Using Kali Linux to Attack a Social Media Account Phishing Attack

- Jayawardhana B.P.W

  IT20600570

- Thisitha.K.L.D

  IT20618872

Abstract— Phishing is a type of network attack in which an attacker creates a fake version of a legitimate website to trick a web user into disclosing personal information. Phishing is a technique that combines social engineering and technological methods to convince someone to provide personal information. This research looks at phishing and social engineering attacks and how they happen in people's lives. The most common methods of phishing are email spoofing and instant messaging. It is intended for people who are unfamiliar with social engineering attacks and web security, such as those who are unconcerned about the privacy of their accounts, such as Facebook, Gmail, credit card accounts, and other financial accounts.

Today, social engineering attacks are common. It uses psychological manipulation to persuade customers to fabricate or provide sensitive information to gain unauthorized access to a computer system. Acts such as abusing human goodwill, avarice, or curiosity to gain access to restricted entrance buildings or persuade consumers to install backdoor software are also examples of the term. The first attacker gathers information about the victim after deciding on an assault strategy. It can be divided into two types: technology-based deception and human-based deception. In a technology-based technique, the individual is led to believe he is interacting with a legitimate utility or system, revealing private information and gaining access to an organization's network.

Keywords—phishing, information security, social engineering

I. Introduction

Cybercriminals who've depended on the illicit use of digital assets—specially personal information—for inflicting damage on individuals are rapid increasing and developing as nicely. Identification robbery, that is defined as impersonating a person's identity to scouse borrow and use their non-public data (i.e., financial institution details, social safety variety, or credit card numbers, and so forth.) via an attacker for the individuals' very own benefit, now not just for stealing money however additionally for committing different crimes, is one of the riskiest crimes that each one net customers face. Cyber thieves have advanced their own approaches for obtaining statistics, although social-engineering-based totally attacks continue to be their favored strategy. A phishing attack is a sort of social engineering crime that permits an attacker to scouse borrow someone's identification. Phishing has been one of the maximum severe troubles, with many internet users falling prey to it. It's far a social engineering attack in which a phisher attempts to persuade humans to offer touchy records via unlawfully the usage of a public or straightforward corporation in an automated sample, in the hopes that the net consumer could believe the message and disclose the victim's sensitive facts. After receiving an email and clicking on an embedded link, phishers employ social engineering approaches to guide traffic to malicious web sites. As a substitute, attackers may use Voice over IP (VoIP), brief Message carrier (SMS), and immediately Messaging to perform their assaults (IM). Phishers have additionally moved far from sending mass-e mail messages to unidentified sufferers and closer to greater focused phishing by way of sending emails to character victims, a exercise referred to as "spear-phishing."

Cybercriminals frequently take advantage of folks that lack digital/cyber ethics or are poorly educated, in addition to technological flaws. For this reason, most phishing efforts depend on human nature rather than sophisticated era. No matter the fact that human beings are to responsible for the facts safety chain's flaws, nobody is aware of which ring is the first to be penetrated. Research reveal that a few personality characteristics make people greater receptive to specific enticements. Individuals who are greater inclined to obey authority, as an example, are more likely to be sufferers of a enterprise e mail Compromise (BEC) that looks like it's far from a economic organization and needs instantaneous reaction. As proven in emails supplying massive reductions, loose present cards, and other incentives, an attacker may also make the most greed.

The attacker makes use of numerous channels to trap the sufferer into a fraud or supply a payload to gather sensitive personal records. But phishing assaults have already ended in sizeable losses, and they may also damage the victim's popularity or national protection. Cybersecurity Ventures estimates worldwide cybercrime damages might reach $6 trillion by means of 2021, up from $3 trillion in 2015. Consistent with the United Kingdom's legitimate cybersecurity breaches survey 2020, phishing attacks are the maximum commonplace. The value of restoration, lack of reputation, penalties from records laws/rules, and missed productivity are all massive costs for firms.

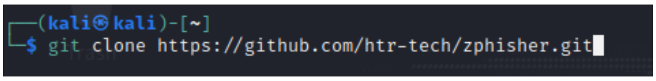
Phishing is a mixture of social psychology, era, safety, and politics. In keeping with a current look at, almost 90% of firms had been phished in 2019. 88 percent pronounced spear-phishing attacks, 83 percent voice phishing (Vishing), 86 percentage social media attacks (Smishing), and eighty-one percentage malicious USB drops. In keeping with the Proofpoint1 annual research, phishing attacks climbed from seventy-six% in 2017 to 83% in 2018. The range of phishing attacks located in Q2 2019 become considerably better than the preceding 3 quarters. The Anti-Phishing working organization (APWG2) located that phishing assaults rose within the first zone of 2020. Facts display that phishing assaults have accelerated in sophistication over the years, attracting the eye of cyber researchers and builders trying to identify and mitigate their effect. This internet site tries to research the phishing trouble through providing distinctive definitions, data, anatomy, and viable countermeasures.

Zphisher is a shell programmed phishing attack inside and out of doors LAN connected to grok. It can be utilized in social engineering pen-testing jobs. It can additionally assist pink group members gather passwords for other functions. Similarly, Blackeye has 32 net templates + 1 customizable. By touring the hyperlink, this tool can collect IP and vicinity records

Figure 1

II. Methodology

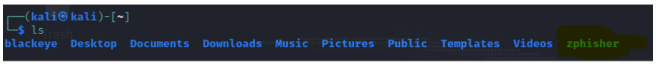
Open the Kali Linux root account on your computer. Next open the terminal in Kali Linux and type the Zphisher clone (git clone https://github.com/htr-tech/zphisher.git) in the terminal and press enter.[Figure 2]



```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/htr-tech/zphisher.git
```

[Figure 2]

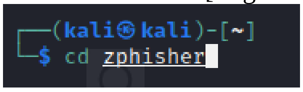
After enter the git clone command then type " ls" we can see zphisher in bar [*Figure 3*]



```
┌──(kali㉿kali)-[~]
└─$ ls
blackeye  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  zphisher
```

[Figure 3]

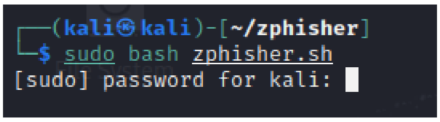
Next enter to the file[Figure 4]



```
┌──(kali㉿kali)-[~]
└─$ cd zphisher
```

[Figure 4]

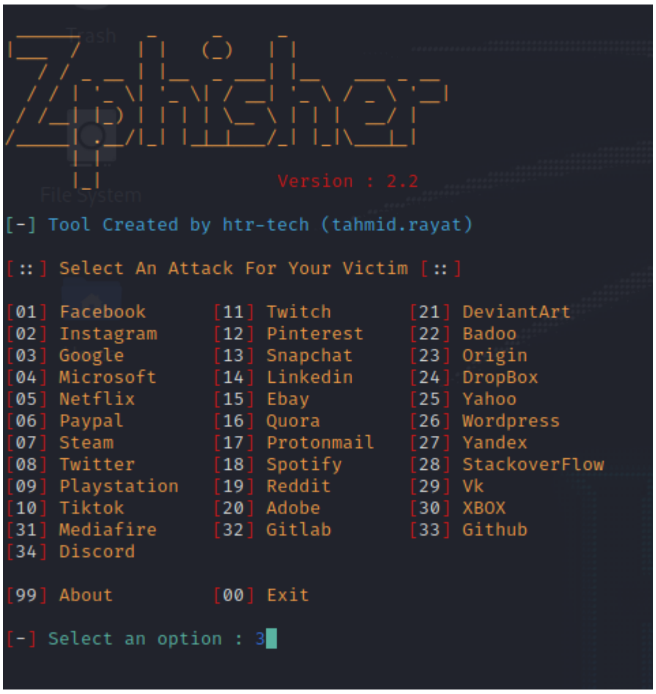
Next type the password and press enter button to go. [Figure 5]



```
┌──(kali㉿kali)-[~/zphisher]
└─$ sudo bash zphisher.sh
[sudo] password for kali:
```

[Figure 5]

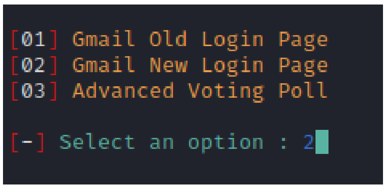
After entering password a menu will show up as in the picture. Select the option what you want. We select "option number 3" [Figure 6]



```
                         Version : 2.2

[-] 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

[99] About         [00] Exit

[-] Select an option : 3
```

[Figure 6]

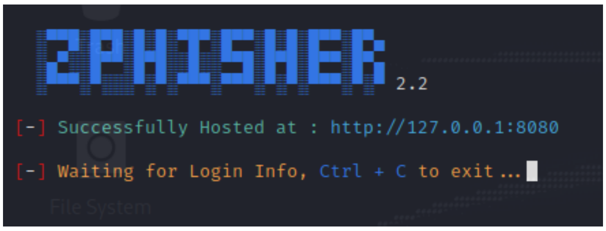
Then we select New login page. Actually it is not suspicion. Because lot of people try to go old login page. We select number 2. [Figure 7]



```
[01] Gmail Old Login Page
[02] Gmail New Login Page
[03] Advanced Voting Poll

[-] Select an option : 2
```

[Figure 7]

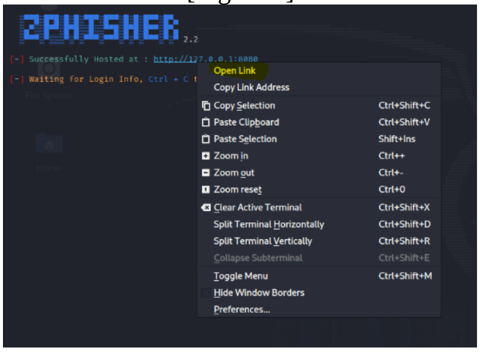
After clicking we can see this [figure 8]



```
ZPHISHER 2.2

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

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

[Figure 8]

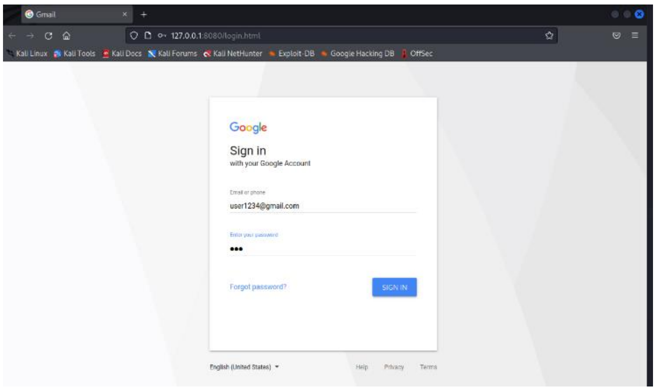
Then click "open link"
[Figure 9]



```
ZPHISHER 2.2
[-] Successfully Hosted at : http://127.0.0.1:8080
[-] Waiting for Login Info, Ctrl + C t
```

Open Link
Copy Link Address
Copy Selection Ctrl+Shift+C
Paste Clipboard Ctrl+Shift+V
Paste Selection Shift+Ins
Zoom in Ctrl++
Zoom out Ctrl+-
Zoom reset Ctrl+0
Clear Active Terminal Ctrl+Shift+X
Split Terminal Horizontally Ctrl+Shift+D
Split Terminal Vertically Ctrl+Shift+R
Collapse Subterminal Ctrl+Shift+E
Toggle Menu Ctrl+Shift+M
Hide Window Borders
Preferences...

[Figure 9]
Then after going to browser and type the attacker's Ip address. Eg -email – user1234@gmail.com
Password - 123. [Figure 10]

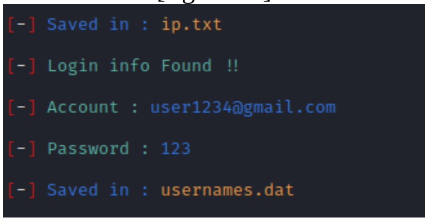


Email or phone
user1234@gmail.com

Enter your password
•••

[Figure 10]

If an unwary visitor enters their information and clicks "Log In," the phony website redirects them to the official login page. Individuals are frequently prone to go.
Gmail first login page.
Following the successful assault, the user's
The login and password are plainly shown on our terminal.
[figure 11]



```
[-] Saved in : ip.txt

[-] Login info Found !!

[-] Account : user1234@gmail.com

[-] Password : 123

[-] Saved in : usernames.dat
```

[Figure11]

III. Results and Decision

Due to the fact phishing is a method for gathering data about a person, it has an immediate effect on that person's personal and social existence. Due to its short increase, social media presently has a big quantity of customers all around the global. Because of the developing quantity of users and the usage of 1/3-party packages to log into money owed, cyber criminals have turn out to be a brand-new target. In popular, social media and its users enjoy a excessive stage of agree with. As a end result, social media customers are more likely to reveal personal records with them, such as wherein they reside, their birthdays, their occupations, and their friends. This gives attackers sufficient information to obtain unlawful get right of entry to social media debts the use of these types of assaults. This outcomes in a vast amount of facts robbery.

It is crucial to appoint a two-thing authentication technique to prevent these styles of assaults. Due to the fact, if a two-component authentication mechanism is in area for an account, everybody may additionally log in the usage of the authentication code this is given to the consumer's trusted network as the second pin code that the social media asks for before granting get right of entry to that account. As a result, really understanding the login or password is insufficient for the attacker. The usage of a hardware safety key's every other way to guard yourself towards social media phishing. Every person who does not have that key might be not able to log in to a social account the usage of a distinct device. Because the attacker does not have the key to log in to the account using their devices, the attacker's try will be rendered useless.

Every other preventative measure we might also take is to never click on a strange internet site that asks for non-public data. Attackers that appoint phishing to gain access to a system frequently utilize this link technique to gain customers' passwords and usernames. If we're unsure about the source of a link, we have to keep away from clicking on it.

IV. Conclusion

Phishing attacks may additionally take many exceptional shapes in an effort to reap touchy records from customers. In keeping with cutting-edge information, phishing tries are still powerful, implying that gift defenses are insufficient to perceive and prevent these attacks, in particular on clever devices.

Phishing is a method that makes use of fraudulent web sites and emails to achieve touchy information about the sufferer. It is one of the most severe cyber-attacks that influences groups, personal computer systems, and different digital system. It might be hard to inform the difference between valid and phishing emails. This assault may be prevented using a selection of techniques. Anti-phishing technologies and platforms which can be up to date on a everyday basis may be quite powerful. This research seems into phishing, the mechanics of the attack, the distinct paperwork it may take, and the available methods for managing it.

References

[1] "Protect Yourself from Fraudulent Emails". PayPal. Archived from the original on April 6, 2011. Retrieved July 7, 2006.

[2] "Phishing Messages May Include Highly-Personalized Information". The SANS Institute. Archived from the original on December 2, 2006.

[3] Doctorow, Cory (August 28, 2015). "Spear phishers with suspected ties to Russian government spoof fake EFF domain,

[4] attack White House". Boing Boing. Archived from the original on March 22, 2019. Retrieved November 29, 2016.

[5] "Phishing | History of Phishing". phishing.org. Archived from the original on 2018-09-09. Retrieved 2019-09-13.

[6] Fruhlinger, J., 2021. What is phishing? How this cyber attack works and how to prevent it. [online] CSO Online. Available at: https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

[7] Strawbridge, G., 2021. How To Protect Yourself From Social Media Phishing | MetaCompliance. [online] MetaCompliance. Available at: https://www.metacompliance.com/blog/how-to-protect-yourself-from-social-media-phishing/