Tarmoq Vositalari: Iftop, ARP-scan, Nmap, va Wireshark

Tarmoq vositalari yordamida tarmoqqa ulangan qurilmalarning faolligi va trafikni tahlil qilish muhimdir. Quyida iftop, arp-scan, nmap, va Wireshark vositalari va ularning qanday ishlashi haqida batafsil ma'lumot keltirilgan.

1. Iftop va Uning Ishlashi:

Iftop - bu real vaqtda tarmoq orqali o'tayotgan trafikni kuzatib borish vositasi. Iftop TCP/IP ulanishlari orqali qaysi qurilma qancha trafikni yuborayotganini yoki olayotganini ko'rsatadi.

- Iftop o'rnatish (Linux/Debian):

  sudo apt install iftop

- Iftop ishlashi:

  1. Terminalda iftop buyruqini kiritib ishga tushiring:

     sudo iftop

  2. Bu sizga real vaqt rejimida qaysi IP manzillar ko'p trafik tortayotganini ko'rsatadi.
  3. Foydali parametrlar:
     - -i [interface]: maxsus tarmoq interfeysini ko'rsatish uchun, masalan, eth0 yoki wlan0.
     - -B: baytlar o'rniga bitlarda ko'rsatish.

- Iftop orqali kuzatiladigan narsalar:

  - Real vaqt rejimida uzatilayotgan va qabul qilinayotgan trafik miqdori.
  - Qurilmalarning IP manzillari va ularning tarmoqqa bo'lgan yuklamalari.

2. ARP-scan va Uning Ishlashi:

ARP-scan - bu ARP protokolidan foydalanib, lokal tarmoqda barcha ulangan qurilmalarni aniqlash uchun ishlatiladigan vosita.

- ARP-scan o'rnatish (Linux/Debian):

```
sudo apt install arp-scan
```

- ARP-scan yordamida tarmoqni skan qilish:

```
sudo arp-scan --interface=eth0 --localnet
```

Bu buyruq lokal tarmoqdagi barcha qurilmalarni IP va MAC manzillari bilan ko'rsatadi.

- ARP-scan qanday ishlaydi:

ARP-scan barcha lokal tarmoqdagi IP manzillarni olish uchun ARP so'rovlar yuboradi va tarmoqda javob berayotgan har bir qurilmani qaytaradi. Bu orqali siz tarmoqdagi barcha faol qurilmalarni aniqlashingiz mumkin.

3. Nmap va Uning Ishlashi:

Nmap - tarmoq skaneri bo'lib, u portlar va tarmoq xizmatlarini tahlil qilish uchun ishlatiladi. U ma'lum bir tarmoqdagi faol qurilmalarni, ularning xizmatlarini va xavfsizlik zaifliklarini aniqlashga yordam beradi.

- Nmap o'rnatish (Linux/Debian):

```
sudo apt install nmap
```

- Nmap yordamida tarmoqni skan qilish:

sudo nmap -sP 192.168.1.0/24

Bu buyruq sizning mahalliy subnetingizdagi barcha faol IP manzillarni ko'rsatadi.

- Nmap asosiy parametrlar:

- -sP: Ping skan qilish (faqat faol qurilmalarni ko'rsatadi).
- -sS: TCP SYN skani (yarim ochiq ulanishlarni ko'rish uchun ishlatiladi).
- -O: Operatsion tizimni aniqlash.
- -p [port raqami]: Muayyan portlarni tekshirish.

- Nmap qanday ishlaydi:

Nmap portlarni skan qilish orqali faol xizmatlar va ulanishlarni aniqlaydi, bu esa tarmoq xavfsizligini yaxshiroq tushunishga yordam beradi.

4. Wireshark va Uning Ishlashi:

Wireshark - bu eng kuchli va mashhur tarmoq paketlarini tahlil qilish vositasi. U tarmoqda o'tayotgan barcha paketlarni to'playdi va ularni batafsil tahlil qiladi.

- Wireshark o'rnatish (Linux/Debian):

sudo apt install wireshark

- Wireshark yordamida tarmoqni kuzatish:

1. Wiresharkni ishga tushiring va interfeysni tanlang.
2. Start tugmasini bosing va barcha paketlarni kuzatib boring.
3. Filtrlar orqali maxsus trafikni ko'rishingiz mumkin (masalan, ip.addr == 192.168.1.1 faqat shu IP

manzil uchun trafikni ko'rsatadi).

- Wiresharkning asosiy xususiyatlari:
  - TCP, UDP, ICMP kabi barcha tarmoq protokollari orqali o'tayotgan trafikni to'plash.
  - Paketlarni tahlil qilish va ular haqidagi chuqur ma'lumotlarni ko'rsatish.
  - Tarmoqdagi hujumlarni aniqlash va xavfsizlik tekshiruvlari o'tkazish.

- Wireshark qanday ishlaydi:

Wireshark tarmoqdan o'tayotgan paketlarni to'playdi va ularni chuqur tahlil qiladi, bu orqali tarmoqdagi har qanday harakatlarni aniqlash mumkin. Bu vosita hujumlar, protokol zaifliklari va trafik anomaliyalarini topishda yordam beradi.

Ushbu vositalar yordamida siz tarmoqda nima sodir bo'layotganini kuzatib borishingiz va tarmoq xavfsizligini ta'minlash uchun kerakli chora-tadbirlarni amalga oshirishingiz mumkin.