USING THE METASPLOIT FRAMEWORK

ASSIGNMENT REPORT

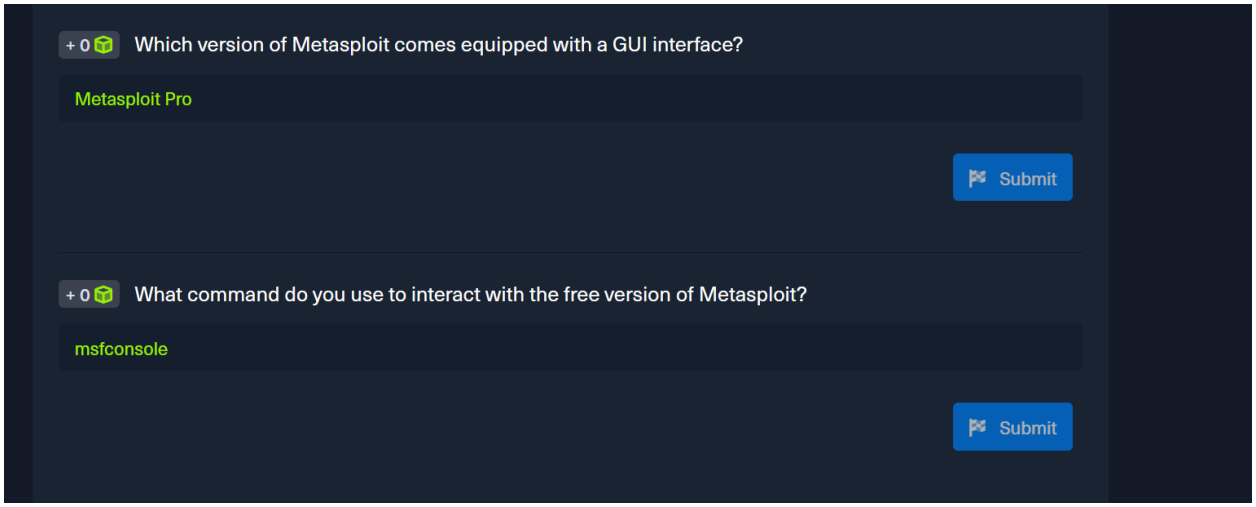
Peter Kinyumu,
cs-sa07-24067,
June 17th, 2024.

1. INTRODUCTION

This module teaches the fundamentals of the Metasploit Framework, an open-source set of tools used for network enumeration, attacks, testing security vulnerabilities, evading detection, performing privilege escalation attacks, and performing post-exploitation.

2. ANSWERS TO QUESTIONS

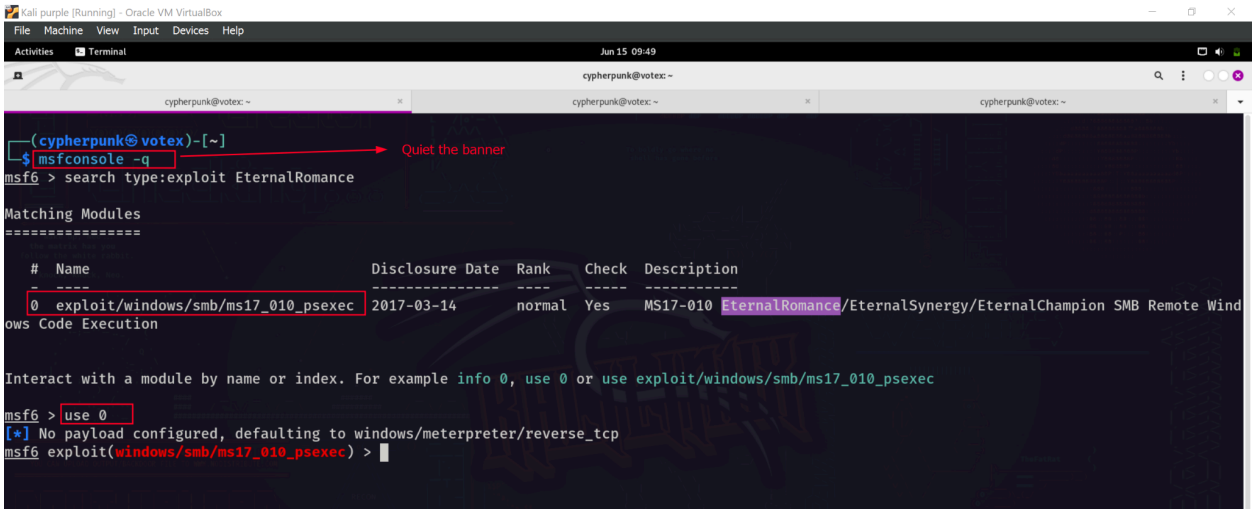
Introduction to Metasploit



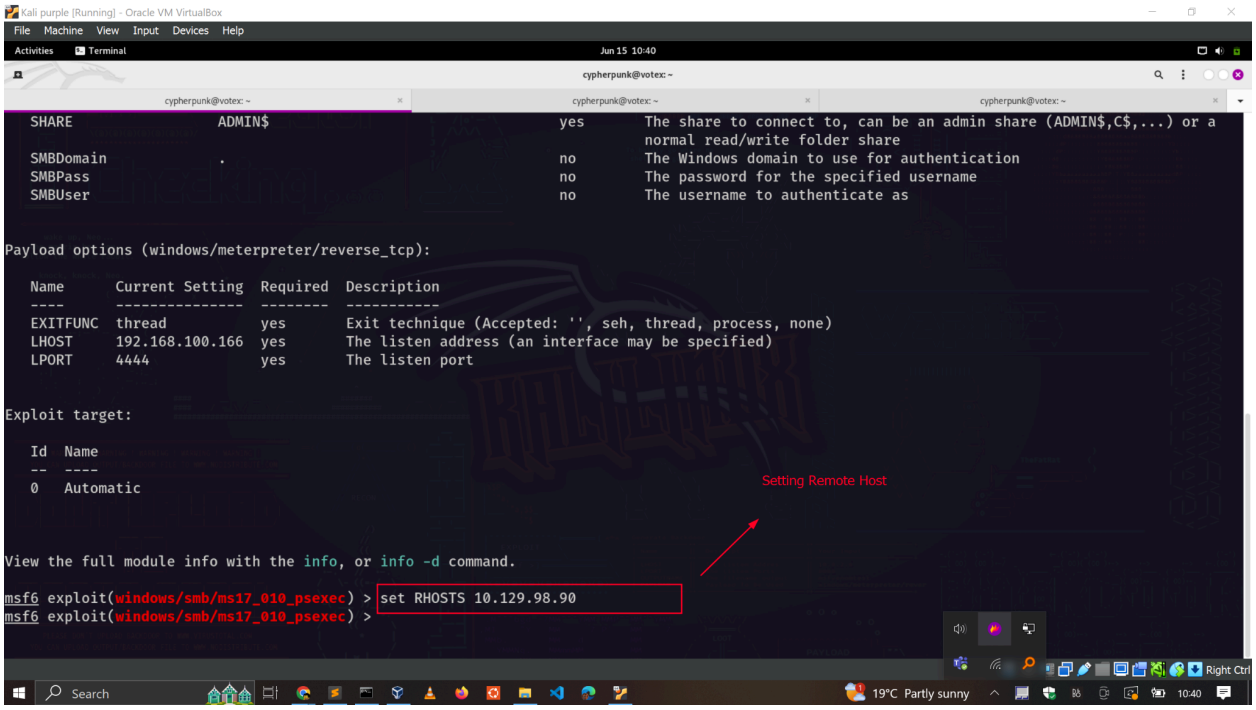
Modules

a. Use the Metasploit-Framework to exploit the target with EternalRomance. Find the flag.txt file on Administrator's desktop and submit the contents as the answer.

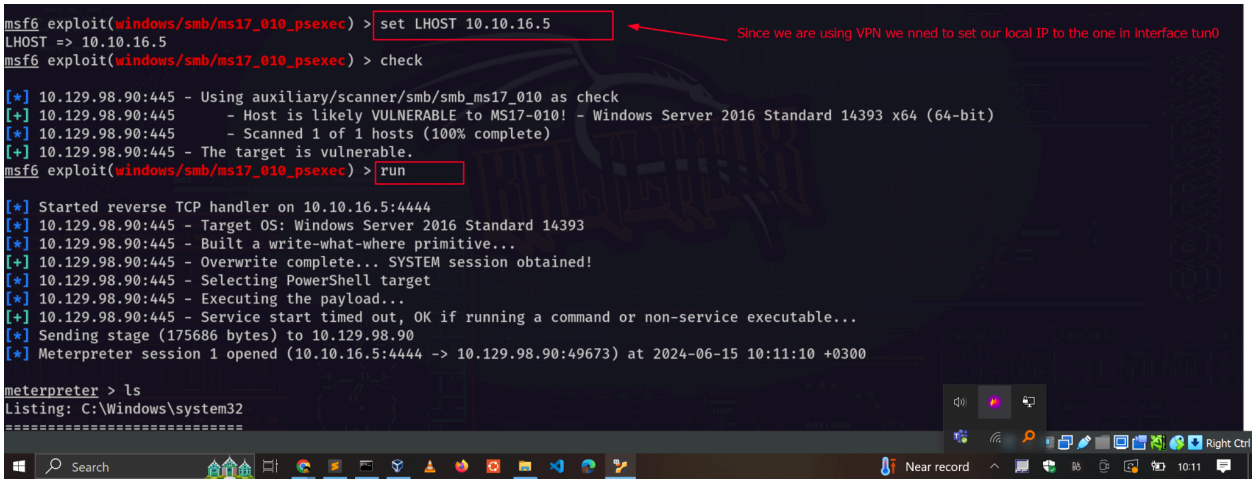
- The first step is to search for an exploit related to EternalRomance in Metasploit.



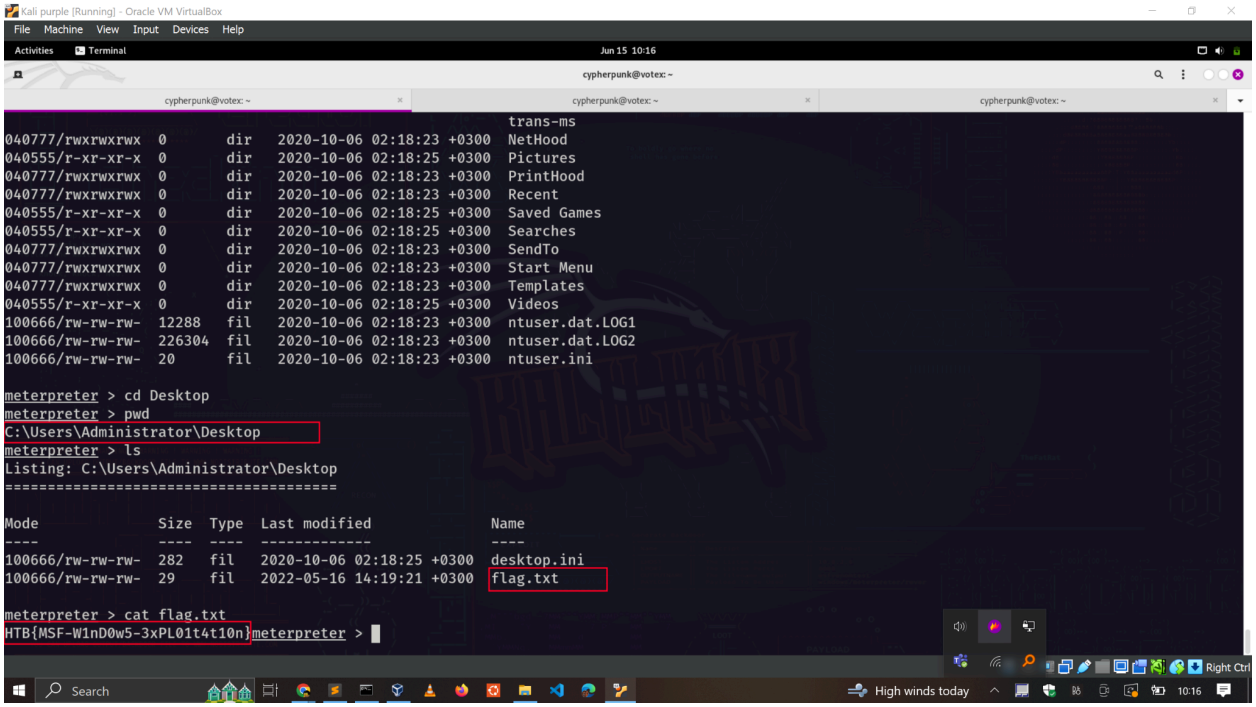
- Then, set all the options as required.



- Run the exploit



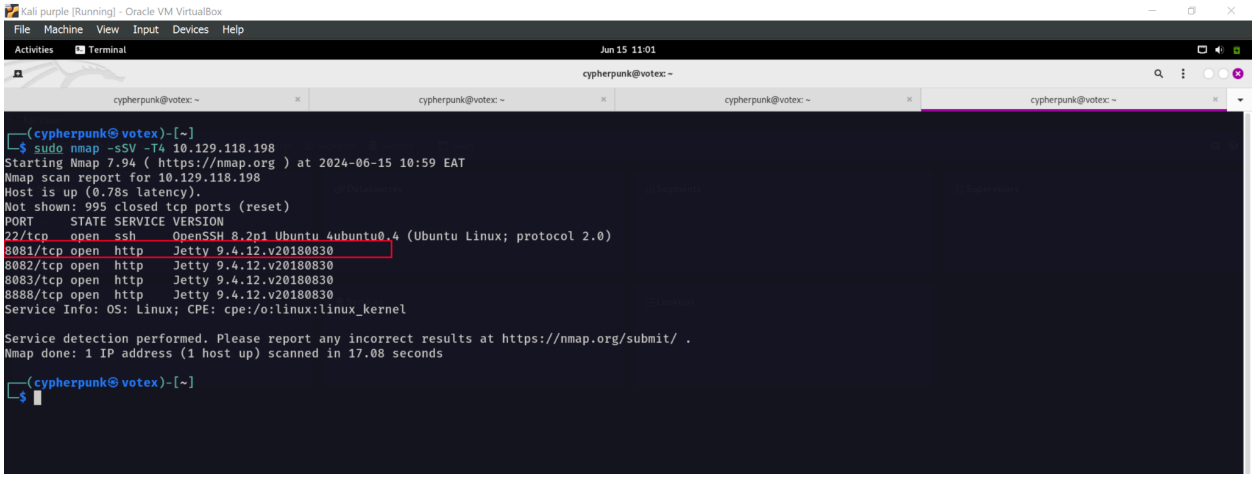
- Upgrade the meterpreter shell to the native shell and retrieve the flag.

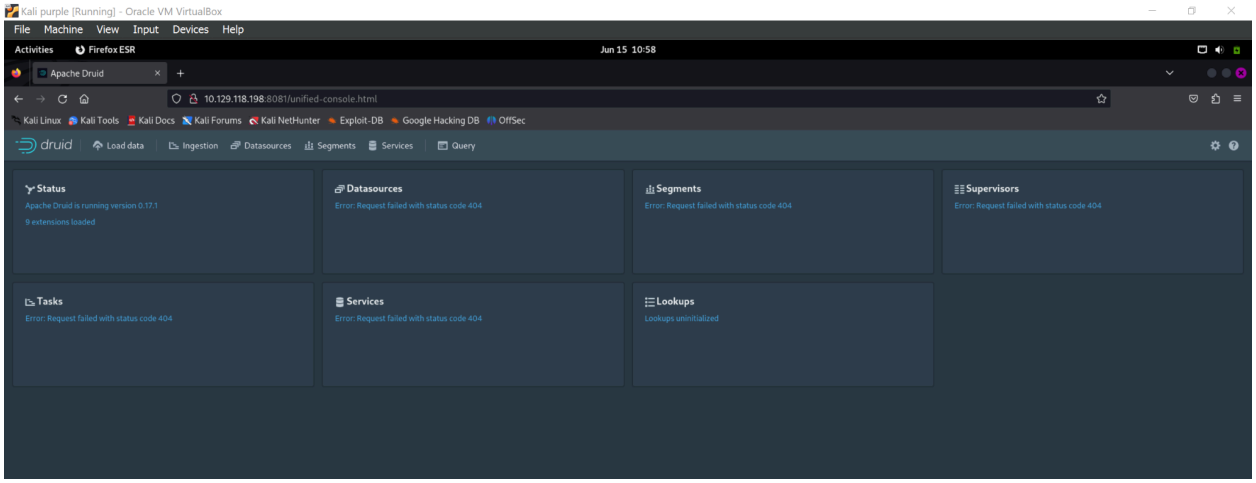


Payloads

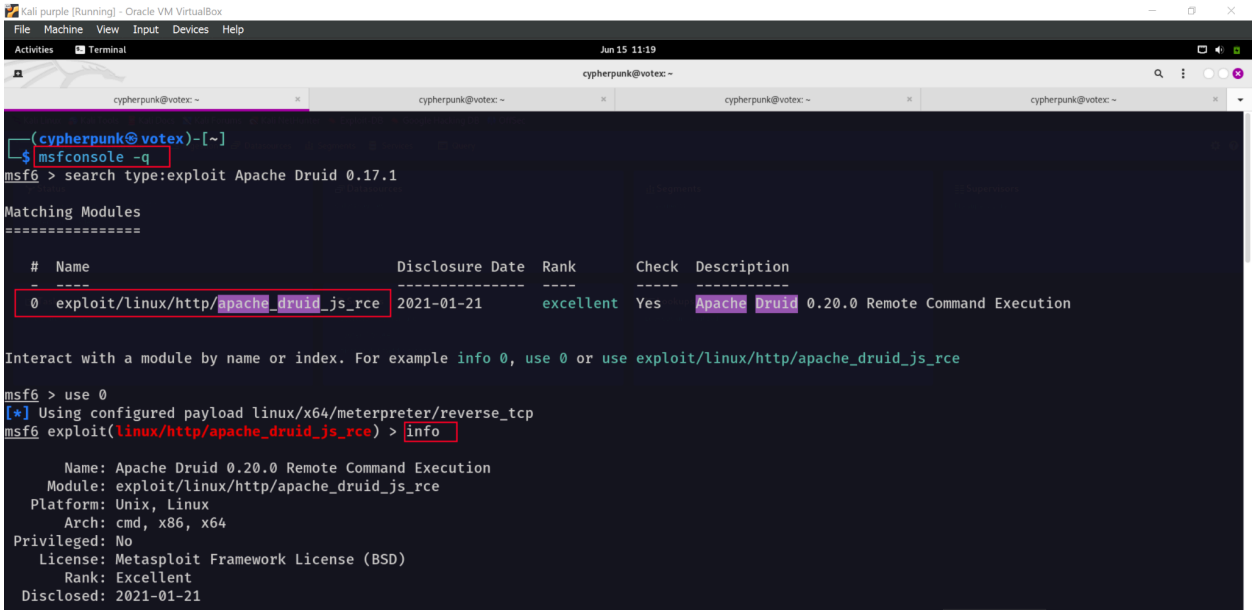
a. Exploit the Apache Druid service and find the flag.txt file. Submit the contents of this file as the answer.

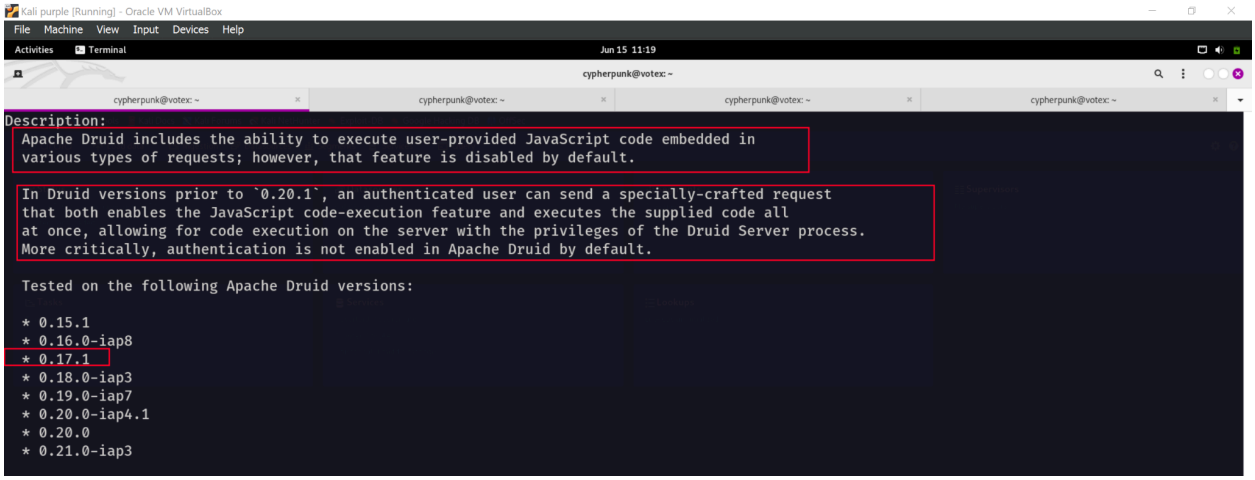
- Run Nmap and identify where the Apache Druid service is running.



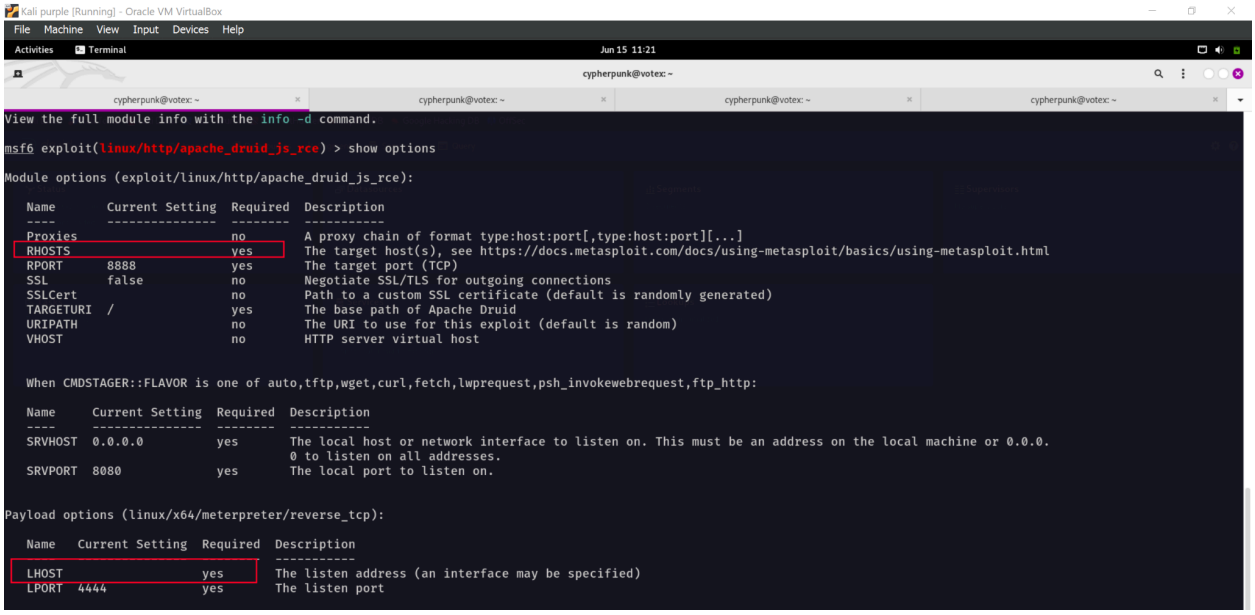


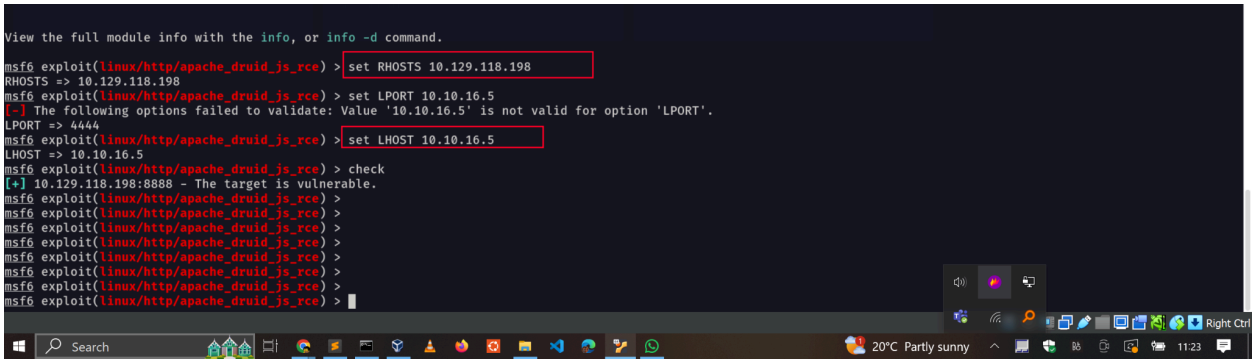
- Identify the version for the Apache Druid application. (version 0.17.1)
- Research for vulnerabilities that exist for that version(Remote Code Execution)
- Search Metasploit for a public exploit for that version.



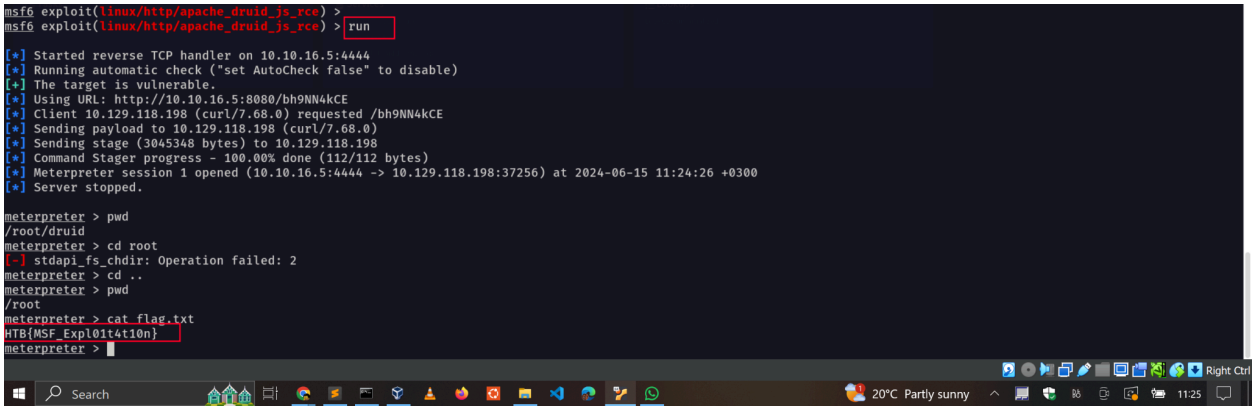


- Use the exploit and set the exploit options as required.



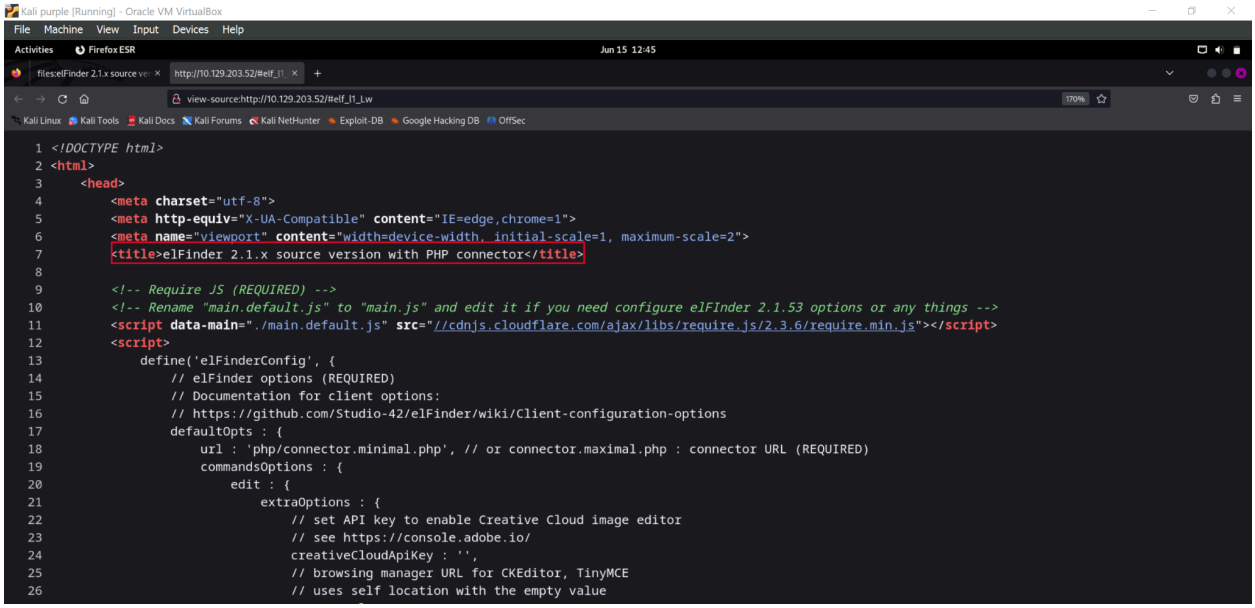


- Run the exploit and retrieve the flag.



Sessions

a. **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

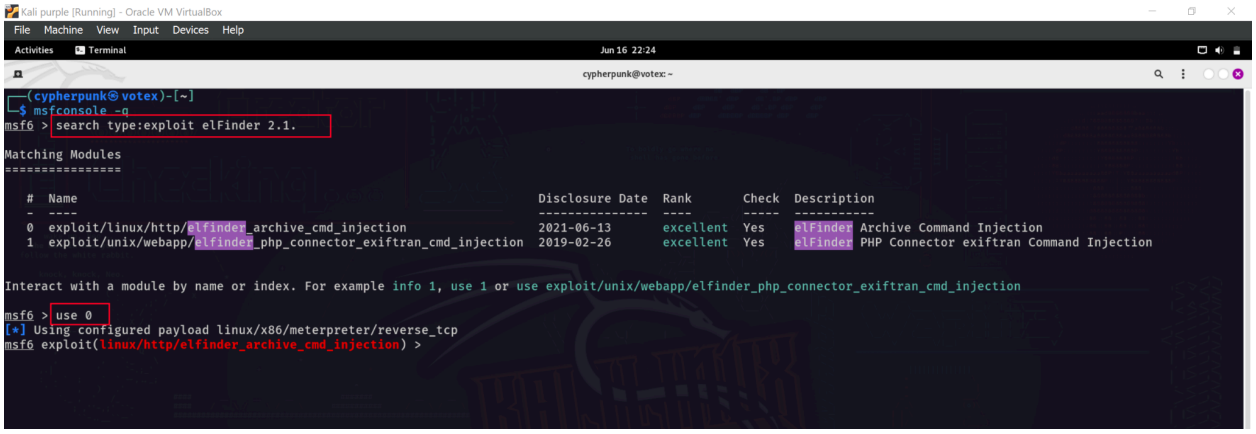


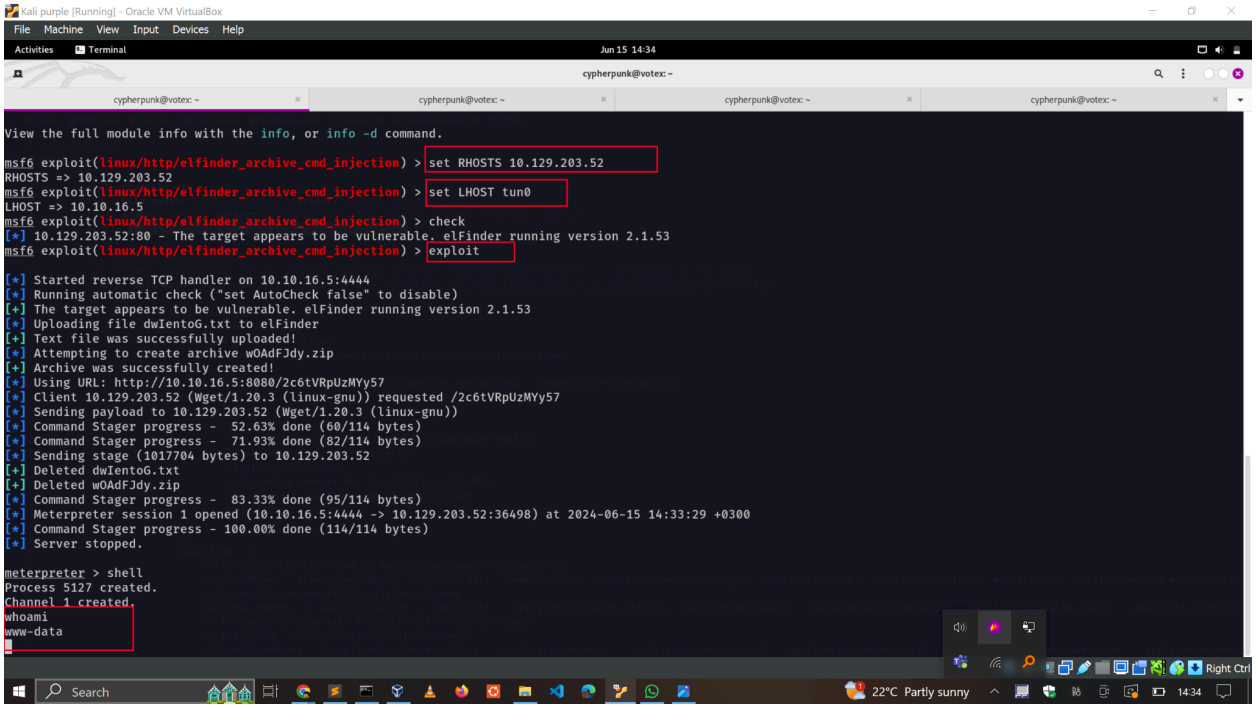
b. **Find the existing exploit in MSF and use it to get a shell on the target. What is the username of the user you obtained a shell with?**

Answer: www-data

- Research whether the identified version of the elFinder application is vulnerable. (Command Injection)
- Search for a suitable exploit in Metasploit.
- Set the exploit options as required.

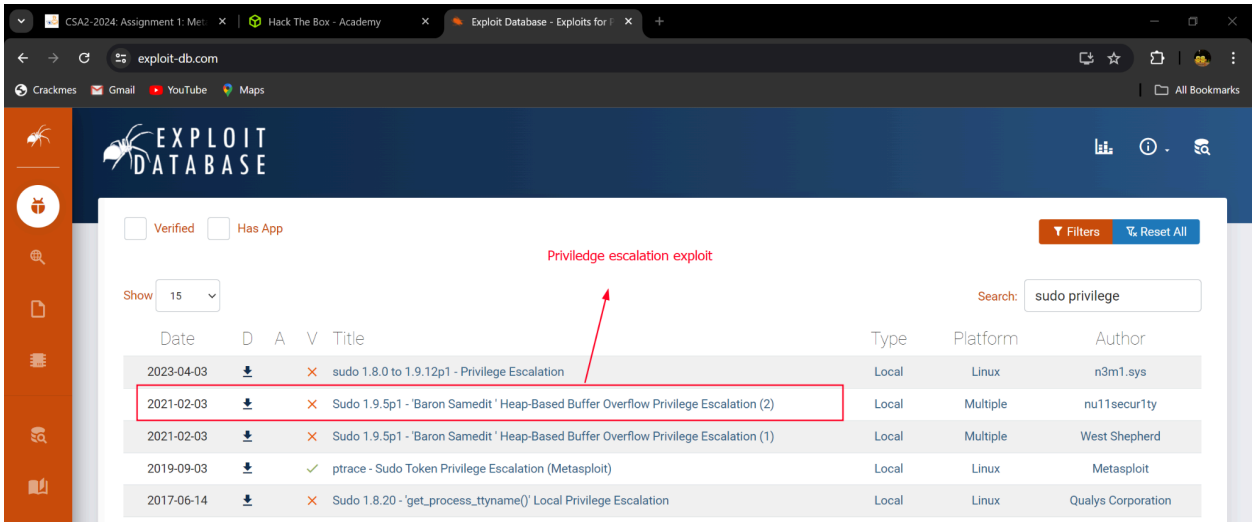
- Run the exploit



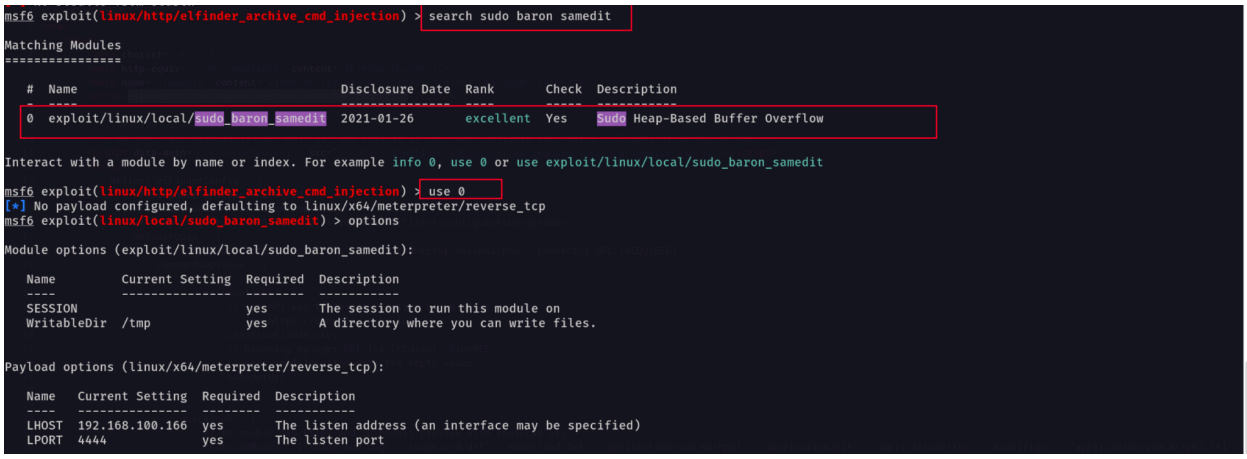


c. The target system has an old version of Sudo running. Find the relevant exploit and get root access to the target system. Find the flag.txt file and submit the contents of it as the answer.

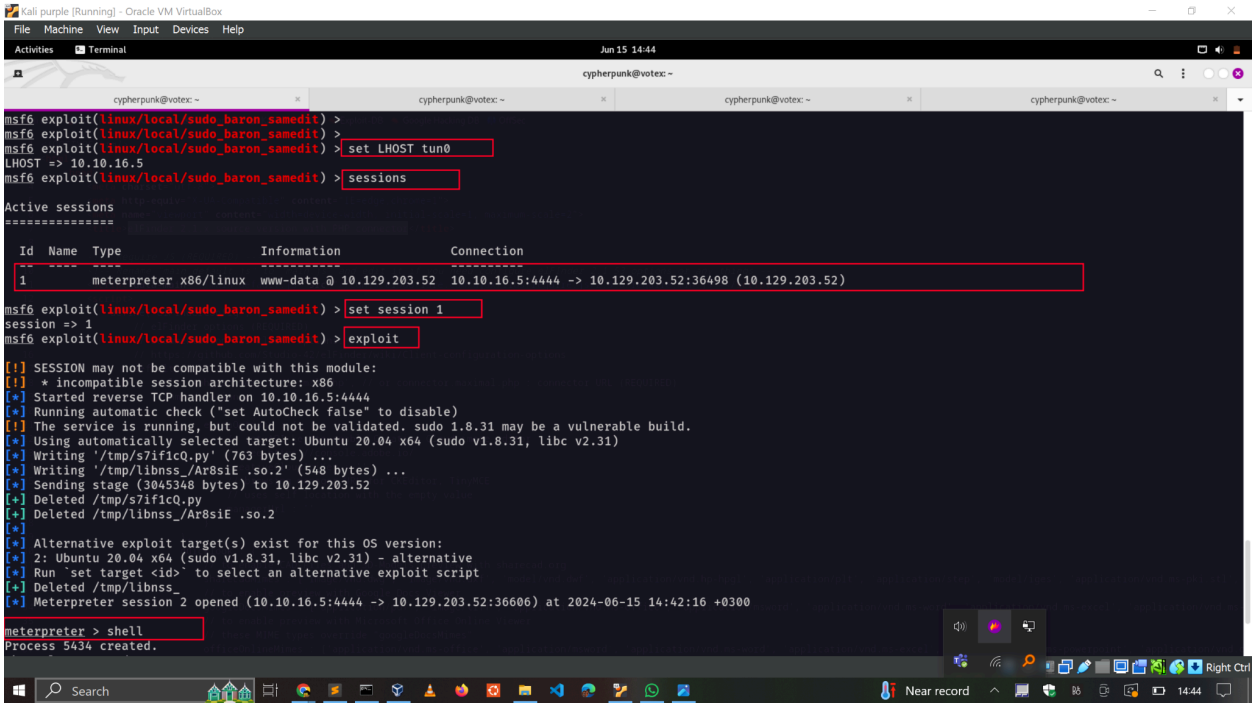
- We know the sudo version is vulnerable.
- Research for any local privilege escalation for vulnerable sudo versions.

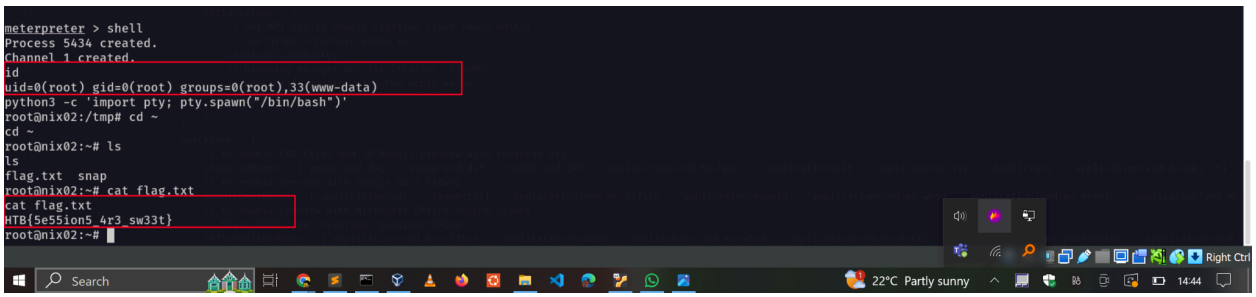


- Background the existing session with the Meterpreter background command.
- Search for the sudo exploit in meterpreter and use it.



- We can then set our sudo sudo exploitation to use our background session with the command set session <id>. When we run the exploit, it performs a privilege escalation and returns the root shell.

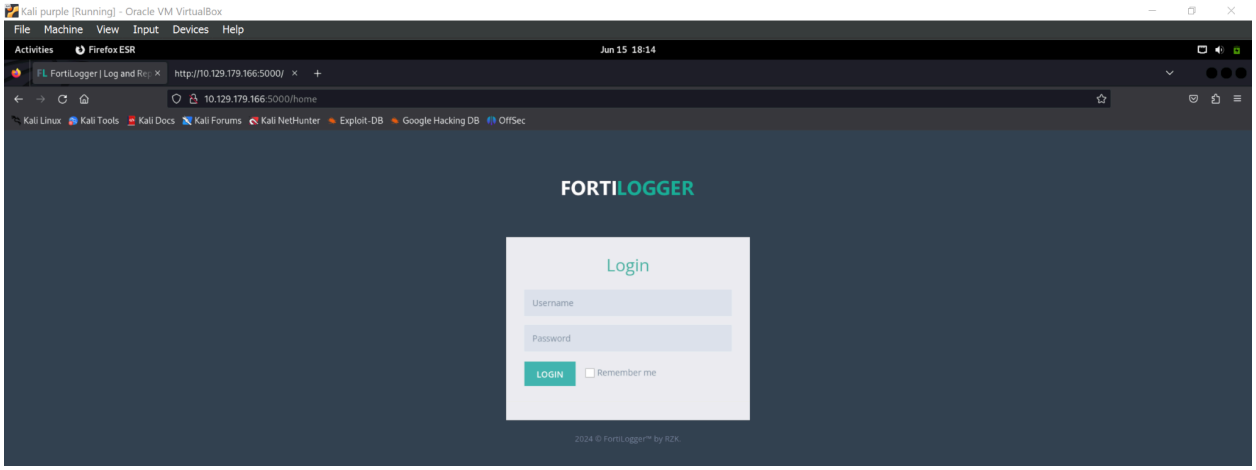


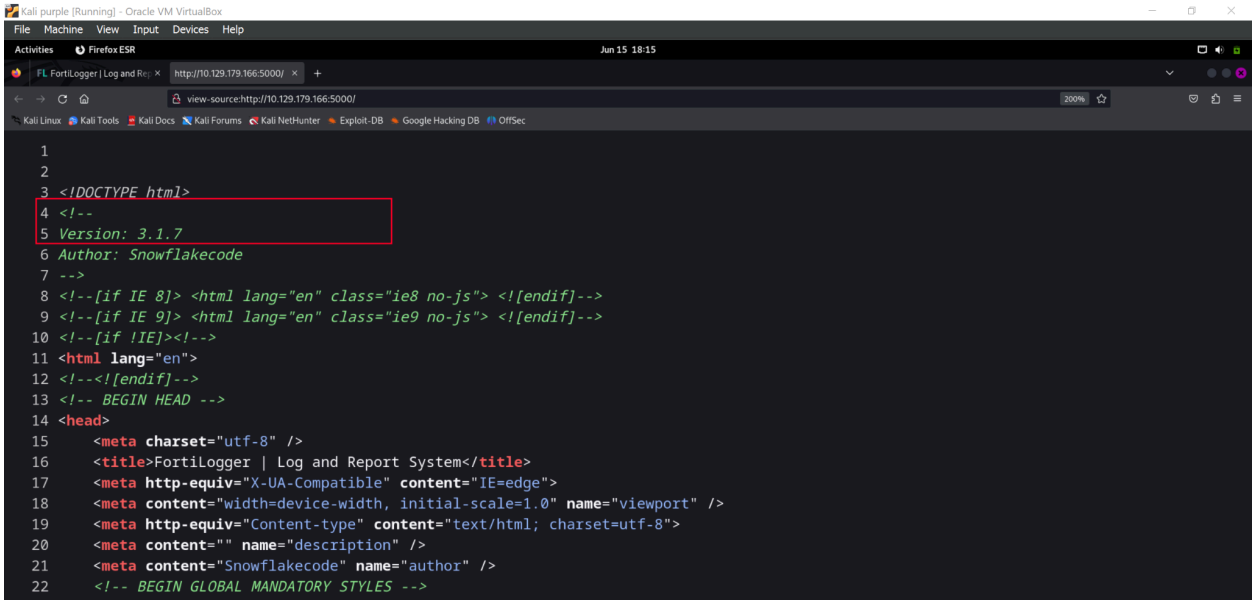


Meterpreter

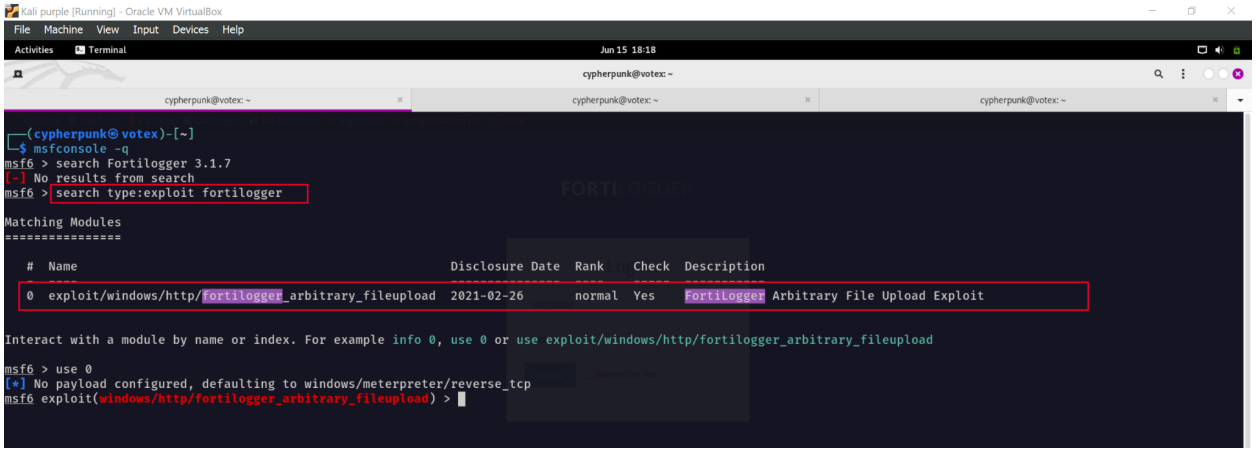
a. Find the existing exploit in MSF and use it to get a shell on the target. What is the username of the user you obtained a shell with?

- Run an Nmap scan and identify any open ports and services.
- A web server is running the Fortlogger application version 3.1.7 on port 5000.
- Research the application's version for potential vulnerabilities. The application version is vulnerable to the Unauthenticated Arbitrary File Upload vulnerability.

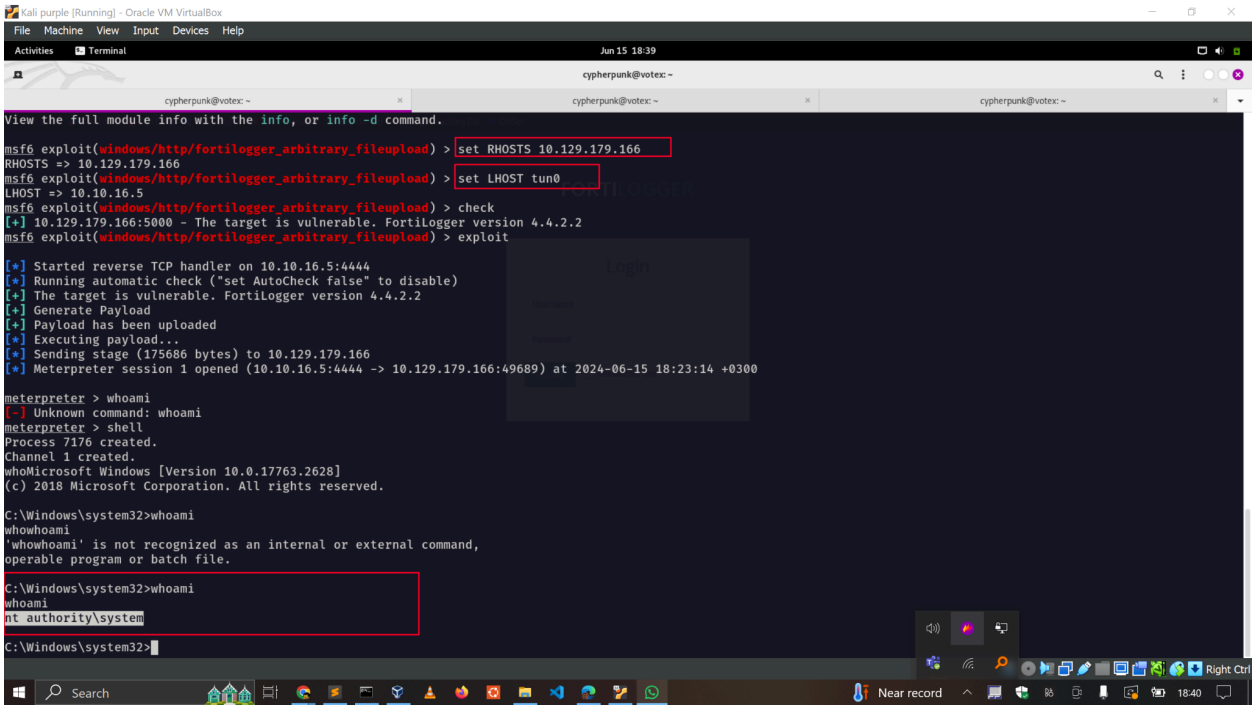




- Search for a suitable exploit in Metasploit.

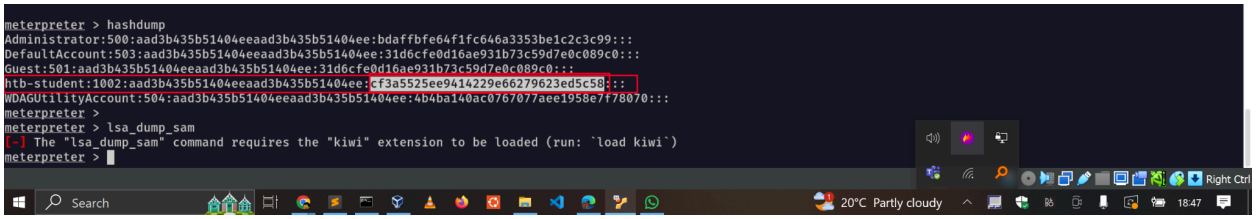


- Set all the required options and run the exploit.
- Get shell as the **nt authority\system** user.



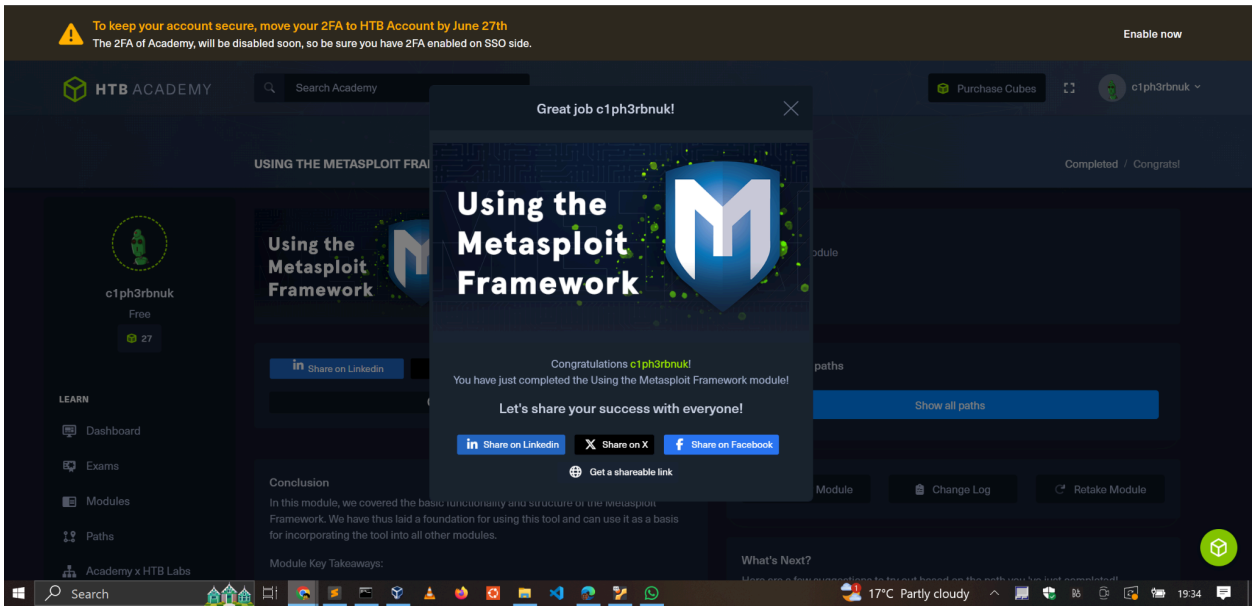
b. Retrieve the NTLM password hash for the "htb-student" user. Submit the hash as the answer.

- Use the meterpreter hashdump utility to dump all the local SAM hashes for the machine.
- The NTML hash is the second part of the hash.



3. MODULE COMPLETION

https://academy.hackthebox.com/achievement/144829/39



4. CONCLUSION

This module was so in-depth. I have gained much knowledge and experience in automating the exploitation process using the Metasploit Framework. I have learned to search and use different exploit modules to exploit vulnerabilities. I have also learned the different types of payloads, how to use them and even how to create them using **msvenom**. Additionally, I have learned how to utilize sessions to run additional post-exploitation exploits that may offer elevated privileges. Lastly, I learned basic meterpreter shell commands, such as dumping the local SAM hash using **hashdump.**