

IDS TIZIMLARINING TURLARI VA ULARNING ISHLASH USULLARI

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 IDS tizimlarining asosiy turlari, ishlash prinsipi hamda ularning tarmoq xavfsizligini ta'minlashdagi o'rni haqida ma'lumot berilgan.

Kalit so'zlar: IDS, NIDS, HIDS, kiberxavfsizlik, tarmoq monitoringi.

Axborot xavfsizligini ta'minlashda IDS tizimlari muhim rol o'ynaydi. IDS tizimlari tarmoq yoki kompyuter tizimida sodir bo'layotgan faoliyatni kuzatib boradi va shubhali harakatlarni aniqlaydi. IDS tizimlari turli usullarda ishlashi mumkin.

IDS tizimlarining asosiy turlari

Network IDS (NIDS)

Network IDS tarmoq orqali uzatilayotgan paketlarni tahlil qiladi. U tarmoqning muhim nuqtalariga o'rnatiladi va barcha trafikni kuzatadi.

Host IDS (HIDS)

Host IDS alohida kompyuter yoki serverda ishlaydi. U tizim fayllari, jarayonlar va log fayllarni tekshiradi.

Distributed IDS

Bu tizim bir nechta IDS sensorlaridan iborat bo'lib, ular markaziy boshqaruv tizimiga ma'lumot yuboradi.

IDS tizimining ishlash usullari

IDS tizimi quyidagi usullar yordamida hujumlarni aniqlaydi:

1. Signature-based detection
2. Anomaly-based detection
3. Protocol-based detection

Har bir usulning o'z afzalliklari va kamchiliklari mavjud.

IPS tizimlarining amaliy qo'llanilishi

Bugungi kunda ko'plab tashkilotlar o'z tarmoqlarini himoya qilish uchun IPS tizimlaridan foydalanadi. IPS tizimlari tarmoqqa qaratilgan hujumlarni aniqlash va bloklash imkonini beradi.

IPS tizimining ishlash prinsipi



IPS tizimi tarmoq orqali uzatilayotgan barcha ma'lumotlarni tekshiradi. Agar tizim zararli faoliyatni aniqlasa, u avtomatik ravishda tegishli choralarni ko'radi.

IPS tizimining qo'llanilish sohalari

IPS tizimlari quyidagi sohalarda keng qo'llaniladi:

- bank tizimlari
- davlat tashkilotlari
- internet provayderlari
- korporativ tarmoqlar

IPS tizimining afzalliklari

- real vaqt rejimida himoya
- avtomatik bloklash
- tarmoq xavfsizligini oshirish

Kiberxavfsizlikda IDS va IPS tizimlarining roli

Kiberxavfsizlik bugungi kunda global muammolardan biri hisoblanadi. Internet orqali amalga oshiriladigan turli kiberhujumlar tashkilotlar va davlatlar uchun katta xavf tug'diradi.

Shuning uchun tarmoqlarni himoya qilish uchun IDS va IPS kabi zamonaviy texnologiyalar qo'llaniladi.

IDS va IPS tizimlarining roli

IDS tizimi tarmoqdagi shubhali faoliyatni aniqlaydi va administratorga ogohlantirish yuboradi. IPS tizimi esa hujumni aniqlash bilan birga uni bloklaydi.

Bu tizimlar birgalikda ishlatilganda tarmoq xavfsizligi sezilarli darajada oshadi.

Zamonaviy tarmoqlarda qo'llanilishi

Bugungi kunda IDS va IPS tizimlari:

- korporativ tarmoqlarda
- davlat tashkilotlarida
- bank tizimlarida
- internet provayderlarda keng qo'llanilmoqda.

Xulosa

IDS tizimlari tarmoq xavfsizligini ta'minlashda muhim vosita hisoblanadi.

Ular tarmoqdagi shubhali faoliyatni aniqlash orqali kiberhujumlarning oldini olishga yordam beradi.

IDS va IPS tizimlari kiberxavfsizlikni ta'minlashda muhim vositalardan biridir.

Ular tarmoqdagi hujumlarni aniqlash va oldini olish orqali axborot tizimlarini himoya qilishga yordam beradi.





FOYDALANILGAN ADABIYOTLAR:

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

