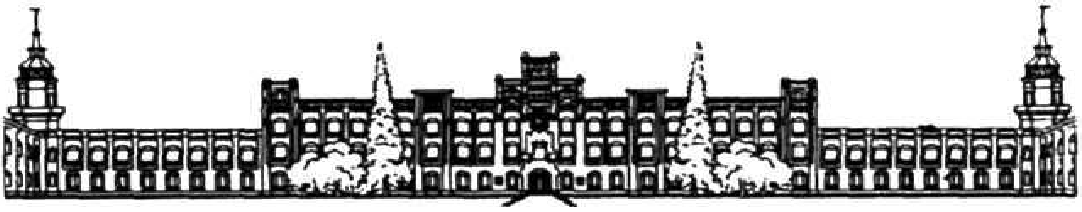


МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра Інформаційної Безпеки

Аналіз та моніторинг кібербезпеки

Практичне завдання №4

Дослідження ІТС за допомогою сканування

Перевірив:
Козленко О. В.

Виконав:
студент IV курсу
групи ФБ-01
Сахній Н. Р.

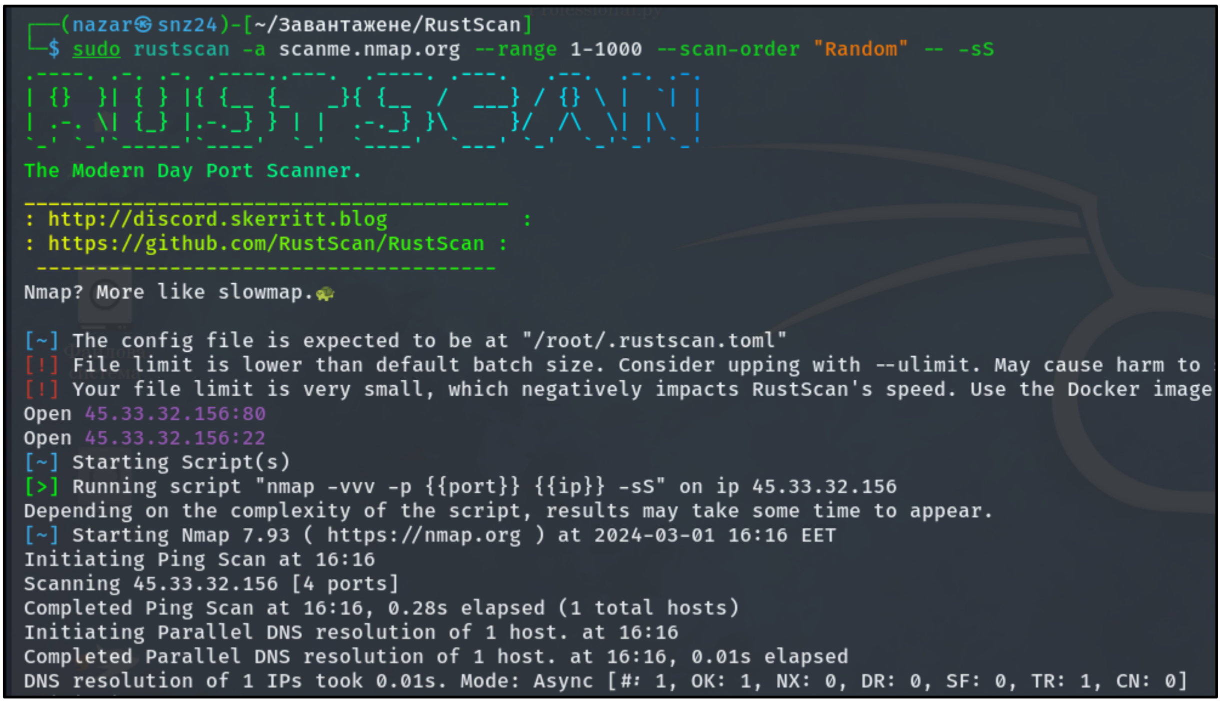
Київ 2024

Мета: Отримання практичних навичок з дослідження топології та структури інформаційного об’єкта за допомогою використання мережевих сканерів.

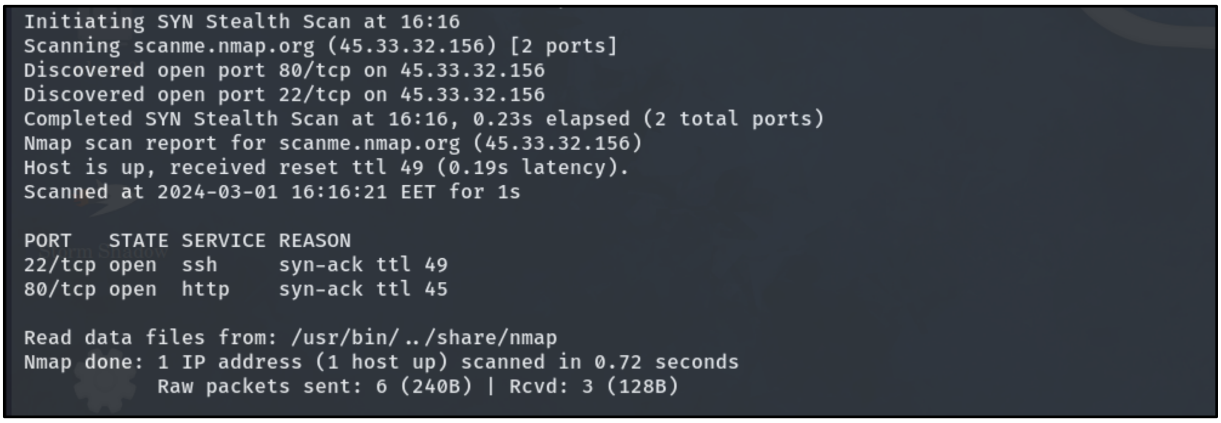
Завдання:

1. Проаналізувати стан мережі на можливі спроби шкідливого втручання за допомогою утиліт Rustscan (https://github.com/RustScan/RustScan) за типами сканування:

– Сканування TCP SYN та рандомізація

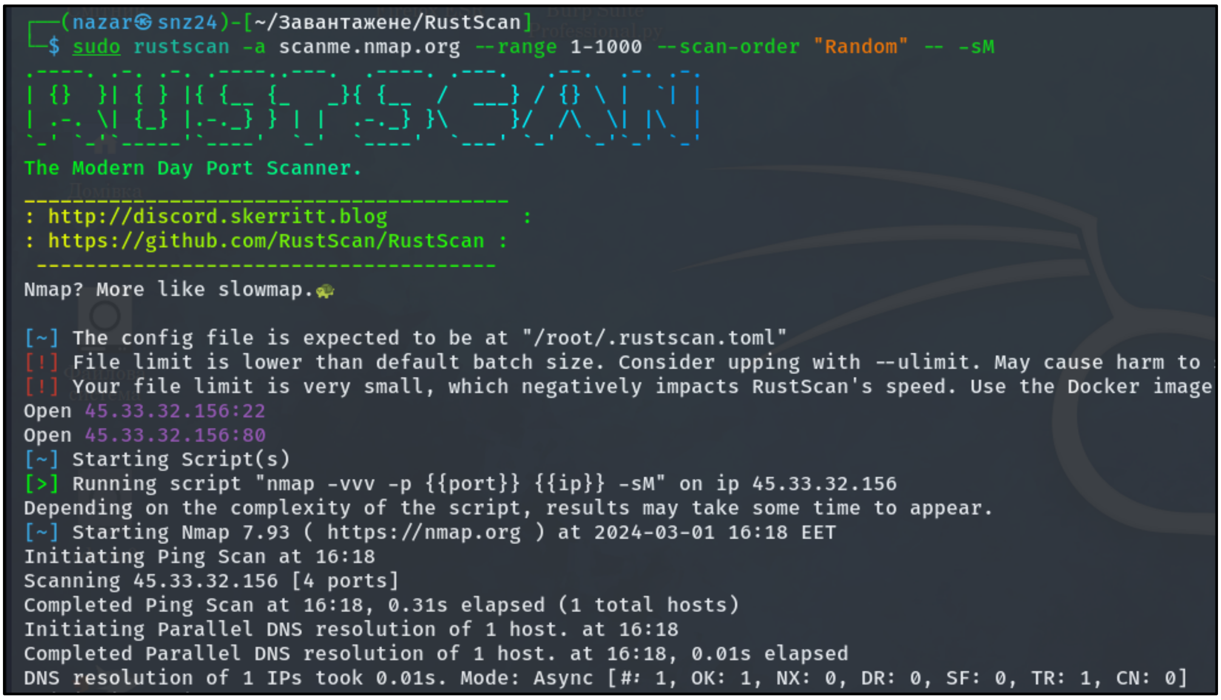


```
┌──(nazar㉿snz24)-[~/Завантажене/RustScan]
└─$ sudo rustscan -a scanme.nmap.org --range 1-1000 --scan-order "Random" -- -sS
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: http://discord.skerritt.blog           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Nmap? More like slowmap.🐢

[~] The config file is expected to be at "/root/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image
Open 45.33.32.156:80
Open 45.33.32.156:22
[~] Starting Script(s)
[>] Running script "nmap -vvv -p {{port}} {{ip}} -sS" on ip 45.33.32.156
Depending on the complexity of the script, results may take some time to appear.
[~] Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-01 16:16 EET
Initiating Ping Scan at 16:16
Scanning 45.33.32.156 [4 ports]
Completed Ping Scan at 16:16, 0.28s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:16
Completed Parallel DNS resolution of 1 host. at 16:16, 0.01s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]
```

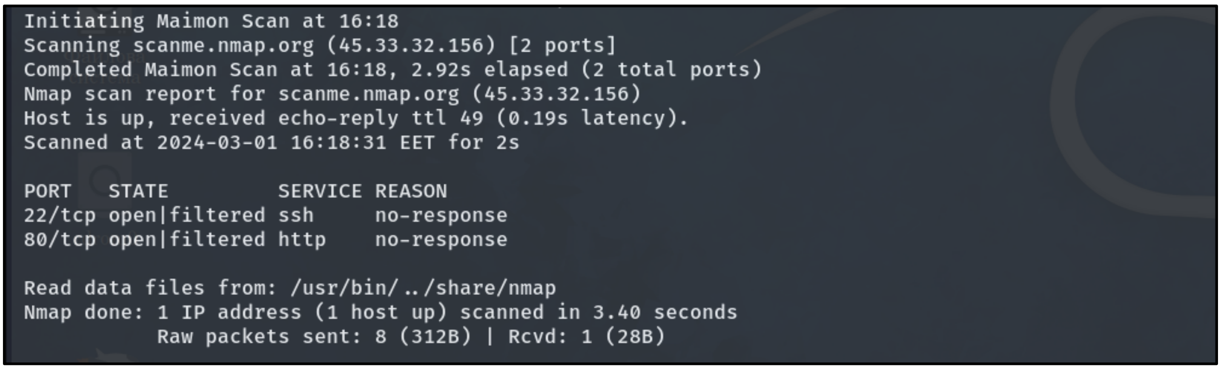


```
Initiating SYN Stealth Scan at 16:16
Scanning scanme.nmap.org (45.33.32.156) [2 ports]
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 22/tcp on 45.33.32.156
Completed SYN Stealth Scan at 16:16, 0.23s elapsed (2 total ports)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up, received reset ttl 49 (0.19s latency).
Scanned at 2024-03-01 16:16:21 EET for 1s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 49
80/tcp open  http    syn-ack ttl 45

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.72 seconds
           Raw packets sent: 6 (240B) | Rcvd: 3 (128B)
```

– Сканування Meiman та рандомізація

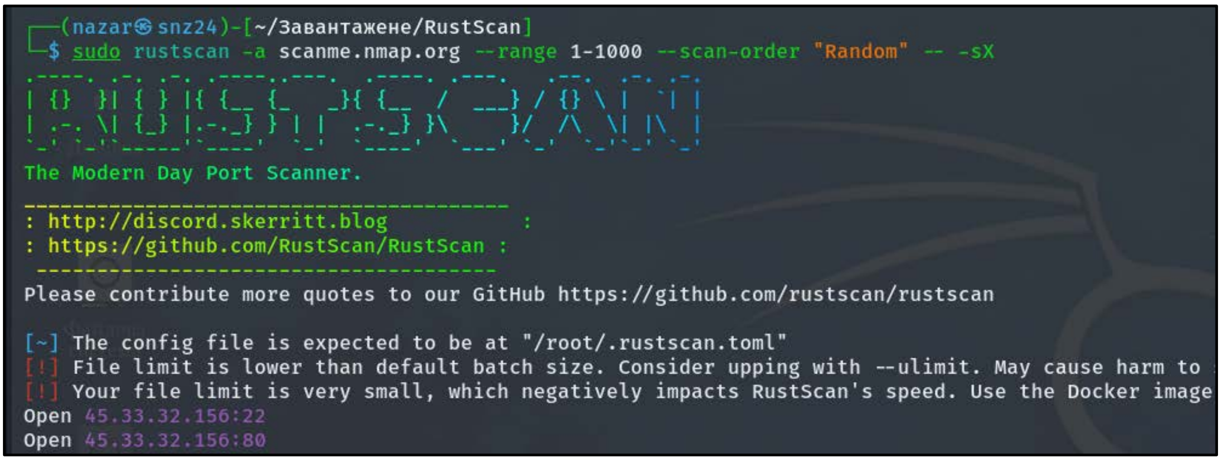


```
┌──(nazar㉿snz24)-[~/Завантажене/RustScan]
└─$ sudo rustscan -a scanme.nmap.org --range 1-1000 --scan-order "Random" -- -sM
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: http://discord.skerritt.blog           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Nmap? More like slowmap.🐢

[~] The config file is expected to be at "/root/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image
Open 45.33.32.156:22
Open 45.33.32.156:80
[~] Starting Script(s)
[>] Running script "nmap -vvv -p {{port}} {{ip}} -sM" on ip 45.33.32.156
Depending on the complexity of the script, results may take some time to appear.
[~] Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-01 16:18 EET
Initiating Ping Scan at 16:18
Scanning 45.33.32.156 [4 ports]
Completed Ping Scan at 16:18, 0.31s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:18
Completed Parallel DNS resolution of 1 host. at 16:18, 0.01s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]
```

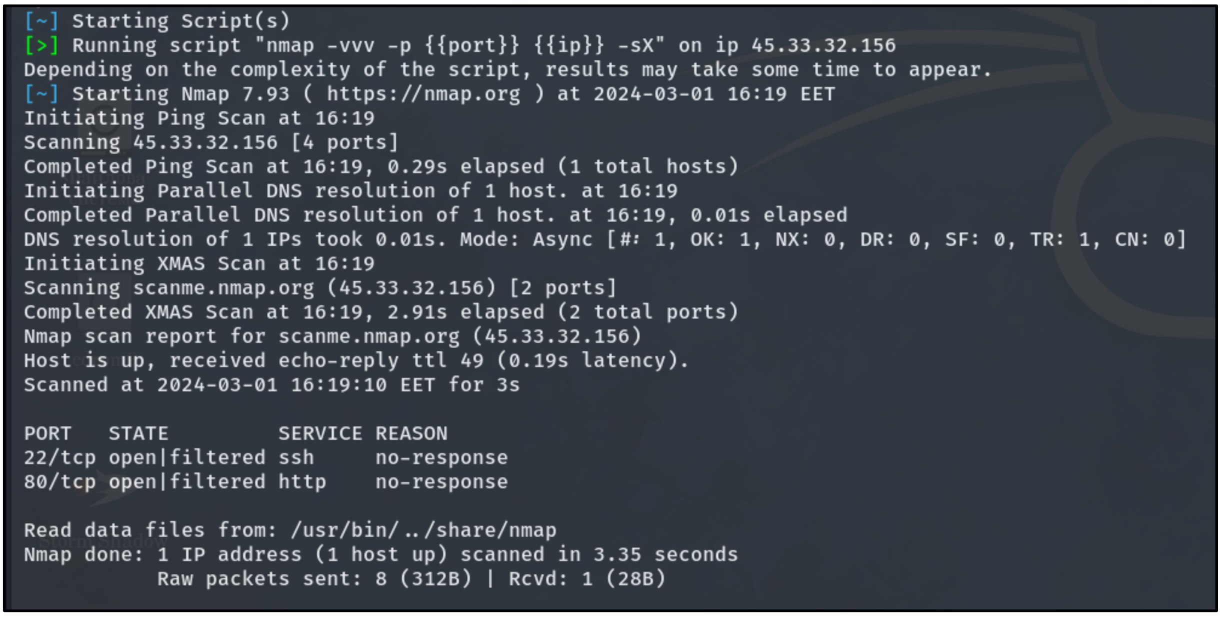


```
Initiating Maimon Scan at 16:18
Scanning scanme.nmap.org (45.33.32.156) [2 ports]
Completed Maimon Scan at 16:18, 2.92s elapsed (2 total ports)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up, received echo-reply ttl 49 (0.19s latency).
Scanned at 2024-03-01 16:18:31 EET for 2s

PORT   STATE         SERVICE REASON
22/tcp open|filtered ssh     no-response
80/tcp open|filtered http    no-response

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 3.40 seconds
           Raw packets sent: 8 (312B) | Rcvd: 1 (28B)
```

– Сканування Xmas tree та рандомізація

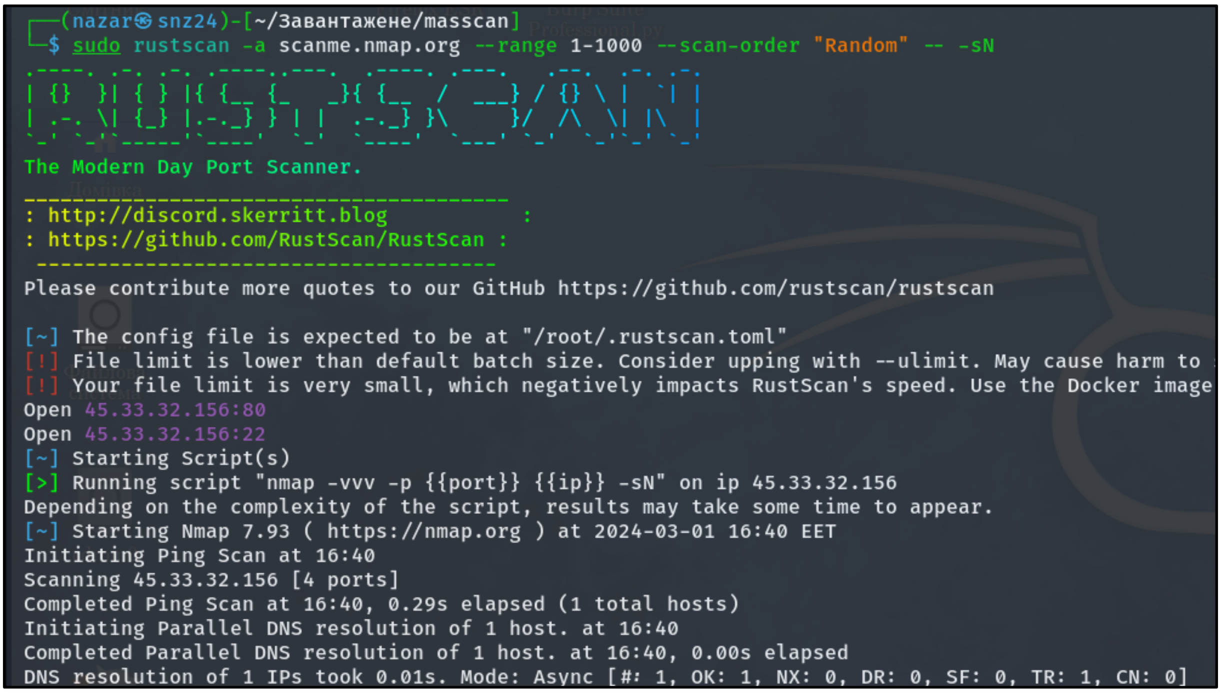


```
┌──(nazar㉿snz24)-[~/Завантажене/RustScan]
└─$ sudo rustscan -a scanme.nmap.org --range 1-1000 --scan-order "Random" -- -sX
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: http://discord.skerritt.blog           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Please contribute more quotes to our GitHub https://github.com/rustscan/rustscan

[~] The config file is expected to be at "/root/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image
Open 45.33.32.156:22
Open 45.33.32.156:80
```

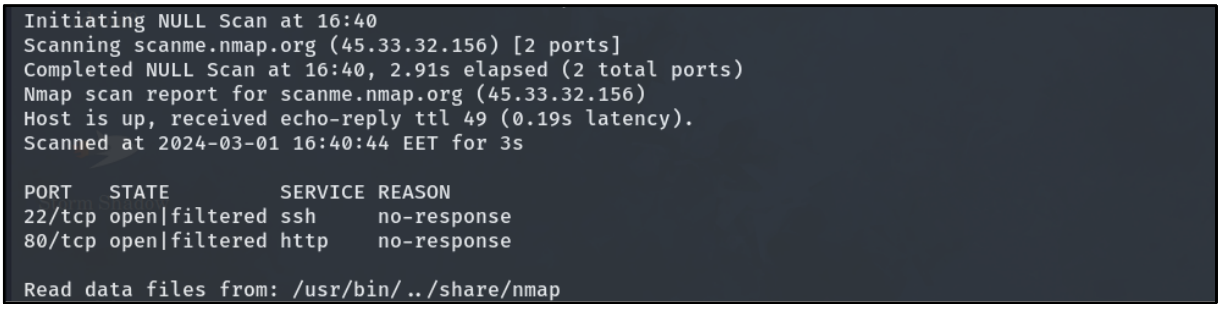


```
[~] Starting Script(s)
[>] Running script "nmap -vvv -p {{port}} {{ip}} -sX" on ip 45.33.32.156
Depending on the complexity of the script, results may take some time to appear.
[~] Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-01 16:19 EET
Initiating Ping Scan at 16:19
Scanning 45.33.32.156 [4 ports]
Completed Ping Scan at 16:19, 0.29s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:19
Completed Parallel DNS resolution of 1 host. at 16:19, 0.01s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating XMAS Scan at 16:19
Scanning scanme.nmap.org (45.33.32.156) [2 ports]
Completed XMAS Scan at 16:19, 2.91s elapsed (2 total ports)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up, received echo-reply ttl 49 (0.19s latency).
Scanned at 2024-03-01 16:19:10 EET for 3s

PORT   STATE         SERVICE REASON
22/tcp open|filtered ssh     no-response
80/tcp open|filtered http    no-response

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 3.35 seconds
           Raw packets sent: 8 (312B) | Rcvd: 1 (28B)
```

– Сканування Null та рандомізація



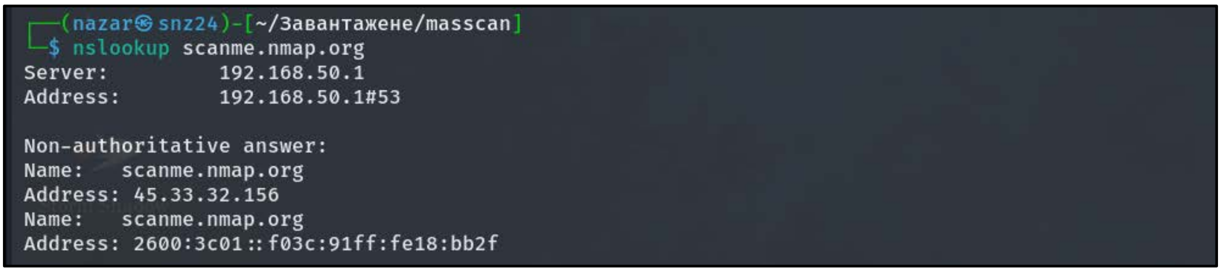
```
┌──(nazar㉿snz24)-[~/Завантажене/masscan]
└─$ sudo rustscan -a scanme.nmap.org --range 1-1000 --scan-order "Random" -- -sN
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: http://discord.skerritt.blog           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Please contribute more quotes to our GitHub https://github.com/rustscan/rustscan

[~] The config file is expected to be at "/root/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image
Open 45.33.32.156:80
Open 45.33.32.156:22
[~] Starting Script(s)
[>] Running script "nmap -vvv -p {{port}} {{ip}} -sN" on ip 45.33.32.156
Depending on the complexity of the script, results may take some time to appear.
[~] Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-01 16:40 EET
Initiating Ping Scan at 16:40
Scanning 45.33.32.156 [4 ports]
Completed Ping Scan at 16:40, 0.29s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:40
Completed Parallel DNS resolution of 1 host. at 16:40, 0.00s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]
```



```
Initiating NULL Scan at 16:40
Scanning scanme.nmap.org (45.33.32.156) [2 ports]
Completed NULL Scan at 16:40, 2.91s elapsed (2 total ports)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up, received echo-reply ttl 49 (0.19s latency).
Scanned at 2024-03-01 16:40:44 EET for 3s

PORT   STATE         SERVICE REASON
22/tcp open|filtered ssh     no-response
80/tcp open|filtered http    no-response

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

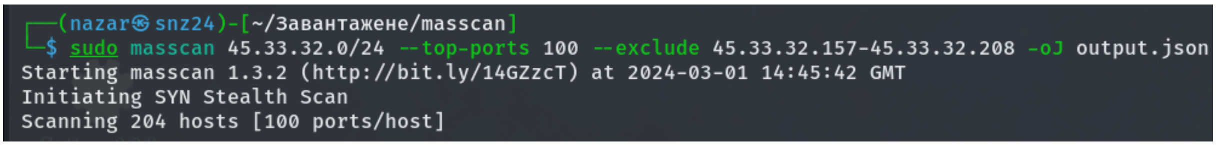
2. Проаналізувати стан мережі на можливі спроби шкідливого втручання за допомогою утиліти masscan (https://github.com/robertdavidgraham/masscan) за списком найпопулярніших портів, із використанням блокліста та збереженням результатів у форматі JSON.

- Дізнаємося IP-адресу цільової мережі:



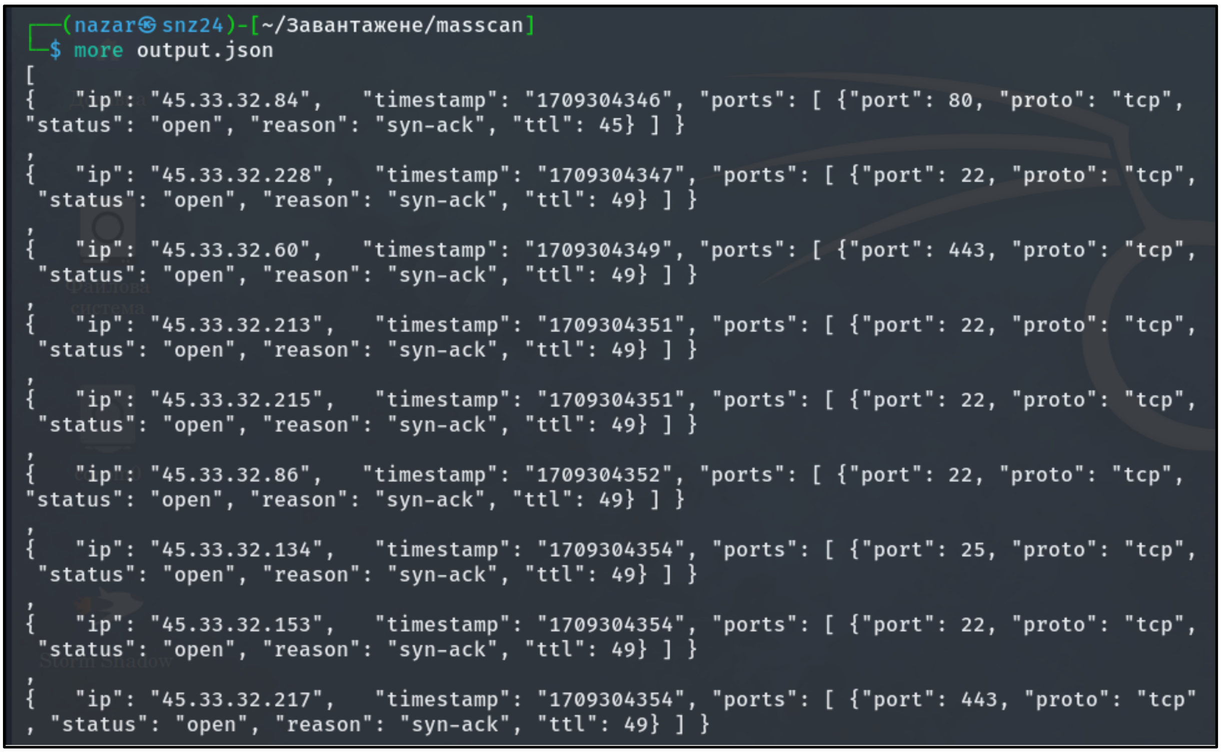
```
┌──(nazar㉿snz24)-[~/Завантажене/masscan]
└─$ nslookup scanme.nmap.org
Server:         192.168.50.1
Address:        192.168.50.1#53

Non-authoritative answer:
Name:   scanme.nmap.org
Address: 45.33.32.156
Name:   scanme.nmap.org
Address: 2600:3c01::f03c:91ff:fe18:bb2f
```

- Запустимо відповідну команду сканування:



```
┌──(nazar㉿snz24)-[~/Завантажене/masscan]
└─$ sudo masscan 45.33.32.0/24 --top-ports 100 --exclude 45.33.32.157-45.33.32.208 -oJ output.json
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2024-03-01 14:45:42 GMT
Initiating SYN Stealth Scan
Scanning 204 hosts [100 ports/host]
```

- Переглянемо вмісту вихідного файлу:



```
┌──(nazar㉿snz24)-[~/Завантажене/масscan]
└─$ more output.json
[
{   "ip": "45.33.32.84",   "timestamp": "1709304346", "ports": [ {"port": 80, "proto": "tcp",
"status": "open", "reason": "syn-ack", "ttl": 45} ] }
,
{   "ip": "45.33.32.228",   "timestamp": "1709304347", "ports": [ {"port": 22, "proto": "tcp",
 "status": "open", "reason": "syn-ack", "ttl": 49} ] }
,
{   "ip": "45.33.32.60",   "timestamp": "1709304349", "ports": [ {"port": 443, "proto": "tcp",
 "status": "open", "reason": "syn-ack", "ttl": 49} ] }
,
{   "ip": "45.33.32.213",   "timestamp": "1709304351", "ports": [ {"port": 22, "proto": "tcp",
 "status": "open", "reason": "syn-ack", "ttl": 49} ] }
,
{   "ip": "45.33.32.215",   "timestamp": "1709304351", "ports": [ {"port": 22, "proto": "tcp",
 "status": "open", "reason": "syn-ack", "ttl": 49} ] }
,
{   "ip": "45.33.32.86",   "timestamp": "1709304352", "ports": [ {"port": 22, "proto": "tcp",
"status": "open", "reason": "syn-ack", "ttl": 49} ] }
,
{   "ip": "45.33.32.134",   "timestamp": "1709304354", "ports": [ {"port": 25, "proto": "tcp",
 "status": "open", "reason": "syn-ack", "ttl": 49} ] }
,
{   "ip": "45.33.32.153",   "timestamp": "1709304354", "ports": [ {"port": 22, "proto": "tcp",
 "status": "open", "reason": "syn-ack", "ttl": 49} ] }
,
{   "ip": "45.33.32.217",   "timestamp": "1709304354", "ports": [ {"port": 443, "proto": "tcp"
, "status": "open", "reason": "syn-ack", "ttl": 49} ] }
```