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.

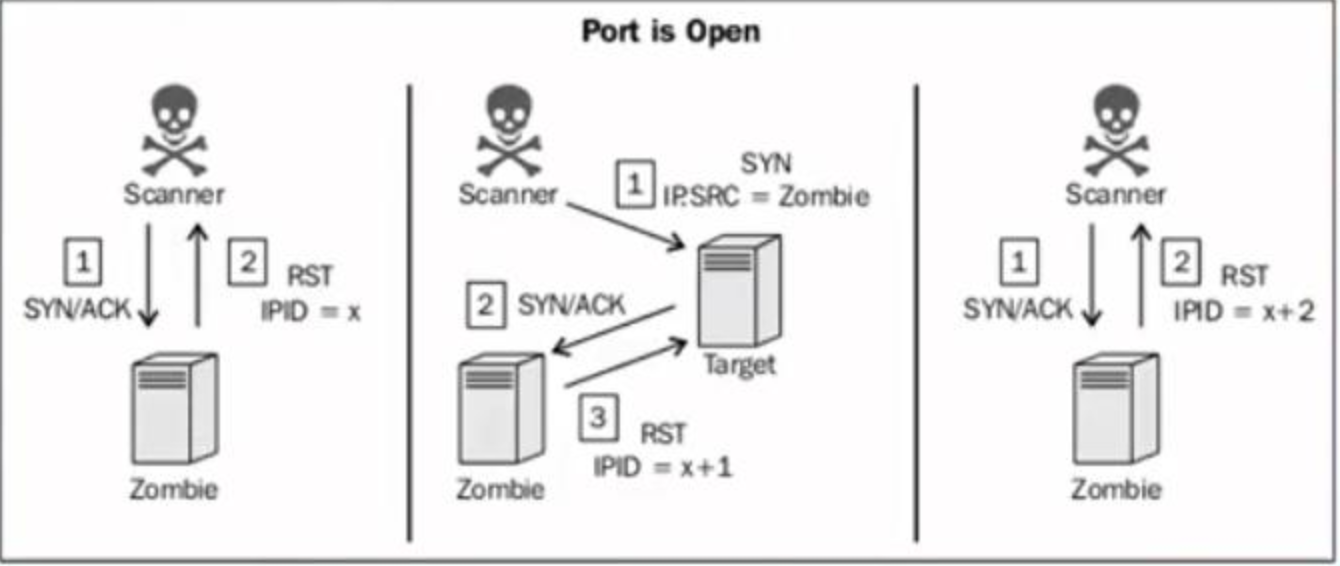


Рисунок 2 – Пример работы «зомби» сканирования при открытом порте

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.

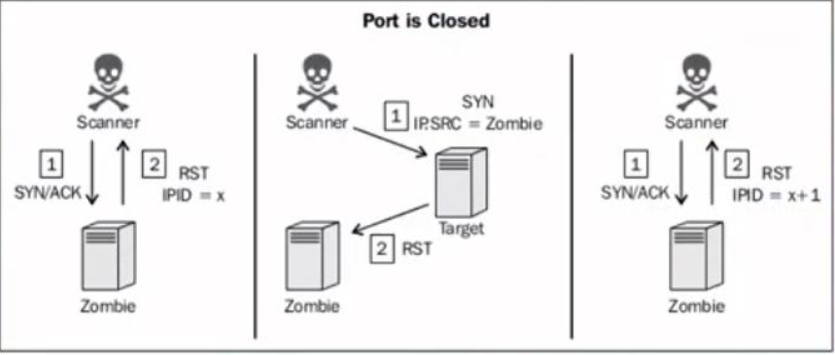
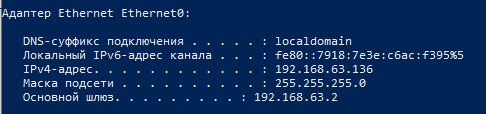


Рисунок 3 – Пример работы «зомби» сканирования при закрытом порте на целевом хосте

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.



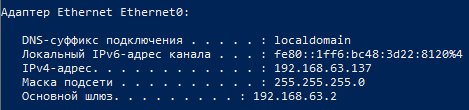


Рисунок 4 – IP адреса машин, на которые будет совершаться атака.

Для начала сканирования требуется прописать команду:



Далее требуется прописать команду:



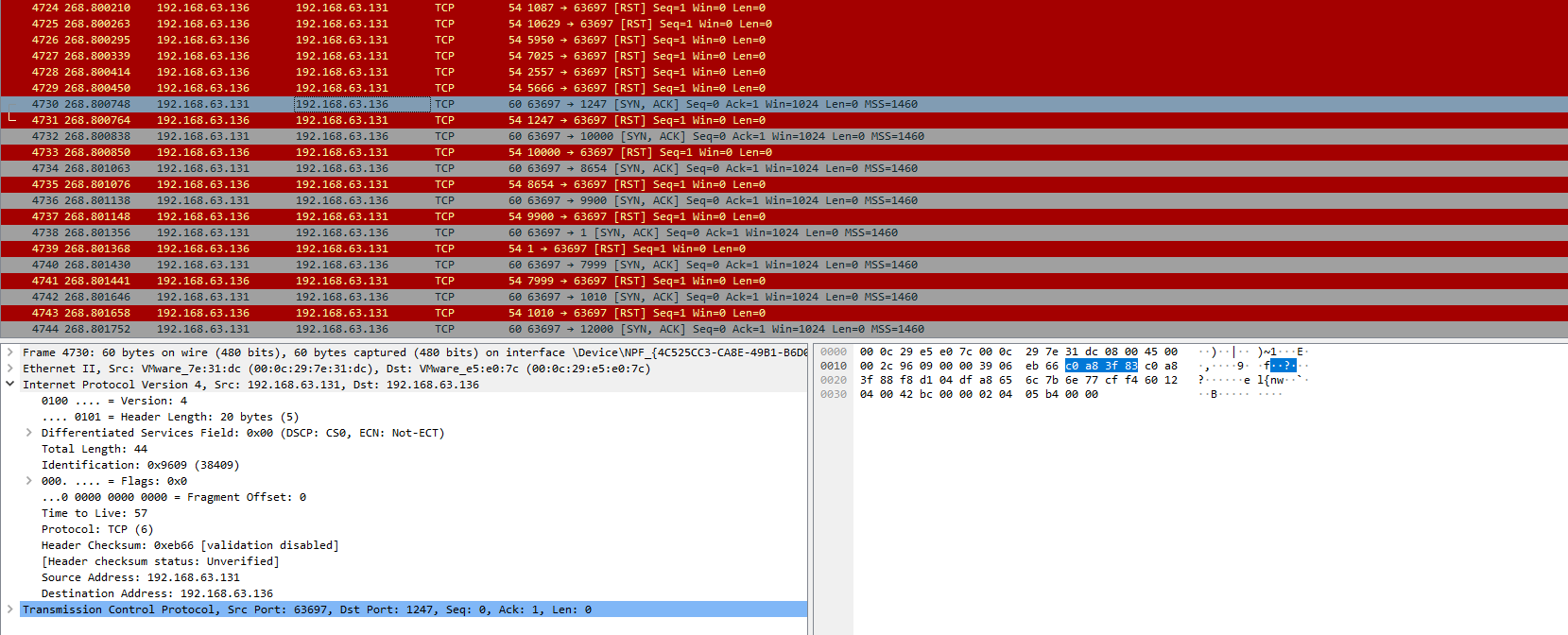
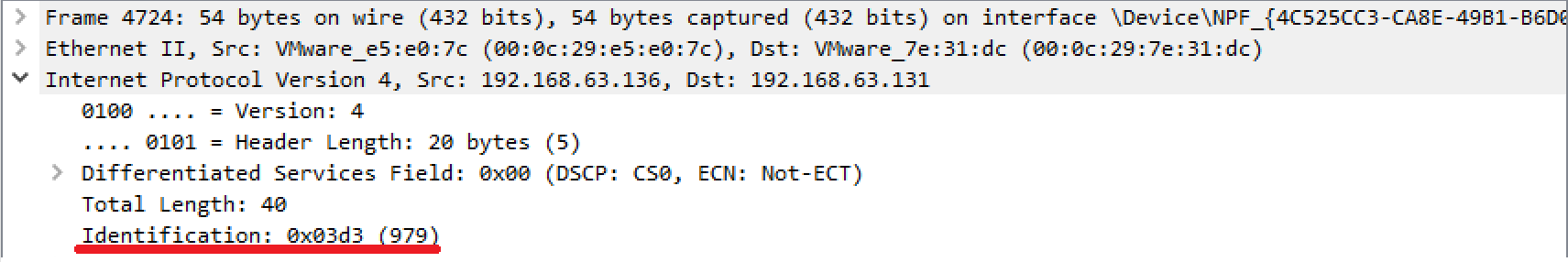


Рисунок 5 – Результат отправки пакетов типа SYNACK на «зомби» машину

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.



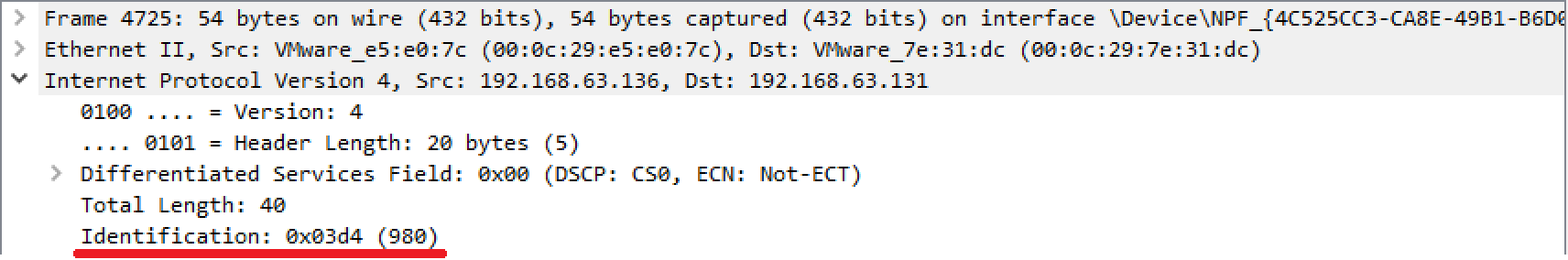


Рисунок 6 – Отображение ID пакетов RST

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:



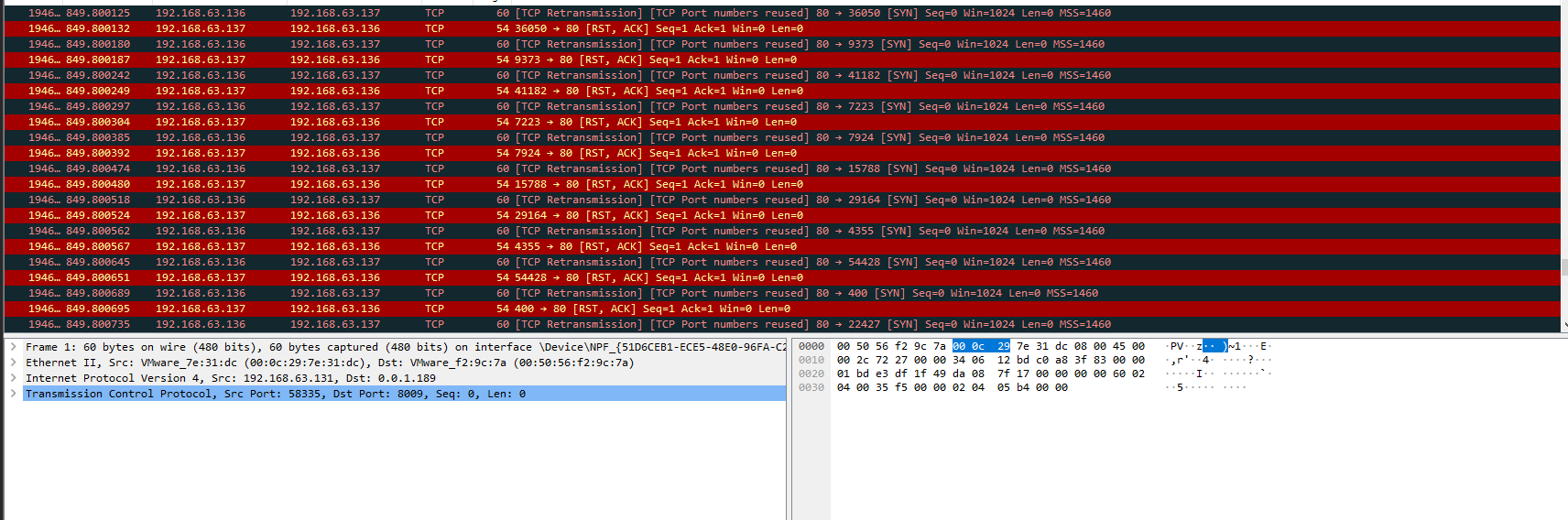


Рисунок 7 – Результат сканирования портов с подменой IP адреса

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

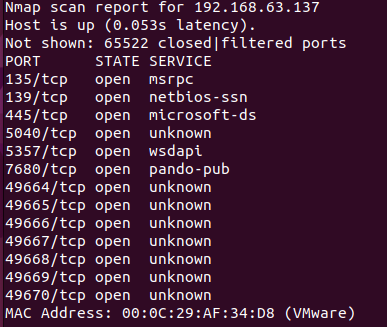
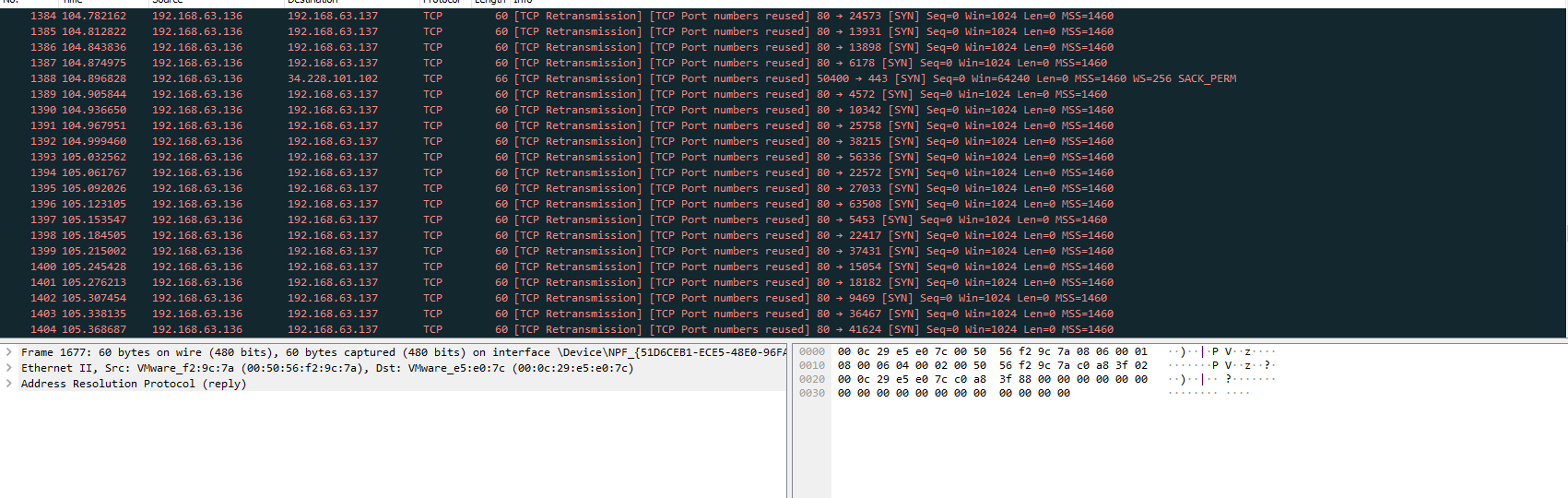
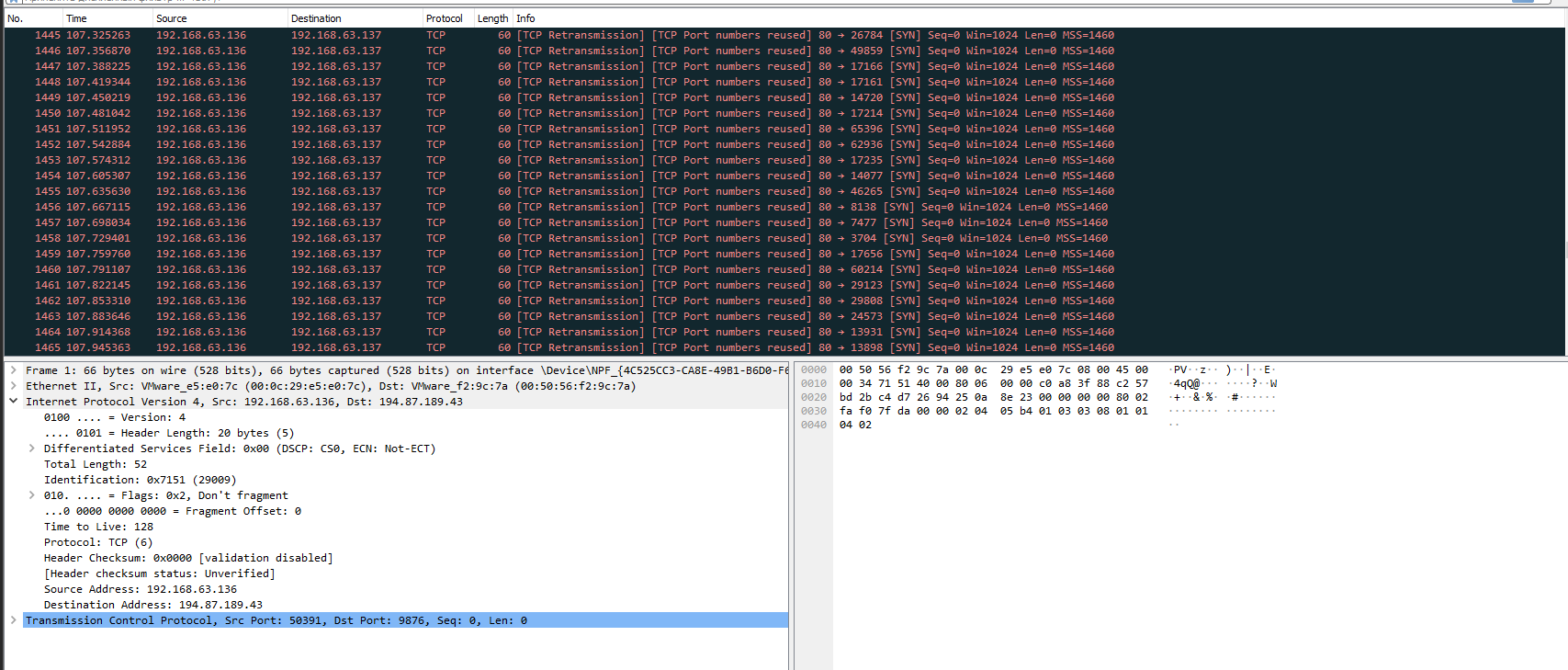


Рисунок 8 – Результат проведенного сканирования

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





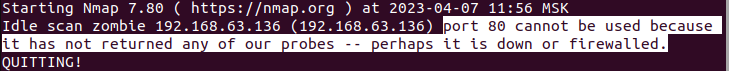


Рисунок 9 – Результат сканирования портов с включенным брандмауэром.

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