Latin American Journal of Education
www.lajoe.org

IDS (INTRUSION DETECTION SYSTEM) TIZIMI VA UNING AXBOROT XAVFSIZLIGIDAGI AHAMIYATI

https://doi.org/10.5281/zenodo.19005369

Ramazonova Madina Shavkatovna
Muxammad al – Xorazmiy nomidagi TATU
"Kiberxavfsizlik va kriminalistika" kafedrasi assistenti,
O'razaliyeva Rayxona Qaxramon qizi
Hafizov Shukrullo Fayzullo o'g'li
O'ktamov Doston Rustam o'g'li
Muxammad al – Xorazmiy nomidagi TATU talabalari

Annotatsiya: *Ushbu maqolada zamonaviy axborot tizimlarida keng qo'llanilayotgan IDS (Intrusion Detection System) – ya'ni ruxsatsiz kirishlarni aniqlash tizimining mohiyati, ishlash prinsipi, asosiy turlari hamda axborot xavfsizligini ta'minlashdagi ahamiyati haqida batafsil ma'lumot berilgan. Shuningdek, IDS tizimining afzalliklari, kamchiliklari va uni qo'llash sohalari ham tahlil qilingan.*

Kalit so'zlar: *IDS, kiberxavfsizlik, tarmoq xavfsizligi, hujumlarni aniqlash tizimi, NIDS, HIDS, axborot himoyasi.*

Bugungi kunda axborot texnologiyalarining jadal rivojlanishi natijasida internet va kompyuter tarmoqlari inson hayotining barcha sohalarida keng qo'llanilmoqda. Davlat tashkilotlari, bank tizimlari, ta'lim muassasalari va yirik kompaniyalar o'z faoliyatida turli axborot tizimlaridan foydalanadi. Bu esa axborot xavfsizligini ta'minlash masalasini yanada dolzarb qiladi.

Axborot tizimlariga qaratilgan kiberhujumlar soni yildan-yilga ortib bormoqda. Hujumchilar turli usullar orqali tarmoqqa kirib, maxfiy ma'lumotlarni o'g'irlashi, tizim ishini izdan chiqarishi yoki zararli dasturlarni joylashtirishi mumkin. Shuning uchun axborot tizimlarini himoya qilish uchun turli himoya mexanizmlari ishlab chiqilgan. Shulardan biri IDS tizimidir.

IDS tizimining mohiyati. IDS (Intrusion Detection System) – bu kompyuter tizimi yoki tarmoqda sodir bo'layotgan jarayonlarni kuzatib boradigan va ruxsatsiz kirish yoki zararli faoliyatni aniqlaydigan xavfsizlik tizimidir. IDS tizimi tarmoq orqali uzatilayotgan ma'lumotlarni tahlil qiladi va shubhali harakatlarni aniqlaydi.

Agar tizim shubhali faoliyatni aniqlasa, u tizim administratoriga ogohlantirish yuboradi. Bu esa xavfsizlik mutaxassislariga tezkor choralar ko'rish imkonini beradi.

Latin American Journal of Education
www.lajoe.org

IDS tizimlari ko‘pincha firewall, antivirus va boshqa xavfsizlik vositalari bilan birgalikda ishlaydi. Bu esa tarmoq xavfsizligini kompleks ravishda ta’minlash imkonini beradi.

1.1-rasm. IDS tizimlari.

IDS tizimlarining asosiy turlari. IDS tizimlari bir nechta turlarga bo‘linadi. Eng keng tarqalganlari quyidagilar:

Network IDS (NIDS). Network IDS tarmoq darajasida ishlaydi va tarmoq orqali uzatilayotgan paketlarni tahlil qiladi. U tarmoqning muhim nuqtalariga o‘rnatiladi va butun tarmoq trafikini nazorat qiladi.

Host IDS (HIDS). Host IDS esa alohida kompyuter yoki serverga o‘rnatiladi. U aynan o‘sha tizimdagi fayllar, jarayonlar va foydalanuvchi faoliyatini nazorat qiladi.

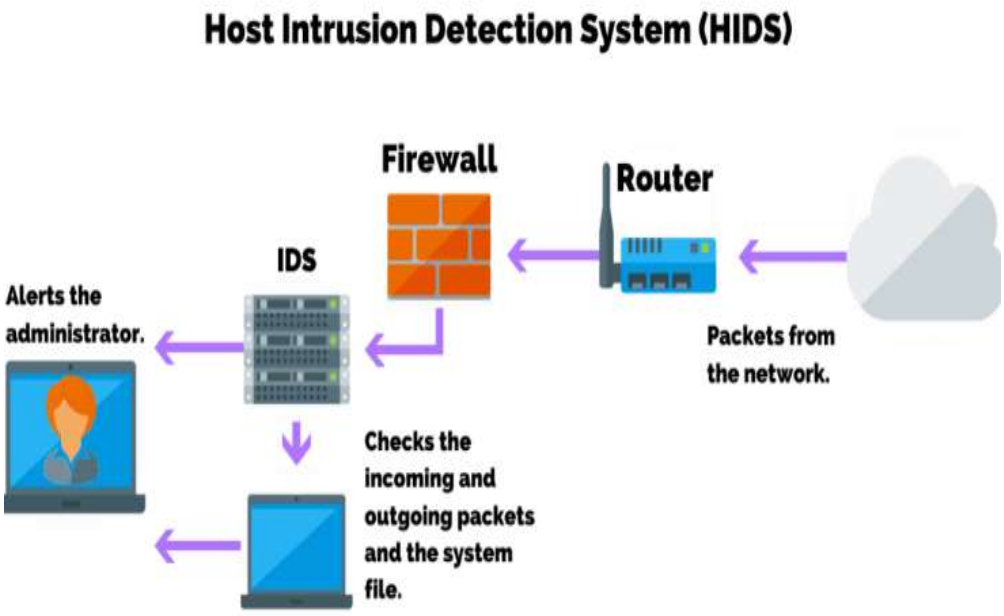
Hybrid IDS. Ba’zi hollarda NIDS va HIDS tizimlari birgalikda ishlatiladi. Bunday tizimlar hybrid IDS deb ataladi va ular tarmoqni yanada samarali himoya qiladi.

IDS tizimining ishlash prinsipi. IDS tizimi asosan ikki xil usul yordamida hujumlarni aniqlaydi.

Signature asosida aniqlash. Bu usul oldindan ma’lum bo‘lgan hujum belgilariga asoslanadi. Agar tizim aniqlagan trafik ma’lum hujum namunalariga mos kelsa, u hujum sifatida qayd etiladi.

Anomaliya asosida aniqlash. Bu usulda tizim tarmoqning odatiy faoliyatini o‘rganadi. Agar odatiy faoliyatdan keskin farq qiladigan holat yuz bersa, tizim uni shubhali deb hisoblaydi.

Latin American Journal of Education
www.lajoe.org



1.2-rasm. *Host IDS (HIDS)*

IDS tizimining afzalliklari

IDS tizimi bir qator afzalliklarga ega:

– tarmoq faoliyatini doimiy monitoring qilish

– ruxsatsiz kirishlarni aniqlash

– kiberhujumlarni erta bosqichda aniqlash

– tizim administratoriga ogohlantirish yuborish

IDS tizimining kamchiliklari

Shu bilan birga IDS tizimining ayrim kamchiliklari ham mavjud:

– noto‘g‘ri ogohlantirishlar bo‘lishi mumkin

– hujumni to‘xtatmaydi, faqat aniqlaydi

– sozlash jarayoni murakkab bo‘lishi mumkin.

XULOSA

Xulosa qilib aytganda, IDS tizimi zamonaviy axborot tizimlarini himoya qilishda muhim rol o‘ynaydi. U tarmoqdagi shubhali faoliyatni aniqlash orqali kiberhujumlarning oldini olishga yordam beradi. IDS tizimi boshqa xavfsizlik vositalari bilan birgalikda ishlatilganda tarmoq xavfsizligi yanada samarali ta’minlanadi.

FOYDALANILGAN ADABIYOTLAR:

1. William Stallings – Network Security Essentials
2. Behrouz A. Forouzan – Data Communications and Networking
3. Eric Cole – Network Security Bible
4. www.cisco.com
5. www.kaspersky.com