IDS/IPS TIZIMLARINING ISHLASH PRINSIPI VA ULARNI ALDASH USULLARI TAHLILI

Behzod Sobirjonov Qahramonivich
FarDu Axborot texnologiyalari kafedrasi o‘qituvchisi
behzodbekqahramonovich@gmail.com
Mohlaroyim Rahmonaliyeva Baxodir qizi
rahmonaliyevamohlaroy6@gmail.com
FarDu Axborot tizimlari va texnologiyalari yo‘nalishi 2-bosqich talabasi
Telefon raqam: +998 88 627 15 51
https://doi.org/10.5281/zenodo.20025844

ANNOTATSIYA

Ushbu maqolada tarmoq xavfsizligining muhim komponentlari bo‘lgan Bostirilishni aniqlash (IDS) va Bostirilishning oldini olish tizimlari (IPS) tadqiq etiladi. Maqolada ushbu tizimlarning signaturali va anomaliyali tahlil usullari, kiberjinoyatchilar tomonidan qo‘llaniladigan fragmentatsiya, fragmentlarni qayta tartiblash va shifrlangan trafik orqali tizimlarni aldash (evasion) strategiyalari ilmiy jihatdan yoritilgan. Shuningdek, zamonaviy kibertahdidlarga qarshi turish uchun IDS/IPS tizimlarini takomillashtirish bo‘yicha tavsiyalar berilgan.

Kalit so‘zlar: Kiberxavfsizlik, IDS, IPS, Tarmoq trafigi, Signatura, Anomaliya, Evasion, Fragmentatsiya, Ma’lumotlar xavfsizligi.

АННОТАЦИЯ

В данной статье исследуются важные компоненты сетевой безопасности — системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS). В статье научно освещены методы сигнатурного и аномального анализа данных систем, а также стратегии обхода (evasion), такие как фрагментация, изменение порядка фрагментов и использование зашифрованного трафика, применяемые киберпреступниками. Также даны рекомендации по совершенствованию систем IDS/IPS для противодействия современным киберугрозам.

Ключевые слова: Кибербезопасность, IDS, IPS, Сетевой трафик, Сигнатура, Аномалия, Обход (Evasion), Фрагментация, Информационная безопасность.

ANNOTATION

This article examines critical components of network security: Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). The paper scientifically highlights the operational mechanisms of signature-based and anomaly-based analysis, along with evasion strategies such as fragmentation, packet reordering, and encrypted traffic utilized by cybercriminals. Furthermore, it provides recommendations for enhancing IDS/IPS systems to mitigate modern cyber threats.

Keywords: Cybersecurity, IDS, IPS, Network traffic, Signature, Anomaly, Evasion, Fragmentation, Data security.

KIRISH

Bugungi kunda raqamli iqtisodiyot va axborot almashinuvi jadallashgan davrda axborot tizimlarini tashqi kiberhujumlardan himoya qilish strategik ahamiyat kasb etmoqda. Texnik himoya vositalari orasida tarmoq darajasidagi monitoring tizimlari — IDS (Intrusion Detection System) va IPS (Intrusion Prevention System) markaziy o‘rinni egallaydi. Agar IDS faqatgina

shubhali faoliyatni aniqlash va administratorni ogohlantirish bilan shug‘ullansa, IPS hujumni real vaqt rejimida to‘xtatish (bloklash) imkoniyatiga ega. Biroq, kiberjinoyatchilar tomonidan qo‘llanilayotgan "Evasion techniques" (tizimni aldash usullari) ushbu himoya vositalarining samaradorligini pasaytirmoqda. Tizimlarning ishlash prinsipini chuqur o‘rganish va ularning zaif nuqtalarini tahlil qilish xavfsiz tarmoq arxitekturasini yaratishning asosiy shartidir.

IDS VA IPS TIZIMLARINING FUNDAMENTAL TAHLIL USULLARI

IDS/IPS tizimlari asosan ikkita fundamental uslubga tayanadi. Birinchi yondashuv bu signaturali tahlil (Signature-based) bo'lib, u ma'lum bo‘lgan zararli dasturlar va hujumlarning "barmoq izlari" bazasiga asoslanadi. Agar tarmoq trafigidagi paketlar bazadagi namunaga mos kelsa, tizim uni xavf deb belgilaydi. Ikkinchi yondashuv esa anomaliyali tahlil (Anomaly-based) hisoblanib, bunda tizim normal tarmoq faoliyatining "etalon" modelini yaratadi. Ushbu modeldan har qanday keskin chetlanish, masalan, kutilmagan portlararo trafik yoki ma'lumotlar hajmining kutilmaganda oshishi shubhali deb topiladi.

EVASION STRATEGIYALARI VA TARMOQ PROTOKOLLARIDAGI ZAIFLIKLAR

Kiberhujumchilar himoya tizimlarini chetlab o‘tish uchun tarmoq protokollarining xususiyatlaridan ustalik bilan foydalanadilar. IP Fragmentatsiya (IP Fragmentation) usulida hujumchi zararli kodni bir nechta kichik paketlarga bo‘lib yuboradi. IDS tizimi har bir paketni alohida tahlil qilganda hech qanday xavfni ko‘rmasligi mumkin, chunki zararli kod faqat nishon kompyuterda qayta yig‘ilganda ishga tushadi. Agar IDS fragmentlarni qayta yig‘ib tahlil qilish imkoniyatiga ega bo‘lmasa, hujum muvaffaqiyatli o‘tadi.

Paketlarni qayta tartiblash va ustma-ust tushirish (Overlapping Fragments) usulida hujumchi paketlarni ketma-ketlik tartibini buzgan holda yuboradi yoki fragmentlarning bir qismini bir-birining ustiga tushadigan qilib jo‘natadi. Turli operatsion tizimlar, xususan Windows va Linux, bunday paketlarni turlicha qayta ishlaydi. Agar IDS paketi bitta usulda, server esa boshqa usulda yig‘sa, IDS "toza" deb hisoblagan trafik serverda zararli kodga aylanadi. Protokollarni manipulyatsiya qilish orqali hujumchilar standart bo‘lmagan portlar orqali ma'lumot uzatish yoki protokollarning kam ishlatiladigan maydonlaridan foydalanish orqali filtrlarni aylanib o‘tadilar. Masalan, HTTP trafigini boshqa port orqali yuborish signaturali tahlilni chalg‘itishi mumkin.

SHIFRLANGAN TRAFIK VA MONITORING MUAMMOLARI

Hozirgi kunda trafikning katta qismi HTTPS/TLS orqali shifrlangan bo'lib, bu kiberjinoyatchilar uchun "xavfsiz yo‘lak" hisoblanadi. Agar IDS tizimi shifrni ochish (SSL Inspection) imkoniyatiga ega bo‘lmasa, u paket ichidagi zararli kodni ko‘ra olmaydi. Bu muammo ayniqsa zamonaviy shifrlash standartlari (TLS 1.3) keng tarqalishi bilan yanada murakkablashdi, chunki ular monitoring tizimlari uchun ma'lumotlarni tahlil qilish jarayonini qiyinlashtiradi.

TADQIQOT NATIJALARI VA HIMOYANI TAKOMILLASHTIRISH

IDS/IPS tizimlarining samaradorligini oshirish bo‘yicha o‘tkazilgan tahlillar shuni ko‘rsatadiki, faqat signaturaga tayanish bugungi kunda yetarli emas. Fragmentatsiya hujumlariga qarshi "Statefull Inspection" (holatli tekshirish) metodidan foydalanish zarur bo'lsa, obfuskatsiya va shifrlash kabi usullarga qarshi de-obfuskatsiya algoritmlari va SSL/TLS Interception texnologiyalarini qo'llash tavsiya etiladi. DoS hujumlari natijasida resurslarning tugashini oldini olish uchun esa "Rate Limiting" va bulutli himoya texnologiyalari (Cloud-based protection) samarali hisoblanadi.

IDS/IPS tizimlarining barqarorligini ta'minlash uchun sun’iy intellekt va Machine Learning modellaridan foydalanish "nol kungi" hujumlarni aniqlash imkonini beradi. Faqat sarlavhalarni emas, balki paketning butun mazmunini (payload) tekshirish uchun chuqur paket tahlili (DPI - Deep Packet Inspection) metodini joriy etish lozim. Shuningdek, tarmoqda sun'iy zaif nuqtalarni yaratish, ya'ni Honeypots (Tuzoqlar) orqali hujumchining harakatlarini o‘rganish va tizimni oldindan tayyorlash ham muhim strategiya hisoblanadi.

XULOSA

IDS va IPS tizimlari axborot xavfsizligi tizimining ajralmas qismi bo‘lib qolmoqda. Biroq, texnologiyalar rivojlangani sari, ularni aldash usullari ham murakkablashib bormoqda. Tadqiqotlar shuni ko‘rsatadiki, eng samarali himoya — bu ko‘p darajali yondashuvdir. Bunda faqatgina texnik filtrlar bilan cheklanib qolmasdan, balki tarmoq trafigining chuqur intellektual tahlili va administratorlarning doimiy hushyorligi talab etiladi. Raqamli makonda xavfsizlik — bu tugamaydigan jarayon bo‘lib, u doimiy yangilanish va moslashuvchanlikni talab qiladi.

Adabiyotlar, References, Литературы:

1. Scarfone, K., & Mell, P. (2020). Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94.
2. Caswell, B., & Roesch, M. (2019). Snort: The Open Source Network Intrusion Detection System. O'Reilly Media.
3. Zubayev, A. T. (2025). Axborot xavfsizligi: Tarmoq himoyasi va kiberhujumlar tahlili. Toshkent, "Fan va texnologiya".
4. ISO/IEC 27033. Information technology — Security techniques — Network security.
5. SANS Institute. (2024). Evasion Techniques and Mitigating Strategies in Modern Networks. Annual Technical Report.