EVALUATION OF INTERNSHIP REPORT

B.TECH: III Year

Department of Computer Science & Information Technology

Name of the Student:	**PARTH SHARMA**
Branch & section:	**CSIT 2**
Roll No:	**0827CI201128**
Year:	**2022**

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 in fifth semester by "*PARTH SHARMA*" in partial fulfilment for the award of the degree of Bachelor of Technology in Computer Science and Information Technology from "*Prof. Nidhi NIgam/Assistant professor CSIT department*"of Acropolis Institute of Technology and Research during the academic year 2022-23.

Prof. Praveen Gupta *Prof. Nidhi Nigam*

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 "*Prof. Nidhi Nigam /Assistant professor CSIT department*", 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. 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.

PARTH SHARMA

0827CI201128

ACROPOLIS INSTITUTE OF TECHNOLOGY & RESEARCH, INDORE

INDEX

Cyber Security Introduction - Cyber Security Basics:

Cyber security is the most concerned matter as cyber threats and attacks are overgrowing. Attackers are now using more sophisticated techniques to target the systems. Individuals, small-scale businesses or large organization, are all being impacted. So, all these firms whether IT or non-IT firms have understood the importance of Cyber Security and focusing on adopting all possible measures to deal with cyber threats.

What is cyber security?

"Cyber security is primarily about people, processes, and technologies working together to encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, etc."

OR

Cyber security is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

· The term cyber security refers to techniques and practices designed to protect digital data.

· The data that is stored, transmitted or used on an information system.

Why is cyber security important?

Listed below are the reasons why cyber security is so important in what's become a predominant digital world:

· Cyber-attacks can be extremely expensive for businesses to endure.

· In addition to financial damage suffered by the business, a data breach can also inflict untold reputational damage.

· Cyber-attacks these days are becoming progressively destructive. Cybercriminals are using more sophisticated ways to initiate cyber-attacks.

Cyber security Fundamentals – Confidentiality:

Confidentiality is about preventing the disclosure of data to unauthorized parties.

It also means trying to keep the identity of authorized parties involved in sharing and holding data private and anonymous.

Often confidentiality is compromised by cracking poorly encrypted data, Man-in-the-middle (MITM) attacks, disclosing sensitive data.

Standard measures to establish confidentiality include:

· Data encryption
· Two-factor authentication
· Biometric verification
· Security tokens

Availability

Availability is making sure that authorized parties are able to access the information when needed. Standard measures to guarantee availability include:

· backing up data to external drives
· implementing firewalls
· having backup power supplies
· Data redundancy

Integrity

Integrity refers to protecting information from being modified by unauthorized parties. Standard

measures to guarantee integrity include:

· Cryptographic checksums
· Using file permissions
· Uninterrupted power supplies
· Data backups

.

.

.

Types of Cyber Attacks

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.

1) **Web-based attacks**
2) **System-based attacks**

Web-based attacks

These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows

1. DNS Spoofing

DNS spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

2. Injection attacks

It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

Example- SQL Injection, code Injection, log Injection, XML Injection etc. **2.**

3. Phishing

Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication

4. Session Hijacking

It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

5. Brute force

It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.

System-based attacks

These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows

1. Worm

It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted sender.

2. Virus

It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of it into other computer programs when executed. It can also execute instructions that cause harm to the system.

3. Trojan horse

It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

4. Backdoors

It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

5. Bots

A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

PROJECT UNDERTAKEN:

The aim of this project is to perform a DOS attack, A Denial-of-Service (DoS) attack is **an attack meant to shut down a machine or network, making it inaccessible to its intended users**. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.

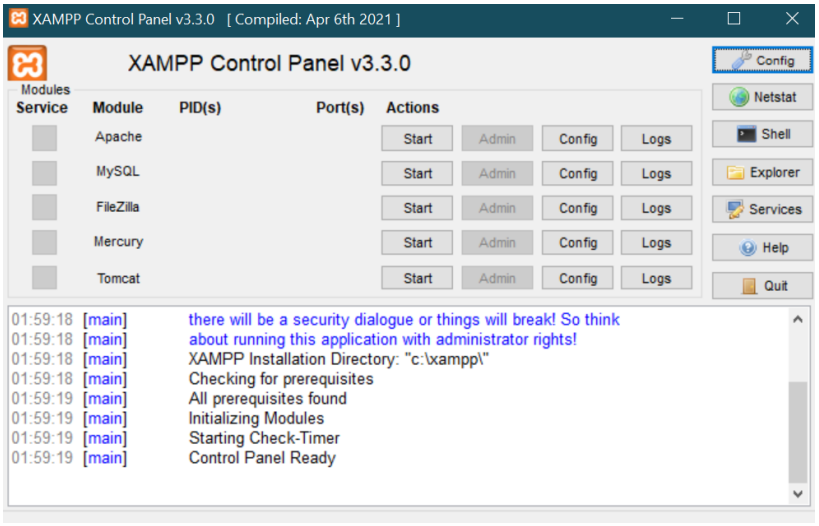
About DOS attack:

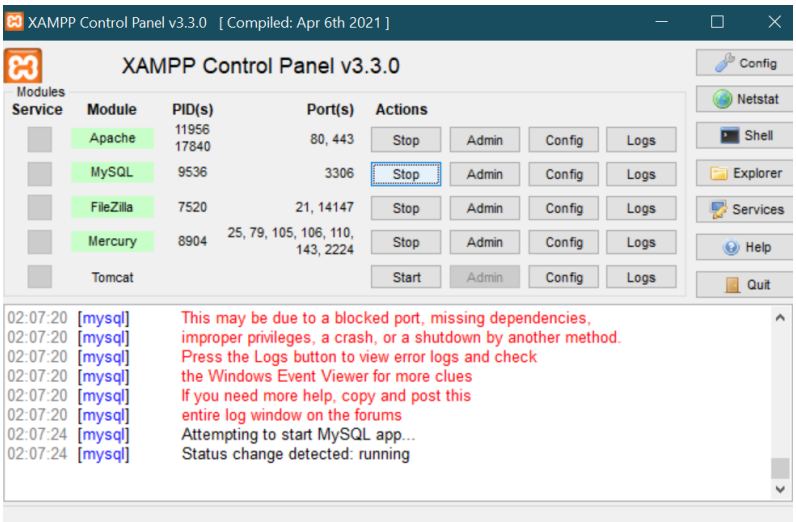
A denial of service occurs when a legitimate user is denied access to a network, system, device, or other resources that they are otherwise authorized to access. That can include their email, e-banking account, public online services, etc.

PROJECT SCREENSHOTS

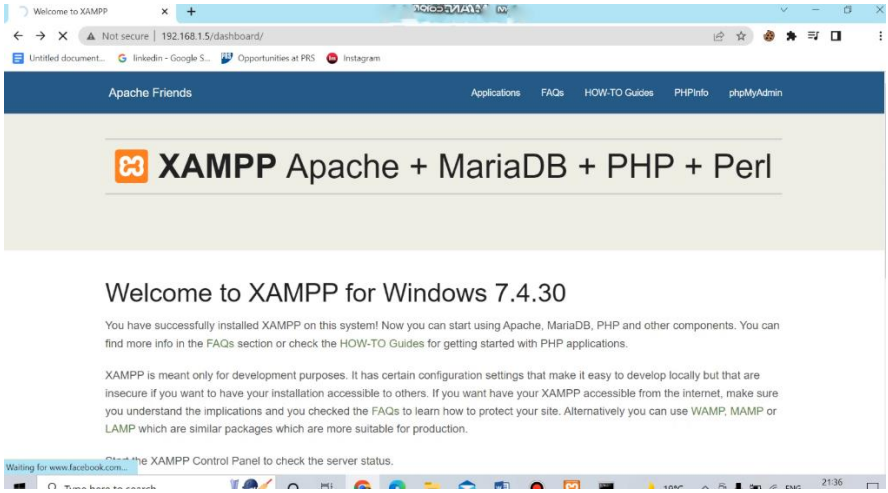
PROCESS

Here, we will use (**XAMPP**) and also we have to need of **Command PROMPT** for perform this attack here XAMPP gives a website on local host on which we perform this attack
We start xampp and get a website on local host

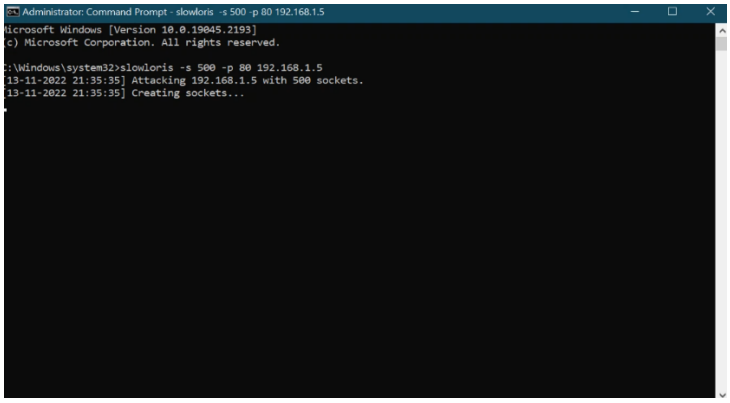




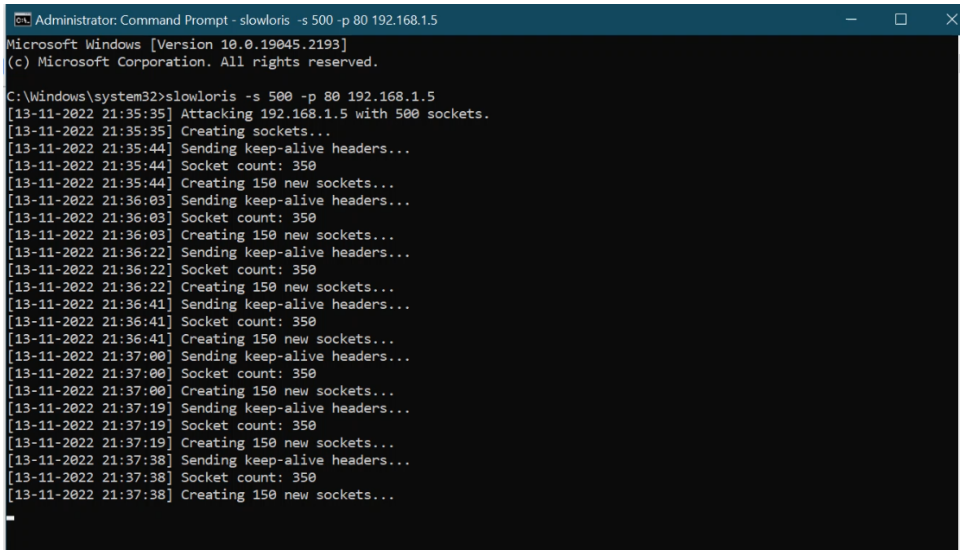
First The website is working-



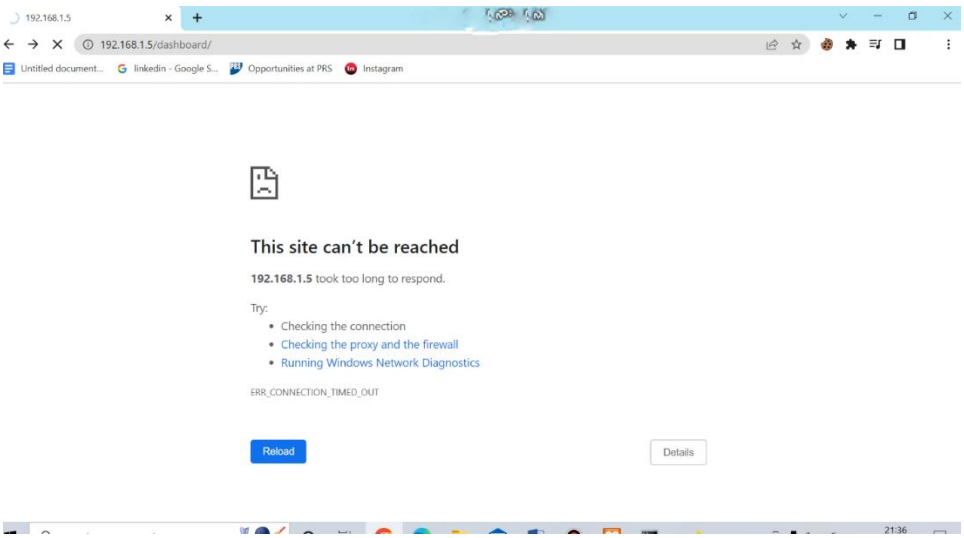
Then we open the command prompt, on which we use command and use the SlowLoris.



and by that command it creats port and send the multiple botnets to access that website.



Finally the website get down and attack get Successful-



CONCLUSION:

Cyber security is one of the most important aspects of the fast-paced growing digital world. The threats of it are hard to deny, so it is crucial to learn how to defend from them and teach others how to do it too.

Conclusion. **DoS attacks usually happen by generating mass bot traffic**. Denial of Service attacks are usually generated for malicious intentions and, sometimes, they can happen unintentionally as well. Several DoS attack tools are available on the internet.

REFERENCES

1. www.Google.com
2. www.Youtube.com
3. https://www.cybersecurity.com