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

Practical Project – Cyber-attack with Phishing

Introduction

Phishing attacks are a type of social engineering. Unlike other cyberattacks that focus on networks, these attacks manipulate people using false narratives, human mistakes, and pressure tactics to get them to harm themselves or their organizations unintentionally. In a typical phishing scam, a hacker pretends to be someone the victim trusts, such as a coworker, boss, or a representative from a well-known brand. They send a message asking the victim to pay an invoice, open a file, click a link, or perform another action.

Because the victim trusts the sender, they follow the instructions, falling into the scammer's trap. That "invoice" may redirect money to the hacker's account, that attachment could install ransomware, and that link might lead to a site that steals personal information like credit card numbers or login credentials.

The origins of phishing date to the 1990s as internet access and use expanded, and email became more widely used. A particular milestone was marked in May 2000 when email users worldwide received messages with the subject line “ILOVEYOU”. The message included a .txt file that launched a worm to, among other things, overwrite image files. Another milestone was a 2004 legal claim against a teenager who spoofed an ISP website to attain access to users’ credit card and bank accounts.

Phishing is popular among cybercriminals and highly effective. Phishing is a significant threat because it exploits people rather than technological vulnerabilities. Attackers don't need to breach systems directly or outsmart cybersecurity tools. Phishers can be lone scammers or sophisticated criminal gangs. They can use phishing for many malicious ends, including

identity theft, credit card fraud, monetary theft, extortion, account takeovers, espionage 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 refers to an attack executed through platforms like Instagram, LinkedIn, Facebook, or Twitter. The purpose of such an attack is to steal personal data or gain control of your 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.

It has been reported that online industries from worldwide like social media are most targeted by phishing attacks. It is 37.6% of social media phishing attacks in first quarter of 2024. It is the most common form of cyber-crime and estimated 3.4 billion of spam mails are sent to victims every day. According to statistics, 24.77% of spam mails are sent from Russia, followed by Germany with 14.12%, 10.46% from USA and 8.73% from China. Millennials and Gen-Z internet users (18-40 year olds) are most likely to fall victim to phishing attacks – 23% compared to 19% of Generation X internet users (41-55 year olds). Between 2020 – 2021, cyber crime increased by 168% in the Asia-pacific region including phishing and aero-day attack. Phishing attack was risen by 220% compared to annual average at the height of Covid-19 pandemic.

There are many types of phishing. Among them, most common types of phishing are

- Email Phishing – It is also known as deception phishing. It uses social engineering techniques and malicious actors impersonate a

legitimate company and encourage users to click on a link or download a document. Usually the links lead to the websites which would either steal a person's credentials or install malicious software upon clicking the link called malware.

- Spear Phishing – It targets a small group of people. Malicious actors imposter. Malicious attackers trick the recipients into believing that they have a personal connection with sender addressing with target's name and personal information. (eg.Notice from 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 prepetrated 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 pretends 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:** Keeping your device's software up to date is vital for security. Software updates often include patches that fix vulnerabilities that could be exploited by cybercriminals. 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 also work with the Social Engineering Toolkit to send harmful links to specific people, hoping to steal their personal information. While there are more advanced tools, many 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.

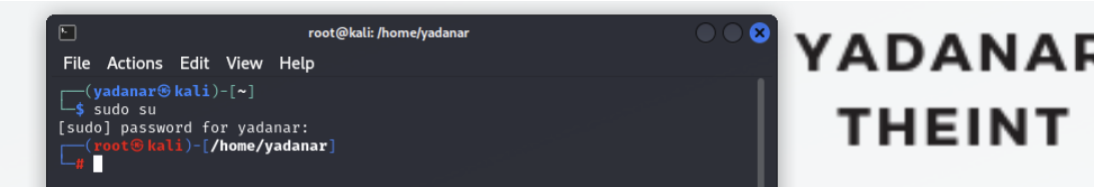
Overall, Zphisher is a powerful tool that makes phishing easier for attackers, especially in scams like the LinkedIn one mentioned above.

Criteria 2

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

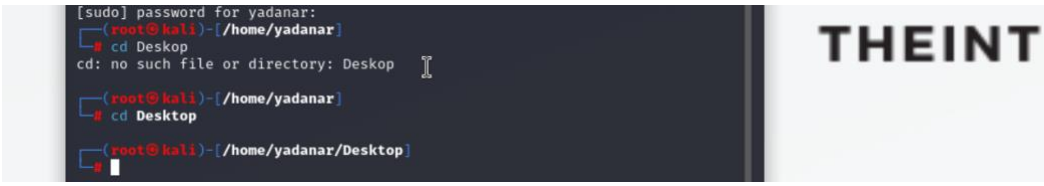
1. Change to root access is kali

   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.



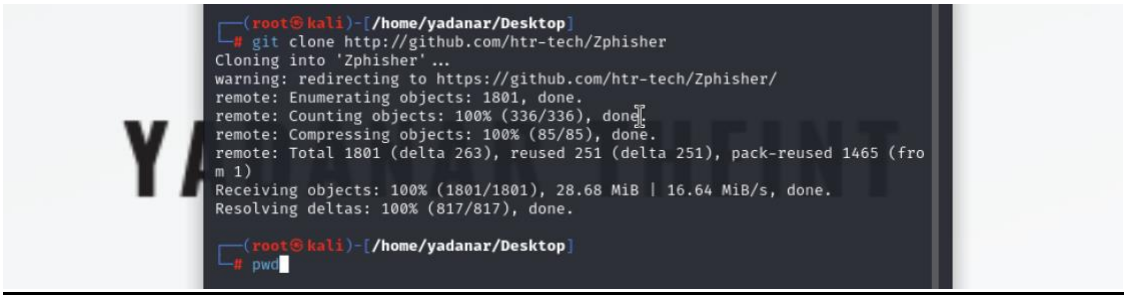
2. Change folder to store Zphisher

   I want to store Zphisher in a specific location.



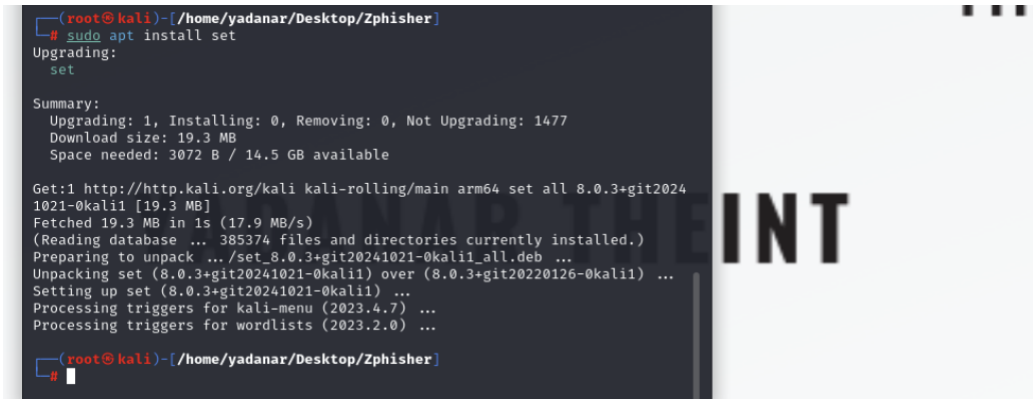
3. Zphisher Installation in Kali Linux

Create a git clone of Zphisher in terminal. This will automatically clone the package of a zphisher in the current location.



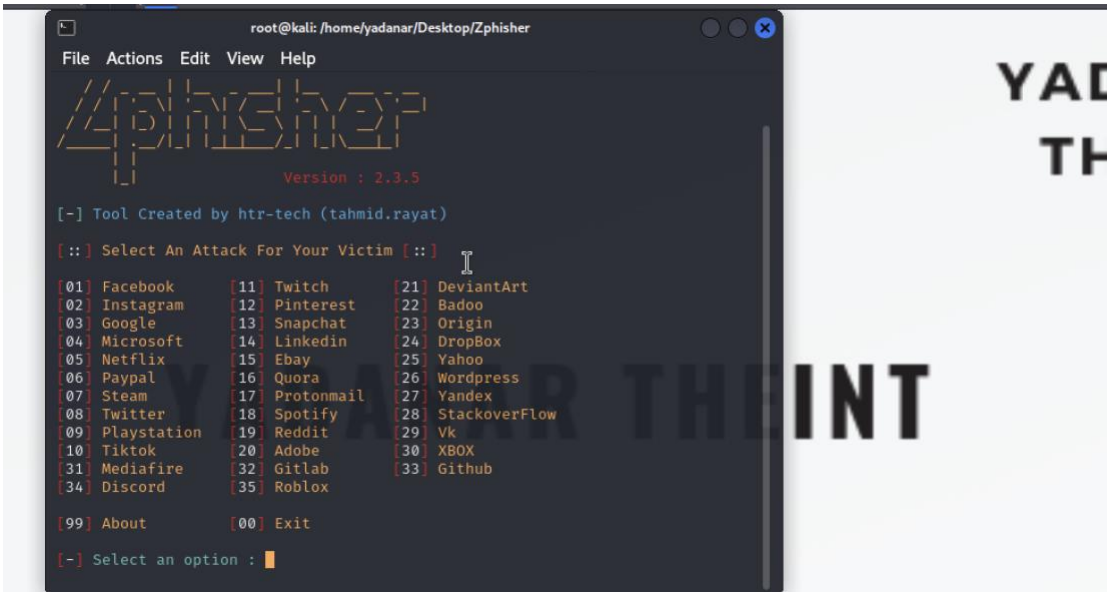
4. Installing tool

Entering “sudo apt install set” will download any required assets and automatically install the tool within your virtual environment .



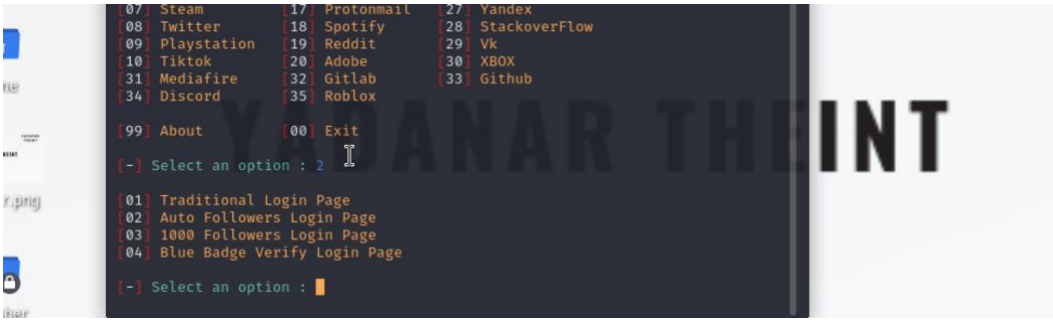
5. Running Zphisher

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



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 replicate rendition of the official Instagram login screen is constructed. Consequently, this will generate a link that directed to this fabricated webpage.

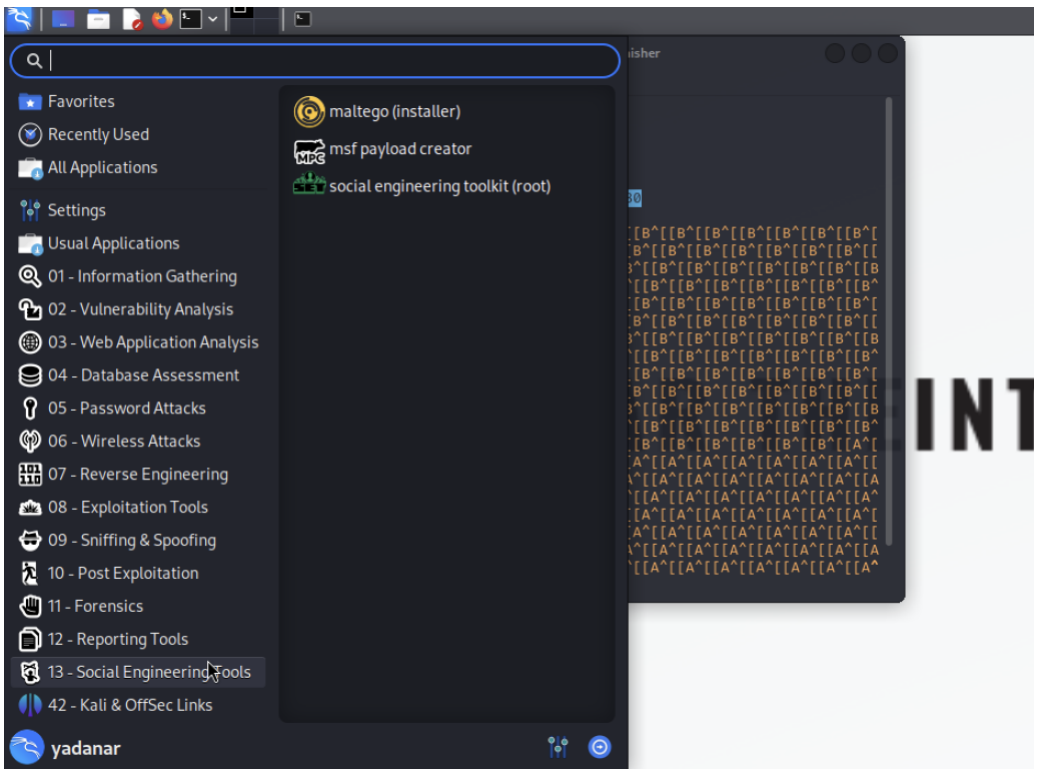


After that, I can see several options to attract victim. Right now, I will choose an option 1.

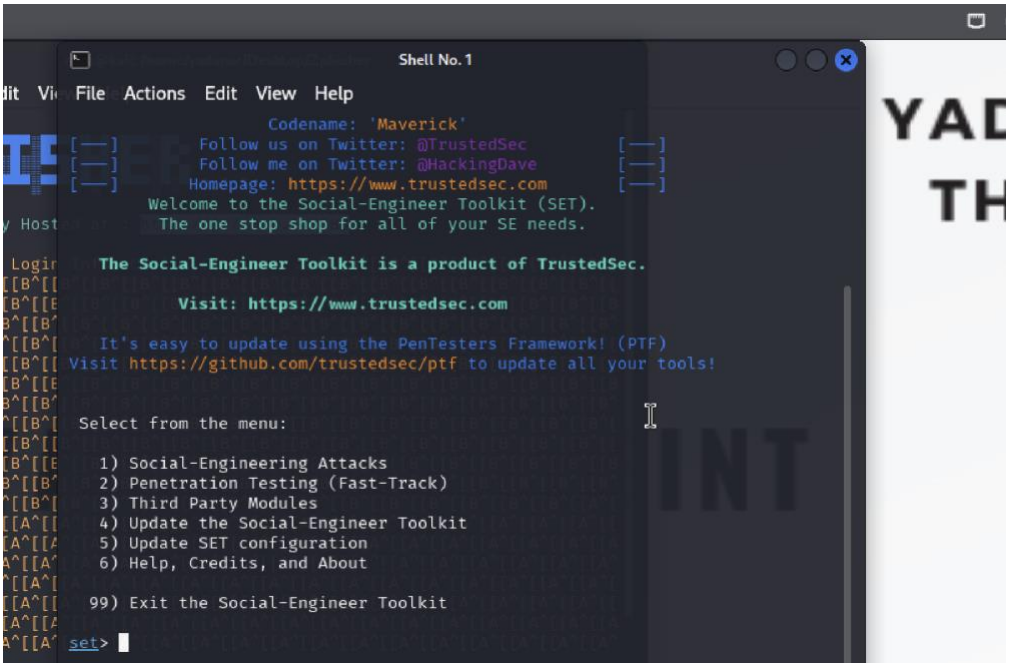
Now, I have succesfully hosted a clone instagram webpage at http://127.0.0.1:8080.

7. SET Tool

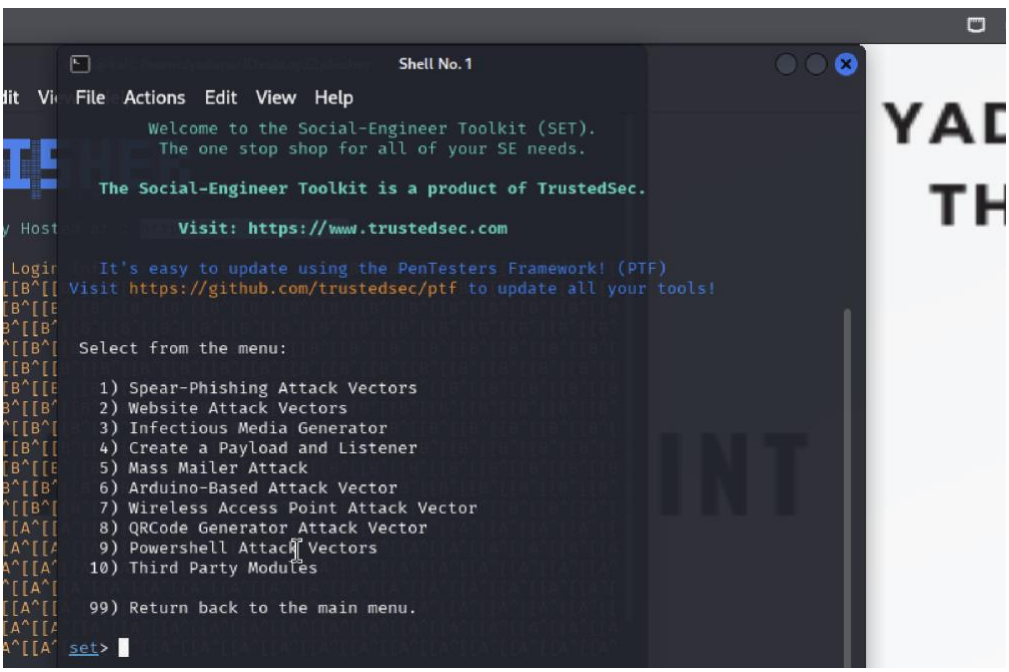
After I have created a clone Instragram webpage, I will launch the SET tool to send email to victims. SET tool is one of the built in tool in Kali Linux, located in the top left corner,Kali linux logo.



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



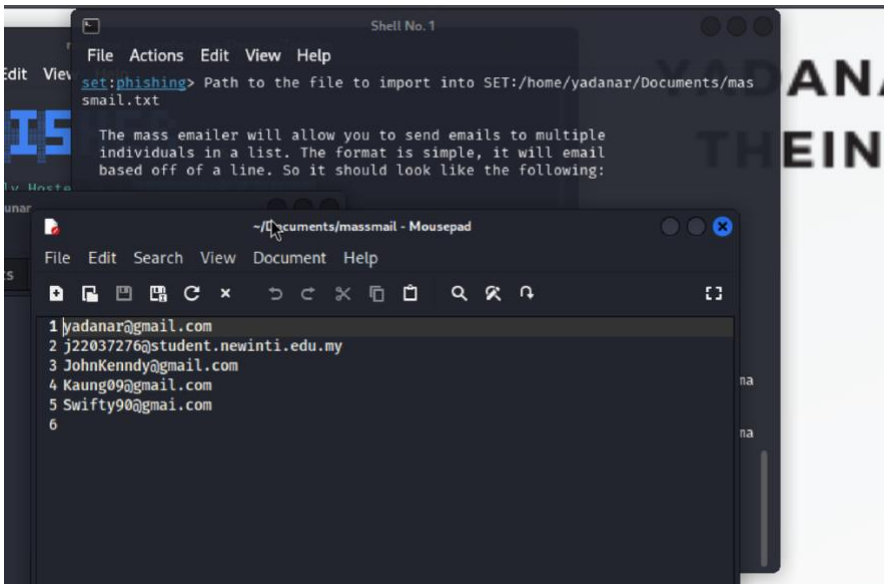
Since I want to send the phishing link to victims, I have to choose the option 1. This will show a series of phishing attacks that I can perform. Choosing option 5 will help to perform action that I want.



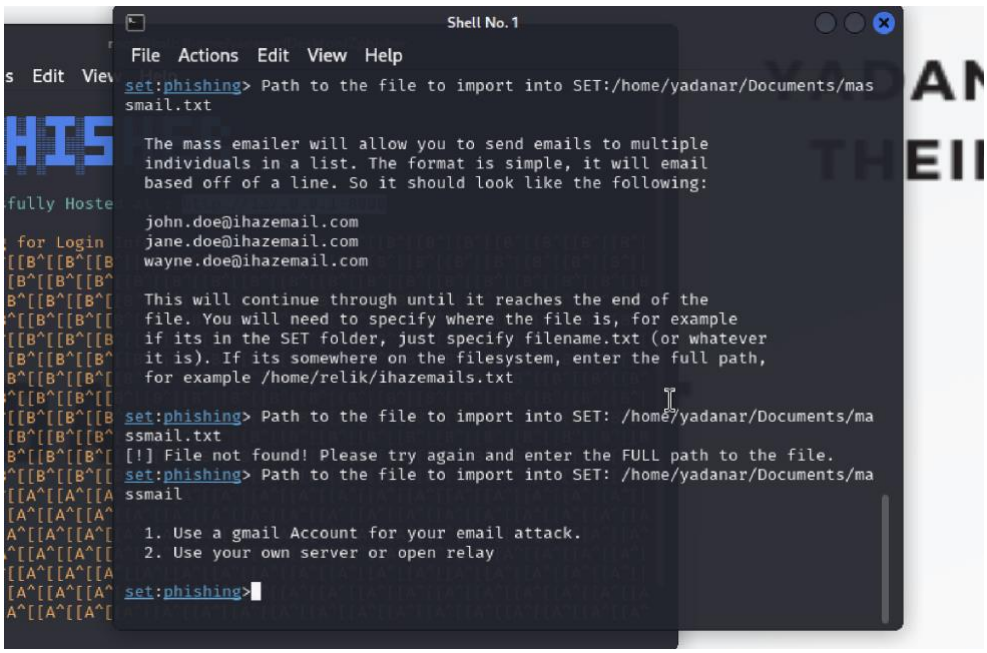
When I choose option 5: Mass Mail Attack, I will see another 2 options for attacking. If we want to send only one specific victim, we can choose option 1: Attack single mail address. But in my case, I want to send to several victims and I will need a text file which contains a list of email address.

8. Mass Mail Attacking

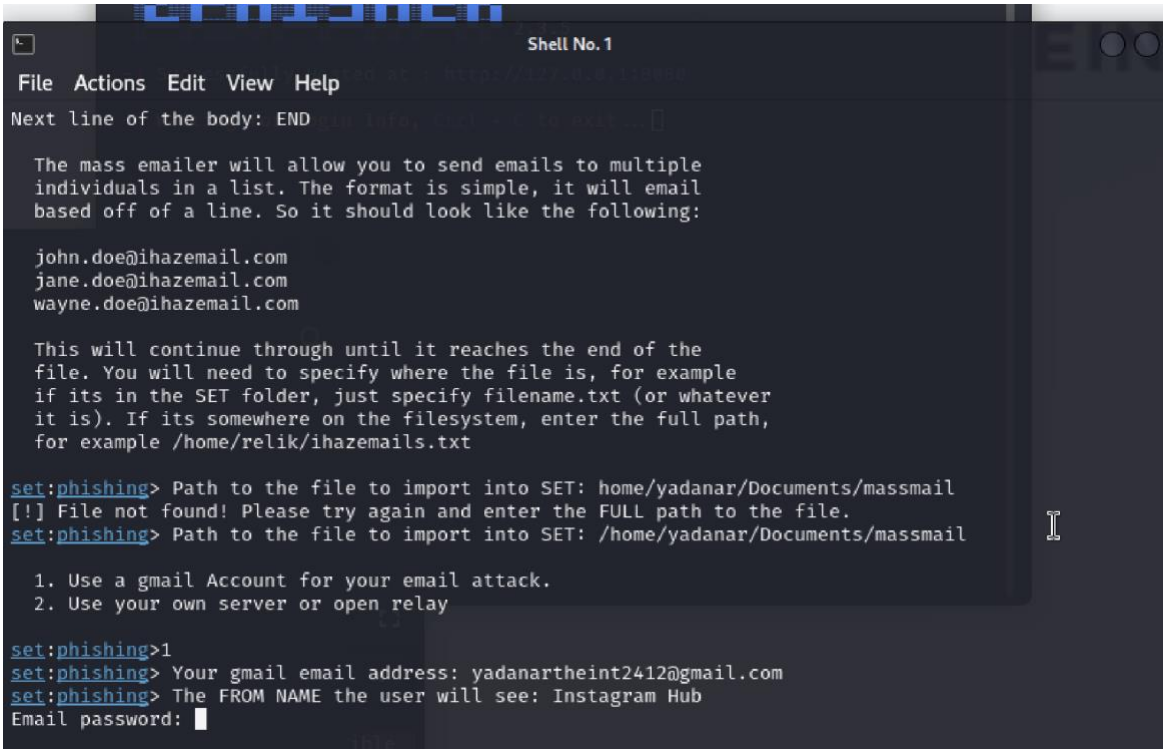
To create a mass mail attack, I need to create a list of emails first.



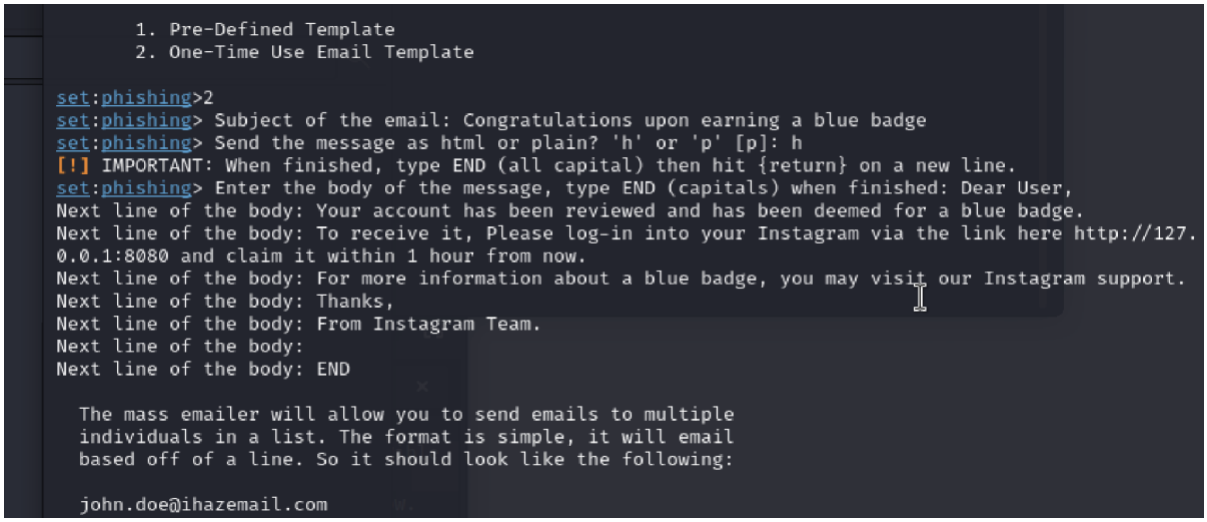
Then I can copy the path of the file and load in SET terminal to perform attacking.

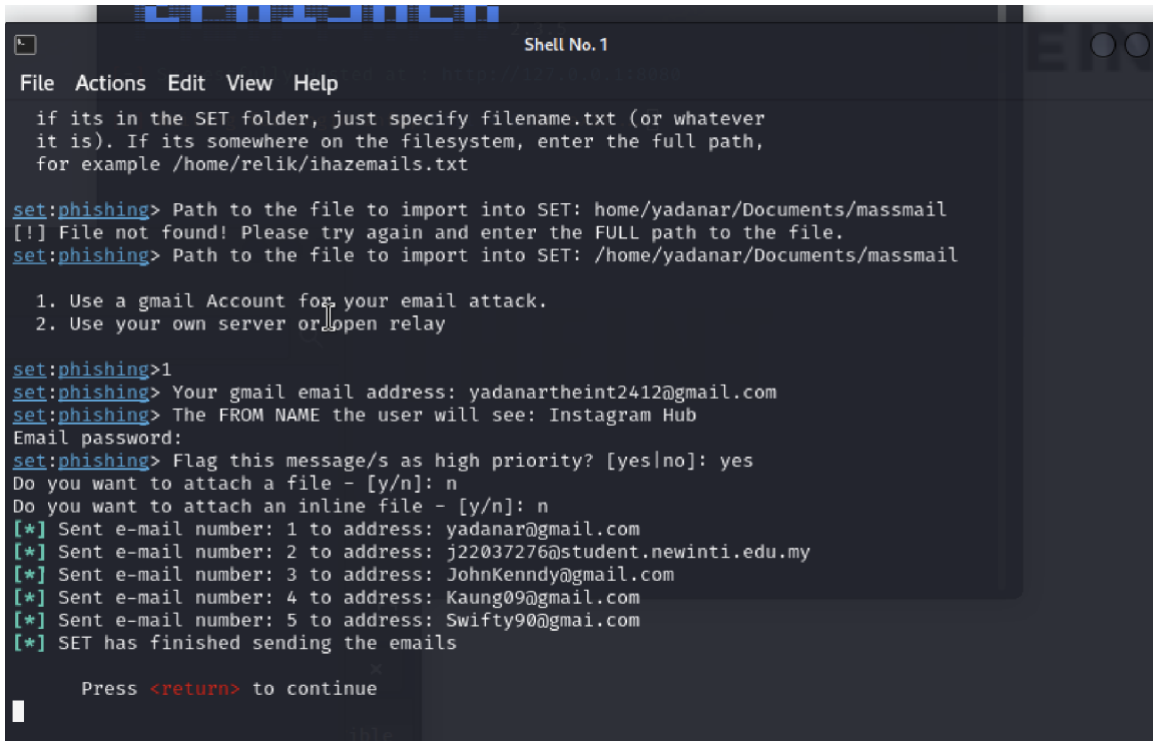


2 options pop up again. In this step I will use my own email to send phishing mails. After I choose option 1 for it, I need to enter my email and set the FROM NAME. In this case, I want pretend like a customer service from Instagram, so I will set it as “Instagram Hub”. I have included an email subject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

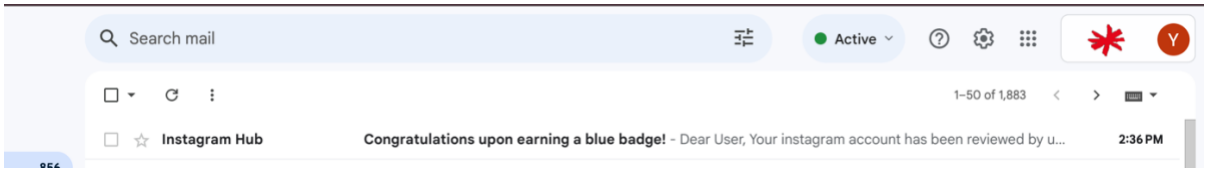


After I have entered the password for sender’s email, I am ready to send phishing mails. Phishing mail has been sent to all the victim mail address that I have created in the text file above. Now, I can go and check to one of those email address whether my phishing mail has successfully sent or not.

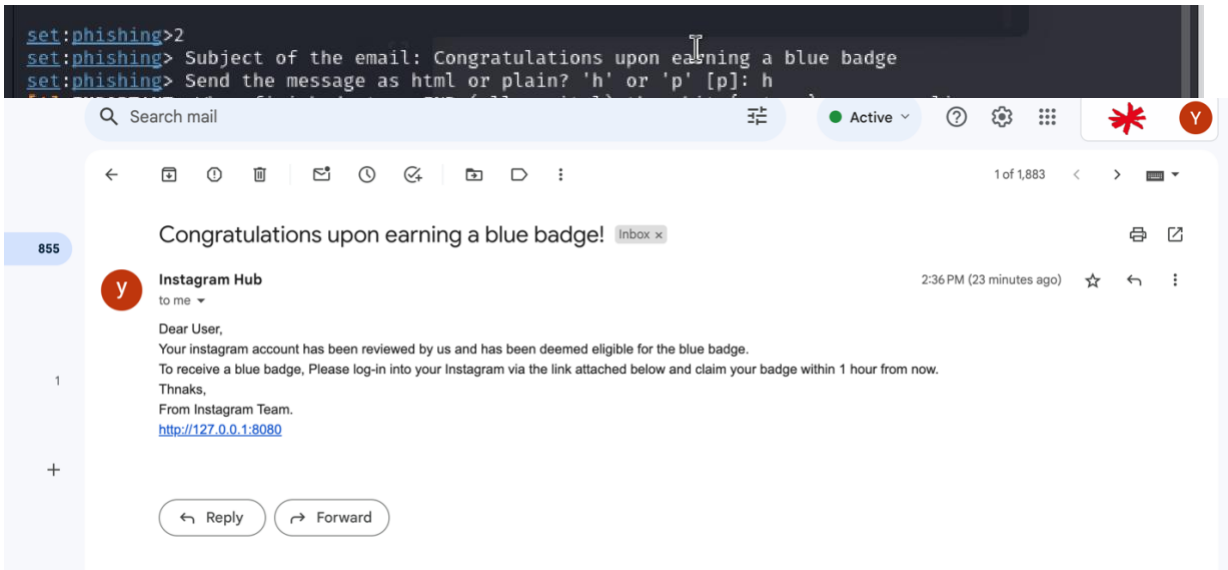




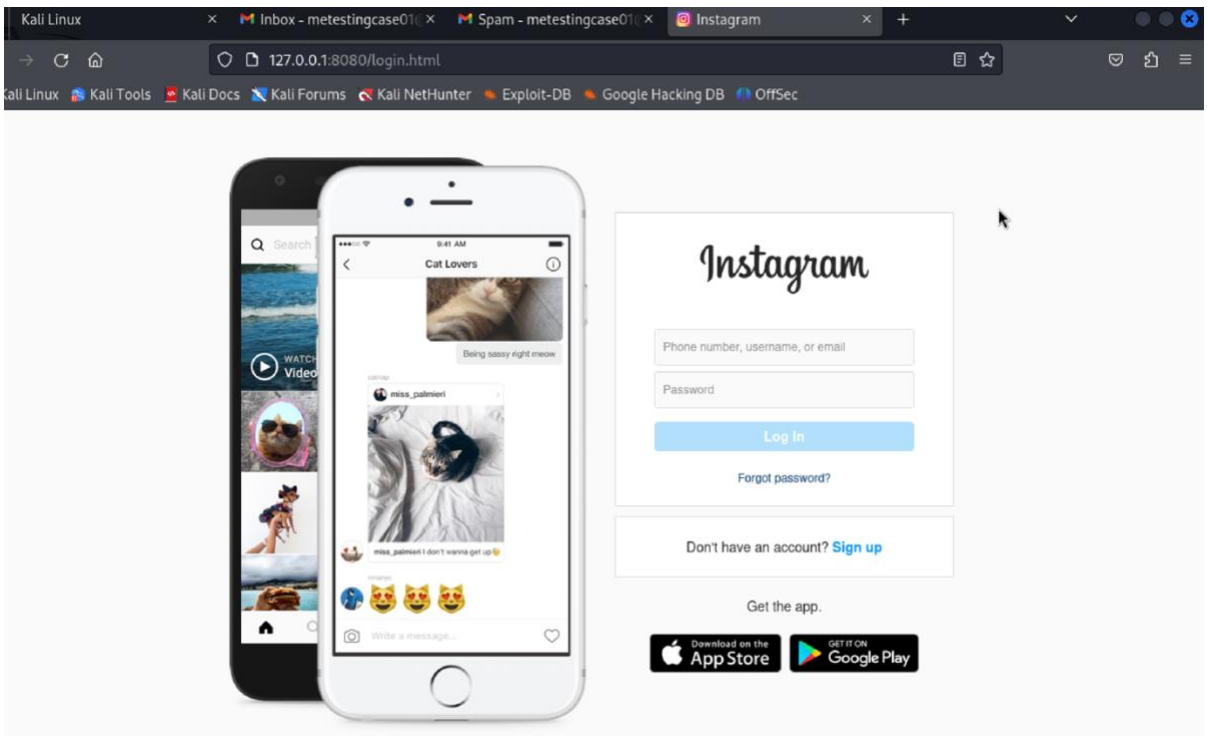
In one of my victim mail addresses, I have received a phishing mail with the From Name – Instagram Hub that I have set. Since I have set phishing mail option as the high priority mail, it goes directly into the victim's inbox instead of spam mail.



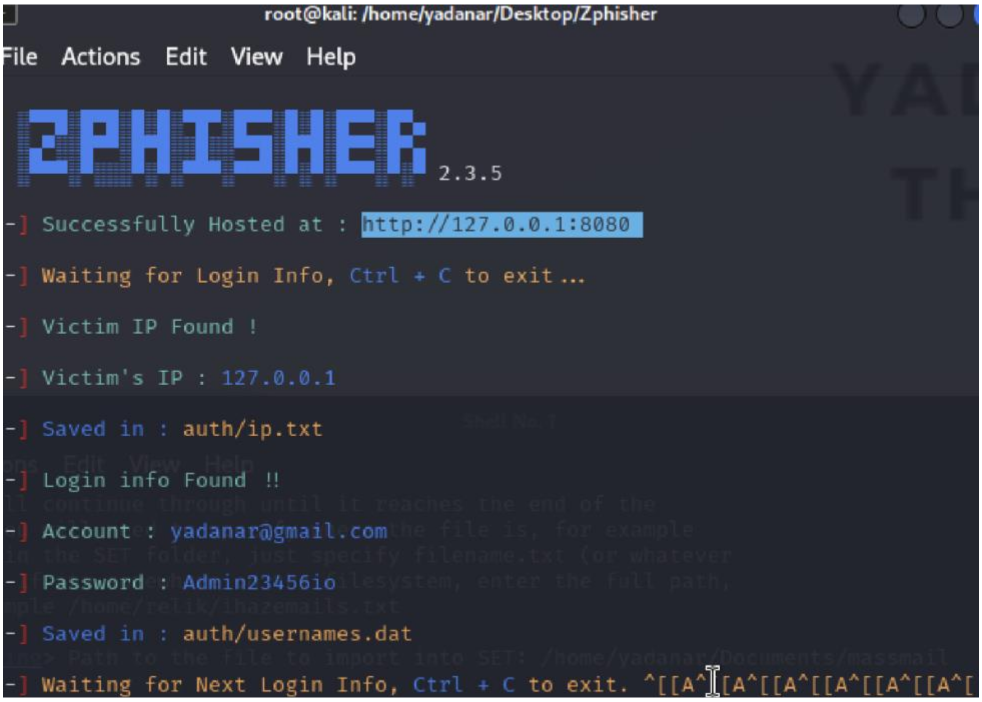
Before I send the phishing mail, I have two options whether I want to send it as a plain text or html template form. If I choose to send it as plain text, the phishing mail will be like this which is all in text form.

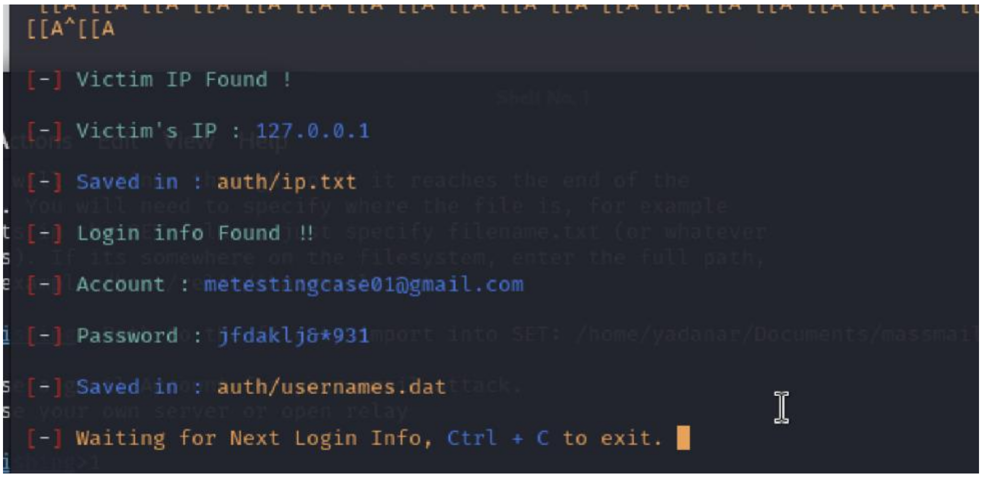


This is the clone phishing site of Instagram for victims.



Once the victims enter the login credentials, I can see their login mail and password on my Linux site including the victims' Ips.

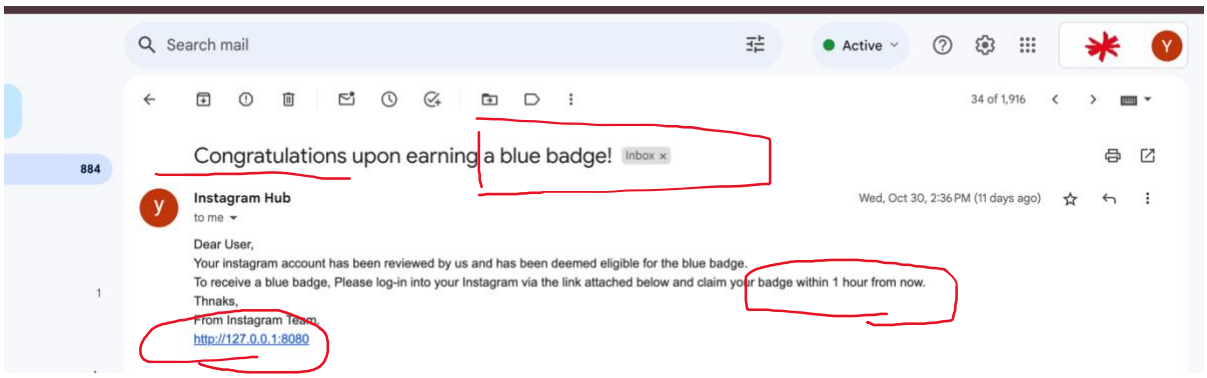




<u>Defending tool</u>

To prevent phishing and others unnecessary cookies, virus, we can use firewall as it can protect against outside cyber attackers by shielding your computer or network from malicious or unnecessary network traffic. Firewalls can also prevent malicious software from accessing a computer or network via 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.



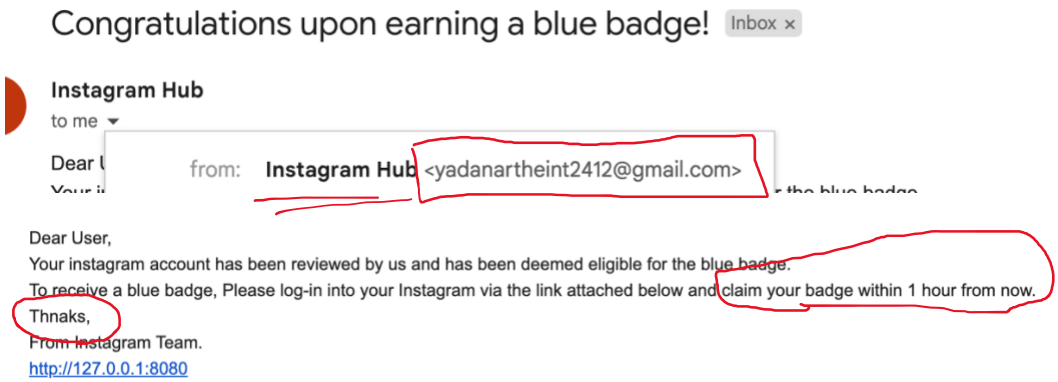
Criteria 3

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.
11. [online] Available at: https://bit.ly/3pTQLVS.