

## Модуль 2. Построение системы защиты сети

### 1. Проведите сканирование домашней сети.

Сканируем локальную сеть 192.168.1.0 с помощью ping scan

```
nmap -sn 192.168.1.0/24
```

```
PS C:\Users\lmz> nmap -sn 192.168.1.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2025-10-04 10:59 RTZ 3 (чшър)
Nmap scan report for 192.168.1.1
Host is up (0.0040s latency).
MAC Address: 50:FF:20:D4:DE:47 (Keenetic Limited)
Nmap scan report for 192.168.1.37
Host is up (0.0090s latency).
MAC Address: 84:25:19:34:30:6C (Samsung Electronics)
Nmap scan report for 192.168.1.43
Host is up (0.0060s latency).
MAC Address: CC:4B:73:EF:E4:6A (Ampak Technology)
Nmap scan report for 192.168.1.61
Host is up (0.054s latency).
MAC Address: BE:94:CC:81:0A:D4 (Unknown)
Nmap scan report for 192.168.1.71
Host is up (0.099s latency).
MAC Address: F4:FE:FB:32:25:E6 (Samsung Electronics)
Nmap scan report for 192.168.1.100
Host is up (0.067s latency).
MAC Address: AE:F0:09:7E:10:4B (Unknown)
Nmap scan report for 192.168.1.104
Host is up (0.013s latency).
MAC Address: F0:B0:40:59:A2:17 (Hunan FN-Link Technology Limited)
Nmap scan report for 192.168.1.44
Host is up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 17.21 seconds
```

### 2. Обнаружьте все хосты, входящие в сеть.

Хосты входящие в сеть:

- 192.168.1.1 (Keenetic Limited)
- 192.168.1.37 (Samsung Electronics)
- 192.168.1.43 (Ampak Technology)
- 192.168.1.61 (Unknown)
- 192.168.1.71 (Samsung Electronics)
- 192.168.1.100 (Unknown)
- 192.168.1.104 (Hunan FN-Link Technology Limited)
- 192.168.1.44 (Unknown)

Если сопоставлять с данными о клиентах сети из интерфейса роутера, то nmap показал все.

### 3. Определите операционную систему всех устройств.

Определим ОС всех доступных хостов с помощью команды

```
nmap -O --osscan-guess -v 192.168.1.0/24
```

```
PS C:\Users\lmnz\ nmap -O --osscan-guess -v 192.168.1.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2025-10-04 12:00 RTZ 3 (чшрь)
Initiating ARP Ping Scan at 12:00
Scanning 254 hosts [1 port/host]
Completed ARP Ping Scan at 12:00, 1.93s elapsed (254 total hosts)
Initiating Parallel DNS resolution of 7 hosts, at 12:00
Completed Parallel DNS resolution of 7 hosts, at 12:00, 6.54s elapsed
Nmap scan report for 192.168.1.0 [host down]
Nmap scan report for 192.168.1.2 [host down]
Nmap scan report for 192.168.1.3 [host down]
Nmap scan report for 192.168.1.4 [host down]
Nmap scan report for 192.168.1.5 [host down]
Nmap scan report for 192.168.1.6 [host down]
Nmap scan report for 192.168.1.7 [host down]
Nmap scan report for 192.168.1.8 [host down]
Nmap scan report for 192.168.1.9 [host down]
Nmap scan report for 192.168.1.10 [host down]
Nmap scan report for 192.168.1.11 [host down]
Nmap scan report for 192.168.1.12 [host down]
Nmap scan report for 192.168.1.13 [host down]
Nmap scan report for 192.168.1.14 [host down]
Nmap scan report for 192.168.1.15 [host down]
Nmap scan report for 192.168.1.16 [host down]
Nmap scan report for 192.168.1.17 [host down]
Nmap scan report for 192.168.1.18 [host down]
Nmap scan report for 192.168.1.19 [host down]
Nmap scan report for 192.168.1.20 [host down]
Nmap scan report for 192.168.1.21 [host down]
Nmap scan report for 192.168.1.22 [host down]
Nmap scan report for 192.168.1.23 [host down]
Nmap scan report for 192.168.1.24 [host down]
Nmap scan report for 192.168.1.25 [host down]
Nmap scan report for 192.168.1.26 [host down]
Nmap scan report for 192.168.1.27 [host down]
Nmap scan report for 192.168.1.28 [host down]
Nmap scan report for 192.168.1.29 [host down]
Nmap scan report for 192.168.1.30 [host down]
Nmap scan report for 192.168.1.31 [host down]
Nmap scan report for 192.168.1.32 [host down]
Nmap scan report for 192.168.1.33 [host down]
Nmap scan report for 192.168.1.34 [host down]
Nmap scan report for 192.168.1.35 [host down]
Nmap scan report for 192.168.1.36 [host down]
Nmap scan report for 192.168.1.37 [host down]
Nmap scan report for 192.168.1.38 [host down]
Nmap scan report for 192.168.1.39 [host down]
Nmap scan report for 192.168.1.40 [host down]
Nmap scan report for 192.168.1.41 [host down]
Nmap scan report for 192.168.1.42 [host down]
Nmap scan report for 192.168.1.43 [host down]
Nmap scan report for 192.168.1.44 [host down]
Nmap scan report for 192.168.1.45 [host down]
Nmap scan report for 192.168.1.46 [host down]
```

| IP адрес      | Семейство ОС      | ОС (по версии Nmap)                            |
|---------------|-------------------|--|
| 192.168.1.1   | Linux (Embedded)  | Linux 3.x–4.x (встроенная ОС роутера)          |
| 192.168.1.37  | HP Embedded       | HP embedded OS (LaserJet M451dn, CM1415fnw...) |
| 192.168.1.43  | Embedded / Citrix | Citrix / Juniper embedded                      |
| 192.168.1.44  | Windows           | Windows 10 / 11 / Server 2022 (99%)            |
| 192.168.1.61  | Apple (macOS/iOS) | macOS 10.13–11 или iOS 12–13 (Darwin 19–20)    |
| 192.168.1.71  | Android / Tizen   | Не определено (возможно Android / Tizen)       |
| 192.168.1.100 | Apple (macOS/iOS) | macOS 10.13–11 / iOS 12–13                     |
| 192.168.1.104 | Linux (Embedded)  | Linksys WRT610Nv3 / Citrix Access Gateway      |

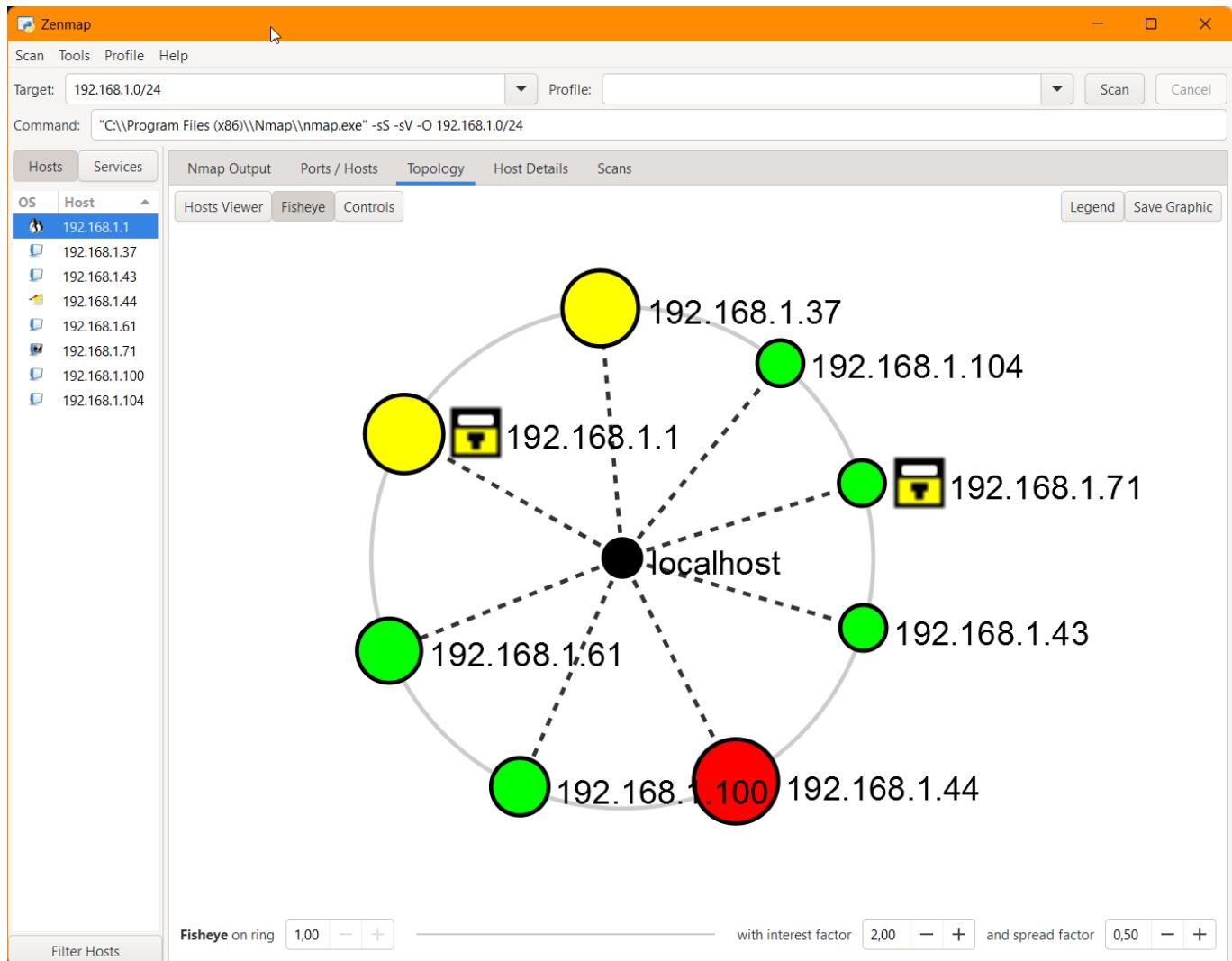
### 4. Постройте топологию сети.

Топология сети была построена командой:

```
nmap -sS -sV -O -oX topology_report.xml 192.168.1.0/24
```

с последующим сохранением отчета в файл **topology\_report.xml**

Результат отображения топологии с помощью программы **Zenmap**



## 5. Обнаружьте открытые порты.

На основе отчета, сгенерированного в предыдущем пункте можно составить таблицу доступности портов:

| IP адрес     | Семейство ОС         | ОС (по версии Nmap)                               | Примечания / открытые порты  |
|--------------|----------------------|---|--|
| 192.168.1.1  | Linux<br>(Embedded)  | Linux 3.x–4.x (встроенная<br>ОС роутера)          | 23/telnet, 53/dns, 80/http, 443/https,<br>1900/upnp, 3517, 22 filtered |
| 192.168.1.37 | HP<br>Embedded       | HP embedded OS (LaserJet<br>M451dn, CM1415fnw...) | 80/http, 515/printer, 631/ipp,<br>9100/jetdirect, 5200/targus-getdata  |
| 192.168.1.43 | Embedded /<br>Citrix | Citrix / Juniper embedded                         | Все порты закрыты (возможно VPN<br>шлюз или firewall)                  |

| <b>IP адрес</b> | <b>Семейство ОС</b> | <b>ОС (по версии Nmap)</b>                  | <b>Примечания / открытые порты</b>   |
|-----------------|---------------------|---|--|
| 192.168.1.44    | Windows             | Windows 10 / 11 / Server 2022 (99%)         | 135/msrpc, 139/netbios, 445/smb, 443/https, 3306/mysql, 2222, 902, 912, 5357 |
| 192.168.1.61    | Apple (macOS/iOS)   | macOS 10.13–11 или iOS 12–13 (Darwin 19–20) | 49152, 62078 (iTunes/iPhone sync)  |
| 192.168.1.71    | Android / Tizen     | Не определено<br>(возможно Android / Tizen) | Все порты фильтруются  |
| 192.168.1.100   | Apple (macOS/iOS)   | macOS 10.13–11 / iOS 12–13                  | 22/ssh открыт  |
| 192.168.1.104   | Linux (Embedded)    | Linksys WRT610Nv3 / Citrix Access Gateway   | Все порты закрыты  |