**Lokal tarmoqni monitoring va tahlil qilish**

Lokal tarmoqni monitoring va tahlil qilish quyidagi bosqichlarga bo‘linadi:

**1. Asosiy talablarni aniqlash**

Tarmoq monitoringini boshlashdan oldin quyidagilarni belgilash kerak:

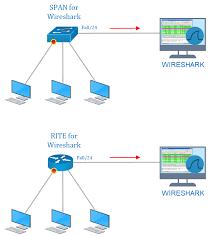
* **Maqsad**: Nima uchun monitoring qilinadi? (Masalan, xavfsizlik, band kengligi nazorati, muammolarni aniqlash).
* **Qo‘llaniladigan vositalar**: Monitoring uchun qanday dasturiy ta’minot yoki uskunalar ishlatiladi?
* **Tarmoq sxemasi**: Lokal tarmoqning topologiyasini aniq belgilash.

**2. Monitoring vositalarini o‘rnatish**

Monitoring va tahlil uchun kerakli vositalarni tanlang va sozlang:

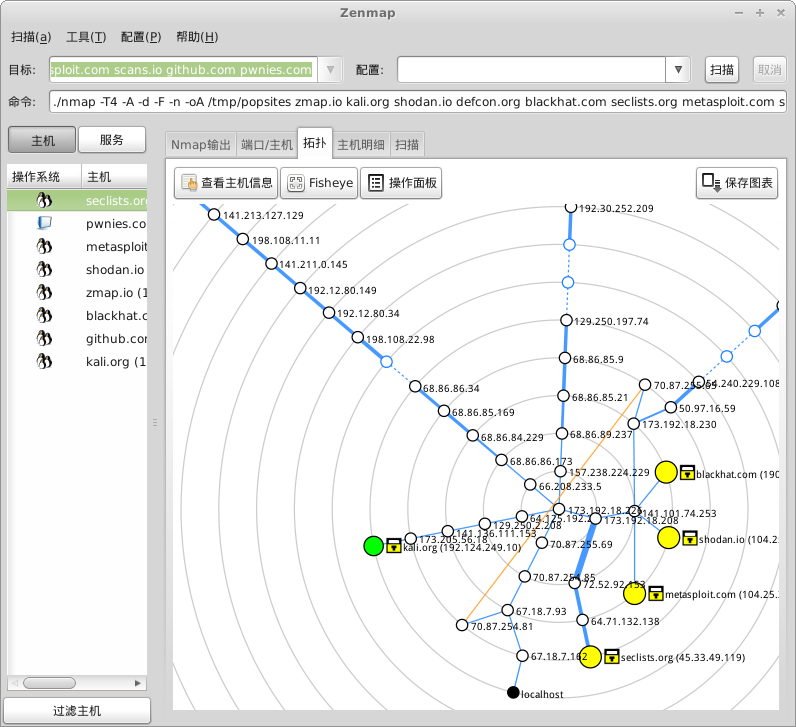
**2.1. Monitoring dasturlarini o‘rnatish**

* **Wireshark**: Trafikni tahlil qilish uchun ishlatiladi.
  + [Wireshark yuklab olish](https://www.wireshark.org/).
  + O‘rnatilgach, monitoring boshlash uchun tarmoq interfeysini tanlang va trafikni yozishni yoqing.
* **Nagios** yoki **Zabbix**: Tarmoq va qurilmalarni monitoring qilish uchun.
  + Bu dasturlar serverga o‘rnatiladi va barcha lokal qurilmalar ularga bog‘lanadi.



**2.2. Qo‘shimcha uskunalar**

* **Tarmoq skaneri**: Nmap kabi vositalar bilan barcha faol portlarni aniqlash.
* **SNMP**: Tarmoq qurilmalari ma’lumotlarini real vaqt rejimida olish uchun.

****

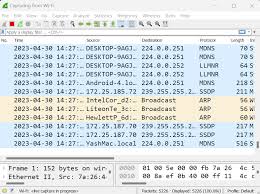
**3. Tarmoqdagi trafikni yozib olish**

**Wireshark yordamida:**

1. Dastur ishga tushiring va kerakli interfeysni tanlang.
2. "Start Capturing" tugmasini bosing.
3. Foydali trafikni filtrlang. Masalan:
   * tcp.port == 80 — HTTP trafikni kuzatish.
   * ip.addr == 192.168.1.1 — Faqat bitta IP adres uchun.

**4. Trafikni tahlil qilish**

1. Yig‘ilgan paketlar bo‘yicha statistikani ko‘ring.
2. Quyidagi narsalarni tahlil qiling:
   * Paketning manba va qabul qiluvchi IP adreslari.
   * Paket hajmi va uzatilish tezligi.
   * Tarmoqdagi odatiy va nojo‘ya trafik.



**5. Xavfsizlikni baholash**

* **Nmap** orqali lokal tarmoqni skanerlash:
* nmap -sS 192.168.1.0/24

Ushbu buyruq barcha ochiq portlarni aniqlashga yordam beradi.

* **IDS/IPS tizimlari** yordamida xakerlik hujumlarini aniqlash. Masalan: **Suricata** yoki **Snort**.

**6. Hisobot tayyorlash**

Monitoring natijalariga asoslanib, tarmoq samaradorligi va xavfsizligi bo‘yicha hisobot tayyorlang:

* Muammo bo‘lsa, ularni tuzatish bo‘yicha tavsiyalar bering.
* Tarmoqdagi har bir qurilma va trafikni tahlil qilish bo‘yicha statistika qo‘shing.

**Qo‘shimcha maslahatlar**

* **Avtomatlashtirish**: Trafik kuzatuvini avtomatlashtirish uchun Python’da **Scapy**, **Pyshark** kabi kutubxonalardan foydalaning.
* **Ma’lumotlarni vizualizatsiya qilish**: Grafana yoki Kibana orqali statistik ma’lumotlarni vizual qiling.



**Mavuz doirasidan savollar**

Quyidagi savollar **Lokal tarmoqni monitoring va tahlil qilish** bo‘yicha ko‘rsatma mazmunini mustahkamlash uchun tuzilgan:

**1. Tarmoq monitoringini boshlashdan oldin qaysi uchta asosiy talabni aniqlash kerak?**

* A) Tarmoq sxemasi, foydalanuvchilar soni, xizmatlar talabi
* B) Maqsad, qo‘llaniladigan vositalar, tarmoq sxemasi
* C) Tizimning IP-manzili, xavfsizlik darajasi, qurilmalar soni
* D) Qo‘llaniladigan vositalar, band kengligi, dastur versiyasi

**2. Wireshark’da faqat bitta IP manzil uchun trafikni kuzatish uchun qanday filtr ishlatiladi?**

* A) tcp.port == 443
* B) ip.addr == 192.168.1.1
* C) udp.port == 53
* D) ip.src == 192.168.1.1

**3. Nmap yordamida lokal tarmoqdagi barcha faol qurilmalarni aniqlash uchun qaysi buyruq ishlatiladi?**

* A) nmap -sn 192.168.1.0/24
* B) nmap -sS 192.168.1.0/24
* C) nmap --osscan 192.168.1.1
* D) nmap -O 192.168.1.1

**4. Tarmoq xavfsizligini baholashda IDS/IPS tizimlaridan foydalanish qaysi maqsadga xizmat qiladi?**

* A) Band kengligini boshqarish
* B) Tarmoqdagi nojo‘ya trafikni aniqlash va himoya qilish
* C) Ochiq portlarni yopish
* D) Paketlar hajmini tahlil qilish

**5. Lokal tarmoq monitoringi natijalari asosida tayyorlanadigan hisobotda nimalarni o‘z ichiga olishi kerak?**

* A) Yangi qurilmalar sonini va trafik hajmini
* B) Muammolar va ularni bartaraf etish bo‘yicha tavsiyalar
* C) Qo‘llaniladigan dasturlar va ularning versiyalarini
* D) Tarmoq sxemasining grafik ko‘rinishini