombinatsiyalash orqali bypass samaradorligi yanada oshadi. Shu sababli zamonaviy IDS/IPS tizimlarida traffic normalization, deep packet inspection, TLS inspection, machine learning based anomaly detection kabi yangi yondashuvlar joriy qilinmoqda. Bu usullar eski va yangi turdagi hujumlarni aniqlash samaradorligini sezilarli darajada oshiradi.

Python dasturlash tilida oddiy IDS tizimi modelini yaratish.

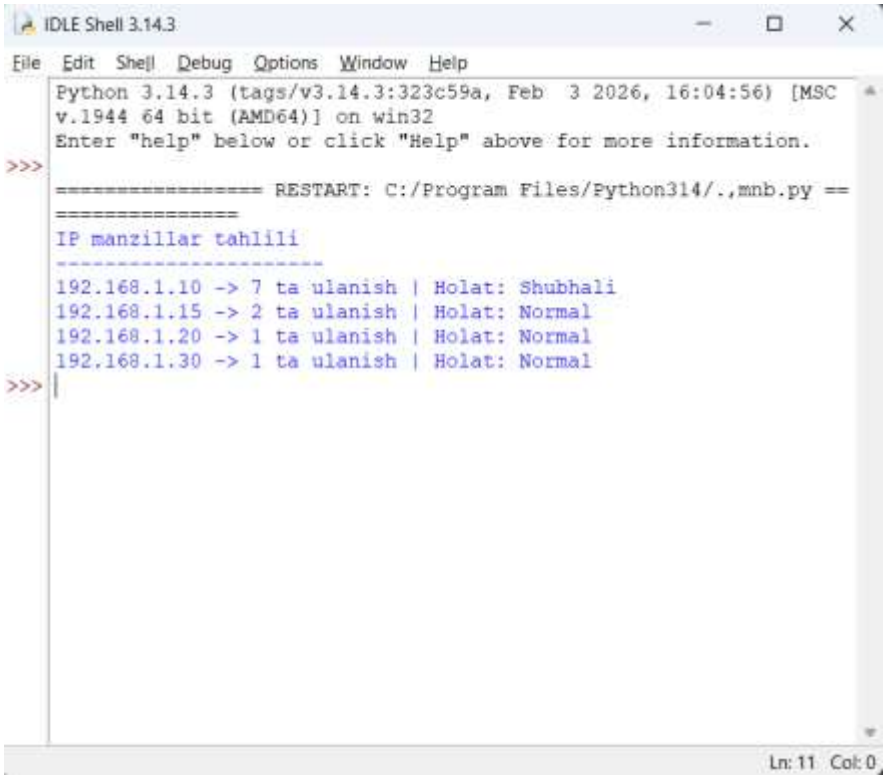
Ishdan maqsad: Ushbu amaliy mashg‘ulotning maqsadi Python dasturlash tili yordamida IDS (Intrusion Detection System) tizimining soddalashtirilgan modelini yaratish, tarmoq loglarini tahlil qilish va shubhali IP manzillarni aniqlashdan iborat. Mazkur amaliy mashg‘ulot orqali IDS tizimlarining anomaliya asosidagi aniqlash (anomaly-based detection) prinsipi amaliy ko‘rinishda namoyish etiladi.

(1-rasm)



Python dasturlash tilida oddiy IDS modelining dastur kodi:

(2-rasm)



Dastur bajarilish natijasi:

Dastur ishga tushirilganda tarmoq loglaridagi IP manzillar bo‘yicha ulanishlar soni hisoblandi. Natijalarga ko‘ra, 192.168.1.10 IP manzili 7 marta tizimga murojaat qilgani aniqlandi. Berilgan chegaraviy qiymat 4 ga teng bo‘lgani sababli ushbu IP manzil dastur tomonidan shubhali deb belgilandi. Qolgan IP manzillar, ya’ni 192.168.1.15, 192.168.1.20 va 192.168.1.30 manzillari belgilangan me’yordan oshmaganligi sababli normal holat sifatida baholandi. Mazkur natija IDS tizimlarida qo‘llaniladigan anomaliya asosidagi aniqlash usulining sodda modelini ko‘rsatadi. Ya’ni ma’lum chegaradan ortiq faoliyat tizim tomonidan xavfli holat sifatida qabul qilinadi.

Mazkur amaliy mashg‘ulot davomida Python dasturlash tili yordamida IDS tizimining sodda modeli yaratildi. Dastur tarmoq loglaridagi IP manzillarni tahlil qilib, takroriy va ko‘p sonli ulanishlarni aniqlashga xizmat qildi. Natijada ma’lum chegaradan oshgan IP manzillar shubhali faoliyat sifatida belgilandi. Ushbu amaliy mashg‘ulot IDS tizimlarining anomaliya asosidagi ishlash prinsipini sodda va tushunarli ko‘rinishda amaliy jihatdan namoyish etdi.

Xulosa

Xulosa qilib aytganda, IDS (Intrusion Detection System) va IPS (Intrusion Prevention System) tizimlari zamonaviy axborot xavfsizligini ta’minlashda eng muhim himoya vositalaridan biri hisoblanadi. Hozirgi kunda internet tarmoqlari, serverlar, bulutli xizmatlar

va turli raqamli platformalarga bo‘ladigan kiberhujumlar soni tobora ortib borayotganligi sababli ushbu tizimlarning ahamiyati yanada kuchaymoqda. Maqolada ko‘rib chiqilganidek, IDS tizimi asosan tarmoq yoki tizim faoliyatini doimiy kuzatib borish, shubhali holatlarni aniqlash va administratorga ogohlantirish yuborish vazifasini bajaradi. IPS esa bundan tashqari aniqlangan hujumni real vaqt rejimida to‘xtatish, zararli trafikni bloklash va tizimga zarar yetkazilishining oldini olish imkoniyatiga ega. Shu jihatdan IPS tizimlari amaliy himoya nuqtai nazaridan yanada samaraliroq hisoblanadi. Tahlillar shuni ko‘rsatdiki, IDS/IPS tizimlari asosan signatura asosidagi aniqlash, anomaliya asosidagi aniqlash va stateful protocol analysis metodlari asosida ishlaydi. Har bir metodning o‘ziga xos afzallik va kamchiliklari mavjud. Masalan, signatura usuli ma’lum hujumlarni tez va aniq topishda samarali bo‘lsa, yangi turdagi hujumlarni aniqlashda anomaliya va sun’iy intellektga asoslangan usullar muhim ahamiyat kasb etadi. Shu bilan birga maqolada IDS/IPS tizimlarini aldashga qaratilgan zamonaviy usullar — ya’ni packet fragmentation, payload obfuscation, timing attack va protocol ambiguity kabi evasion techniques lar ham ko‘rib chiqildi. Ushbu usullar kiberjinoyatchilar tomonidan xavfsizlik tizimlarini chetlab o‘tishda keng qo‘llanilayotgani sababli himoya tizimlarini muntazam ravishda yangilab borish zarur. Bugungi kunda mashinaviy o‘rganish, sun’iy intellekt, deep packet inspection va traffic normalization kabi zamonaviy yondashuvlar IDS/IPS tizimlarining samaradorligini sezilarli darajada oshirmoqda. Kelajakda ushbu texnologiyalar asosida yanada aqlli va moslashuvchan xavfsizlik tizimlari yaratilishi kutilmoqda. Umuman olganda, IDS/IPS tizimlari axborot xavfsizligini ta’minlashda muhim o‘rin tutadi va ularni chuqur o‘rganish hamda amaliyotga samarali joriy etish bugungi kunning dolzarb masalalaridan biri hisoblanadi.

Foydalanilgan adabiyotlar:

1. Scarfone, K., Mell, P. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94. National Institute of Standards and Technology, 2007.

2. Yeo, L. H., Che, X. Understanding Modern Intrusion Detection Systems: A Survey. arXiv preprint, 2017.

3. Alsubhi, K., Alqahtani, S. Overview on Intrusion Detection Systems for Computers and Networks. Computers, 2025.

4. Gibbs, P. Intrusion Detection Evasion Techniques and Case Studies. GIAC Research Paper, SANS Institute, 2017.

5. Northcutt, S. Network Intrusion Detection: An Analyst’s Handbook. New Riders Publishing, 1999.

6. Bejtlich, R. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. No Starch Press, 2013.

7. Endorf, C., Schultz, E., Mellander, J. Intrusion Detection and Prevention Systems. McGraw-Hill, 2004.

8. Cole, E. Network Security Bible. Wiley Publishing, 2011.

9. NIST. Computer Security Resource Center. Available at: https://csrc.nist.gov

10. OWASP. Open Web Application Security Project. Available at: https://owasp.org

11. SANS Institute. Available at: https://www.sans.org

12. Snort Official Documentation. Available at: https://www.snort.org

13. Suricata Documentation. Available at: https://suricata.io

14. Zeek Documentation. Available at: https://zeek.org