International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 06 | Jun 2022 www.irjet.net p-ISSN: 2395-0072

Credential Harvesting Using Man in the Middle Attack via Social Engineering

Mounika V[1], Dr. Vibha M B[2]

[1]Student Dept. of MCA, Dayananda Sagar College of Engineering, Bangalore, Karnataka, India
[2]Associate Professor, Dept. of MCA, Dayananda Sagar College of Engineering, Bangalore, Karnataka, India

---

ABSTRACT – With growing internet users threat landscape is also increasing widely. Even following standard security policies and using multiple security layers will not keep users safe unless they are well aware of the emerging cyber threats and risks involved. Humans are the weakest people in the security system as they possess emotions that can be exploited with minimum reconnaissance. Social engineering is a type of cyberattack where it exploits human behaviour or emotions to collect sensitive information such as username, password, personal details, etc.

This paper proposes a system that helps end-users to understand that even using security mechanisms such as two-factor authentication can be useless when the user is not aware of basic security elements and make internet users aware of cyber threats and the risk involved.

KEYWORDS: *Phishing, toolkits, social engineering, cyber awareness*

1. INTRODUCTION

Phishing is the most common type of social engineering attack. The nature of this attack makes it more dangerous. As humans can be exploited easily with emotions and various other factors, even training them gives no guarantee of being safe from these attacks. Making awareness of these threats to users has been a very important part of organizations.

Phishing is when an attacker sends phony messages to a human victim in the hopes of tricking them into revealing sensitive information or installing malware on their computer. Phishing attacks have evolved, allowing the attacker to track everything the victim does while on the site and evading any additional security measures. Phishing attacks can be carried out by anyone with rudimentary expertise, making them a dangerous and common threat [7].

Internet users need to be trained about these types of attacks and also need to be thought about how to respond to the attacks.

There are many phishing toolkits available in the market that are used by organizations to train their employees. These toolkits help to simulate a real-world phishing attack and have many other features such as launching and managing multiple campaigns, generating reports, GUI, and many more. But these toolkits require a setup environment and are specific to the use case. These toolkits are not suitable for novice users [7].

At present irrespective of occupation, age probably most people have a smartphone, have interest access, and use online services such as social media, online banking, and many more. Most of the users are not aware of common cyber threats and are at risk of cyber-attacks [3].

This project proposes a system that is a lightweight simple to use phishing simulation toolkit consisting of pre-loaded social networking sites which help train users on cyber threats such as phishing attacks.

2. LITERATURE REVIEW

The poll was done in 2019 with approximately 4800 participants, and the results led to the following conclusions. According to the survey results, 55 percent of respondents are unfamiliar with two-factor authentication, and 68 percent use the same password for several authorizations. Only 30 percent of users use strong password with at least a number, an alphabet, and a special character, and only 50 percent of users employ powerful security mechanisms like two-factor authentication and backup. 90 percent of people will not change their password unless they are prompted to [3].

The results of a poll on internet usage and cyber security awareness were done in 2017 across age groups ranging from 8 to 21 years. Antivirus was the most familiar term among all age groups, followed by firewalls and security warnings. Tracker and phishing were unfamiliar terms to the responders in the 8-12 age range. This emphasizes the necessity for people to become more aware of the phishing aspects of cybersecurity. Phishing and tracker are terms that less than half of people are familiar with [4].

The other poll, on the trust factors of social engineering attacks on social networking sites, was done in 2021 with 35 participants using a pseudo-social-networking-service application that was subjected to a social engineering attack. The findings show that characteristics such as the attacker's personal information and the content of the message have little bearing on trust. Only the display of a negative response to the post has an impact on trust [5].

3. PROPOSED SYSTEM

This project can be said to be a tool that helps train internet users on cyber awareness. Unlike other toolkits [1][2] available on the market for phishing attack simulation, this toolkit is a menu-driven interactive application that shows how sophisticated a phishing attack can be. The proposal system consists of cloned social networking sites with two factor authentication templates allowing users to choose a template to simulate an attack. The following figure shows the phishing process.

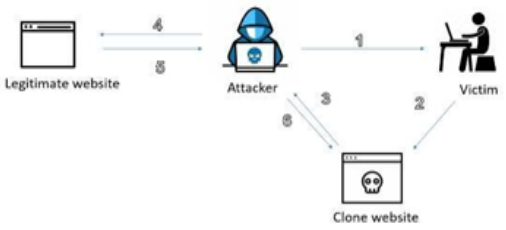

Fig 1 Proposed flow

Phase-1: Capturing credential and validate

1. Attacker chooses pre-defined clone website, hosts it on his personal server, and sends a phishing link to the victim.
2. Assuming the victim visits cloned website which is hosted on the attacker system and submits credentials.
3. Attackers extracts these credentials and validates them with the legitimate server (imitates as a genuine user).
4. Legitimate server responds to the attacker with the message stating whether the credentials are valid or not.
5. If the response is successful from the server and there is no 2FA then the victim is redirected to the genuine website and, the attacker will be established with a valid session.

Else if credentials are not valid, the attacker responds with a message to the victim stating that the given credential are incorrect and requests to login again.

Phase-2: Capturing 2FA token and validate

6. After successful validating credentials If the application has 2FA then the attacker serves the webpage requesting for 2FA token to the victim
7. The same process continues from step 2 for 2FA validation.

After successfully completing the above steps, the attacker will be established with a valid session and the victim is redirected to the landing page which will be a genuine page.

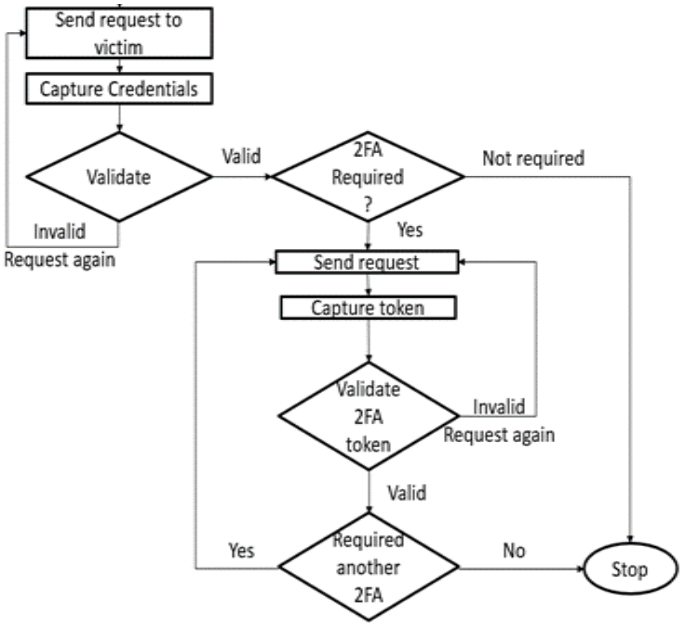

fig 2 Dataflow diagram

Hence if the victim is not aware of phishing attacks or do not ensure security elements such as domain name integrity and use a secure protocol (HTTPS), at every stage of authentication and authorization, then using security mechanism like two-factor authentication can be bypassed by the attacker via social engineering.

4. FUTURE SCOPE

Every user on the internet should be aware of cyber-attacks and their risk. Educating internet users on common threats is important to successfully fight against cyber threats.

5. CONCLUSION

Proposing a basic, interactive, and menu-driven phishing toolkit that requires minimal setup to launch phishing attack simulation. Even a novice user can use the tool to launch phishing attack simulations to educate internet users on cyber awareness.

This project has been developed to shows how sophisticated a phishing attack can be, hence bringing cybersecurity awareness among people has been a challenge. Launching phishing attack exercises on people helps them understand the risk even better than reading from books or posters. Experimental learning helps better understanding.

6. ACKNOWLEDGMENT

I want to specially thank **Dr. Vibha M B** for guiding me throughout this research paper, which has expanded my knowledge on data security. Without her support I do not think this research paper will be been success, I am very thankful.

7. REFERENCES

[1] https://github.com/xHak9x/socialPhish

[2] https://www.trustedsec.com/tools/the-social-engineer-toolkit-set/

[3] S. S. Tirumala, M. R. Valluri and G. Babu, "A survey on cybersecurity awareness concerns, practices and conceptual measures," 2019 International conference on computer communication and informatics (ICCCI), 2019, pp. 1-6, doi:10.1109/ICCCI.2019.8821951.

[4] S. S. Tirumala, A.sarrafzadeh, and P. Pang, "A survey on internet usage and cybersecurity awareness in students," in 2016 14th Annual Conference on Privacy, Security and Trust, PST 2016, 2016, pp. 223-228. Doi:10.1109/PST.2016.7906931.

[5] P. Y. Leonov, A. V. Vorobyev, A. A. Ezhova, O. S. Kotelyanets, A. K. Zavalishina and N. V. Morozov, "the main Social Engineering Techniques Aimed at Hacking Information Systems," 2021 Ural Symposium on Biomedical Engineering, Radio electronics and Information Technology (USBEREIT), 2021, pp. 0471-0473, doi:10.1109/USBEREIT51232.2021.9455031.