IPS (INTRUSION PREVENTION SYSTEM) TIZIMI VA UNING ISHLASH PRINSIPI

Hafizov Shukrullo Fayzullo o‘g‘li
O‘ktamov Doston Rustam o‘g‘li
Quyliyev Behro‘z Sherzod o‘g‘li
O‘razaliyeva Rayxona Qaxramon qizi
Muxammad al – Xorazmiy nomidagi TATU talabalari

Annotatsiya: *Mazkur maqolada IPS (Intrusion Prevention System) tizimining mohiyati, ishlash prinsipi, turlari hamda tarmoq xavfsizligini ta’minlashdagi ahamiyati haqida ma’lumot berilgan. Shuningdek, IPS tizimining IDS tizimidan farqlari ham tahlil qilingan.*

Kalit so‘zlar: *IPS, tarmoq xavfsizligi, kiberhujum, trafik nazorati, xavfsizlik tizimi.*

Axborot texnologiyalari rivojlanishi bilan birga internet orqali amalga oshiriladigan kiberhujumlar ham ortib bormoqda. Tarmoqqa noqonuniy kirish, zararli dasturlarni tarqatish yoki xizmatni rad etish hujumlari ko‘plab tashkilotlarga zarar yetkazmoqda. Shuning uchun tarmoq xavfsizligini ta’minlash uchun turli himoya tizimlari ishlab chiqilgan. Shulardan biri IPS tizimidir.

IPS tizimining mohiyati. IPS (Intrusion Prevention System) – bu tarmoqqa qaratilgan hujumlarni aniqlash bilan birga ularni avtomatik ravishda bloklaydigan xavfsizlik tizimidir. IPS tizimi real vaqt rejimida tarmoq trafikini nazorat qiladi va zararli faoliyatni aniqlaydi.

Agar tizim hujumni aniqlasa, u darhol quyidagi choralarni ko‘radi:

- zararli trafikni bloklash
- IP manzilni bloklash
- sessiyani uzish
- administratorga ogohlantirish yuborish

IPS tizimining ishlash prinsipi. IPS tizimi tarmoq orqali o‘tayotgan barcha ma’lumotlarni tekshiradi. U maxsus algoritmlar yordamida zararli faoliyatni aniqlaydi.

IPS tizimi quyidagi usullar yordamida ishlaydi:

- Signature asosida aniqlash
- Anomaliya asosida aniqlash
- Protokol tahlili

IPS tizimining turlari

IPS tizimlari quyidagi turlarga bo‘linadi:

1. Network-based IPS
2. Host-based IPS

3. Wireless IPS
4. Network Behavior Analysis IPS

IPS tizimining afzalliklari

IPS tizimi quyidagi afzalliklarga ega:

- hujumlarni real vaqt rejimida bloklash
- tarmoq xavfsizligini oshirish
- zararli trafikni filtrlash
- avtomatik himoya mexanizmi

IDS va IPS tizimlari bir-biriga o‘xshash bo‘lsa-da, ularning vazifalari va ishlash prinsiplari bir-biridan farq qiladi.

IDS tizimining vazifasi. IDS tizimining asosiy vazifasi tarmoq yoki tizimda sodir bo‘layotgan faoliyatni kuzatish va shubhali harakatlarni aniqlashdir. IDS tizimi hujumni aniqlagandan so‘ng administratorga ogohlantirish yuboradi.

Biroq IDS tizimi hujumni to‘xtatmaydi, balki faqat uning mavjudligi haqida xabar beradi.

IPS tizimining vazifasi. IPS tizimi esa hujumlarni aniqlash bilan birga ularni avtomatik ravishda bloklaydi. IPS tizimi zararli trafikni to‘xtatish, IP manzillarni bloklash yoki sessiyani uzish kabi choralarni ko‘rishi mumkin. Shuning uchun IPS tizimi IDS tizimiga qaraganda faol himoya mexanizmi hisoblanadi.

IDS va IPS o‘rtasidagi asosiy farqlar. IDS va IPS tizimlari o‘rtasidagi asosiy farqlar quyidagilardan iborat:

- IDS hujumni aniqlaydi, IPS esa hujumni to‘xtatadi.
- IDS administratorni ogohlantiradi, IPS esa avtomatik choralar ko‘radi.
- IDS ko‘pincha monitoring vositasi sifatida ishlatiladi, IPS esa himoya tizimi hisoblanadi.

IDS va IPS tizimlarini birgalikda qo‘llash. Ko‘pgina tashkilotlarda IDS va IPS tizimlari birgalikda qo‘llaniladi. IDS tizimi tarmoqdagi faoliyatni monitoring qiladi va xavf haqida ma’lumot beradi, IPS esa zararli faoliyatni avtomatik ravishda bloklaydi. Bu esa tarmoq xavfsizligini yanada samarali ta’minlash imkonini beradi.

Xulosa

IPS tizimi zamonaviy tarmoqlarni himoya qilishda muhim vositalardan biridir. U hujumlarni aniqlash bilan birga ularni avtomatik ravishda bloklash imkonini beradi. Shu sababli IPS tizimi axborot xavfsizligini ta’minlashda keng qo‘llaniladi.

FOYDALANILGAN ADABIYOTLAR:

1. Eric Cole – Network Security Bible

2. William Stallings – Network Security Essentials
3. www.cisco.com
4. www.ibm.com