МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ

«Брестский государственный технический университет»

Кафедра «Интеллектуальные информационные технологии»

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-23

Романюк А. П.

Проверил:

Степанчук В.И.

Брест 2024

Цель: Изучение и практическое применение утилиты для сканирования и исследования безопасности сети nmap.

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

**TCP Connect Scan (-sT)** (nmap *flag* localhost)**:**

Not shown: 997 filtered tcp ports (no-response)

PORT STATE SERVICE

135/tcp open msrpc

445/tcp open microsoft-ds

1434/tcp open ms-sql-m

**TCP SYN Scan (-sS)** (nmap *flag* localhost)**:**

Not shown: 997 closed tcp ports (reset)

PORT STATE SERVICE

135/tcp open msrpc

445/tcp open microsoft-ds

1434/tcp open ms-sql-m

**TCP XMAS Scan (-sX)** (nmap *flag* localhost)**:**

All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.

Not shown: 1000 closed tcp ports (reset)

**TCP Null Scan (-sN)** (nmap *flag* localhost)**:**

All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.

Not shown: 1000 closed tcp ports (reset)

**Ping Scan (-sP)** (nmap *flag* localhost)**:**

Host is up.

**Service Version Scan (-sV)** (nmap *flag* localhost)**:**

Not shown: 997 closed tcp ports (reset)

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

445/tcp open microsoft-ds?

1434/tcp open ms-sql-s Microsoft SQL Server 2022 16.00.1000

**UDP Scan (-sU)** (nmap *flag* localhost)**:**

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

**IP Protocol Scan (-sO)** (nmap *flag* localhost)**:**

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

**ACK Scan (-sA)** (nmap *flag* localhost)**:**

All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.

Not shown: 1000 unfiltered tcp ports (reset)

**Window Scan (-sW)** (nmap *flag* localhost)**:**

All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.

Not shown: 1000 closed tcp ports (reset)

**RPC Scan (-sR)** (nmap *flag* localhost)**:**

Not shown: 997 closed tcp ports (reset)

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

445/tcp open microsoft-ds?

1434/tcp open ms-sql-s Microsoft SQL Server 2022 16.00.1000

1. Определите операционную систему этой же машины

❯ nmap -O localhost

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-06 19:43 Беларусь (зима)

Nmap scan report for localhost (127.0.0.1)

Host is up (0.019s latency).

Other addresses for localhost (not scanned): ::1

Not shown: 997 closed tcp ports (reset)

PORT STATE SERVICE

135/tcp open msrpc

445/tcp open microsoft-ds

1434/tcp open ms-sql-m

Device type: general purpose

Running: Microsoft Windows 10|11

OS CPE: cpe:/o:microsoft:windows\_10 cpe:/o:microsoft:windows\_11

OS details: Microsoft Windows 10 1703 - 11 21H2, Microsoft Windows 11 21H2

Network Distance: 0 hops

1. Узнать адреса активных хостов в сети

❯ nmap -sn 192.168.0.102/24

MAC Address: 3C:B2:33:6C:D2:4B (Huawei Device)

Nmap scan report for 192.168.0.103

Host is up (0.039s latency).

MAC Address: 50:8E:49:23:7A:00 (Xiaomi Communications)

Nmap scan report for 192.168.0.105

Host is up (0.092s latency).

MAC Address: 2C:6D:C1:B0:0F:40 (Intel Corporate)

Nmap scan report for 192.168.0.109

Host is up (0.13s latency).

MAC Address: 86:00:BC:6B:CA:27 (Unknown)

Nmap scan report for 192.168.0.102

Host is up.

1. 4. Просканируйте хост №1, разными методами. Сравните результаты.
2. 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.

*Задания 4 и 5 выполнены для хоста случайного пользователя(26.167.67.179) в локальной сети RadminVPN по причине того, что не было найдено акивных хостов в моей сети.*

❯ nmap -sS 26.167.67.179

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-06 19:59 Беларусь (зима)

Nmap scan report for 26.167.67.179

Host is up (0.022s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT STATE SERVICE

2179/tcp open vmrdp

5985/tcp open wsman

MAC Address: 02:50:5F:1A:98:42 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 6.54 seconds

*Здесь указаны два поддерживаемых протокола.*

❯ nmap -sU 26.167.67.179

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-06 20:01 Беларусь (зима)

Nmap scan report for 26.167.67.179

Host is up (0.023s latency).

All 1000 scanned ports on 26.167.67.179 are in ignored states.

Not shown: 1000 open|filtered udp ports (no-response)

MAC Address: 02:50:5F:1A:98:42 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 25.98 seconds

❯ nmap -sO 26.167.67.179

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-06 20:01 Беларусь (зима)

Nmap scan report for 26.167.67.179

Host is up (0.024s latency).

Not shown: 255 open|filtered n/a protocols (no-response)

PROTOCOL STATE SERVICE

1 open icmp

MAC Address: 02:50:5F:1A:98:42 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 5.79 seconds

❯ nmap -sA 26.167.67.179

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-06 20:02 Беларусь (зима)

Nmap scan report for 26.167.67.179

Host is up (0.022s latency).

All 1000 scanned ports on 26.167.67.179 are in ignored states.

Not shown: 1000 filtered tcp ports (no-response)

MAC Address: 02:50:5F:1A:98:42 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 25.93 seconds

*порты защищены за счет фильтрации трафика через межсетевой экран, который блокирует попытки соединения с этими портами*

❯ nmap -O 26.167.67.179

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-06 20:04 Беларусь (зима)

Nmap scan report for 26.167.67.179

Host is up (0.023s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT STATE SERVICE

2179/tcp open vmrdp

5985/tcp open wsman

MAC Address: 02:50:5F:1A:98:42 (Unknown)

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose

Running (JUST GUESSING): Microsoft Windows 2016|10|11 (96%)

OS CPE: cpe:/o:microsoft:windows\_server\_2016 cpe:/o:microsoft:windows\_10 cpe:/o:microsoft:windows\_11

Aggressive OS guesses: Microsoft Windows Server 2016 (96%), Microsoft Windows 10 - 11 (89%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 22.70 seconds

Вывод: изучил и практически применил утилиту nmap для сканирования и исследования безопасности сети nmap