Министерство образования Республики Беларусь

Учреждение образования

«Брестский Государственный технический университет»

Кафедра ИИТ

**Лабораторная работа №8**

По дисциплине «Аппаратное и программное обеспечение сетей»

Тема: «Утилита для сканирования и исследования безопасности сети NMAP»

**Выполнил:**

Студент 3 курса

Группы ИИ-21

Карагодин Д.Л.

**Проверил:**

Степанчук В.И.

Брест 2023

**Цель работы:** изучение и практическое применение утилиты для сканирования и исследования безопасности сети nmap.

**Ход работы:**

1. Получите список открытых портов (TCP и UDP) машины, за которой выполняется лабораторная работа (localhost). Воспользуйтесь несколькими методами сканирования. Сравните результаты.

2. Определите операционную систему этой же машины.

3. Узнайте адреса активных хостов в сети лаборатории (без сканирования портов).

4. Просканируйте хост №1, разными методами. Сравните результаты.

5. Для четырех хостов (№2-5), выполните следующие действия:

1. Определите, защищен ли хост межсетевым экраном.

2. Определите поддерживаемые протоколы.

3. Выберите оптимальный метод сканирования портов, чтобы избежать обнаружения. Определите открытые и фильтрованные порты и по возможности версии служб. При необходимости используйте RPC-сканирование.

4. Определите операционную систему.

**1.**

C:\Users\Danik>nmap -sT localhost Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 19:31 ┴хырЁєё№ (чшьр) Nmap scan report for localhost (127.0.0.1) Host is up (0.00062s latency). Other addresses for localhost (not scanned): ::1 Not shown: 991 filtered tcp ports (no-response) PORT STATE SERVICE 135/tcp open msrpc 445/tcp open microsoft-ds 902/tcp open iss-realsecure 912/tcp open apex-mesh 2869/tcp open icslap 7070/tcp open realserver 9010/tcp open sdr 9080/tcp open glrpc 9100/tcp open jetdirect

C:\Users\Danik>nmap -sU localhost Nmap scan report for localhost (127.0.0.1) Host is up (0.000072s latency). Other addresses for localhost (not scanned): ::1 Not shown: 992 closed udp ports (port-unreach) PORT STATE SERVICE 123/udp open|filtered ntp 137/udp open|filtered netbios-ns 500/udp open|filtered isakmp 1900/udp open|filtered upnp 4500/udp open|filtered nat-t-ike 5050/udp open|filtered mmcc 5353/udp open|filtered zeroconf 5355/udp open|filtered llmnr

**2.**

C:\Users\Danik>nmap -O localhost Device type: general purpose Running: Microsoft Windows 10 OS CPE: cpe:/o:microsoft:windows\_10:1607 OS details: Microsoft Windows 10 1607 Network Distance: 0 hops

**3.**

C:\Users\Danik>nmap -sn 192.168.\*.\* Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 19:44 ┴хырЁєё№ (чшьр) Nmap scan report for dlinkrouter.local (192.168.0.1) Host is up (0.00013s latency). MAC Address: F0:B4:D2:30:15:A8 (D-Link International) Nmap scan report for 192.168.0.120 Host is up (0.00s latency). MAC Address: E4:27:71:54:2D:77 (Smartlabs) Nmap scan report for 192.168.0.123 Host is up (0.079s latency). MAC Address: 40:2F:86:F8:A6:94 (LG Innotek) Nmap scan report for Samsung (192.168.0.125) Host is up (0.00s latency). MAC Address: 00:C3:F4:93:84:1B (Samsung Electronics) Nmap scan report for HOME-PC (192.168.0.175) Host is up. Nmap scan report for 192.168.1.1 Host is up (0.016s latency). Nmap scan report for 192.168.11.0 Host is up (0.0059s latency). Nmap scan report for 192.168.11.151 Host is up (0.0073s latency). Nmap scan report for 192.168.11.152 Host is up (0.0087s latency). Nmap scan report for 192.168.11.255 Host is up (0.0050s latency).

**4.**

C:\Users\Danik>nmap -sT 192.168.0.125 Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 20:03 ┴хырЁєё№ (чшьр) Nmap scan report for Samsung (192.168.0.125) Host is up (0.00086s latency). Not shown: 997 filtered tcp ports (no-response) PORT STATE SERVICE 8001/tcp open vcom-tunnel 8002/tcp open teradataordbms 8080/tcp open http-proxy MAC Address: 00:C3:F4:93:84:1B (Samsung Electronics) Nmap done: 1 IP address (1 host up) scanned in 5.09 seconds

C:\Users\Danik>nmap -sU 192.168.0.125 Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 20:03 ┴хырЁєё№ (чшьр) Nmap scan report for Samsung (192.168.0.125) Host is up (0.0013s latency). Not shown: 997 closed udp ports (port-unreach) PORT STATE SERVICE 1900/udp open|filtered upnp 5353/udp open zeroconf 8001/udp open|filtered vcom-tunnel MAC Address: 00:C3:F4:93:84:1B (Samsung Electronics)

**5.1.**

C:\Users\Danik>nmap -sA 192.168.0.123 Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 20:07 ┴хырЁєё№ (чшьр) Nmap scan report for 192.168.0.123 Host is up (0.0015s latency). All 1000 scanned ports on 192.168.0.123 are in ignored states. Not shown: 1000 unfiltered tcp ports (reset) MAC Address: 40:2F:86:F8:A6:94 (LG Innotek) Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds

C:\Users\Danik>nmap -sO 192.168.0.123 Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 20:09 ┴хырЁєё№ (чшьр) Nmap scan report for 192.168.0.123 Host is up (0.071s latency). Not shown: 249 closed n/a protocols (proto-unreach) PROTOCOL STATE SERVICE 1 open icmp 2 open|filtered igmp 4 open|filtered ipv4 6 open tcp 17 open udp 41 open|filtered ipv6 136 open|filtered udplite MAC Address: 40:2F:86:F8:A6:94 (LG Innotek) Nmap done: 1 IP address (1 host up) scanned in 298.96 seconds

C:\Users\Danik>nmap -sS -sV 192.168.0.123 Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 20:15 ┴хырЁєё№ (чшьр) Nmap scan report for 192.168.0.123 Host is up (0.0020s latency). Not shown: 995 closed tcp ports (reset) PORT STATE SERVICE VERSION 1030/tcp open upnp Platinum unpnd 1.0.4.9 (arch: i686; UPnP 1.0; DLNADOC 1.50) 3000/tcp open tcpwrapped 3001/tcp open ssl/http LG smart TV http service 7000/tcp open rtsp AirTunes rtspd 377.25.06 49152/tcp open upnp MAC Address: 40:2F:86:F8:A6:94 (LG Innotek) Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel Nmap done: 1 IP address (1 host up) scanned in 74.23 seconds

C:\Users\Danik>nmap -O 192.168.0.123 Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 20:17 ┴хырЁєё№ (чшьр) Nmap scan report for 192.168.0.123 Host is up (0.0019s latency). Not shown: 995 closed tcp ports (reset) PORT STATE SERVICE 1030/tcp open iad1 3000/tcp open ppp 3001/tcp open nessus 7000/tcp open afs3-fileserver 49152/tcp open unknown MAC Address: 40:2F:86:F8:A6:94 (LG Innotek) Device type: general purpose Running: Linux 3.X|4.X OS CPE: cpe:/o:linux:linux\_kernel:3 cpe:/o:linux:linux\_kernel:4 OS details: Linux 3.2 - 4.9 Network Distance: 1 hop Nmap done: 1 IP address (1 host up) scanned in 1.86 seconds

**5.2.**

C:\Users\Danik>nmap -sA 192.168.0.120 Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 20:19 ┴хырЁєё№ (чшьр) Nmap scan report for 192.168.0.120 Host is up (0.0018s latency). All 1000 scanned ports on 192.168.0.120 are in ignored states. Not shown: 1000 unfiltered tcp ports (reset) MAC Address: E4:27:71:54:2D:77 (Smartlabs) Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

C:\Users\Danik>nmap -sO 192.168.0.120 Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 20:19 ┴хырЁєё№ (чшьр) Warning: 192.168.0.120 giving up on port because retransmission cap hit (10). Nmap scan report for 192.168.0.120 Host is up (0.0046s latency). Not shown: 251 closed n/a protocols (proto-unreach) PROTOCOL STATE SERVICE 1 open icmp 2 open|filtered igmp 6 open tcp 17 open udp 136 open|filtered udplite MAC Address: E4:27:71:54:2D:77 (Smartlabs) Nmap done: 1 IP address (1 host up) scanned in 274.46 seconds

C:\Users\Danik>nmap -sS -sV 192.168.0.120 Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 20:24 ┴хырЁєё№ (чшьр) Nmap scan report for 192.168.0.120 Host is up (0.00089s latency). Not shown: 998 closed tcp ports (reset) PORT STATE SERVICE VERSION 22/tcp open ssh Dropbear sshd 2016.74 (protocol 2.0) 53/tcp open domain dnsmasq 2.82 MAC Address: E4:27:71:54:2D:77 (Smartlabs) Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel Nmap done: 1 IP address (1 host up) scanned in 6.41 seconds

C:\Users\Danik>nmap -O 192.168.0.120 Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 20:25 ┴хырЁєё№ (чшьр) Nmap scan report for 192.168.0.120 Host is up (0.00068s latency). Not shown: 998 closed tcp ports (reset) PORT STATE SERVICE 22/tcp open ssh 53/tcp open domain MAC Address: E4:27:71:54:2D:77 (Smartlabs) Device type: general purpose Running: Linux 3.X|4.X OS CPE: cpe:/o:linux:linux\_kernel:3 cpe:/o:linux:linux\_kernel:4 OS details: Linux 3.2 - 4.9 Network Distance: 1 hop

**5.3.**

C:\Users\Danik>nmap -sA 192.168.0.175 Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 20:33 ┴хырЁєё№ (чшьр) Nmap scan report for HOME-PC (192.168.0.175) Host is up (0.000012s latency). All 1000 scanned ports on HOME-PC (192.168.0.175) are in ignored states. Not shown: 1000 unfiltered tcp ports (reset) Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds

C:\Users\Danik>nmap -sO 192.168.0.175 Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 20:33 ┴хырЁєё№ (чшьр) Nmap scan report for HOME-PC (192.168.0.175) Host is up (0.00017s latency). Not shown: 247 closed n/a protocols (proto-unreach) PROTOCOL STATE SERVICE 1 open icmp 2 open|filtered igmp 4 open|filtered ipv4 6 open tcp 17 open udp 41 open|filtered ipv6 50 open|filtered esp 51 open|filtered ah 58 open|filtered ipv6-icmp Nmap done: 1 IP address (1 host up) scanned in 3.40 seconds

C:\Users\Danik>nmap -sS -sV 192.168.0.175 Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 20:34 ┴хырЁєё№ (чшьр) Nmap scan report for HOME-PC (192.168.0.175) Host is up (0.0000020s latency). Not shown: 994 closed tcp ports (reset) PORT STATE SERVICE VERSION 135/tcp open msrpc Microsoft Windows RPC 139/tcp open netbios-ssn Microsoft Windows netbios-ssn 445/tcp open microsoft-ds? 902/tcp open ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP) 912/tcp open vmware-auth VMware Authentication Daemon 1.0 (Uses VNC, SOAP) 7070/tcp open ssl/realserver? Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

C:\Users\Danik>nmap -O 192.168.0.175 Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 20:35 ┴хырЁєё№ (чшьр) Nmap scan report for HOME-PC (192.168.0.175) Host is up (0.000095s latency). Not shown: 994 closed tcp ports (reset) PORT STATE SERVICE 135/tcp open msrpc 139/tcp open netbios-ssn 445/tcp open microsoft-ds 902/tcp open iss-realsecure 912/tcp open apex-mesh 7070/tcp open realserver Device type: general purpose Running: Microsoft Windows 10 OS CPE: cpe:/o:microsoft:windows\_10:1607 OS details: Microsoft Windows 10 1607 Network Distance: 0 hops

**5.4.**

C:\Users\Danik>nmap -sA 192.168.0.1 Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 20:37 ┴хырЁєё№ (чшьр) Nmap scan report for dlinkrouter.local (192.168.0.1) Host is up (0.0042s latency). All 1000 scanned ports on dlinkrouter.local (192.168.0.1) are in ignored states. Not shown: 1000 unfiltered tcp ports (reset) MAC Address: F0:B4:D2:30:15:A8 (D-Link International) Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds

C:\Users\Danik>nmap -sO 192.168.0.1 Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 20:37 ┴хырЁєё№ (чшьр) Warning: 192.168.0.1 giving up on port because retransmission cap hit (10). Nmap scan report for dlinkrouter.local (192.168.0.1) Host is up (0.00052s latency). Not shown: 251 closed n/a protocols (proto-unreach) PROTOCOL STATE SERVICE 1 open icmp 2 open|filtered igmp 6 open tcp 17 open udp 136 open|filtered udplite MAC Address: F0:B4:D2:30:15:A8 (D-Link International) Nmap done: 1 IP address (1 host up) scanned in 256.46 seconds

C:\Users\Danik>nmap -sR -sV 192.168.0.1 Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 20:42 ┴хырЁєё№ (чшьр) Nmap scan report for dlinkrouter.local (192.168.0.1) Host is up (0.0040s latency). Not shown: 994 closed tcp ports (reset) PORT STATE SERVICE VERSION 53/tcp open domain dnsmasq 2.84 80/tcp open http 81/tcp open hosts2-ns? 443/tcp open ssl/https 4443/tcp open ssl/pharos? 4445/tcp open ssl/upnotifyp? 4 MAC Address: F0:B4:D2:30:15:A8 (D-Link International) Nmap done: 1 IP address (1 host up) scanned in 46.74 seconds

C:\Users\Danik>nmap -O 192.168.0.1 Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 20:43 ┴хырЁєё№ (чшьр) Nmap scan report for dlinkrouter.local (192.168.0.1) Host is up (0.0016s latency). Not shown: 994 closed tcp ports (reset) PORT STATE SERVICE 53/tcp open domain 80/tcp open http 81/tcp open hosts2-ns 443/tcp open https 4443/tcp open pharos 4445/tcp open upnotifyp MAC Address: F0:B4:D2:30:15:A8 (D-Link International) Device type: broadband router Running: Linux 3.X OS CPE: cpe:/o:linux:linux\_kernel:3.10 OS details: DD-WRT v24 or v30 (Linux 3.10) Network Distance: 1 hop

**Вывод:** изучил и практически применил утилиты для сканирования и исследования безопасности сети nmap.