

## Лабораторная работа

### Метод «зомби» сканирования при помощи Nmap

Процесс зомби сканирования заключается в первоначальном поиске «зомби» хоста под IP адресом которого будет происходить сканирование портов на атакуемом компьютере.

Суть поиска заключается в отправке пакетов SYN/ACK на предполагаемого «зомби», который в свою очередь должен отвечать на такие пакеты RST, а IPID каждого пакета должен увеличиваться на одну единицу в каждом новом пакете.

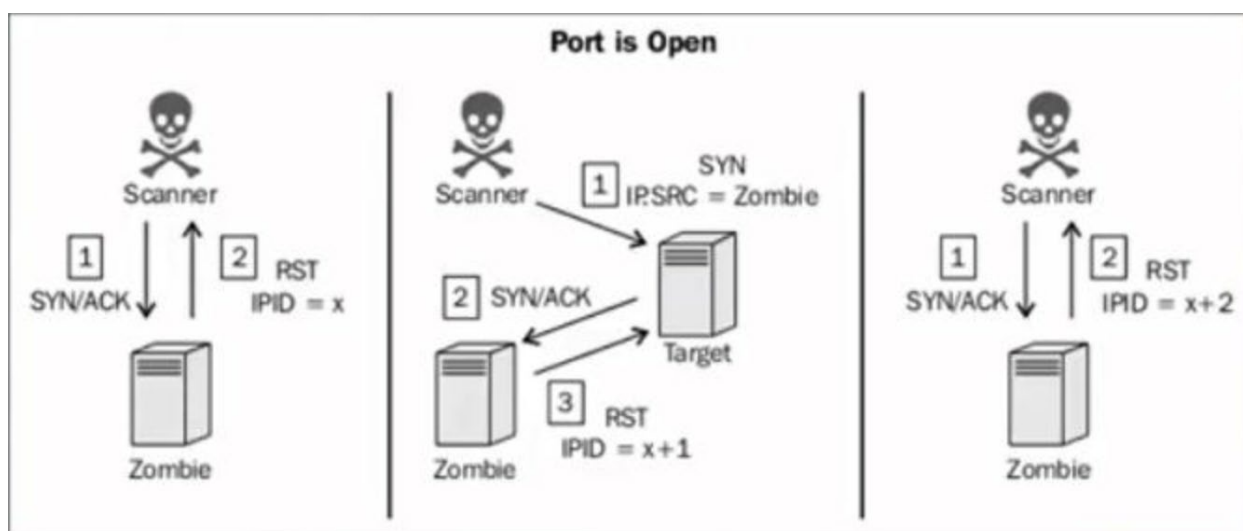


Рисунок 2 – Пример работы «зомби» сканирования при открытом порте

Если порт целевого хоста, не открыт, то тогда целевой хост будет посылать RST в ответ на попытку соединения при помощи «зомби» машины, но при получении пакета RST IPID пакетов, которые были получены зомби не изменится.

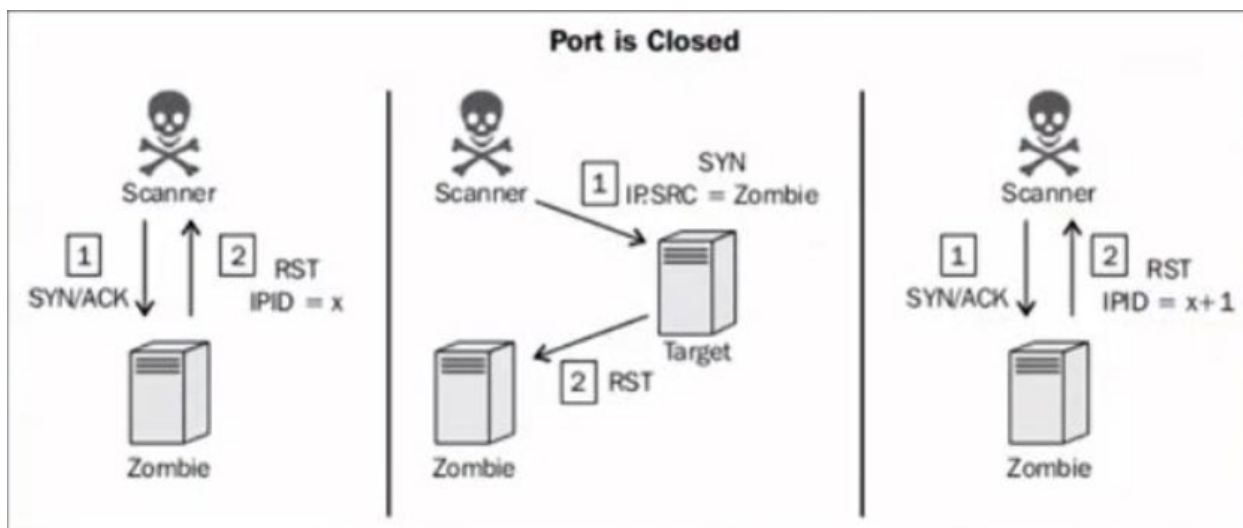


Рисунок 3 – Пример работы «зомби» сканирования при закрытом порте на целевом хосте

Для моделирования данной атаки использовался стенд, состоящий из 3 виртуальных машин: две из которых являлись машинами под управлением ОС семейства Windows, а именно Windows 10 и одна с системой Ubuntu.

Первоначально требуется отыскать «зомби» через которого будет осуществляться сканирование и чей ip-адрес требуется использовать.

Для этого будет использована утилита Nmap, а также Wireshark для анализа трафика, которые будут приходить на атакуемые машины. Первостепенная задача перед началом сканирования портов заключается в получении IP адресов машин, на которые будет совершаться атака.

```
Адаптер Ethernet Ethernet0:

DNS-суффикс подключения . . . . . : localdomain
Локальный IPv6-адрес канала . . . : fe80::7918:7e3e:c6ac:f395%5
IPv4-адрес. . . . . : 192.168.63.136
Маска подсети . . . . . : 255.255.255.0
Основной шлюз. . . . . : 192.168.63.2

Адаптер Ethernet Ethernet0:

DNS-суффикс подключения . . . . . : localdomain
Локальный IPv6-адрес канала . . . : fe80::1ff6:bc48:3d22:8120%4
IPv4-адрес. . . . . : 192.168.63.137
Маска подсети . . . . . : 255.255.255.0
Основной шлюз. . . . . : 192.168.63.2
```

Рисунок 4 – IP адреса машин, на которые будет совершаться атака.

Для начала сканирования требуется прописать команду:

```
nmap -Pn -P 445 --scanflags RST "ip-адрес будущей зомби машины"
```

Далее требуется прописать команду:

```
nmap -Pn -P 445 --scanflags SYNACK "ip адрес зомби машины"
```

4724	268.800210	192.168.63.136	192.168.63.131	TCP	54 1087 → 63697 [RST] Seq=1 Win=0 Len=0
4725	268.800263	192.168.63.136	192.168.63.131	TCP	54 10629 → 63697 [RST] Seq=1 Win=0 Len=0
4726	268.800295	192.168.63.136	192.168.63.131	TCP	54 5958 → 63697 [RST] Seq=1 Win=0 Len=0
4727	268.800339	192.168.63.136	192.168.63.131	TCP	54 7025 → 63697 [RST] Seq=1 Win=0 Len=0
4728	268.800414	192.168.63.136	192.168.63.131	TCP	54 2557 → 63697 [RST] Seq=1 Win=0 Len=0
4729	268.800450	192.168.63.136	192.168.63.131	TCP	54 5666 → 63697 [RST] Seq=1 Win=0 Len=0
4730	268.800748	192.168.63.131	192.168.63.136	TCP	60 63697 → 1247 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0 MSS=1460
4731	268.800764	192.168.63.136	192.168.63.131	TCP	54 1247 → 63697 [RST] Seq=1 Win=0 Len=0
4732	268.800838	192.168.63.131	192.168.63.136	TCP	60 63697 → 10000 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0 MSS=1460
4733	268.800850	192.168.63.136	192.168.63.131	TCP	54 10000 → 63697 [RST] Seq=1 Win=0 Len=0
4734	268.801063	192.168.63.131	192.168.63.136	TCP	60 63697 → 8654 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0 MSS=1460
4735	268.801076	192.168.63.136	192.168.63.131	TCP	54 8654 → 63697 [RST] Seq=1 Win=0 Len=0
4736	268.801138	192.168.63.131	192.168.63.136	TCP	60 63697 → 9900 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0 MSS=1460
4737	268.801148	192.168.63.136	192.168.63.131	TCP	54 9900 → 63697 [RST] Seq=1 Win=0 Len=0
4738	268.801156	192.168.63.131	192.168.63.136	TCP	60 63697 → 1 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0 MSS=1460
4739	268.801368	192.168.63.136	192.168.63.131	TCP	54 1 → 63697 [RST] Seq=1 Win=0 Len=0
4740	268.801430	192.168.63.131	192.168.63.136	TCP	60 63697 → 7999 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0 MSS=1460
4741	268.801441	192.168.63.136	192.168.63.131	TCP	54 7999 → 63697 [RST] Seq=1 Win=0 Len=0
4742	268.801646	192.168.63.131	192.168.63.136	TCP	60 63697 → 1010 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0 MSS=1460
4743	268.801653	192.168.63.136	192.168.63.131	TCP	54 1010 → 63697 [RST] Seq=1 Win=0 Len=0
4744	268.801752	192.168.63.131	192.168.63.136	TCP	60 63697 → 12000 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0 MSS=1460

> Frame 4730: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF\_{4C525CC3-CA8E-49B1-B6D6-000000000000} (00:0c:29:7e:31:dc), Dst: VMware\_e5:e0:7c (00:0c:29:e5:e0:7c)

Ethernet II, Src: VMware\_7e:31:dc (00:0c:29:7e:31:dc), Dst: VMware\_e5:e0:7c (00:0c:29:e5:e0:7c)

Internet Protocol Version 4, Src: 192.168.63.131, Dst: 192.168.63.136

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 44

Identification: 0x0609 (38409)

> 000. .... = Flags: 0x0

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 57

Protocol: TCP (6)

Header Checksum: 0xeb66 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.63.131

Destination Address: 192.168.63.136

Transmission Control Protocol, Src Port: 63697, Dst Port: 1247, Seq: 0, Ack: 1, Len: 0

0000 00 0c 29 e5 e0 7c 00 0c 29 7e 31 dc 00 00 45 00 .....>1...E  
0010 00 2c 96 09 00 00 39 06 eb 66 0a a8 3f 81 c0 a8 .....f033  
0020 3f 88 f8 d1 04 df a8 65 6c 7b 6e 77 cf f4 60 12 .....1(m...  
0030 04 00 42 bc 00 00 02 04 05 b4 00 00 .....0.....

Рисунок 5 – Результат отправки пакетов типа SYNACK на «зомби» машину

Как видно из рисунка 5 «зомби» машина на пакеты SYNACK, которые были посланы Ubuntu отвечает RST, что и требуется от данной машины. Также если просмотреть пакеты RST, то можно будет увидеть, что ID каждого такого пакета идет по порядку, что также является обязательным фактором для выполнения данной атаки.

> Frame 4724: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{4C525CC3-CA8E-49B1-B6D6-000000000000} (00:0c:29:7e:31:dc), Dst: VMware_e5:e0:7c (00:0c:29:e5:e0:7c)
> Ethernet II, Src: VMware_e5:e0:7c (00:0c:29:e5:e0:7c), Dst: VMware_7e:31:dc (00:0c:29:7e:31:dc)
> Internet Protocol Version 4, Src: 192.168.63.136, Dst: 192.168.63.131
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x03d3 (979)

> Frame 4725: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{4C525CC3-CA8E-49B1-B6D6-000000000000} (00:0c:29:7e:31:dc), Dst: VMware_e5:e0:7c (00:0c:29:e5:e0:7c)
> Ethernet II, Src: VMware_e5:e0:7c (00:0c:29:e5:e0:7c), Dst: VMware_7e:31:dc (00:0c:29:7e:31:dc)
> Internet Protocol Version 4, Src: 192.168.63.136, Dst: 192.168.63.131
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x03d4 (980)

Рисунок 6 – Отображение ID пакетов RST

После того как была найдена машина, которая на пакеты SYNACK отвечает RST и ID этих пакетов идёт по порядку происходит сканирование портов на цель с заменой исходного IP адреса на IP адрес «зомби» машины. Для этого требуется прописать следующую команду в командной строке:

```
nmap -P0 -p- -sI "ip-зомби машины" "ip-атакуемой машины"
```

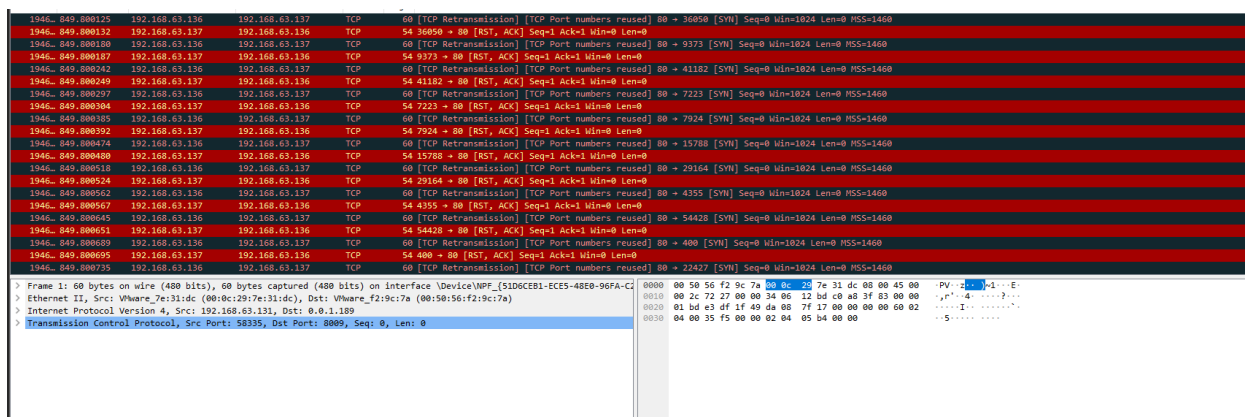


Рисунок 7 – Результат сканирования портов с подменой IP адреса

После осуществления сканирования вы получите информацию по всем открытым портам на атакуемой машине.

```
Nmap scan report for 192.168.63.137
Host is up (0.053s latency).
Not shown: 65522 closed|filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5040/tcp   open  unknown
5357/tcp   open  wsdaapi
7680/tcp   open  pando-pub
49664/tcp  open  unknown
49665/tcp  open  unknown
49666/tcp  open  unknown
49667/tcp  open  unknown
49668/tcp  open  unknown
49669/tcp  open  unknown
49670/tcp  open  unknown
MAC Address: 00:0C:29:AF:34:D8 (VMware)
```

Рисунок 8 – Результат проведенного сканирования

После успешного проведения сканирования, запустите брандмауэр на зомби и атакуемой машинах и повторите первый этап с отправкой пакетов типа RST.

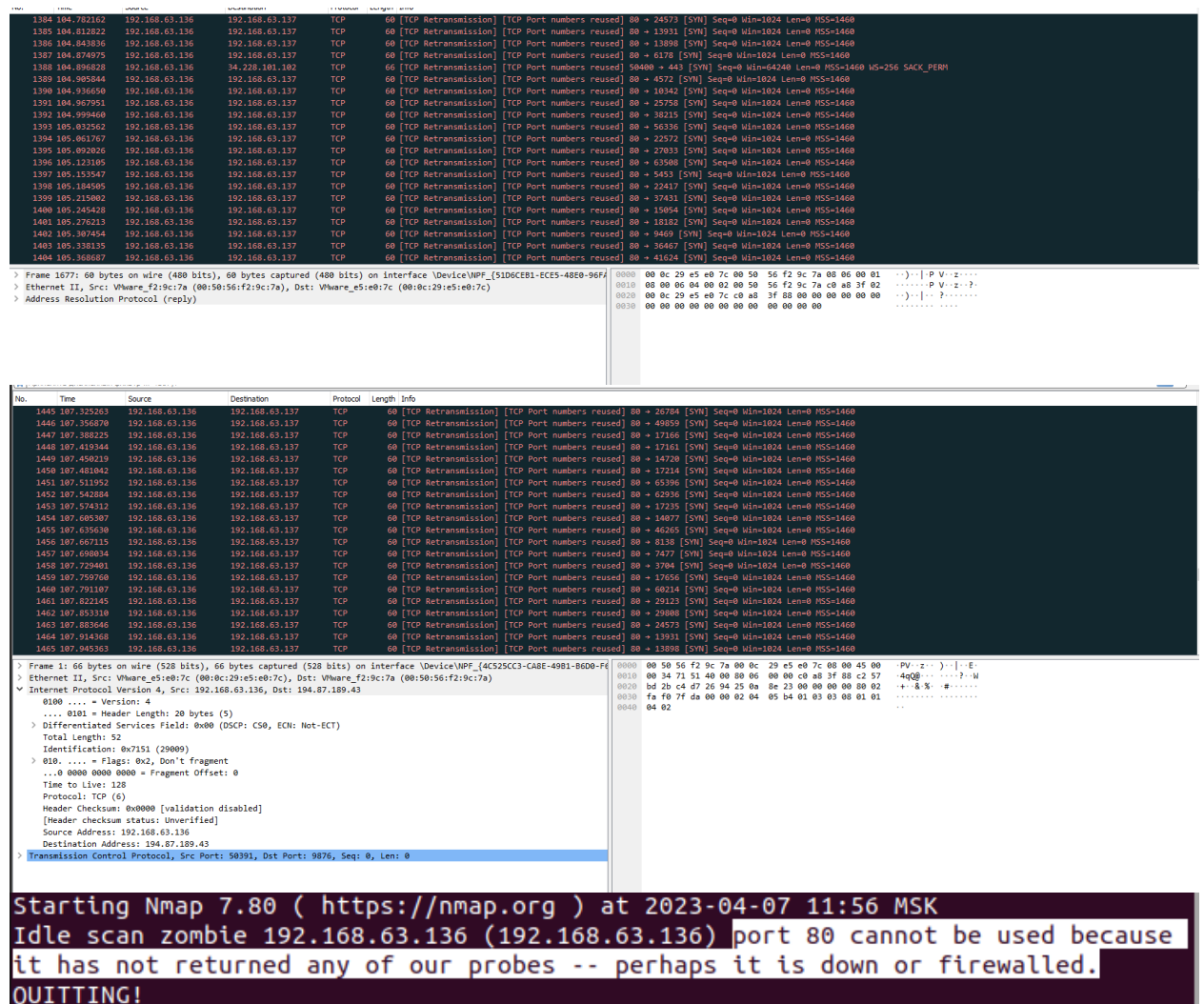


Рисунок 9 – Результат сканирования портов с включенным брандмауэром.

Как видно из рисунка 9 весь процесс сканирования останавливается благодаря работе брандмауэров на обеих машинах под управлением Windows.