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-21(1)

Кирилович А. А.

Проверил:

Степанчук В.И.

Брест 2023

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)**:**

Открыт TCP-порт 631 для службы CUPS (Common Unix Printing System).

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

Тот же открытый порт 631 для службы CUPS.

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

Порт 631 помечен как open|filtered, что может указывать на наличие фильтрации пакетов на этом порту.

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

Аналогично XMAS Scan, порт 631 помечен как open|filtered.

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

Показывает, что хост доступен.

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

Порт 631 открыт для службы CUPS версии 2.4.

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

Открыты UDP-порты 631 (IPP) и 5353 (Zeroconf).

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

Показывает открытые протоколы, такие как ICMP, TCP, UDP, и другие.

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

Все 1000 сканированных портов на localhost отмечены как unfiltered.

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

Все 1000 сканированных портов на localhost отмечены как closed.

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

Аналогично Service Version Scan, порт 631 открыт для службы CUPS версии 2.4.

1. Определите операционную систему этой же машины

❯ sudo nmap -O localhost

Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-19 09:32 +03

Nmap scan report for localhost (127.0.0.1)

Host is up (0.00012s latency).

Not shown: 999 closed ports

PORT STATE SERVICE

631/tcp open ipp

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux\_kernel:2.6.32

OS details: Linux 2.6.32

Network Distance: 0 hops

1. Узнать адреса активных хостов в сети

❯ sudo nmap -sP 192.168.100.4/24

Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-19 09:36 +03

Nmap done: 256 IP addresses (0 hosts up) scanned in 206.31 seconds

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 bstu.by по причине того, что не было найдено акивных хостов в моей сети.*

❯ sudo nmap -sS bstu.by

Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-19 09:57 +03

Nmap scan report for bstu.by (93.125.24.147)

Host is up (0.058s latency).

Other addresses for bstu.by (not scanned): 2a00:c827:9:1::1147

rDNS record for 93.125.24.147: svh12.g-cloud.by

Scanned at 2023-12-19 09:57:03 +03 for 214s

Not shown: 997 filtered ports

PORT STATE SERVICE

80/tcp open http

1720/tcp open h323q931

5060/tcp open sip

Read data files from: /usr/bin/../share/nmap

Nmap done: 1 IP address (1 host up) scanned in 214.35 seconds

Raw packets sent: 2042 (89.824KB) | Rcvd: 747 (29.952KB)

*Здесь указаны три поддерживаемых протокола.*

❯ sudo nmap -sU bstu.by

Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-19 10:01 +03

Nmap scan report for bstu.by (93.125.24.147)

Host is up (0.050s latency).

Other addresses for bstu.by (not scanned): 2a00:c827:9:1::1147

rDNS record for 93.125.24.147: svh12.g-cloud.by

All 1000 scanned ports on bstu.by (93.125.24.147) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 12.84 seconds

❯ sudo nmap -sO bstu.by

Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-19 10:02 +03

Nmap scan report for bstu.by (93.125.24.147)

Host is up (0.023s latency).

Other addresses for bstu.by (not scanned): 2a00:c827:9:1::1147

rDNS record for 93.125.24.147: svh12.g-cloud.by

All 256 scanned ports on bstu.by (93.125.24.147) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 7.09 seconds

❯ sudo nmap -sA bstu.by

Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-19 10:04 +03

Nmap scan report for bstu.by (93.125.24.147)

Host is up (0.047s latency).

Other addresses for bstu.by (not scanned): 2a00:c827:9:1::1147

rDNS record for 93.125.24.147: svh12.g-cloud.by

All 1000 scanned ports on bstu.by (93.125.24.147) are filtered

Nmap done: 1 IP address (1 host up) scanned in 9.68 seconds

*Все порты защищены только покетными фильтрами.*

❯ sudo nmap -O bstu.by

Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-19 10:07 +03

Nmap scan report for bstu.by (93.125.24.147)

Host is up (0.016s latency).

Other addresses for bstu.by (not scanned): 2a00:c827:9:1::1147

rDNS record for 93.125.24.147: svh12.g-cloud.by

Not shown: 997 filtered ports

PORT STATE SERVICE

80/tcp open http

443/tcp open https

1720/tcp open h323q931

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

Device type: specialized|WAP|phone

Running: iPXE 1.X, Linux 2.4.X|2.6.X, Sony Ericsson embedded

OS CPE: cpe:/o:ipxe:ipxe:1.0.0%2b cpe:/o:linux:linux\_kernel:2.4.20 cpe:/o:linux:linux\_kernel:2.6.22 cpe:/h:sonyericsson:u8i\_vivaz

OS details: iPXE 1.0.0+, Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson U8i Vivaz mobile phone

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

Nmap done: 1 IP address (1 host up) scanned in 41.87 seconds

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