

**EVALUATION OF INTERNSHIP REPORT**

## B.Tech: III Year

**Department of Computer Science & Information Technology**

**Name of the Student: Naman Mehta**

**Branch & section: CSIT – 2**

**Roll No: 0827CI201114**

**Year: 2022-23**

## Department of Computer Science & Information Technology

**AITR, Indore,**

**ACROPOLIS INSTITUTE OF TECHNOLOGY & RESEARCH, INDORE**

# Department of Computer Science & Information Technology

**Certificate**

Certified that training work entitled “Cyber Security” is a bonafied work carried out after sixth semester by “Naman Mehta” in partial fulfilment for the award of the degree of Bachelor of Technology in Computer Science and Information Technology from “Prof. Nidhi Nigam &

Yash Arya” Acropolis Institute of Technology and Research during the academic year 2022-23.

*Name and Sign of Training Coordinator Name & Sign of Internship Coordinator*

**ACROPOLIS INSTITUTE OF TECHNOLOGY & RESEARCH, INDORE**

# Department of Computer Science & Information Technology

**ACKNOWLEDGEMENT**

I would like to acknowledge the contributions of the following people without whose help and guidance this report would not have been completed. I acknowledge the counsel and support of our training coordinator, Prof. Nidhi Nigam, & Mr. Yash Arya, CSIT Department, with respect and gratitude, whose expertise, guidance, support, encouragement, and enthusiasm has made this report possible. Their feedback vastly improved the quality of this report and provided an enthralling experience. I am indeed proud and fortunate to be supported by him/her. I am also thankful to Dr. Shilpa Bhalerao, H.O.D of Computer Science Information Technology Department, for her constant encouragement, valuable suggestions and moral support and blessings. Although it is not possible to name individually, I shall ever remain indebted to the faculty members of CSIT Department, for their persistent support and cooperation extended during this work.

*Naman Mehta*

*0827CI201114*

### ACROPOLIS INSTITUTE OF TECHNOLOGY & RESEARCH, INDORE

### INDEX

S.no CONTENTS Page no

1. Introduction to technology Undertaken…….... 5

2. Objectives ………..……………………………….... 6

3. Project undertaken ……………………….. 7

4. Screenshots of Project and Certificates……………………….. 13

5. Github Links (Project/certificate/video/copy of report).………. 15

6. Conclusion……….. ……………………………………. 15

7. References/ Bibilography………………………………..…………… 15

# Introduction to technology Undertaken

**Phising Attack**

Phishing messages appear to be from a legitimate source but, in reality, they are from cyber criminals who are attempting to trick you into sharing sensitive information. In these messages, cyber criminals frequently use scare tactics, such as threatening to close your accounts or arrest you unless you give them information that you would ordinarily keep secure. If successful, the cyber criminal can use that information to steal your identity or to gain access to your accounts.

Phishing refers to any attempt to steal information, whatever the means. Phishing messages can come in almost any form: Emails, text messages, social media  direct messages, or phone calls.

**Zphisher** is a powerful open-source tool Phishing Tool. It became very popular nowadays that is used to do phishing attacks on Target. Zphisher is easier than Social Engineering Toolkit.  It contains some templates generated by tool called Zphisher and offers phishing templates webpages for 18 popular sites **such as Facebook, Instagram, Google, Snapchat, GitHub, Yahoo, Proton mail, Spotify, Netflix, LinkedIn, WordPress, Origin, Steam, Microsoft, etc**. It also provides an option to use a custom template if someone wants. This tool makes it easy to perform a phishing attack. Using this tool you can perform phishing in (wide area network). This tool can be used to get credentials such as **id, password.**

# Objectives

The objective of our research is to study and analyse various security issues in Phishing Attacks on Internet with an attempt to suggest a model of security implementation, which will cover the advantages of the available process used to handle the security issues in Internet Computing and will be able to provide more reliable aspect for implementation of Security in Internet. Our research will effort to examine security issues of Phishing Attacks in Internet computing. The objective of this study is to provide benefit to the Internet computing users as well as Cyber Laws so that a systematic and more reliable approach can be used to recover vulnerability issues in Phishing Attacks on Internet. Main objectives of this research are to identify and consolidate the vulnerabilities associated with security of Internet Computing, and to formulate a methodology to evaluate and categorize these vulnerabilities. The insights gained from the research would form a set of guidelines for designing less vulnerable Internet Computing Security, in the form of a structured framework for risk evaluation

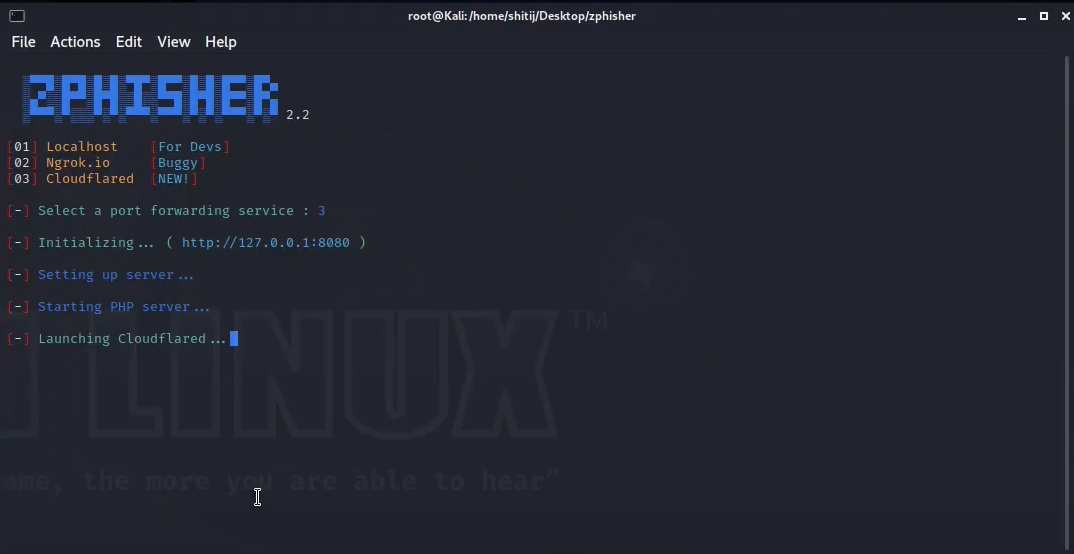
# Project undertaken

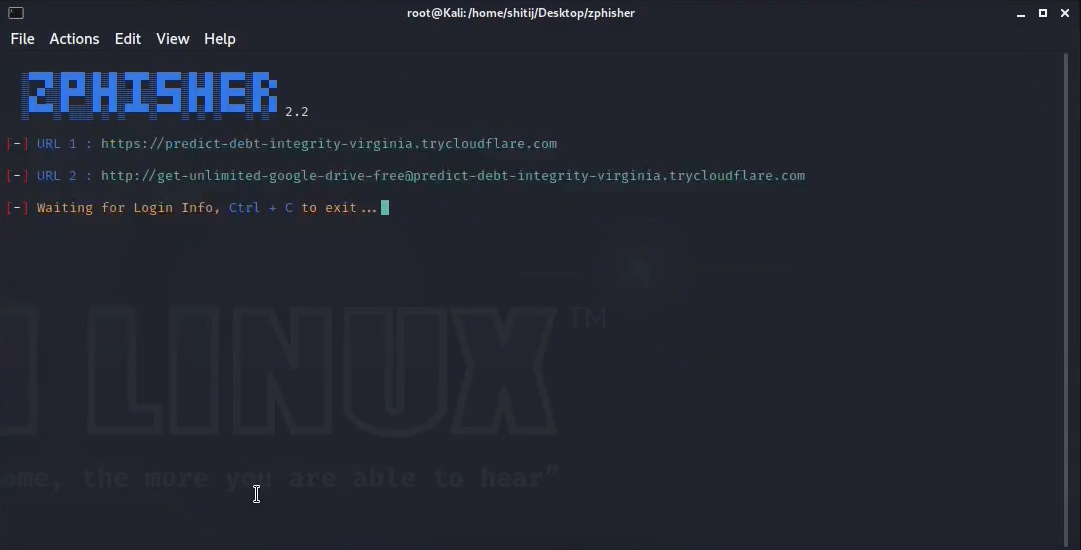
Text

Description automatically generated

Text

Description automatically generated





Text

Description automatically generated

Text

Description automatically generated

# Screenshots of Project and Certificates





Text

Description automatically generated

Text

Description automatically generated

# Github Links (Project/certificate/video/copy of report)

* [naman1102/EOI\_NAMAN\_MEHTA (github.com)](https://github.com/naman1102/EOI_NAMAN_MEHTA)

# Conclusion

Like many security tools, the MP has great potential with all of the features that have been presented. But again like many security tools there is the possibility of misuse. It is up to the individual end user to decide how it will be used. The bad guys already possess the tools capable of doing what is now possible with the MP. Security practitioners need to know how those same bad guys might attack and what is possible. Layered security is not just ACL’s, firewalls, network segregation, IDS, etc. The most important layer in the security process is the human layer. What that human layer can bring to the table is every bit as important as the rule base on the firewall and being armed with the Anit-phising techniques will only add to that human value.

# References/ Bibilography

* [www.geeksforgeeks.org](http://www.geeksforgeeks.org)
* <https://tools.kali.org/exploition-tools/metasploit-framework>
* [www.security.net](http://www.security.net)
* [www.google.com](http://www.google.com)
* [www.youtube.com](http://www.youtube.com)