p

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
| Program name and code : (CO6I) Academic Year : 2021-2022 Course name and code : CPP (22058) Semester : 6th  A STUDY ON  CAPSTONE PROJECT REPORT BASED ON  **H.M HACKING TOOL**  **(Phishing Tool)** | | | | |
|  | Sr  .no | Name of Student | Seat No. | Enrollment No. |
| 1) | Ahire Manoday Anil | 3102 | 1914320071 |
| 2) | Sonawane Yogesh B. |  | 19143200 |
| 3) | Mahajan Bhushan P. |  | 1914320080 |
| 4) | Ahire Khushal Santosh |  | 1914320070 |
| 5) | Sonawane Siddhesh S. |  | 19143200 |
| 6) | Bhavesh Kumavat |  | 19143200 |
| Submitted on / 05 /2022 by the group of 5 student Under the guidance of  **Mr. Sir**  Third year Diploma Program in Engineering & Technology of Maharashtra State Board of Technical Education, Mumbai (Autonomous  ISO 9001:2008 (ISO/IEC-27001:2013)  At  1432 GOVERNMENT POLYTECHNIC, NANDURBAR.  Maharashtra State Board Of Technical Education, Mumbai. | | | | |
|  | | | | |

)

**Certificate**

Is to certify that:- 1) Ahire Manoday Anil

Sonawane Yogesh Baburao

Mahajan Bhushan Pandurang

Ahire Khushal Santosh

Sonawane Siddhesh Sunil

Kumavat Bhavesh

Of Sixth Semester of Computer Engineering– Diploma Program in Computer Engineering & Technology At 1432 GOVERNMENT POLYTECHNIC, NANDURBAR.

Has completed

The Capstone Project (22058) in the academic year 2021- 2022 As prescribed in the MSBTE curriculum of I Scheme.

Place: Nandurbar Enrollment No: 1) 1914320071

2) 19143200

3) 1914320080

4) 1914320070

5) 19143200

6) 19143200

Date: / 05 / 2022

|  |  |  |
| --- | --- | --- |
| **Mr. S. N. Patil Sir** | **Dr. S. D. Pabale Sir** | **Dr. S. D. Pabale Sir** |
| **Project Guide** | **Principle** | **Head of Department** |

## ANNEXURE-I

#### Evaluation Sheet for the Micro Project (Teachers Copy)

|  |  |
| --- | --- |
| **Academic Year: 2021-22** | **Name of Guider: Mr. S. N. Patil Sir** |
| **Sem: Sixth** | **Program Name: Computer Engg.** |
| **Course Name: CPP** | **Course Code: 22058** |
| **Name of Students:** | **Manoday Anil Ahire Yogesh Baburav Sonawane**  **Bhushan Pandurang Mahajan Khushal Santosh Ahire Siddhesh Sonawane**  **Bhavesh Kumavat** |
| **Title of the Project:** | **“H.M Hacking Tool (Phishing Tool) ”** |

**Addressed by the Capstone Project:**

**Major Learning Outcomes achieved by students by doing the Project:**

**Practical Outcomes:**

### Out comes (in Cognitive domain)

**Out comes in Affective Domain**

#### Comment/Suggestions about team Work/leadership/inter personal Communication

+ All the team members were co-operative and helped each other. The team members gave full support. Rather, there were no any miss-understanding among any of any of the team members

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Seat No.** | **Students**  **Name** | **Total marks ( Project )** | **Total marks**  **(Oral)** | **Total** | **Remark** |
| **3102** | **Manoday Anil Ahire** |  |  |  |  |
| **3102** | **Sonawane Yogesh B.** |  |  |  |  |
| **3102** | **Mahajan Bhushan P.** |  |  |  |  |
| **3105** | **Ahire Khushal Santosh** |  |  |  |  |
| **3108** | **Sonawane Siddhesh S.** |  |  |  |  |
| **3085** | **Kumavat Bhavesh** |  |  |  |  |

## ACKNOWLEGDEMENT

We would like to sincerely thank all the people directly or indirectly involved in this project without whose help the completion of this project would have been impossible.

I would like to express my sincere gratitude to my guide Mr. S. N. Patil Sir who in spite his busy schedule took keen interest in giving me all the necessary information for developing a good software and for his unlisted encouragement and timely support till my successful completion of the project work.

We thank Mr M. M. Goswami sir , Head of Computer Department has guided us and provided support and genuine replies to our queries. He has not only guided us in the project but also helped us by providing suggestions without which we couldn’t improve at work. Her certain suggestions and interest in helping us complete the project has led me to the successful result of my project and also all the other Lecturers and lab instructors who had been more of a support to us than ever.

INDEX

SYNOPSIS 7

[Title of the Project 7](#_TOC_250020)

[Objective of the Project… 7](#_TOC_250019)

[Project Category 7](#_TOC_250018)

[Language(s) to be used… 7](#_TOC_250017)

[HARDWARE AND SOFTWARE REQUIREMENTS. 7](#_TOC_250016)

[LANGUAGES TO BE USED 7](#_TOC_250015)

[LIMITATIONS 8](#_TOC_250014)

[FUTURE SCOPE 8](#_TOC_250013)

[SOFTWARE REQUIREMENTS SPECIFICATION… 10](#_TOC_250012)

[Introduction 10](#_TOC_250011)

[Purpose 10](#_TOC_250010)

[Scope 10](#_TOC_250009)

[Definitions, Acronyms and Abbreviations 11](#_TOC_250008)

[References 11](#_TOC_250007)

[Overview 11](#_TOC_250006)

1.3 Overall description 11

[Specific requirements 11](#_TOC_250005)

[External Interface Requirements 11](#_TOC_250004)

[User Interfaces 12](#_TOC_250003)

[Hardware Interfaces 12](#_TOC_250002)

[Software Interfaces 12](#_TOC_250001)

[Communication Interfaces 12](#_TOC_250000)

SYSTEM DESIGN… 14

Introduction 14

System Context Diagram… 14

Data Flow Diagram… 14

DFD for Level 1 Admin… 16

DFD for Level 1 Customer 16

DFD for Level 2 Customer… 17

DFD for Level 1 Employee 18

DATABASE DESIGN 20

INTRODUCTION… 20

Internal level… 20

Conceptual level 20

External level 20

WHAT IS DATABASE 20

DATABASE DESIGN 21

ENTITY RELATIONSHIP DIAGRAM 21

ER Diagram… 24

DETAILED DESIGN 26

Introduction 26

Applicable documents 26

Structure of the software package 26

STRUCTURE CHART OF ADMIN 28

STRUCTURE CHART OF Employee 28

STRUCTURE CHART OF Customer… 29

Modular Decomposition Of Components… 29

Customer Account Component 30

Product list Component… 30

Category Component 31

Search Component… 32

5.12 Bidding Component… 32

Purchase Component 33

Chat Component 34

5.15 Report Component 34

Dashboard Component 35

Settings Component 36

USER MANUAL 38

Software Interfaces 38

User classes and characteristics 38

Design and implementation constraints 38

Functional Requirements 39

7 . CONCLUSION… 43

# CHAPTER-1

## SYNOPSIS

**PROJECT SYNOPSIS**

### Title of the Project

H.M Hacking Tool

### Objective of the Project

*H.M hacking tool is one of the Phishing Tool In Cyber Security and Ethical Hacking. H.M hacking tool is terminal based tool which can be used in ethical hacking to gather information of the end user or to gather the IP address of that user. This tool has been design for the cyber security purpose.*

### Project Category

Hacking Tool

### Language(s) to be used

BASH, Python, HTML, PHP.

### HARDWARE AND SOFTWARE REQUIREMENTS

**HARDWARE REQUIREMENTS**

Processor - Intel Pentium IV

Processor Speed – 1.40 GHz

RAM – 2 GB or above.

OS- Kali Linux/Windows.

Monitor resolution- A colour monitor with minimum resolution of 1000\*700

### FUTURE SCOPE

In future we can integrate this Hacking Tool in Software.

Currently This Tool is working with limited phishing pages so in future we will try to add more features in it.

Will try to gather more information from it as its advanced version.

We can add GPS tracking in this tool whether by clicking on phishing site information as well location of that user will get tracked..

# CHAPTER-2

## HACKING

**What Is Hacking?**

Hacking is the technique of finding the weak links or loopholes in the computer systems or the networks and exploiting it to gain unauthorized access to data or to change the features of the target computer systems or the networks. Hacking describes the modification in the computer hardware, software or the networks to accomplish certain goals which are not aligned with the user goals. In contrast, it is also called breaking into someone's security and stealing their personal or secret data such as phone numbers, credit card details, addresses, online banking passwords etc.

**Hackers: -**

The term HACKER in popular media is used to describe someone who breaks in to someone else's security using bugs and exploits or use his expert knowledge to act productively or maliciously. Hackers are the computer experts in both hardware as well as software. A hacker is a computer enthusiast and master in a programming language, security and networks. He is kind of person who loves to learn various technologies, details of the computer system and enhances his capability and skills. According to the way of working or based on their intensions HACKERS can be classified into three groups

1. White Hat Hackers

2. Black Hat Hackers

3. Grey Hat Hackers

**1. White Hat Hackers: -**

A white hat hacker is a computer security specialist that breaks into and find loopholes in the protected networks or the computer systems of some organization or company and corrects them to improve the security. White Hat Hackers use their skills and knowledge to protect the organization before malicious or bad hackers find it and make any harm to the company or the organization. White Hat Hackers are the authorized persons in the industry, although the methods used by them are similar to those of bad hackers but they have permission from the organization or the company who hires them to do so.

**2. Black Hat Hackers: -**

A Black Hat Hacker also known as a “Cracker” is a computer hardware and software expert who breaks into the security of someone with malicious intent or bad intentions of stealing or damaging their important or secret information, compromising the security of big organizations, shutting down or altering functions of websites and networks. They violate the computer security for their personal gain. These are persons who typically wants proves their extensive knowledge in the computers and commits various cybercrimes like identity stealing, credit card fraud etc.

**3. Grey Hat Hackers: -**

A Grey Hat Hacker is a computer hacker or security expert who sometimes violates the laws but does not have any malicious intentions like the black hat hackers. The term Grey Hat is derived from the Black Hat and the White Hat as the white hat hackers finds the vulnerabilities in the computer system or the networks and does not tells anybody until it is being fixed, while on the other hand the black hat hackers illegally exploits the computer system or network to find vulnerabilities and tells others how to do so whereas the grey hat hacker neither illegally exploits it nor tells anybody how to do so. Grey Hat Hackers represents between the white hat hackers who operate to maintain system security and the black hat hackers who operate maliciously to exploits computer systems.

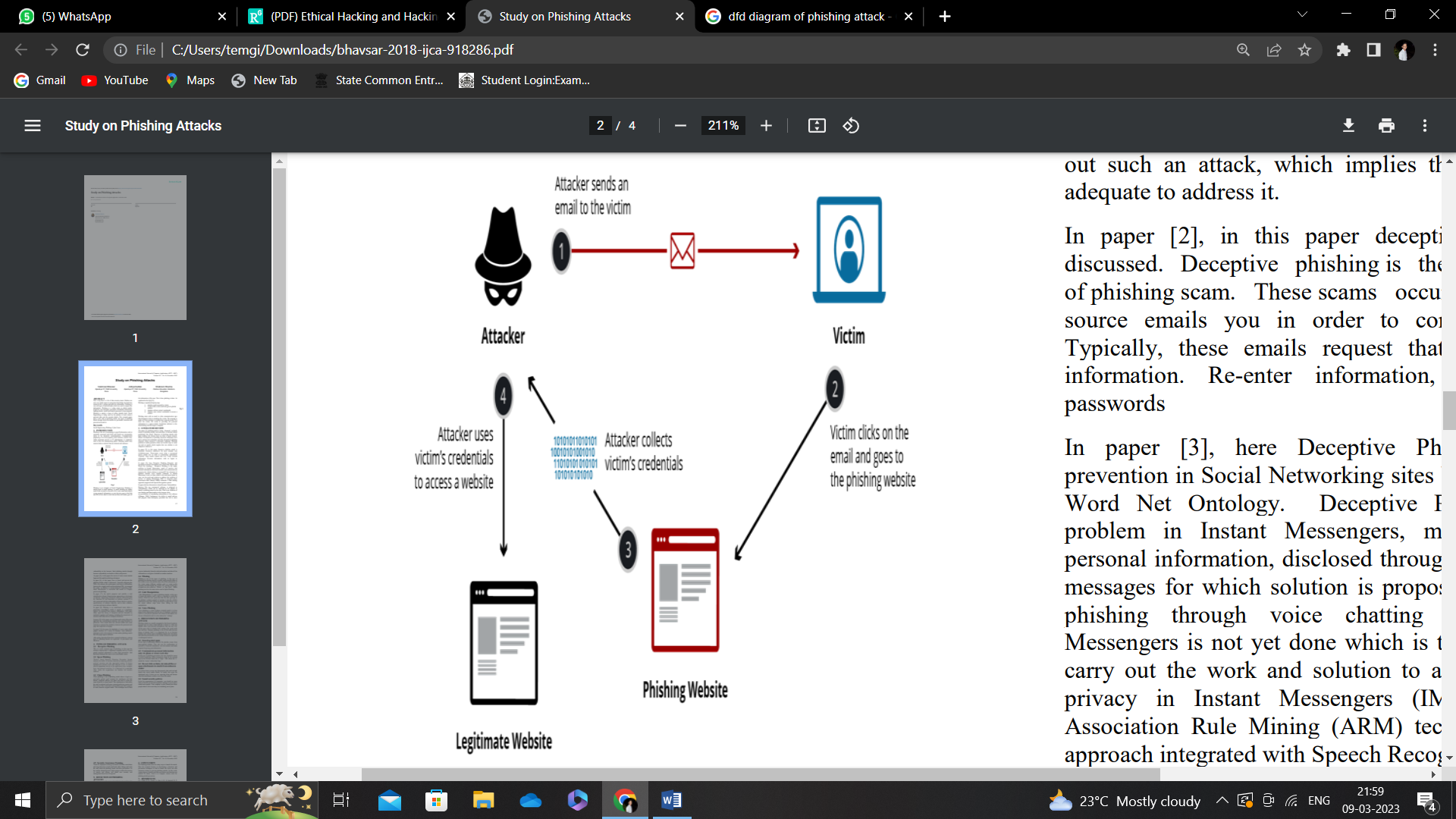
# CHAPTER-3

## DETAILED DESIGN

### DETAILED DESIGN

**Introduction:**

Phishing is the act of attempting to payoff information such as username, password and credit card details as a trustworthy entity in an electronic communication. Communication purporting to be from popular social websites, auction sites, online payments process or IT administrator is commonly used to lure the unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Fig.1 Phishing is an example of Social Engineering. Phishing is mainly used in email hacking, in email phishing the hacker send a link via mail to the user of let’s say some bank details or any personal information, so now the user goes to that link and fills all the detail in that link and then the hacker gets all the information of the user. This is how phishing is done. As explained in the fig1.[11].



Phishing is explained step-by-step: 1. Attacker sends an email to victim. 2. Victim clicks on the email and goes to phishing website. 3. Attacker collects victim’s credentials. 4. Attacker uses victim’s credentials to access a website. Phishing starts with an email or other communication type that designed to help in attacking the victim. The message is made as if that message is coming from a trusted sender. If it fools the victim, the victim is providing the personal information to a spam website. Sometimes malware is also downloading onto the target’s computer.

**TYPES OF PHISHING ATTACK**

**3.1 Deceptive Phishing**

This is a most common type of phishing, in this type the attackers impersonates a legitimate company and try to steal people personal information or their login passwords. And then they blackmail the users to do as the hacker wants.

**3.2 Spear Phishing**

Wireless based Intrusion Detection Prevention System analyses the traffic of wireless network by analyzing wireless protocol activities and take appropriate actions. It detects unauthorized wireless local area network in use. It cannot identify suspicious activity in the application layer, transport layer and protocol activities. It is deployed in a particular range where the organization can monitor the wireless network.

**3.3 Clone Phishing**

Clone phishing is one of phishing attack where a legal or a previously gained email contains the attachment and link shared, recipients address (es) taken and used to create the same identical or cloned email. That attachment or link within the mail is replaced with some external malicious version and then sent it to the victim from email address spoofed to appear to come from the original sender. This technique can be used to pivot (indirectly) from the infected machine and take all the information or can gain a foothold on another machine.

**3.4 Whaling**

Whaling is one of the types of phishing, in this type of phishing the attacker aims at a wealthy and powerful status of the victim or user; the attacker takes out all the information of the victim using different medium such as social media accounts and then attacks the victim. The victims of this type of attack are also called as “Whales” or “Big Phish”. Whale phishing involves the same tactics used in Spear Phishing.

**3.5 Link Manipulation**

Link Manipulation is a type of phishing attacks; in this type of attack the phisher send a link to a spoofed or malicious website. When the user opens that link, the link open ups in the phisher’s website instead of opening it into the website mentioned in the link. Taking the mouse on that link to view the actual address stops users from falling for link manipulation.

**3.6 Voice Phishing**

Voice phishing is a form of phone criminal attack it is done using social engineering with the use of telephone system to look at to the private personal and financial information for the use of financial work it is also referred as “vishing”.

**PREVENTION OF PHISHING ATTACK**

Phishing attacks are usually presented in the form of spam or pop-ups and are many times difficult to detect it. Once the attacker takes your personal information, they can use it for all the types such as identify theft, putting your good credit into bad once. Because phishing is one of the most devious forms of identity theft, it is important for us to become familiar with various types of phishing attacks and also know that what the prevention on it are. Some of them are explained in subsequent sections.

4.1 **Guard against spam**

In this type of prevention method, the attacker comes from unrecognized senders. They ask you for confirmation of personal or financial information over the internet and make requests for giving your information.

**Communicate personal information only via phone or secure web sites**

In this type of phishing prevention, the user should be aware of while conducting online transactions, look for the secured sign on the browser status bar or” https.” URL where the “s” stands for “secure” rather than’ http.”.

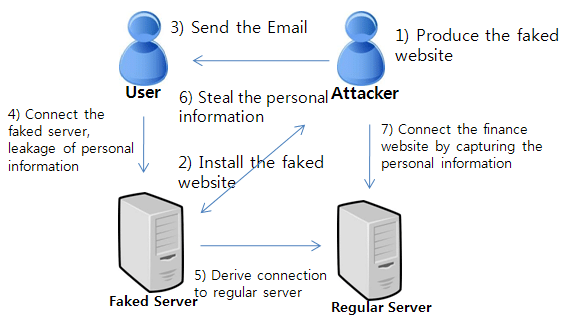
**Do not click on links, download files or open attachments in emails from unknown sender**

It is always best to secure any data properly data such as bank details any social media details, in emails also open the attachment only if when you are expecting them and known what that attachment contains even if you the sender.

**Sound security policies**

In the big organizations or companies, you should set some rules as to how you should respond to strange or out of place emails and requests. Your company’s policy should also show people what to do in case they see something out of place.

### DFD Diagram



# CHAPTER-4

## USER MANUAL

### USER MANUAL

**INTRODUCTION**

H.M Hacking tool is Linux Terminal Based Phishing tool. Which is used to gather information as well IP address of the user. specially purpose behind design of this tool is for the Ethical Hacking. As in this Section We will see the execution of this tool.

### Software Interfaces:

### As this tool is terminal based so the execution of this tool has been done on any linux based terminal as on personal computer, Mobile, Cloud Based Terminals.

### Following are some of the linux based terminal:

### Termux (Mobile Based Linux Terminal.

### Debian ( Kali Linux operating system Terminal)

### Cloud shell ( Its develop by google clod platforms)

### Installation:

### Termux:

### Installation of this tool is done on mobile also. As there is linux based terminal for mobile phone / Android is available on the playstore.

### Steps:

### Download Termux From PlayStore.

### Follow following Command On The Termux as below:

### $ apt update && apt upgrade –y

### (This command updates all the directories of the termux terminal)

### $ pkg install git -y

### (This command install git on termux terminal whether we hosted our tool on github so we need to access it so we need to install git for that)

### $ git clone https://github.com/MAHIRE-7/H.M-hacking-tool

### (This command clones all the directories of the project in termux terminal to execute them there)

### $ cd

### $ ls

### (This commands open the directories and projects of the termux terminal)

### $ cd H.M-hacking-tool

### (This command opens our tool directory in the termux terminal)

### $ bash H.M-hacking-tool.sh

### (This command install our tool into the termux terminal)

### 

### Here by using this given commands we can install H.M hacking tool

### (Phishing Tool) in termux Terminal after the successfully installing tool in termux following dashboard will occur.

### Cloud Shell

### Installation of this tool can done on cloud also. As there is linux based terminal for cloud is available. Which has been developed by Google Cloud Platforms (GDP), Microsoft Azure, IBM Cloud and so on.

### Here, we are using Google cloud platforms cloud shell for the installation and execution of H.M hacking tool.

### Illustration of Using Cloud Shell directly in docs when building new skills

### Steps:

### Got to <https://cloud.google.com/shell> on any Browser.

### Click on Go to console.

### 

### Follow below commands on cloud shell terminal

### $ git clone <https://github.com/MAHIRE-7/H.M-hacking-tool>

### $ cd

### $ ls

### $ cd H.M-hacking-tool

### $ ls

### $ bash HM.sh

### Here by using this given commands we can install H.M hacking tool

### (Phishing Tool) in Google Cloud Shell Terminal after the successfully installing tool following dashboard will occur.

### 

### 

### 6.3.3: Debian Terminal (Kali Linux Operating System)

### Installation of this tool can done on Debian Terminal can done as it is one of the powerful terminal to perform various types of ethical hacking. Which has been developed by Kali Linux.

### Вышла Kali Linux 2022.3 с пятью новыми инструментами и свежим ядром Linux

### Steps:

### Open Kali Linux operating system.

### Automatically terminal will occur on screen follow the below commands and install as well execute H.M hacking tool on Debian Terminal.

### $ apt-get update

### $ sudo apt install git

### $ git clone <https://github.com/MAHIRE-7/H.M-hacking-tool>

### $ cd

### $ ls

### $ cd H.M-hacking-tool

### $ ls

### $ bash HM.sh

### Following screen will appear after the successfully installing the tool:

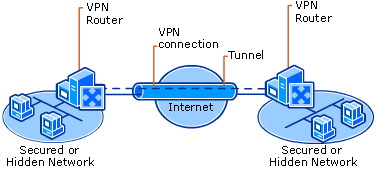
# CHAPTER-5

## TUNNELS

**INTRODUCTION**

In the physical world, tunneling is a way to cross terrain or boundaries that could not normally be crossed. Similarly, in networking, tunnels are a method for transporting data across a network using [protocols](https://www.cloudflare.com/learning/network-layer/what-is-a-protocol/) that are not supported by that network. Tunneling works by encapsulating packets: wrapping packets inside of other [packets](https://www.cloudflare.com/learning/network-layer/what-is-a-packet/). (Packets are small pieces of data that can be re-assembled at their destination into a larger file.)

Tunneling is often used in [virtual private networks (VPNs)](https://www.cloudflare.com/learning/access-management/what-is-a-vpn/). It can also set up efficient and secure connections between networks, enable the usage of unsupported network protocols, and in some cases allow users to bypass [firewalls](https://www.cloudflare.com/learning/security/what-is-a-firewall/).



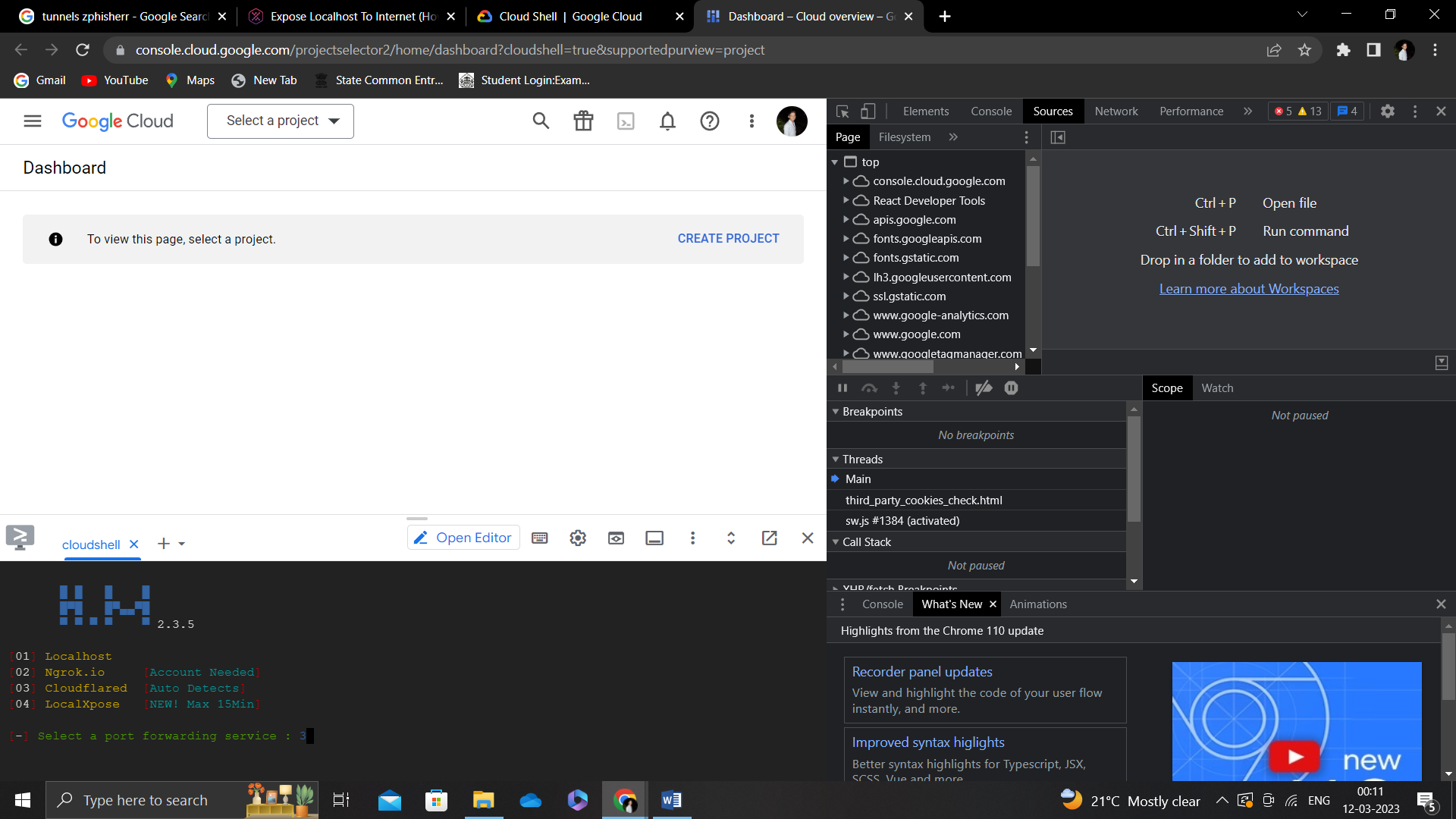
In our H.M Hacking Tool we used 3 type of tunnel for port forwarding. That are as follow:

Local Host

Cloudflared

Ngrok

LocalXpose



### Localhost

### A localhost tunnel establishes a connection between your local machine and a remote connection. The connection is intended to proxy traffic from a publicly-addressable IP address and URL to your local machine.

### Probably Localhost tunnel in H.M Hacking Tool can be used to check that the installation and execution of the tool is working or not is there any error occurs or not. Another way of using it for the computers in same network or of group of computers connected with each other.

### Link obtain from terminal will as follow:

### <https://127.0.0.1:8080/>

### It will work on Computers only.

### CloudFlared

### Cloudflare Tunnel provides you with a secure way to connect your resources to Cloudflare without a publicly routable IP address. With Tunnel, you do not send traffic to an external IP — instead, a lightweight daemon in your infrastructure ( cloudflared ) creates outbound-only connections to Cloudflare's edge.

### Cloudflare - Wikipedia

**What are the benefits of Cloudflare tunnel?**

Improve security posture with integrated DDoS mitigation, threat intelligence, and more. Caching, dynamic compression, optimized route requests, and more. Secure any user accessing any application, on any device, in any location. Network security, performance, & reliability on a global scale.

### Ngrok

### Ngrok Secure Tunnels allow you to instantly open access to remote systems without touching any of your network settings or opening any ports on your router. This means you get a secure, reliable tunnel for your developer box, IoT device, or just about anything that has access to the internet.

### Secure Tunnels to localhost using ngrok - DevOpsSchool.com

### ngrok is a cross-platform application that enables developers to expose a local development server to the Internet with minimal effort. The software makes your locally-hosted web server appear to be hosted on a subdomain of ngrok.com, meaning that no public IP or domain name on the local machine is needed.

### LocalXpose

### Local Xpose works by providing users with a secure tunnel service that enables them to access their local or private network services from the internet. This is achieved through the use of a reverse proxy, which acts as an intermediary between the user's device and their local server.

### Expose Localhost To Internet (How To Get Started) - Blog

# CHAPTER-6

## CONCLUSION

### 6.CONCLUSION

So, from above all elaboration here in short we would say H.M Hacking Tool will give new approaches and dimensions to the information gathering.

During The creation and execution we studied and followed all the software

Engineering approaches as well learned about new techniques regarding tunneling ,

Servers and hacking tools.