



МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра Інформаційної Безпеки

Безпека комп'ютерних мереж
Лабораторна робота “Мережне сканування”

Перевірів:

Виконав:

студент III курсу

групи ФБ-01

Сахній Н.Р.

Київ 2022

ФБ-01 Сахній Назар

Завдання 1:

Ознайомлення з роботою NMAP та особливостями різних видів сканування.

- Connect сканування: *ntar -Pn -sT -p 80,1194 -v 10.0.2.15*

```
(nazar@snz24) ~$ nmap -Pn -sT -p 80,1194 -v 10.0.2.15
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-27 21:57 EET
Initiating Parallel DNS resolution of 1 host. at 21:57
Completed Parallel DNS resolution of 1 host. at 21:57, 0.01s elapsed
Initiating Connect Scan at 21:57
Scanning 10.0.2.15 [2 ports]
Discovered open port 1194/tcp on 10.0.2.15
Completed Connect Scan at 21:57, 0.00s elapsed (2 total ports)
Nmap scan report for 10.0.2.15
Host is up (0.0022s latency).

PORT      STATE SERVICE
80/tcp    closed http
1194/tcp  open  openvpn

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	10.0.2.15	TCP	76	45336 → 80 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=138055321 TSecr=0 WS=128
2	0.000012150	10.0.2.15	10.0.2.15	TCP	56	80 → 45336 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3	0.000058536	10.0.2.15	10.0.2.15	TCP	76	56802 → 1194 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=138055321 TSecr=0 WS=128
4	0.000065942	10.0.2.15	10.0.2.15	TCP	76	1194 → 56802 [SYN, ACK] Seq=0 Ack=1 Win=65495 SACK_PERM=1 TSval=138055321 TSecr=138055321 WS=128
5	0.000072941	10.0.2.15	10.0.2.15	TCP	68	56802 → 1194 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=138055321 TSecr=138055321
6	0.002248835	10.0.2.15	10.0.2.15	TCP	68	56802 → 1194 [RST, ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=138055323 TSecr=138055321

- SYN сканування: *ntar -Pn -sS -p 80,1194 -v 10.0.2.15*

```
(nazar@snz24) ~$ sudo nmap -Pn -sS -p 80,1194 -v 10.0.2.15
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-27 22:02 EET
Initiating Parallel DNS resolution of 1 host. at 22:02
Completed Parallel DNS resolution of 1 host. at 22:02, 0.01s elapsed
Initiating SYN Stealth Scan at 22:02
Scanning 10.0.2.15 [2 ports]
Discovered open port 1194/tcp on 10.0.2.15
Completed SYN Stealth Scan at 22:02, 0.09s elapsed (2 total ports)
Nmap scan report for 10.0.2.15
Host is up (0.000073s latency).

PORT      STATE SERVICE
80/tcp    closed http
1194/tcp  open  openvpn

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
Raw packets sent: 2 (88B) | Rcvd: 4 (172B)
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	10.0.2.15	TCP	60	65072 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2	0.000017940	10.0.2.15	10.0.2.15	TCP	56	80 → 65072 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3	0.000031286	10.0.2.15	10.0.2.15	TCP	60	65072 → 1194 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4	0.000071657	10.0.2.15	10.0.2.15	TCP	60	1194 → 65072 [SYN, ACK] Seq=0 Ack=1 Win=65495 Len=0 MSS=65495
5	0.000076747	10.0.2.15	10.0.2.15	TCP	56	65072 → 1194 [RST] Seq=1 Win=0 Len=0

- ACK сканування: *ntar -Pn -sA -p 80,1194 -v 10.0.2.15*

```
(nazar@snz24) ~$ sudo nmap -Pn -sA -p 80,1194 -v 10.0.2.15
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-27 22:12 EET
Initiating Parallel DNS resolution of 1 host. at 22:12
Completed Parallel DNS resolution of 1 host. at 22:12, 0.01s elapsed
Initiating ACK Scan at 22:12
Scanning 10.0.2.15 [2 ports]
Completed ACK Scan at 22:12, 0.05s elapsed (2 total ports)
Nmap scan report for 10.0.2.15
Host is up (0.000038s latency).

PORT      STATE SERVICE
80/tcp    unfiltered http
1194/tcp  unfiltered openvpn

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
Raw packets sent: 2 (80B) | Rcvd: 4 (160B)
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	10.0.2.15	TCP	56	34014 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
2	0.000011430	10.0.2.15	10.0.2.15	TCP	56	80 → 34014 [RST] Seq=1 Win=0 Len=0
3	0.000020404	10.0.2.15	10.0.2.15	TCP	56	34014 → 1194 [ACK] Seq=1 Ack=1 Win=1024 Len=0
4	0.000024676	10.0.2.15	10.0.2.15	TCP	56	1194 → 34014 [RST] Seq=1 Win=0 Len=0

- FIN сканування: *ntar -Pn -sF -p 80,1194 -v 10.0.2.15*

```
(nazar@snz24:~)$ sudo nmap -Pn -sF -p 80,1194 -v 10.0.2.15
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-27 22:25 EET
Initiating Parallel DNS resolution of 1 host. at 22:25
Completed Parallel DNS resolution of 1 host. at 22:25, 0.01s elapsed
Initiating FIN Scan at 22:25
Scanning 10.0.2.15 [2 ports]
Completed FIN Scan at 22:25, 1.34s elapsed (2 total ports)
Nmap scan report for 10.0.2.15
Host is up (0.000054s latency).

PORT      STATE      SERVICE
80/tcp    closed    http
1194/tcp  open|filtered openvpn

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.43 seconds
Raw packets sent: 3 (120B) | Rcvd: 4 (160B)
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	10.0.2.15	TCP	56	64951 → 80 [FIN] Seq=1 Win=1024 Len=0
2	0.000014868	10.0.2.15	10.0.2.15	TCP	56	80 → 64951 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
3	0.000024294	10.0.2.15	10.0.2.15	TCP	56	64951 → 1194 [FIN] Seq=1 Win=1024 Len=0
4	1.101687410	10.0.2.15	10.0.2.15	TCP	56	64952 → 1194 [FIN] Seq=1 Win=1024 Len=0

- XMAS сканування: *ntar -Pn -sX -p 80,1194 -v 10.0.2.15*

```
(nazar@snz24:~)$ sudo nmap -Pn -sX -p 80,1194 -v 10.0.2.15
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-27 22:23 EET
Initiating Parallel DNS resolution of 1 host. at 22:23
Completed Parallel DNS resolution of 1 host. at 22:23, 0.01s elapsed
Initiating XMAS Scan at 22:23
Scanning 10.0.2.15 [2 ports]
Completed XMAS Scan at 22:23, 1.31s elapsed (2 total ports)
Nmap scan report for 10.0.2.15
Host is up (0.000039s latency).

PORT      STATE      SERVICE
80/tcp    closed    http
1194/tcp  open|filtered openvpn

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds
Raw packets sent: 3 (120B) | Rcvd: 4 (160B)
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	10.0.2.15	TCP	56	47999 → 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2	0.000012688	10.0.2.15	10.0.2.15	TCP	56	80 → 47999 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
3	0.000020144	10.0.2.15	10.0.2.15	TCP	56	47999 → 1194 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
4	1.130769550	10.0.2.15	10.0.2.15	TCP	56	48000 → 1194 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0

- NULL сканування: *ntar -Pn -sN -p 80,1194 -v 10.0.2.15*

```
(nazar@snz24:~)$ sudo nmap -Pn -sN -p 80,1194 -v 10.0.2.15
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-27 22:29 EET
Initiating Parallel DNS resolution of 1 host. at 22:29
Completed Parallel DNS resolution of 1 host. at 22:29, 0.01s elapsed
Initiating NULL Scan at 22:29
Scanning 10.0.2.15 [2 ports]
Completed NULL Scan at 22:29, 1.31s elapsed (2 total ports)
Nmap scan report for 10.0.2.15
Host is up (0.000064s latency).

PORT      STATE      SERVICE
80/tcp    closed    http
1194/tcp  open|filtered openvpn

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds
Raw packets sent: 3 (120B) | Rcvd: 4 (160B)
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	10.0.2.15	TCP	56	57139 → 80 [None] Seq=1 Win=1024 Len=0
2	0.000022288	10.0.2.15	10.0.2.15	TCP	56	80 → 57139 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3	0.000033511	10.0.2.15	10.0.2.15	TCP	56	57139 → 1194 [None] Seq=1 Win=1024 Len=0
4	1.102180501	10.0.2.15	10.0.2.15	TCP	56	57140 → 1194 [None] Seq=1 Win=1024 Len=0

- WIN сканування: *nmmap -Pn -sW -p 80,1194 -v 10.0.2.15*

```
(nazar@snz24) ~$ sudo nmap -Pn -sW -p 80,1194 -v 10.0.2.15
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-27 22:31 EET
Initiating Parallel DNS resolution of 1 host. at 22:31
Completed Parallel DNS resolution of 1 host. at 22:31, 0.01s elapsed
Initiating Window Scan at 22:31
Scanning 10.0.2.15 [2 ports]
Completed Window Scan at 22:31, 0.07s elapsed (2 total ports)
Nmap scan report for 10.0.2.15
Host is up (0.000042s latency).

PORT      STATE SERVICE
80/tcp    closed http
1194/tcp  closed openvpn

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
Raw packets sent: 2 (80B) | Rcvd: 4 (160B)
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	10.0.2.15	TCP	56	56853 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
2	0.000011979	10.0.2.15	10.0.2.15	TCP	56	80 → 56853 [RST] Seq=1 Win=0 Len=0
3	0.000021982	10.0.2.15	10.0.2.15	TCP	56	56853 → 1194 [ACK] Seq=1 Ack=1 Win=1024 Len=0
4	0.000025756	10.0.2.15	10.0.2.15	TCP	56	1194 → 56853 [RST] Seq=1 Win=0 Len=0

- UDP сканування: *nmmap -sU -p 1-1024 -v 10.0.2.15*

```
(nazar@snz24) ~$ sudo nmap -sU -p 1-1024 -v 10.0.2.15
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-27 22:51 EET
Initiating Parallel DNS resolution of 1 host. at 22:51
Completed Parallel DNS resolution of 1 host. at 22:51, 0.01s elapsed
Initiating UDP Scan at 22:51
Scanning 10.0.2.15 [1024 ports]
Completed UDP Scan at 22:51, 0.06s elapsed (1024 total ports)
Nmap scan report for 10.0.2.15
Host is up (0.000099s latency).
All 1024 scanned ports on 10.0.2.15 are closed

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
Raw packets sent: 1024 (29.799KB) | Rcvd: 2048 (88.176KB)
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	10.0.2.15	UDP	44	48344 → 143 Len=0
2	0.000022756	10.0.2.15	10.0.2.15	ICMP	72	Destination unreachable (Port unreachable)
3	0.000043847	10.0.2.15	10.0.2.15	UDP	44	48344 → 915 Len=0
4	0.000049951	10.0.2.15	10.0.2.15	ICMP	72	Destination unreachable (Port unreachable)
5	0.000058405	10.0.2.15	10.0.2.15	UDP	44	48344 → 922 Len=0
6	0.000062939	10.0.2.15	10.0.2.15	ICMP	72	Destination unreachable (Port unreachable)
7	0.000071624	10.0.2.15	10.0.2.15	UDP	44	48344 → 672 Len=0
8	0.000076911	10.0.2.15	10.0.2.15	ICMP	72	Destination unreachable (Port unreachable)
9	0.000083970	10.0.2.15	10.0.2.15	UDP	44	48344 → 16 Len=0
10	0.000088603	10.0.2.15	10.0.2.15	ICMP	72	Destination unreachable (Port unreachable)
11	0.000096439	10.0.2.15	10.0.2.15	UDP	44	48344 → 487 Len=0
12	0.000101278	10.0.2.15	10.0.2.15	ICMP	72	Destination unreachable (Port unreachable)
13	0.000110166	10.0.2.15	10.0.2.15	UDP	44	48344 → 343 Len=0
14	0.000114610	10.0.2.15	10.0.2.15	ICMP	72	Destination unreachable (Port unreachable)

Початкове сканування деякої мережі на наявність активних хостів.

```
(nazar@snz24) ~$ nmap -sn 10.0.2.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-27 23:10 EET
Nmap scan report for 10.0.2.15
Host is up (0.00075s latency).
Nmap done: 256 IP addresses (1 host up) scanned in 3.26 seconds
```

Сканування обраного хоста різними способами на наявність відкритих TCP та UDP портів і аналіз отриманих різними способами результатів.

↓ TCP ↓

```
(nazar@snz24) ~  
$ nmap -sT -sV -p- -v 10.0.2.15  
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-27 23:08 EET  
NSE: Loaded 45 scripts for scanning.  
Initiating Ping Scan at 23:08  
Scanning 10.0.2.15 [2 ports]  
Completed Ping Scan at 23:08, 0.00s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 23:08  
Completed Parallel DNS resolution of 1 host. at 23:08, 0.01s elapsed  
Initiating Connect Scan at 23:08  
Scanning 10.0.2.15 [65535 ports]  
Discovered open port 1194/tcp on 10.0.2.15  
Completed Connect Scan at 23:08, 1.14s elapsed (65535 total ports)  
Initiating Service scan at 23:08  
Scanning 1 service on 10.0.2.15  
Completed Service scan at 23:08, 31.83s elapsed (1 service on 1 host)  
NSE: Script scanning 10.0.2.15.  
Initiating NSE at 23:08  
Completed NSE at 23:08, 0.00s elapsed  
Initiating NSE at 23:08  
Completed NSE at 23:08, 0.00s elapsed  
Nmap scan report for 10.0.2.15  
Host is up (0.000072s latency).  
Not shown: 65534 closed ports  
PORT      STATE SERVICE  
1194/tcp  open  openvpn?  
  
Read data files from: /usr/bin/./share/nmap  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 33.31 seconds
```

↓ UDP ↓

```
(nazar@snz24) ~  
$ sudo nmap -sU -sV -p- -v 10.0.2.15  
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-27 23:11 EET  
NSE: Loaded 45 scripts for scanning.  
Initiating Parallel DNS resolution of 1 host. at 23:11  
Completed Parallel DNS resolution of 1 host. at 23:11, 0.01s elapsed  
Initiating UDP Scan at 23:11  
Scanning 10.0.2.15 [65535 ports]  
Completed UDP Scan at 23:11, 1.01s elapsed (65535 total ports)  
Initiating Service scan at 23:11  
NSE: Script scanning 10.0.2.15.  
Initiating NSE at 23:11  
Completed NSE at 23:11, 0.00s elapsed  
Initiating NSE at 23:11  
Completed NSE at 23:11, 0.00s elapsed  
Nmap scan report for 10.0.2.15  
Host is up (0.000070s latency).  
All 65535 scanned ports on 10.0.2.15 are closed  
  
Read data files from: /usr/bin/./share/nmap  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 1.39 seconds  
Raw packets sent: 65535 (3.163MB) | Rcvd: 131070 (8.160MB)
```

Ідентифікація засобами NMAP версії ОС, що використовується на даному хості.
Відповісти, за якими параметрами здійснюється ідентифікація версії ОС?

```
(nazar@snz24) ~  
$ sudo nmap -O -p 1194 10.0.2.15  
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-27 23:15 EET  
Nmap scan report for 10.0.2.15  
Host is up (0.000051s latency).  
  
PORT      STATE SERVICE  
1194/tcp  open  openvpn  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
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  
  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
```

Утиліта **nmap** з параметром **"-O"** використовує різні ознаки для ідентифікації версії операційної системи, такі як відповіді на ICMP та TCP пакети, MTU, TTL, TCP прапорці, параметри та наявність опцій, розмір вікна TCP, затримка між пакетами та тип (версія) програмного забезпечення.

Ознайомлення з наявними у NMAP скриптами та синтаксисом їх застосування. Спроба застосувати до системи, яка сканується, якомога більше NSE-модулів.

↓ **ssh-auth-methods** ↓

```
(nazar@snz24)~$ nmap --script-help ssh-auth-methods
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-27 23:41 EET

ssh-auth-methods
Categories: auth intrusive
https://nmap.org/nse/doc/scripts/ssh-auth-methods.html
Returns authentication methods that a SSH server supports.

This is in the "intrusive" category because it starts an authentication with a
username which may be invalid. The abandoned connection will likely be logged.
```

↓ **http-waf-detect** ↓

```
(nazar@snz24)~$ nmap --script-help http-waf-detect
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-27 23:47 EET

http-waf-detect
Categories: discovery intrusive
https://nmap.org/nse/doc/scripts/http-waf-detect.html
Attempts to determine whether a web server is protected by an IPS (Intrusion
Prevention System), IDS (Intrusion Detection System) or WAF (Web Application
Firewall) by probing the web server with malicious payloads and detecting
changes in the response code and body.

To do this the script will send a "good" request and record the response,
afterwards it will match this response against new requests containing
malicious payloads. In theory, web applications shouldn't react to malicious
requests because we are storing the payloads in a variable that is not used by
the script/file and only WAF/IDS/IPS should react to it. If aggro mode is set,
the script will try all attack vectors (More noisy)

This script can detect numerous IDS, IPS, and WAF products since they often
protect web applications in the same way. But it won't detect products which
don't alter the http traffic. Results can vary based on product configuration,
but this script has been tested to work against various configurations of the
following products:

* Apache ModSecurity
* Barracuda Web Application Firewall
* PHPIDS
* dotDefender
* Imperva Web Firewall
* Blue Coat SG 400
```

Після того, як NMAP виявив відкриті порти (активні мережні служби) – запустити на них відповідні NSE скрипти, щоб добути більше інформації.

↓ **1194 (openvpn): open** ↓

```
(nazar@snz24)~$ nmap --script ssh-auth-methods -p 1194 10.0.2.15
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-27 23:50 EET
Nmap scan report for 10.0.2.15
Host is up (0.00014s latency).

PORT      STATE SERVICE
1194/tcp  open  openvpn

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds

(nazar@snz24)~$ nmap --script http-waf-detect -p 80 10.0.2.15
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-27 23:50 EET
Nmap scan report for 10.0.2.15
Host is up (0.00017s latency).
```

↓ **80 (http): closed** ↓

```
(nazar@snz24)~$ nmap --script http-waf-detect -p 80 10.0.2.15
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-27 23:50 EET
Nmap scan report for 10.0.2.15
Host is up (0.00017s latency).

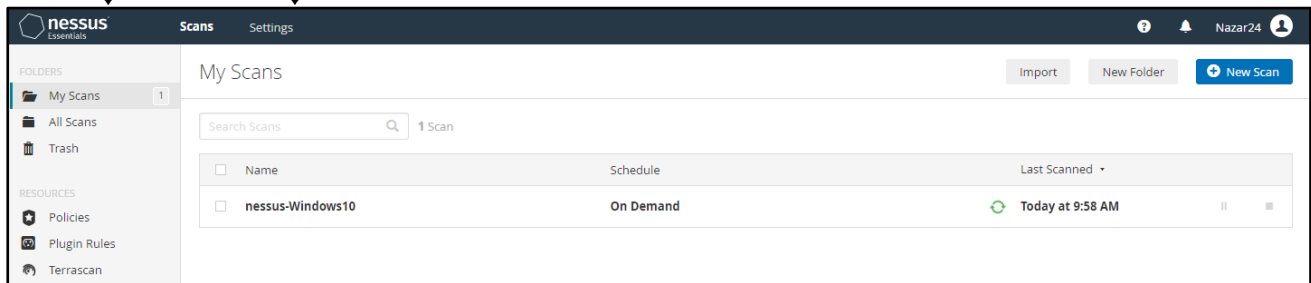
PORT      STATE SERVICE
80/tcp    closed http

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

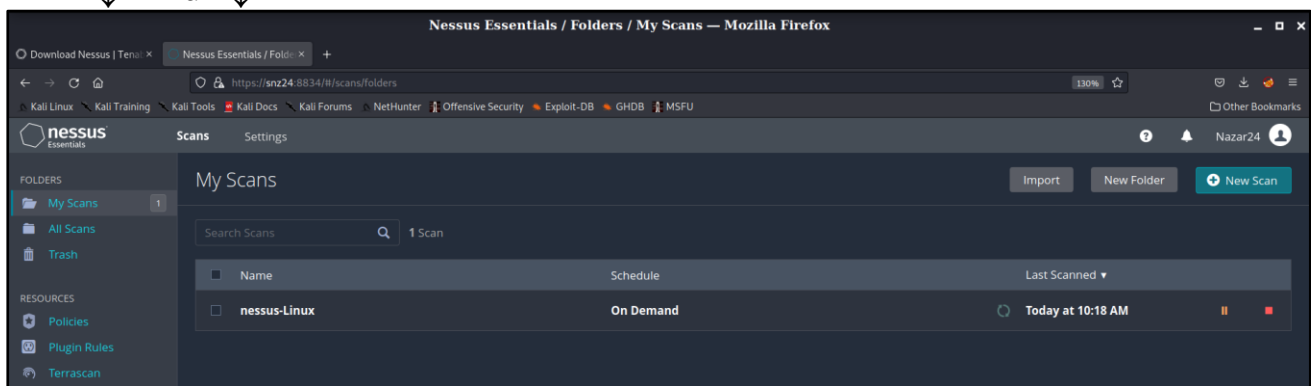
Завдання 2:

Сканування однієї Windows та однієї Linux системи на предмет наявності вразливостей сканером Nessus.

↓ Windows ↓

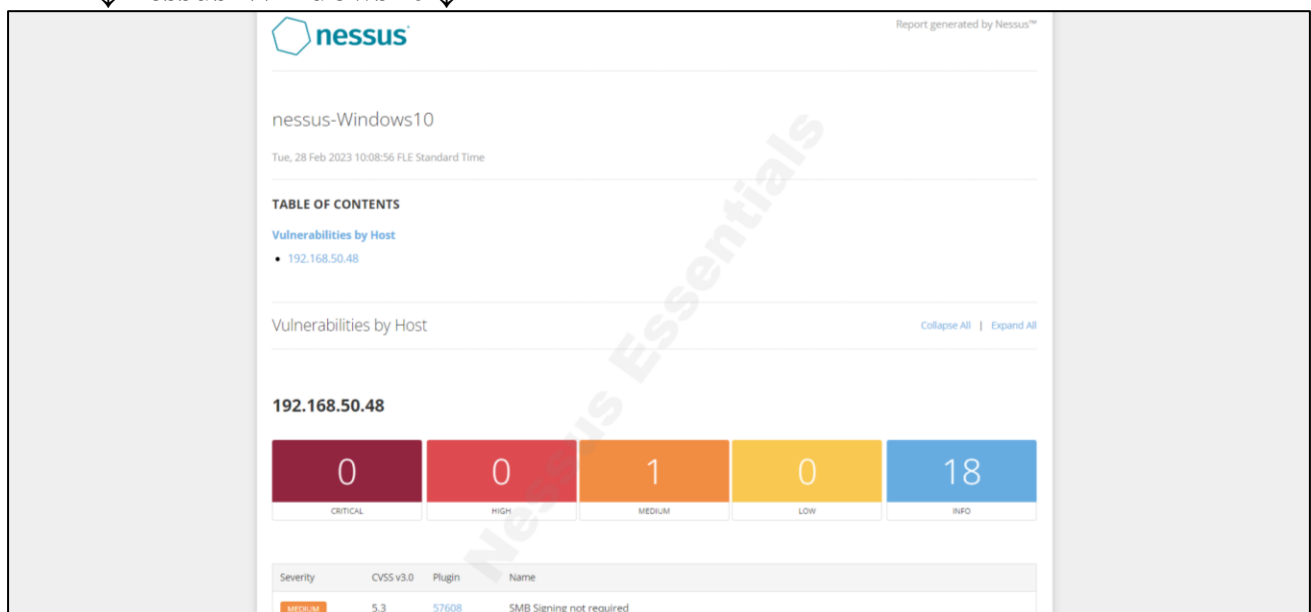


↓ Linux ↓



За наявними базами даних вразливостей отримайте інформацію про знайдені вразливості, ступінь їх значущості, наявність експлоїтів, версії ПЗ, до яких вони застосовні, та хронологію вразливості (час публікації інформації, час появи оновлення безпеки або оновленої версії ПЗ в яких вразливість усунуто).

↓ nessus-Windows10 ↓



↓ **nessus-Linux** ↓

nessus-Linux
Tue, 28 Feb 2023 10:24:45 EET

TABLE OF CONTENTS

Vulnerabilities by Host

- 10.0.2.15

Vulnerabilities by Host

10.0.2.15

Severity	CVSS v3.0	Plugin	Name
CRITICAL	0	0	0
HIGH	0	1	0
MEDIUM	0	0	46
LOW	0	0	0
INFO	0	0	0

SSL Certificate Cannot Be Trusted

Чи зможе зловмисник використати знайдені у вашій системі вразливості?

↓ **SMB Signing not required (Windows)** ↓

SMB Signing not required

Severity: MEDIUM

Nessus Plugin ID: 57608

Language: English

Information Dependencies Dependents Changelog

Synopsis

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

See Also

<http://www.nessus.org/u?df39b8b3>

<http://technet.microsoft.com/en-us/library/cc731957.aspx>

<http://www.nessus.org/u?74b80723>

Plugin Details

Severity: Medium

ID: 57608

File Name: smb_signing_disabled.nasl

Version: 1.20

Type: remote

Family: Misc.

Published: 1/19/2012

Updated: 10/5/2022

Risk Information

CVSS Score Rationale: Based on analysis of vulnerability

↓ **SSL Certificate Cannot Be Trusted (Linux)** ↓

SSL Certificate Cannot Be Trusted

Severity: MEDIUM

Nessus Plugin ID: 51192

Language: English

Information Dependencies Dependents Changelog

Synopsis

The SSL certificate for this service cannot be trusted.

Plugin Details

Severity: Medium

Tenable ot Families About Plugin Families Nessus Release Notes Audits Tenable.sc Policies Tenable.ad Indicators	Description <p>The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :</p> <ul style="list-style-type: none"> - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority. - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates. - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize. <p>If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.</p> Solution <p>Purchase or generate a proper SSL certificate for this service.</p> See Also https://www.its.ucl.ac.uk/REC-X.509/en https://en.wikipedia.org/wiki/X.509	ID: 51192 File Name: ssl_signed_certificate.nasl Version: 1.19 Type: remote Family: General Published: 12/15/2010 Updated: 4/27/2020 Risk Information CVSS v2 Risk Factor: Medium Base Score: 6.4 Vector: AV:N/AC:L/Au:N/C:P/I:P/A:N CVSS v3 Risk Factor: Medium Base Score: 6.5 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N Vulnerability Information Required KB Items: SSL/BrokenCAChain
--	--	---

Висновки:

Під час виконання лабораторної роботи було використано функціонал утиліти *ntar* та сканера *Nessus*. Завдяки цим інструментам було можливо дослідити мережу та виявити потенційні вразливості та проблеми з безпекою. Їхнє використання є важливим для забезпечення безпеки мережі та даних, а також для виявлення потенційних загроз та протидії їм.

Отже, використання утиліти *ntar* та програми *Nessus* є необхідним кроком для забезпечення безпеки мережі та сервісів, які у ній знаходяться.