Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

«Безпека комп'ютерних мереж»

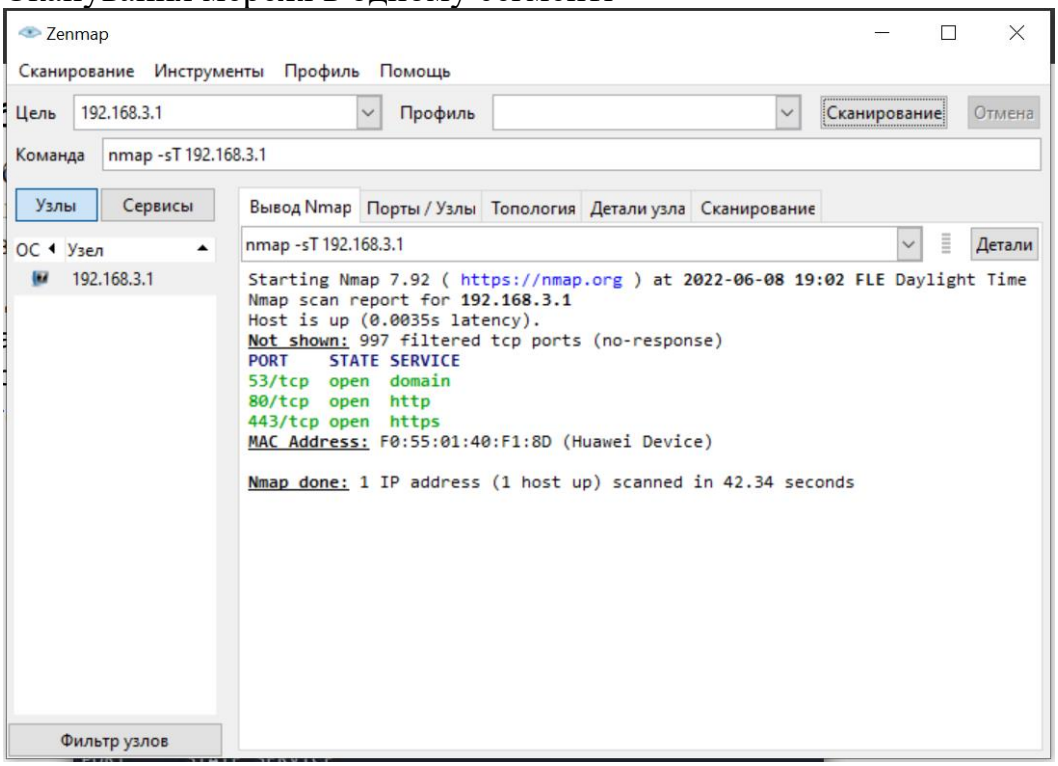
Лабораторна робота №5
«Сканування TCP/IP мереж за допомогою програми NMAP»
Варіант 2

Виконала:
студентка групи ФБ-95
Гурджия Валерія Вахтангівна

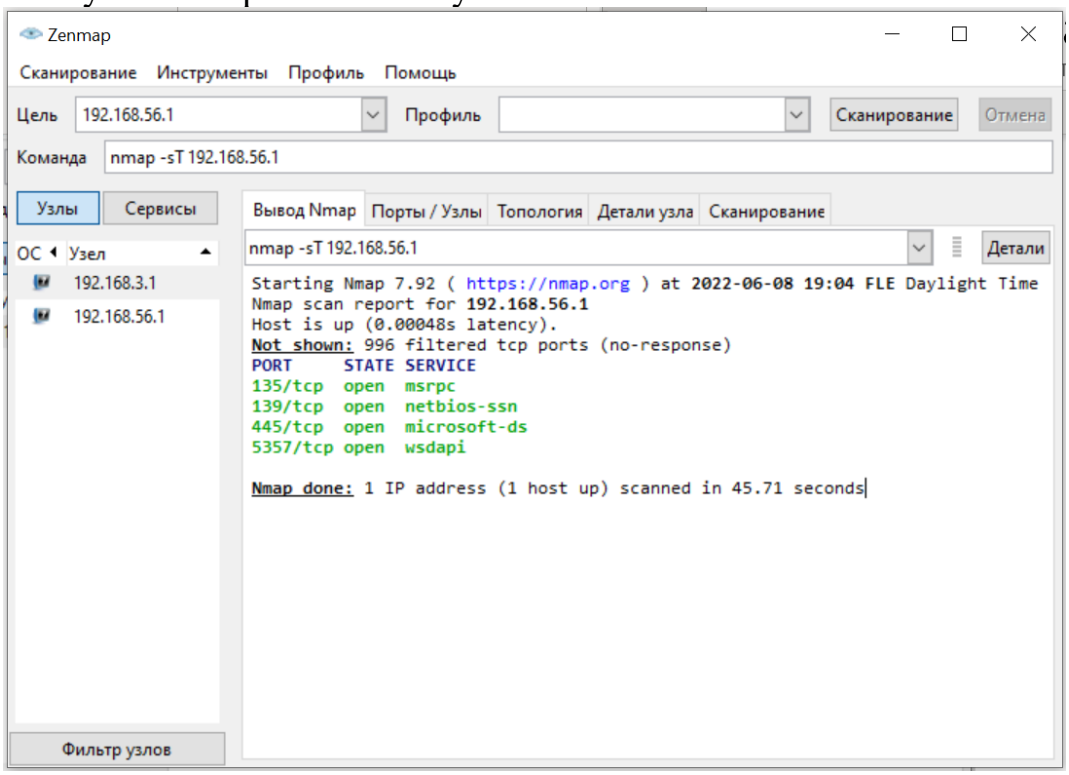
Київ-2022

2. Сканування TCP-портів цілі “повним перебором” з використанням connect().

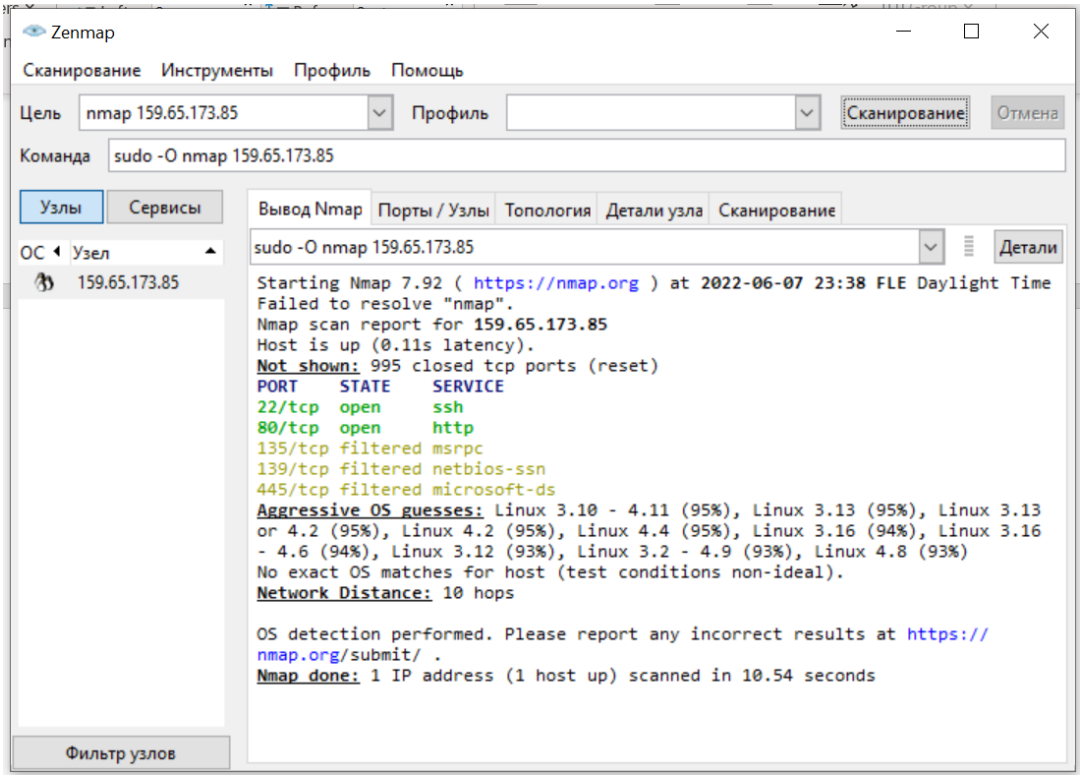
Сканування мережі в одному сегменті



Сканування мережі в іншому сегменті

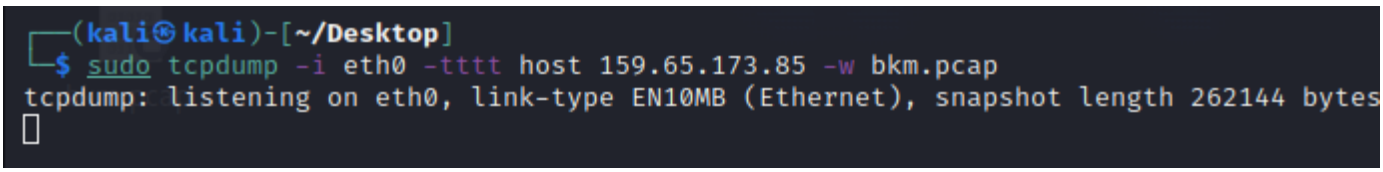


3. Ідентифікуємо ОС цілі, вказавши параметр -O.



Визначили, що ОС – Linux

4. Налаштуємо і запустимо утіліту TCPdump для фіксації своїх дій.



Опції:
-i – ім'я інтерфейсу для перехоплення пакетів.
-tttt – показує час і дату.
-w - записує виведення в файл у бінарному форматі.
Фільтри:
host— адрес вузла мережі

5. Здійснимо “приховане” (з використанням списку сервісів) сканування.

Stealth FIN сканування

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sF 159.65.173.85
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-08 09:40 EDT
Nmap scan report for 159.65.173.85
Host is up (0.00015s latency).
All 1000 scanned ports on 159.65.173.85 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```

TCP SYN сканування

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sS 159.65.173.85
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-08 10:45 EDT
Nmap scan report for 159.65.173.85
Host is up (0.018s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 6.32 seconds
```

6. Порівняння результатів.

- FIN сканування

Візьмемо до прикладу деякий відкритий порт – 80

tcp.port==80

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000036	10.0.2.15	159.65.173.85	TCP	54	59828 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
5	0.000896	159.65.173.85	10.0.2.15	TCP	60	80 → 59828 [RST] Seq=1 Win=0 Len=0
39	0.321967	10.0.2.15	159.65.173.85	TCP	54	60084 → 80 [FIN] Seq=1 Win=1024 Len=0
47	0.322393	159.65.173.85	10.0.2.15	TCP	60	80 → 60084 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Спочатку клієнт відправляє пакет з флагом ACK, потім сервер відповідає пакетом з флагом RST. Далі клієнт відправляє пакет з флагом FIN, потім сервер відповідає пакетом з флагами RST, ACK.

Візьмемо до прикладу деякий закритий порт – 81

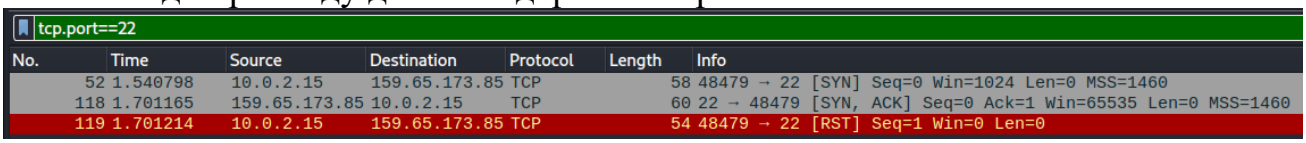
tcp.port==81

No.	Time	Source	Destination	Protocol	Length	Info
1310	0.359872	10.0.2.15	159.65.173.85	TCP	54	60084 → 81 [FIN] Seq=1 Win=1024 Len=0
1313	0.359916	159.65.…	10.0.2.15	TCP	60	81 → 60084 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Спочатку клієнт відправляє пакет з флагом FIN, потім сервер відповідає пакетом з флагами RST, ACK.

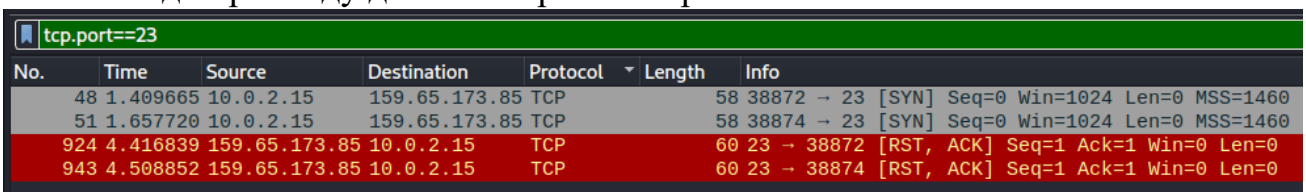
- TCP SYN сканування

Візьмемо до прикладу деякий відкритий порт – 22



Спочатку клієнт відправляє пакет з флагом SYN, потім сервер відповідає пакетом з флагами SYN, ACK, і клієнт відправляє серверу пакет з флагом RST.

Візьмемо до прикладу деякий закритий порт – 23



Спочатку клієнт відправляє пакет з флагом SYN, потім сервер відповідає пакетом з флагами RST, ACK.

Контрольні запитання

1) **За якими ознаками (якщо аналізувати трафік мережі в реальному часі) можна виявити сканування?**

Якщо у короткий проміжок часу з однієї IP-адреси відправлялись пакети на різні порти одного хоста, то це може свідчити про сканування мережі. Можна подивитися на флаги пакетів і в якій послідовності вони відправлялись, тим самим можна визначити який тип сканування відбувся.

2) **Які заходи під час сканування забезпечують непомітність?**

Збільшення затримки між проб портів. Також можна одночасно запустити кілька потоків сканування, замінюючи зворотний IP-адресу у всіх випадках, крім одного, щоб заплутати IDS та адміністратора машини. У логах IDS виявиться відразу кілька спроб сканування з різних адрес, серед яких буде лише одна справжня.

3) **Які чинники впливають на можливість відмови цілі внаслідок сканування? Як цьому запобігти?**

Відмова цілі може трапитись, якщо відбулось масове сканування.

4) **За якими ознаками за результатами сканування портів можна визначити операційну систему цілі?**

Якщо запустити команду nmap з опцією -O, то виведуться на екран найбільш близькі до правильного варіанти ОС з точністю влучення у відсотках.