LINUX OPERATSION TIZIMIDA TARMOQ XAVFSIZLIGI VA KIBERHIMOYA TEXNOLOGIYALARI

Muallif: ***Muhammadyusuf Usmonov***
Matkarimov Abbosbek
Fan: Linux server boshqaruvi

Annotatsiya

Ushbu ilmiy maqolada Linux operatsion tizimida tarmoq xavfsizligini ta’minlash, serverlarni kiberhujumlardan himoyalash hamda zamonaviy himoya texnologiyalaridan foydalanish usullari tahlil qilingan. Linux tizimlarida firewall, SSH xavfsizligi, IDS/IPS tizimlari, log monitoring, paket filtrlash va avtomatlashtirilgan himoya usullarining ahamiyati yoritilgan. Shuningdek, Kali Linux, Fail2Ban, IPTables va Wireshark kabi vositalarning amaliy imkoniyatlari ko‘rib chiqilgan.

Kalit so‘zlar: Linux, kiberxavfsizlik, firewall, SSH, Fail2Ban, IPTables, Wireshark, IDS, IPS, server xavfsizligi.

Kirish

Raqamli texnologiyalar rivojlanishi bilan server va tarmoq tizimlariga bo‘lgan tahdidlar soni ortib bormoqda. Xakerlik hujumlari, zararli dasturlar, DDoS hujumlari va noqonuniy kirish holatlari axborot xavfsizligiga jiddiy xavf tug‘diradi. Shu sababli zamonaviy server tizimlarida kuchli himoya mexanizmlaridan foydalanish muhim vazifalardan biri hisoblanadi.

Linux operatsion tizimi yuqori xavfsizlik darajasi va moslashuvchanligi sababli server boshqaruvi hamda kiberxavfsizlik sohasida keng qo‘llaniladi. Linux asosidagi tizimlar ko‘plab davlat tashkilotlari, banklar va yirik kompaniyalarning server infratuzilmasida ishlatiladi.

Linux tizimlarida xavfsizlikni ta’minlash uchun firewall, foydalanuvchi nazorati, tarmoq monitoringi va avtomatlashtirilgan himoya tizimlari qo‘llaniladi.

Linux tizimida tarmoq xavfsizligi tushunchasi

Tarmoq xavfsizligi — server va tarmoq qurilmalarini noqonuniy kirish, zararli trafik va kiberhujumlardan himoyalash jarayonidir.

Linux tizimlarida xavfsizlikning asosiy maqsadlari:

- Ma’lumotlarni himoyalash
- Tizim yaxlitligini saqlash
- Foydalanuvchilarni autentifikatsiya qilish
- Tarmoq trafikini nazorat qilish
- Hujumlarni aniqlash va bloklash

Linux operatsion tizimi ochiq kodli bo‘lgani sababli xavfsizlik mexanizmlarini chuqur nazorat qilish imkoniyatini beradi.

Firewall texnologiyalari

Firewall serverga kelayotgan va chiqayotgan trafikni nazorat qiladi.

Linux tizimida IPTables va UFW eng mashhur firewall tizimlari hisoblanadi.

IPTables bilan ishlash

Barcha trafikni ko‘rish:

sudo iptables -L

SSH portiga ruxsat berish:

sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT

Keraksiz trafikni bloklash:

sudo iptables -A INPUT -j DROP

IPTables serverni zararli trafiklardan himoyalaydi.

UFW xavfsizlik tizimi

UFW — Ubuntu tizimlaridagi soddalashtirilgan firewall tizimi hisoblanadi.

Firewallni yoqish:

sudo ufw enable

HTTP xizmatiga ruxsat berish:

sudo ufw allow 80/tcp

Firewall holatini tekshirish:

sudo ufw status

SSH xavfsizligini kuchaytirish

SSH protokoli serverga masofadan ulanish imkonini beradi. SSH noto‘g‘ri sozlansa, server xavf ostida qolishi mumkin.

SSH konfiguratsiyasi:

sudo nano /etc/ssh/sshd_config

Root foydalanuvchini bloklash:

PermitRootLogin no

SSH portini o‘zgartirish:

Port 2222

SSH xizmatini qayta ishga tushirish:

sudo systemctl restart ssh

Bu usullar brute-force hujumlarni kamaytiradi.

Fail2Ban yordamida himoya

Fail2Ban tizimi serverga ko‘p marotaba noto‘g‘ri kirishga uringan IP manzillarni avtomatik bloklaydi.

O‘rnatish:

sudo apt install fail2ban

Xizmatni ishga tushirish:

sudo systemctl start fail2ban

Holatini tekshirish:

sudo fail2ban-client status

Fail2Ban SSH hujumlaridan himoyalanishda samarali vosita hisoblanadi.

Wireshark yordamida tarmoq monitoringi

Wireshark tarmoq paketlarini tahlil qiluvchi kuchli dastur hisoblanadi.

O‘rnatish:

sudo apt install wireshark

Trafikni kuzatish:

sudo wireshark

Wireshark yordamida:

- Paketlarni tahlil qilish
- Hujumlarni aniqlash
- Tarmoq muammolarini topish
- Trafik monitoringi amalga oshiriladi

IDS va IPS tizimlari

IDS (Intrusion Detection System) — hujumlarni aniqlaydi. IPS (Intrusion Prevention System) — hujumlarni bloklaydi.

Linux tizimlarida Snort eng mashhur IDS/IPS tizimlaridan biri hisoblanadi.

Snort o‘rnatish:

sudo apt install snort

Trafik monitoringi:

sudo snort -A console -i eth0 -c /etc/snort/snort.conf

Snort zararli trafiklarni aniqlash imkonini beradi.

Log fayllarni monitoring qilish

Linux tizimlarida barcha hodisalar log fayllarga yoziladi.

Muhim log kataloglari:

/var/log/auth.log

/var/log/syslog

Loglarni real vaqtda kuzatish:

sudo tail -f /var/log/auth.log

Bu usul tizimdagi xavfsizlik hodisalarini tezkor aniqlash imkonini beradi.

Kali Linux va penetration testing

Kali Linux kiberxavfsizlik va penetration testing uchun mo‘ljallangan Linux distributivi hisoblanadi.

Kali Linuxdagi mashhur vositalar:

- Nmap
- Metasploit
- Aircrack-ng

- Burp Suite
- Hydra

Portlarni skanerlash:

nmap 192.168.1.1

Zaifliklarni aniqlash:

sudo nikto -h target.com

Bu vositalar tizim xavfsizligini tekshirishda qo‘llaniladi.

Avtomatlashtirilgan xavfsizlik tizimlari

Linux serverlarda Bash script va Cron yordamida xavfsizlikni avtomatlashtirish mumkin.

Oddiy monitoring scripti:

```
#!/bin/bash
echo "Server holati:"
uptime
df -h
free -m
```

Cron orqali ishga tushirish:

```
crontab -e
0 * * * * /home/security.sh
```

Bu script har soatda avtomatik ishlaydi.

Linux xavfsizlik tizimlarining zamonaviy ahamiyati

Bugungi kunda Linux xavfsizlik texnologiyalari quyidagi sohalarda keng qo‘llaniladi:

- Davlat serverlari
- Bank tizimlari
- Bulutli texnologiyalar
- Sun’iy intellekt serverlari
- Telekommunikatsiya tizimlari
- Data center infratuzilmalari

Linux tizimlari yuqori xavfsizlik va barqarorlik sababli global miqyosda keng foydalaniladi.

Xulosa

Linux operatsion tizimi tarmoq xavfsizligini ta’minlashda eng samarali platformalardan biri hisoblanadi. IPTables, SSH, Fail2Ban, Wireshark va Snort kabi texnologiyalar serverlarni kiberhujumlardan himoyalash imkonini beradi.

Tizim monitoringi, avtomatlashtirish va trafik nazorati server xavfsizligini sezilarli darajada oshiradi. Kelajakda kiberxavfsizlik texnologiyalari rivojlanishi bilan Linux tizimlarining ahamiyati yanada ortadi.

Foydalanilgan adabiyotlar

1. William Stallings — Network Security Essentials.
2. Christopher Negus — Linux Bible.
3. Kali Linux Documentation — kali.org
4. Ubuntu Security Documentation.
5. Snort Official Documentation.
6. Wireshark User Guide.
7. Nemeth E. — Linux Administration Handbook.
8. Red Hat Security Guide.