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.

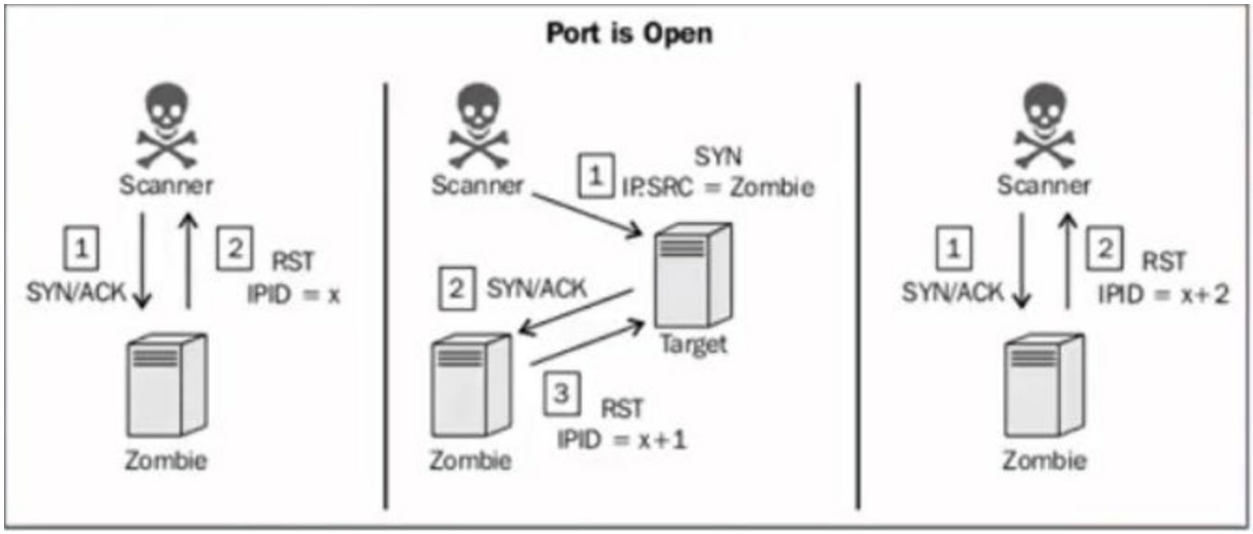

Рисунок 2 – Пример работы «зомби» сканирования при открытом порте

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.

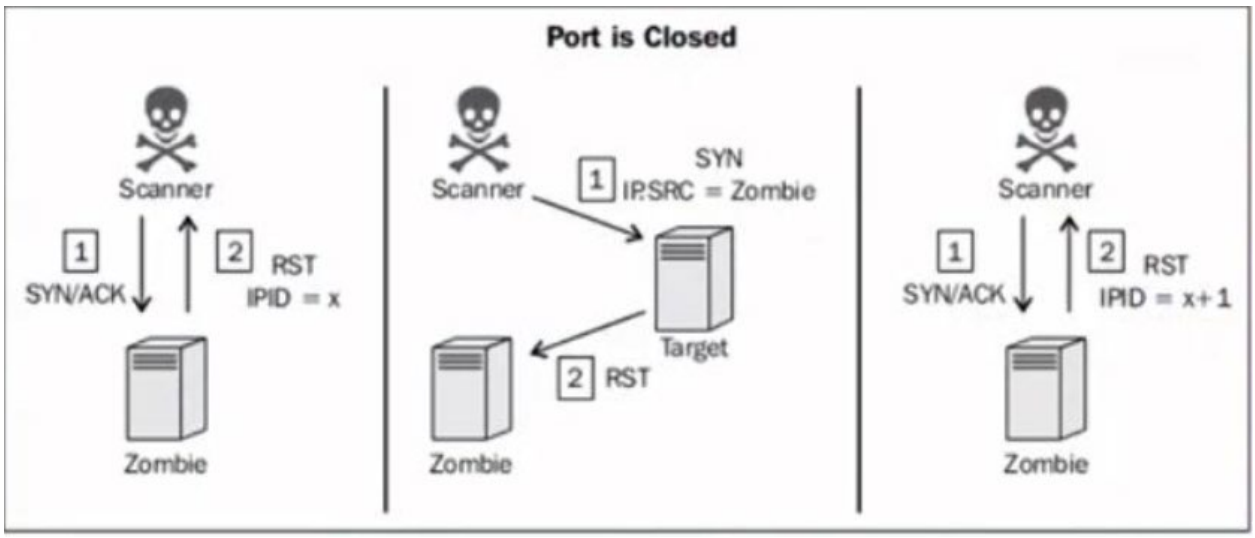

Рисунок 3 – Пример работы «зомби» сканирования при закрытом порте на целевом хосте

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"
```

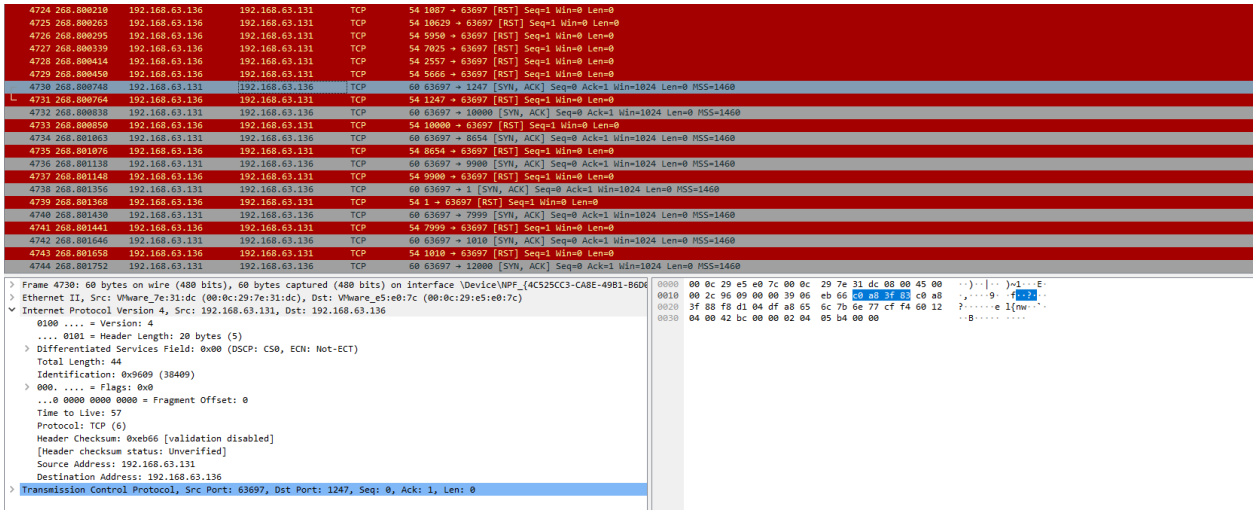

Рисунок 5 – Результат отправки пакетов типа SYNACK на «зомби» машину

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.

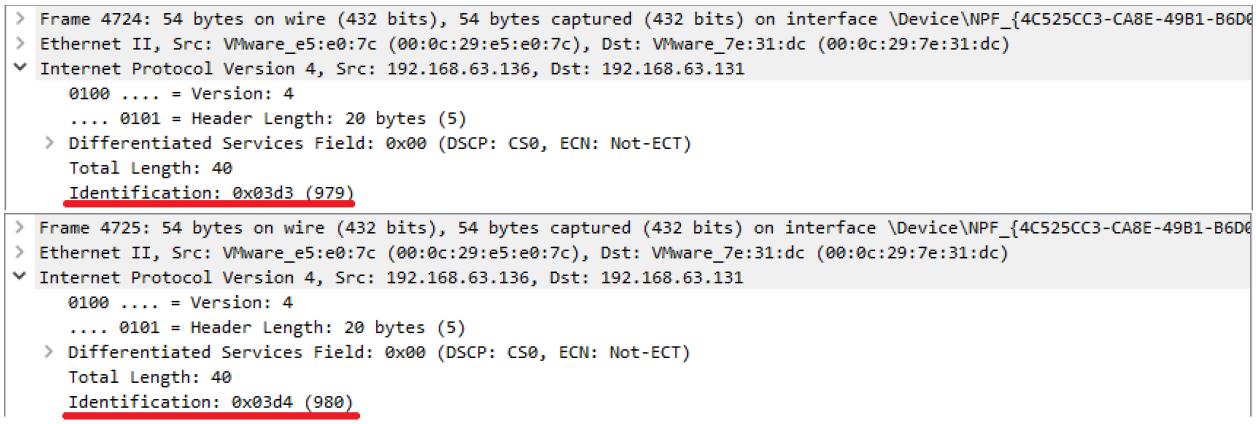

Рисунок 6 – Отображение ID пакетов RST

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"
```

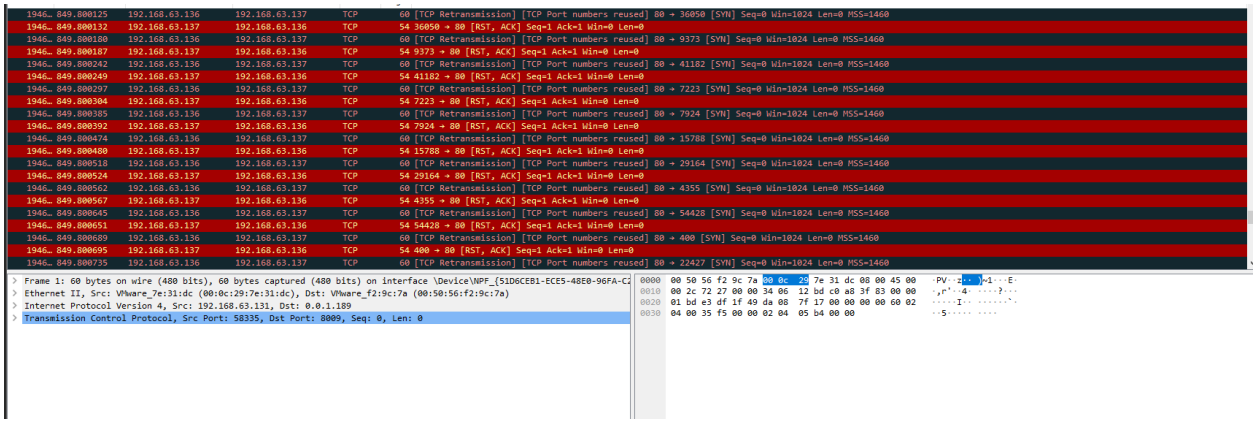

Рисунок 7 – Результат сканирования портов с подменой IP адреса

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  wsdapi
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.

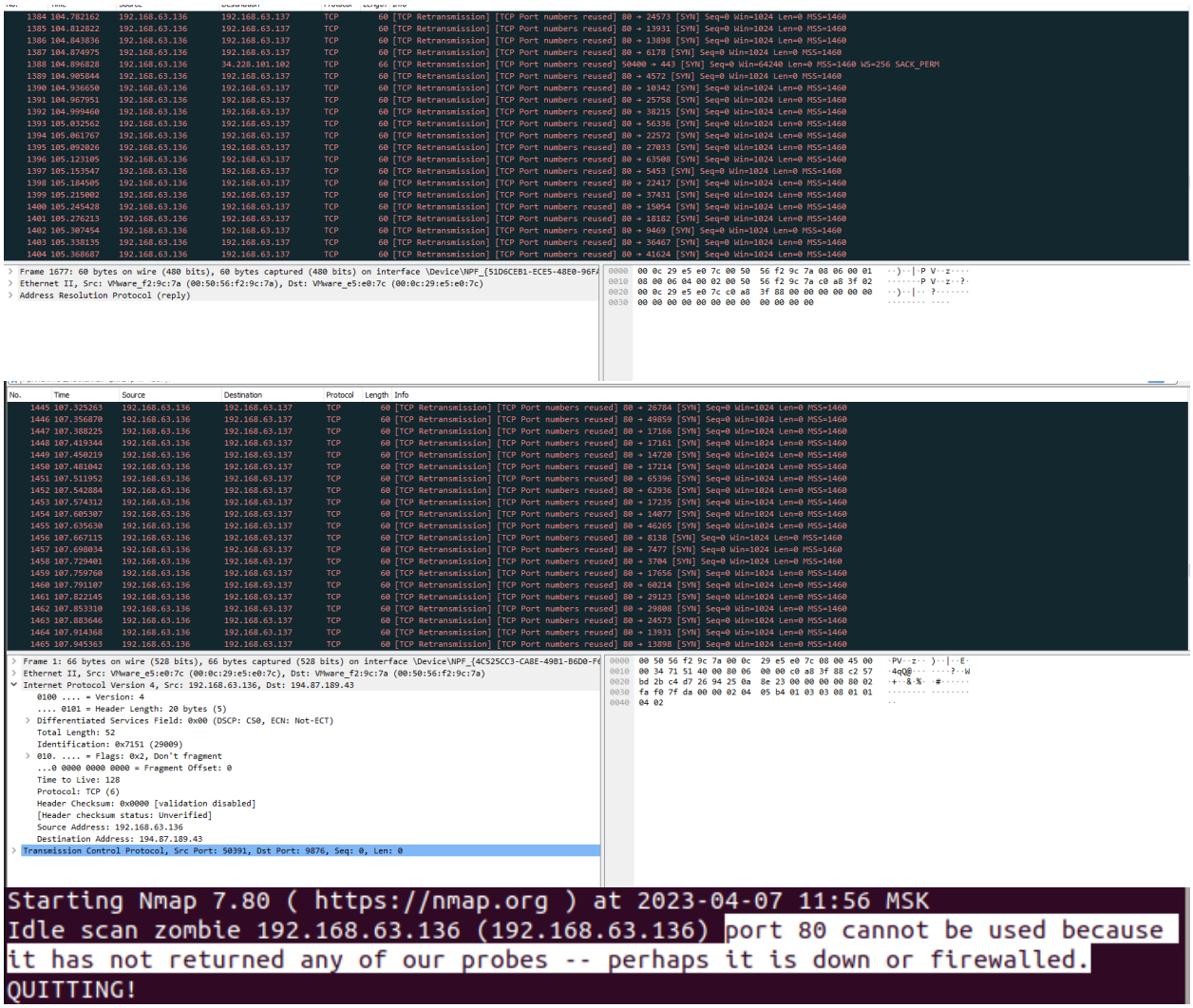

Рисунок 9 – Результат сканирования портов с включенным брандмауэром.

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