

**Министерство науки и высшего образования Российской Федерации**  
федеральное государственное автономное образовательное учреждение высшего  
образования  
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**Отчет**

по лабораторной работе по теме: “Сетевая безопасность”

по дисциплине «**Информационная безопасность**»

Автор: Юрпалов С. Н.

Факультет: ИТиП

Группа: М34051



**УНИВЕРСИТЕТ ИТМО**

Санкт-Петербург 2023

### Используемое оборудование:

- 1) WSL2 Ubuntu 22.04, ip: 172.17.225.169 – производящий атаку
- 2) VirtualBox Ubuntu 22.04, ip: 192.168.56.101 – обнаруживающий атаку
- 3) Windows 11 Pro – основная OS.

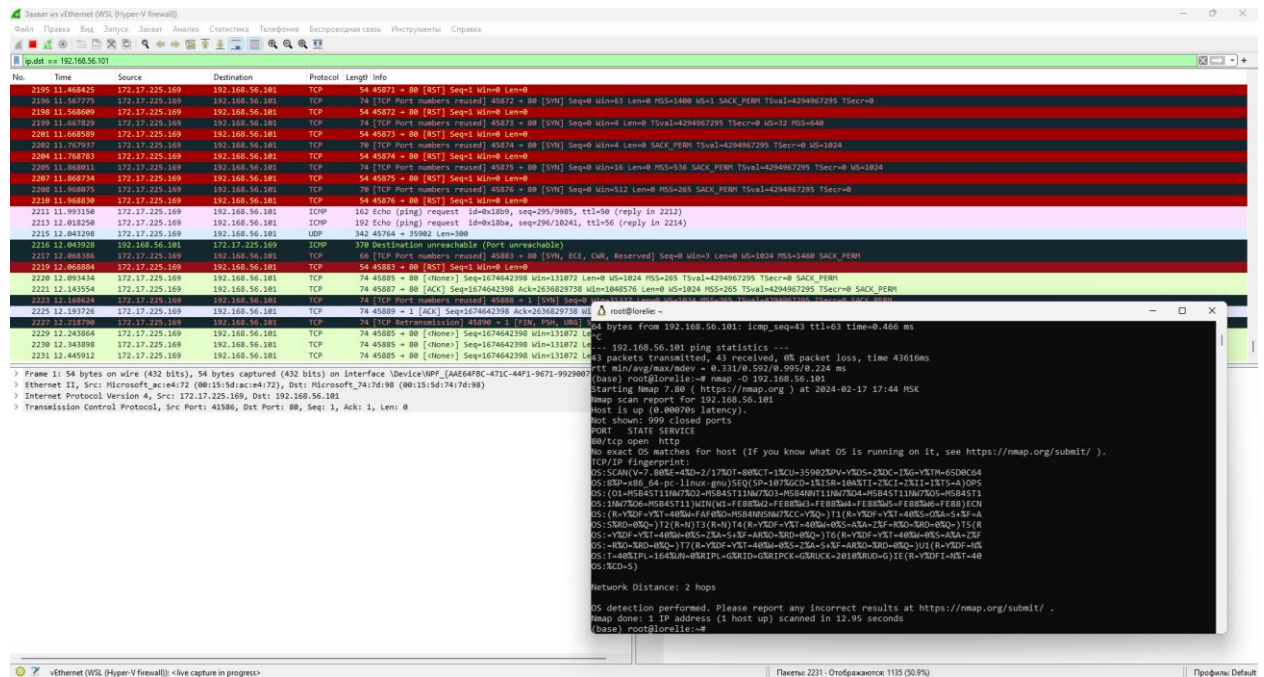
### Ход работы:

### 1) Проведение атаки

Запускаем Wireshark на хосте 3 для удобной работы в GUI, устанавливаем фильтр: `ip.dst == 192.168.56.101`, чтобы отследить пакеты, направленные на хост 2.

Запускаем nmap -O 192.168.56.101 на хосте 1.

Результат:



## 2) Анализ пакетов

В ходе анализа пакетов я отметил следующие моменты:

TCP с заголовком SYN:

Nmap отправляет пакеты TCP SYN на порты целевой машины.

Если порт открыт, целевая машина обычно отвечает пакетом SYN-ACK.

Этот первоначальный обмен пакетами SYN и SYN-ACK используется для определения открытых портов на целевой машине.

1	0.000000	172.17.225.169	192.168.56.101	TCP	54 41586 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
2	0.000000	172.17.225.169	192.168.56.101	TCP	58 41586 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3	0.000000	172.17.225.169	192.168.56.101	ICMP	42 Echo (ping) request id=0x5ac5, seq=0/0, ttl=41 (reply in 6)
4	0.000000	172.17.225.169	192.168.56.101	ICMP	54 Timestamp request id=0xf64d, seq=0/0, ttl=43
20	1.170016	172.17.225.169	192.168.56.101	TCP	58 41842 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21	1.170024	172.17.225.169	192.168.56.101	TCP	58 41842 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22	1.170024	172.17.225.169	192.168.56.101	TCP	58 41842 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
23	1.170025	172.17.225.169	192.168.56.101	TCP	58 41842 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24	1.170031	172.17.225.169	192.168.56.101	TCP	58 41842 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
25	1.170031	172.17.225.169	192.168.56.101	TCP	58 41842 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
26	1.170064	172.17.225.169	192.168.56.101	TCP	58 41842 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
27	1.170064	172.17.225.169	192.168.56.101	TCP	58 41842 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
28	1.170064	172.17.225.169	192.168.56.101	TCP	58 41842 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
29	1.170064	172.17.225.169	192.168.56.101	TCP	58 41842 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
40	1.171638	172.17.225.169	192.168.56.101	TCP	58 41842 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
41	1.171657	172.17.225.169	192.168.56.101	TCP	58 41842 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
42	1.171657	172.17.225.169	192.168.56.101	TCP	58 41842 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
43	1.171660	172.17.225.169	192.168.56.101	TCP	58 41842 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
44	1.171663	172.17.225.169	192.168.56.101	TCP	58 41842 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
45	1.171663	172.17.225.169	192.168.56.101	TCP	58 41842 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
46	1.171669	172.17.225.169	192.168.56.101	TCP	58 41842 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
47	1.171669	172.17.225.169	192.168.56.101	TCP	58 41842 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
48	1.171669	172.17.225.169	192.168.56.101	TCP	58 41842 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
49	1.171682	172.17.225.169	192.168.56.101	TCP	58 41842 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
50	1.171682	172.17.225.169	192.168.56.101	TCP	58 41842 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
51	1.171682	172.17.225.169	192.168.56.101	TCP	58 41842 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
52	1.171697	172.17.225.169	192.168.56.101	TCP	58 41842 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
53	1.171697	172.17.225.169	192.168.56.101	TCP	58 41842 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
54	1.171704	172.17.225.169	192.168.56.101	TCP	58 41842 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
55	1.171704	172.17.225.169	192.168.56.101	TCP	58 41842 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

TCP с заголовком ACK:

Nmap отправляет пакеты TCP ACK на порты целевой машины.

Если порт не фильтруется, целевая машина отвечает пакетом RST (сброс).

Это помогает Nmap отличить открытые порты от портов, которые фильтруются брандмауэром.

1983	1.234234	172.17.225.169	192.168.56.101	TCP	58 41842 → 2001 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1984	1.234234	172.17.225.169	192.168.56.101	TCP	58 41842 → 79 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1985	1.234234	172.17.225.169	192.168.56.101	TCP	58 41842 → 5550 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1986	1.234234	172.17.225.169	192.168.56.101	TCP	58 41842 → 901 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1987	1.234234	172.17.225.169	192.168.56.101	TCP	58 41842 → 1198 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1988	1.234234	172.17.225.169	192.168.56.101	TCP	58 41842 → 1028 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1989	1.234234	172.17.225.169	192.168.56.101	TCP	58 41842 → 1031 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1990	1.234234	172.17.225.169	192.168.56.101	TCP	58 41842 → 7004 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2021	1.409647	172.17.225.169	192.168.56.101	TCP	74 45871 → 80 [SYN] Seq=0 Win=1 Len=0 WS=1024 MSS=1460 TSval=4294967295 TSecr=0 SACK_PERM
2023	1.410375	172.17.225.169	192.168.56.101	TCP	54 45871 → 80 [RST] Seq=1 Win=0 Len=0
2024	1.509728	172.17.225.169	192.168.56.101	TCP	74 45872 → 80 [SYN] Seq=0 Win=63 Len=0 MSS=1400 WS=1 SACK_PERM TSval=4294967295 TSecr=0
2026	1.510532	172.17.225.169	192.168.56.101	TCP	54 45872 → 80 [RST] Seq=1 Win=0 Len=0
2027	1.609787	172.17.225.169	192.168.56.101	TCP	74 45873 → 80 [SYN] Seq=0 Win=4 Len=0 TSval=4294967295 TSecr=0 WS=32 MSS=640
2029	1.610502	172.17.225.169	192.168.56.101	TCP	54 45873 → 80 [RST] Seq=1 Win=0 Len=0
2030	1.709869	172.17.225.169	192.168.56.101	TCP	70 45874 → 80 [SYN] Seq=0 Win=4 Len=0 SACK_PERM TSval=4294967295 TSecr=0 WS=1024
2032	1.710628	172.17.225.169	192.168.56.101	TCP	54 45874 → 80 [RST] Seq=1 Win=0 Len=0
2033	1.809993	172.17.225.169	192.168.56.101	TCP	74 45875 → 80 [SYN] Seq=0 Win=16 Len=0 MSS=536 SACK_PERM TSval=4294967295 TSecr=0 WS=1024
2035	1.810742	172.17.225.169	192.168.56.101	TCP	54 45875 → 80 [RST] Seq=1 Win=0 Len=0
2036	1.910043	172.17.225.169	192.168.56.101	TCP	70 45876 → 80 [SYN] Seq=0 Win=512 Len=0 MSS=265 SACK_PERM TSval=4294967295 TSecr=0
2038	1.910647	172.17.225.169	192.168.56.101	TCP	54 45876 → 80 [RST] Seq=1 Win=0 Len=0

### 3) Обнаружение атаки

На хосте 2 создадим nmap\_os\_detection.rules:

alert tcp any any -> 192.168.56.101 any (msg:"Nmap OS Detection"; dsize:0;

flags:\*SA; detection\_filter: track by\_dst, count 100, seconds 5; sid:100001; rev:1;)

Уведомляем, если на хост поступило 100 и более пакетов SYN и/или АСК за 5 секунд.

Запустим snort с этим правилом:

```
snort -c snort_defaults.lua -R nmap_os_detection.rules -A alert_fast -s 65535 -k none -i enp0s8
```

-c snort\_defaults.lua – стандартный файл конфигурации

-R nmap\_os\_detection.rules – наш файл правил

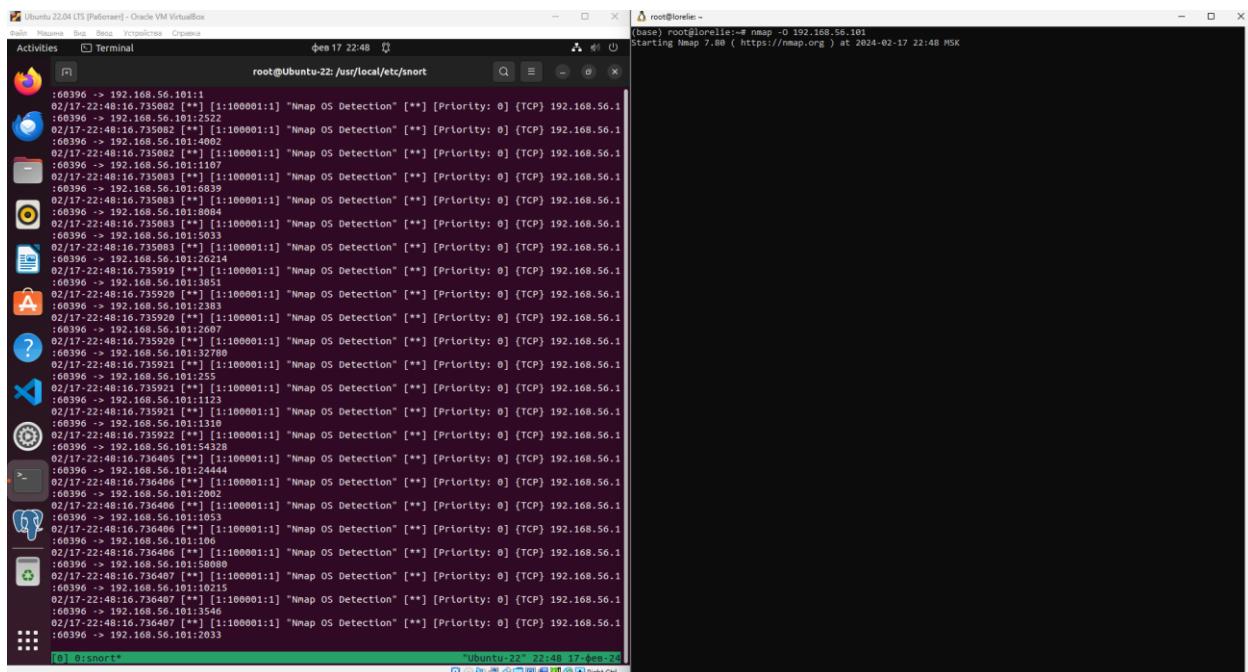
-A alert\_fast – правило кратких оповещений

-s 65535 – максимальная snaplen

-k none – отключим checksum

-i enp0s8 – наш интерфейс ethernet – виртуальный адаптер хоста

На хосте 1 запустим атаку, snort уведомляет о ней.



Теперь запустим telnet также использующий tcp, уведомления от snort нет.

```
Ubuntu 22.04 LTS [Focal] - Oracle VM VirtualBox
Activities Home Run Search Applications Window
root@Ubuntu-22: /usr/local/etc/snort

:60422 -> 192.168.56.101:80
02/17-22:48:19.804209 [**] [1:1000001:1] "Nmap OS Detection" [**] [Priority: 0] (TCP) 192.168.56.1
:60426 -> 192.168.56.101:80
02/17-22:48:19.809372 [**] [1:1000001:1] "Nmap OS Detection" [**] [Priority: 0] (TCP) 192.168.56.1
:60427 -> 192.168.56.101:1
02/17-22:48:19.854733 [**] [1:1000001:1] "Nmap OS Detection" [**] [Priority: 0] (TCP) 192.168.56.1
:60428 -> 192.168.56.101:1
02/17-22:48:21.253161 [**] [1:1000001:1] "Nmap OS Detection" [**] [Priority: 0] (TCP) 192.168.56.1
:60410 -> 192.168.56.101:80
02/17-22:48:21.353344 [**] [1:1000001:1] "Nmap OS Detection" [**] [Priority: 0] (TCP) 192.168.56.1
:60411 -> 192.168.56.101:80
02/17-22:48:21.453510 [**] [1:1000001:1] "Nmap OS Detection" [**] [Priority: 0] (TCP) 192.168.56.1
:60412 -> 192.168.56.101:80
02/17-22:48:21.553432 [**] [1:1000001:1] "Nmap OS Detection" [**] [Priority: 0] (TCP) 192.168.56.1
:60413 -> 192.168.56.101:80
02/17-22:48:21.653545 [**] [1:1000001:1] "Nmap OS Detection" [**] [Priority: 0] (TCP) 192.168.56.1
:60414 -> 192.168.56.101:80
02/17-22:48:21.754009 [**] [1:1000001:1] "Nmap OS Detection" [**] [Priority: 0] (TCP) 192.168.56.1
:60415 -> 192.168.56.101:80
02/17-22:48:21.854183 [**] [1:1000001:1] "Nmap OS Detection" [**] [Priority: 0] (TCP) 192.168.56.1
:60422 -> 192.168.56.101:80
02/17-22:48:21.929303 [**] [1:1000001:1] "Nmap OS Detection" [**] [Priority: 0] (TCP) 192.168.56.1
:60426 -> 192.168.56.101:80
02/17-22:48:21.954435 [**] [1:1000001:1] "Nmap OS Detection" [**] [Priority: 0] (TCP) 192.168.56.1
:60427 -> 192.168.56.101:1
02/17-22:48:21.979560 [**] [1:1000001:1] "Nmap OS Detection" [**] [Priority: 0] (TCP) 192.168.56.1
:60428 -> 192.168.56.101:1
02/17-22:48:24.879835 [**] [1:1000001:1] "Nmap OS Detection" [**] [Priority: 0] (TCP) 192.168.56.1
:60410 -> 192.168.56.101:80
02/17-22:48:24.979748 [**] [1:1000001:1] "Nmap OS Detection" [**] [Priority: 0] (TCP) 192.168.56.1
:60411 -> 192.168.56.101:80
02/17-22:48:25.079837 [**] [1:1000001:1] "Nmap OS Detection" [**] [Priority: 0] (TCP) 192.168.56.1
:60412 -> 192.168.56.101:80
02/17-22:48:25.180133 [**] [1:1000001:1] "Nmap OS Detection" [**] [Priority: 0] (TCP) 192.168.56.1
:60413 -> 192.168.56.101:80
02/17-22:48:25.280441 [**] [1:1000001:1] "Nmap OS Detection" [**] [Priority: 0] (TCP) 192.168.56.1
:60414 -> 192.168.56.101:80
02/17-22:48:25.380360 [**] [1:1000001:1] "Nmap OS Detection" [**] [Priority: 0] (TCP) 192.168.56.1
:60415 -> 192.168.56.101:80
02/17-22:48:25.480802 [**] [1:1000001:1] "Nmap OS Detection" [**] [Priority: 0] (TCP) 192.168.56.1
:60422 -> 192.168.56.101:80
02/17-22:48:25.556215 [**] [1:1000001:1] "Nmap OS Detection" [**] [Priority: 0] (TCP) 192.168.56.1
:60426 -> 192.168.56.101:80
02/17-22:48:25.581410 [**] [1:1000001:1] "Nmap OS Detection" [**] [Priority: 0] (TCP) 192.168.56.1
:60427 -> 192.168.56.101:1
02/17-22:48:25.606392 [**] [1:1000001:1] "Nmap OS Detection" [**] [Priority: 0] (TCP) 192.168.56.1
:60428 -> 192.168.56.101:1

root@snort*
Ubuntu-22 72:49 17-Jun-24
Login Ctrl
```

```
root@lorille:~# telnet 192.168.56.101 80
Trying 192.168.56.101...
Connected to 192.168.56.101.
Escape character is '^['.
```