







## G7 CS – (Assignment 4)

Topic: Tryhackme Blue

Name: Vinayak Vilaspure



< See Windows Exploitation Basics



Blue

Enjoy the room! For future rooms and write-ups, follow [@darkstar7471](#) on Twitter.

Answer the questions below

Scan the machine. (If you are unsure how to tackle this, I recommend checking out the [Nmap](#) room)

No answer needed

✓ Correct Answer

💡 Hint

How many ports are open with a port number under 1000?

3

✓ Correct Answer


💡 Hint

What is this machine vulnerable to? (Answer in the form of: ms??-???, ex: ms08-067)

ms17-010

✓ Correct Answer

💡 Hint



Exploit the machine and gain a foothold.

Answer the questions below

Start [Metasploit](#)

No answer needed

✓ Correct Answer

🔗 Hint

Find the exploitation code we will run against the machine. What is the full path of the code? (Ex: exploit/.....)

exploit/windows/smb/ms17\_010\_eternalblue

✓ Correct Answer

🔗 Hint

Show options and set the one required value. What is the name of this value? (All caps for submission)

RHOSTS

✓ Correct Answer

🔗 Hint

Usually it would be fine to run this exploit as is; however, for the sake of learning, you should do one more thing before exploiting the target. Enter the following command and press enter:

```
set payload windows/x64/shell/reverse_tcp
```

With that done, run the exploit!

No answer needed

✓ Correct Answer

🔗 Hint

Confirm that the exploit has run correctly. You may have to press enter for the DOS shell to appear. Background this shell (CTRL + Z). If this failed, you may have to reboot the target VM. Try running it again before a reboot of the target.

No answer needed

✓ Correct Answer

### Task 3 Escalate

Escalate privileges, learn how to upgrade shells in metasploit.

Answer the questions below

If you haven't already, background the previously gained shell (CTRL + Z). Research online how to convert a shell to meterpreter shell in metasploit. What is the name of the post module we will use? (Exact path, similar to the exploit we previously selected)

post/multi/manage/shell\_to\_meterpreter

✓ Correct Answer

🔗 Hint

Select this (use MODULE\_PATH). Show options, what option are we required to change?

SESSION

✓ Correct Answer

Set the required option, you may need to list all of the sessions to find your target here.

No answer needed

✓ Correct Answer

🔗 Hint

Run! If this doesn't work, try completing the exploit from the previous task once more.

No answer needed

✓ Correct Answer

🔗 Hint

Once the meterpreter shell conversion completes, select that session for use.

No answer needed

✓ Correct Answer

🔗 Hint

Verify that we have escalated to NT AUTHORITY\SYSTEM. Run getsystem to confirm this. Feel free to open a dos shell via the command 'shell' and run 'whoami'. This should return that we are indeed system. Background this shell afterwards and select our meterpreter session for usage again.

No answer needed

✓ Correct Answer

List all of the processes running via the 'ps' command. Just because we are system doesn't mean our process is. Find a process towards the bottom of this list that is running at NT AUTHORITY\SYSTEM and write down the process id (far left column).

No answer needed

✓ Correct Answer

Migrate to this process using the 'migrate PROCESS\_ID' command where the process id is the one you just wrote down in the previous step. This may take several attempts, migrating processes is not very stable. If this fails, you may need to re-run the conversion process or reboot the machine and start once again. If this happens, try a different process next time.

No answer needed

✓ Correct Answer

#### Task 4 ✓ Cracking

Dump the non-default user's password and crack it!

Answer the questions below

Within our elevated meterpreter shell, run the command 'hashdump'. This will dump all of the passwords on the machine as long as we have the correct privileges to do so. What is the name of the non-default user?

✓ Correct Answer

Copy this password hash to a file and research how to crack it. What is the cracked password?

✓ Correct Answer

💡 Hint

#### Task 5 ✓ Find flags!

Find the three flags planted on this machine. These are not traditional flags, rather, they're meant to represent key locations within the Windows system. Use the hints provided below to complete this room!

Completed Blue? Check out Ice: [Link](#)

You can check out the third box in this series, Blaster, here: [Link](#)

Answer the questions below

Flag1? This flag can be found at the system root.

✓ Correct Answer

💡 Hint

Flag2? This flag can be found at the location where passwords are stored within Windows.

\*Errata: Windows really doesn't like the location of this flag and can occasionally delete it. It may be necessary in some cases to terminate/restart the machine and rerun the exploit to find this flag. This relatively rare, however, it can happen.

✓ Correct Answer

💡 Hint

flag3? This flag can be found in an excellent location to loot. After all, Administrators usually have pretty interesting things saved.

✓ Correct Answer

💡 Hint