

Phishing and its prevention

Mini- Project (DCE)

Submitted in partial fulfillment of the requirements for the degree of

Bachelor of Engineering by:

1) Vighnesh Salgaonkar ID No: TU2F1819090

Under the Guidance of

Prof. Vijaypal Yadav



Department of Electronics and Telecommunication Engineering
TERNA ENGINEERING COLLEGE
Plot no.12, Sector-22, Opp. Nerul Railway station,
Phase-11, Nerul (w), Navi Mumbai 400706
UNIVERSITY OF MUMBAI

CERTIFICATE

Project Entitled: Phishing and its prevention

Submitted by:

Vighnesh Salgaonkar

In partial fulfillment of the degree of B.E. in "Electronics and Telecommunication Engineering" is approved.

Guide: Prof. Vijaypal Yadav

HOD
Dr. Jyothi Dighe

Principal
Dr. L.K.Ragha

Index

TABLE OF CONTENTS		
Caption		Page No.
Chapter 1	Introduction	4
Chapter 2	Problem Statement	6
Chapter 3	Implementation	7
Chapter 4	Conclusion	14
	Reference	-

Chapter 1

Introduction

What is a website, a webpage and a webserver?

A webpage is a document which can be displayed in a web browser such as Firefox, Google Chrome, Opera, Microsoft Internet Explorer or Edge, or Apple's Safari. These are also often called just "pages." A collection of web pages which are grouped together and usually connected together in various ways is often called a "website" or simply a "site" and a computer that hosts a website on the Internet is called as webserver.

What are the types of webserver?

A server is a computer or system that provides resources, data, services, or programs to other computers, known as clients, over a network. In theory, whenever computers share resources with client machines they are considered as servers. There are many types of servers, including web servers, mail servers, and virtual servers. Broadly the servers are divided into two types and those are local and remote servers. A local server is again a computer that serves a client within the local network or LAN. That means that in most cases it will not be connected to the internet or if it does it will be protected with a password so not everybody can access its services. But when it comes to a remote server, a client has to send the request of the webpage which it has to access to which the server responds.

What is hosting, and what are the types of hosting?

A local server is only available to the people who are connected over that local network. Thus, to make these stuffs available to others, we

need to host them. When you host something, it becomes available to the people across internet. If you want to host something permanently you need to buy a domain but if you need to host something temporarily, you need to have applications like NGROK or SERVEO. These applications provide us free and temporary hosting a certain amount of time.

What is phishing?

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords. The information is then used to access important accounts and can result in identity theft and financial loss.

Chapter 2

Problem Statement

Nowadays hosting a website or a webpage at a cheap rate or without paying a single penny has become very easy. Along with these facilities, the risk of hosting dummy site is also increasing. A dummy page is basically a page which looks as that of the original page but the login credentials of these webpages are directed towards the hacker or the host of that particular page. Thus, it becomes very important for us to know whether the page or the URL we are accessing is valid and secure.

Chapter 3

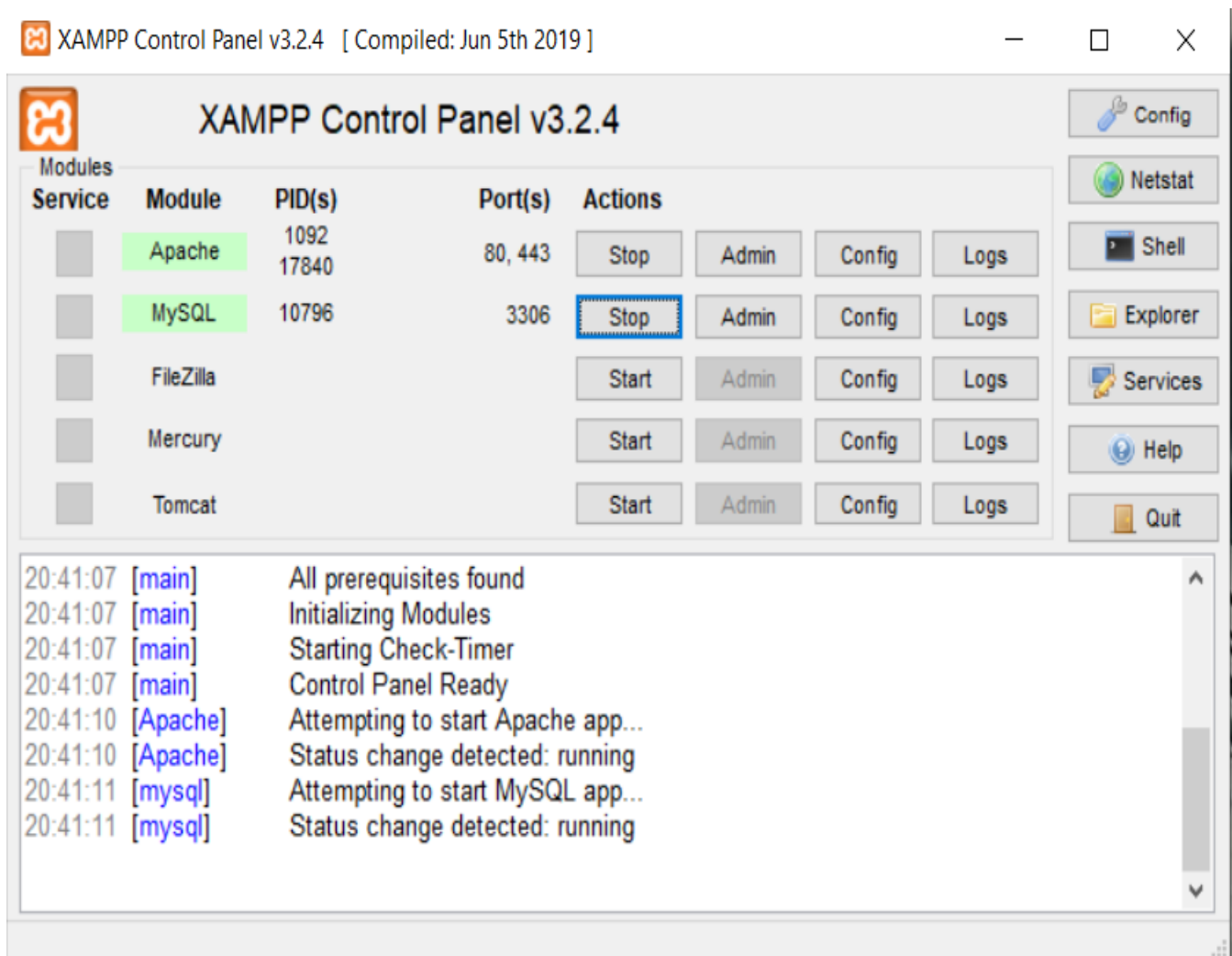
Implementation

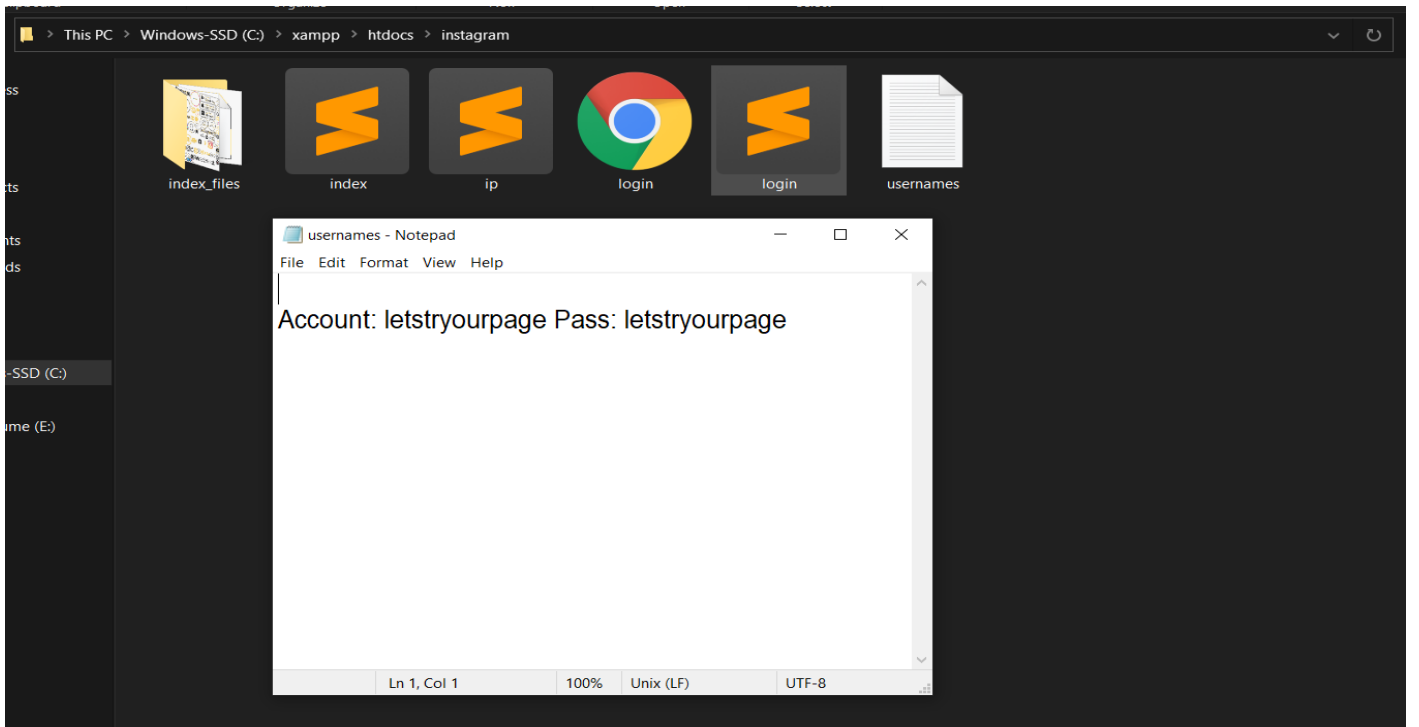
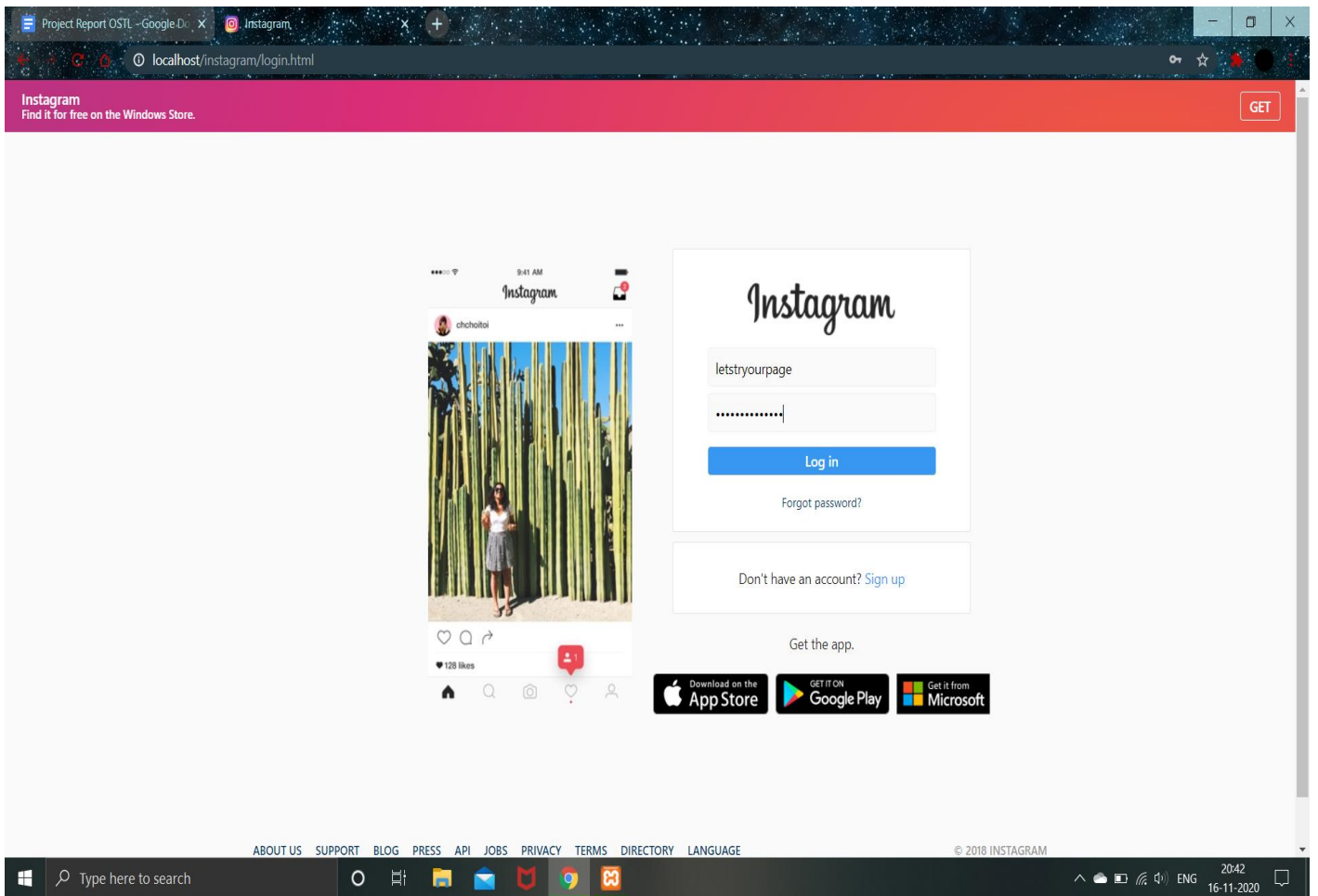
In the implementation part we will focus on how can someone host a phishing page and capture the details or credentials of the targeted victim. We will even focus on how to perform this on a local network and even how to make it available on internet.

At first, we will need to clone the webpage which we are going to host. To do this one can use “HTTrack Website copier” or “Phishbait Maker”. All we have to do is just copy the webpage we need to clone and paste the URL and simply clone it. Once the page is cloned, we need to verify if it looks similar to the original webpage. Most of the time stuffs like logos are missing in the clone so we need to add them manually with the help of CSS and html. Once we are done cloning the webpage, we need to link the php file which will capture the victim’s credentials. So, we just open the html file using a text editor and link that text file to it. Usually when you login on some page it redirects you to your account. But since this is a clone, we will need to redirect the clone to the original webpage. Thus, to do so we will copy the link of the original page and link it in our clone. Now to keep these files together make a folder and add them together in it. This basically completes our setup for a phishing page.

Now that we are done with the basic setup for our clone, we need to host it locally. To do so we will use XAMPP server. One can get XAMPP easily downloaded just by searching for it. Once the downloading and installation is complete, we need to copy the folder which we created into the “htdocs” folder. Now open the server and start APACHE and MYSQL service and go to your browser and type localhost/[foldername]/[filename.html] and you will be able to access the page which you have created. Try to enter your

credentials and proceed with the login process. Once you will do this, you will notice that you have been redirected to the original login page. Now if you will check the folder you have created it will be having a text file with your credentials inside it. You can repeat the login process and next time the credentials will get added to the same text file. The drawback of the system which we made now is that, it not accessible to a person over internet and thus to fill this gap we will use “Ngrok” as a bridge.





Similar to “XAMPP” we can even search and download “Ngrok” easily. Once you download and install “Ngrok”, we need to configure it via command prompt. To do this just visit their website and create an account. Once the account is created you will get an authtoken. Open the directory using command prompt in which you have installed “Ngrok” and verify the token. Now to run Ngrok we need to command it as: “ngrok.exe http 80”. This command will basically start a http session at port 80. This port is by default similar to the “XAMPP” server port. Now since the session has started copy the .io link and append [foldername]/[filename.html] and hit enter. Now again we will have access to our clone page but this time anyone with the link can access it. One can even use link shortners on the generated link to make it less suspicious.

The screenshot shows a web browser window with the Instagram login page. The browser's address bar shows a URL from a ngrok.io domain. Overlaid on the browser is a Windows Command Prompt window titled "Command Prompt - ngrok.exe http 80". The prompt shows the command "ngrok by @inconshreveable" and its output, which includes session status, account information, and a table of connections.

Command Prompt Output:

```
ngrok by @inconshreveable (Ctrl+C to quit)

Session Status      online
Account             vighneshsalgaonkar.vs@gmail.com (Plan: Free)
Version             2.3.35
Region              United States (us)
Web Interface       http://127.0.0.1:4040
Forwarding           http://c53fb601a670.ngrok.io -> http://localhost:80
Forwarding          https://c53fb601a670.ngrok.io -> http://localhost:80

Connections
  ttl   opn   rt1   rt5   p50   p90
    9    0    0.06  0.03  6.88  10.21

HTTP Requests
-----
```

The background browser window shows the Instagram login page with fields for "Phone number, username, or email" and "Password", a "Log in" button, and links for "Forgot password?" and "Don't have an account? Sign up". At the bottom, there are links to download the app from the App Store, Google Play, and Microsoft.

There are other methods to make the URL looks exactly the same as that of the original URL but I will avoid the demonstration of that method here. The method I am talking above generates a hollow URL which looks exactly the same as that of original. The only difference is in the ASCII values of the alphabets. A symbol gets its identity cause of its ASCII value and thus if the ASCII value of the symbol changes then the significance of the symbol changes. This what exactly happens in a hollow URL.

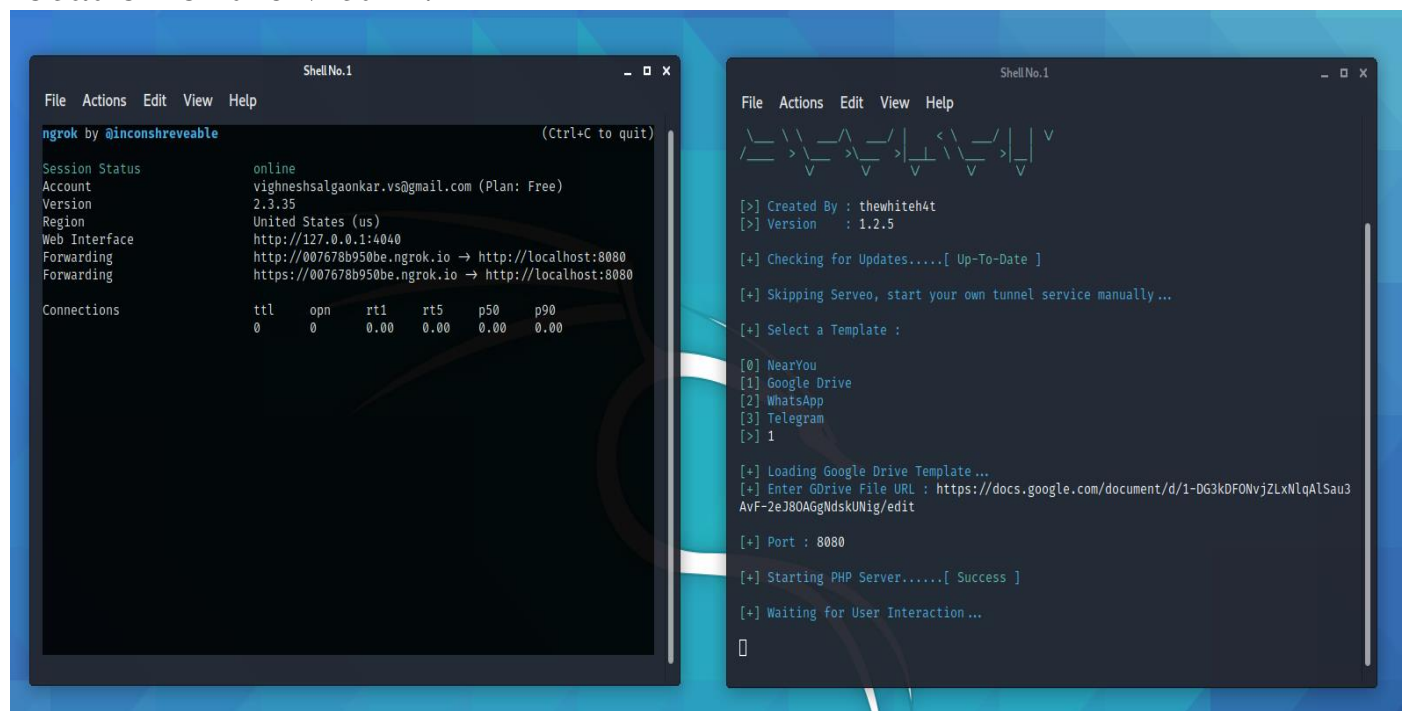
These are the examples of hollow URL:

Original URL: www.instagram.com

Hollow URL: www.instagram.com

They look exactly the same but if we try to use the second link then it will redirect us to some another page.

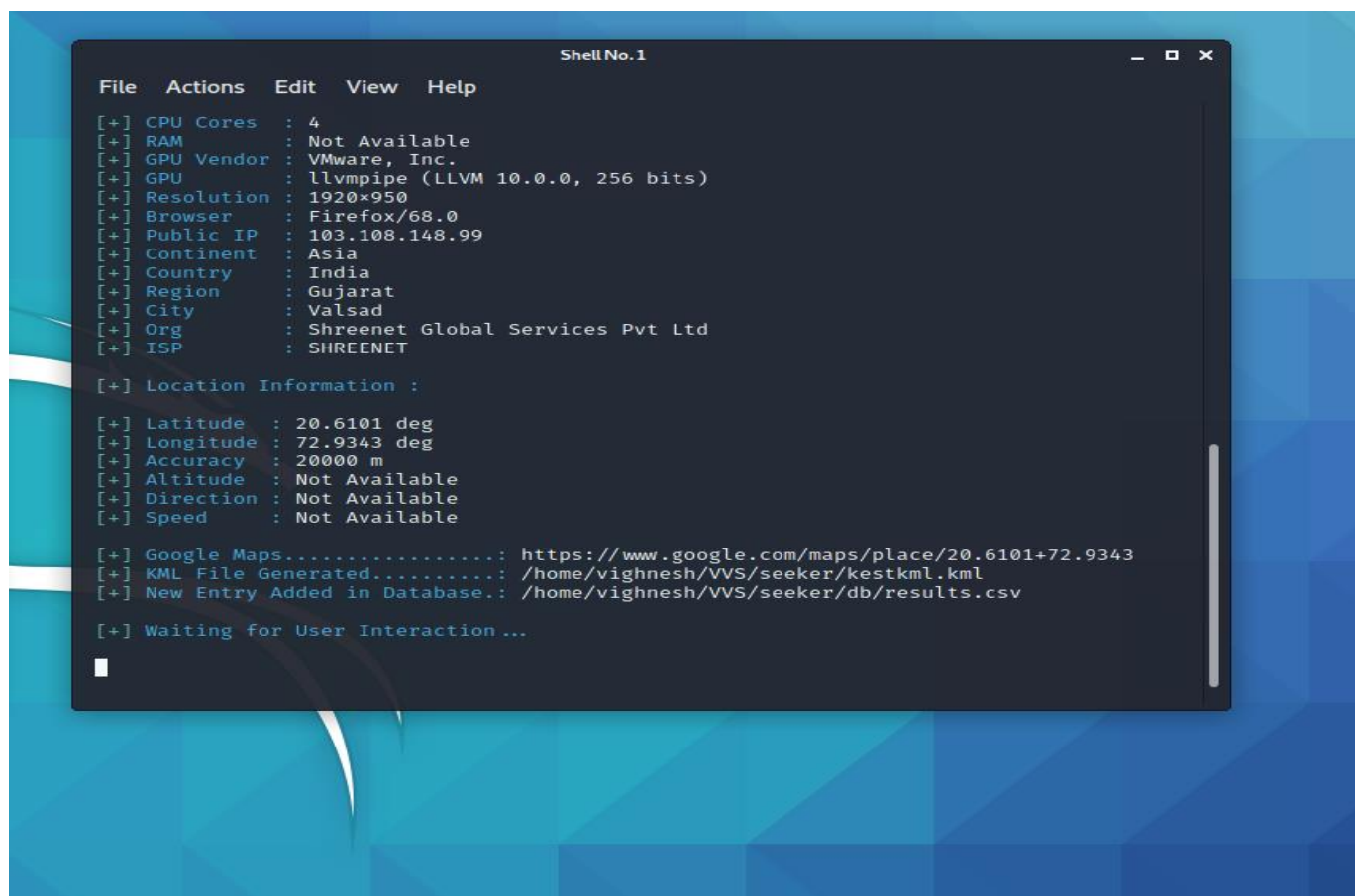
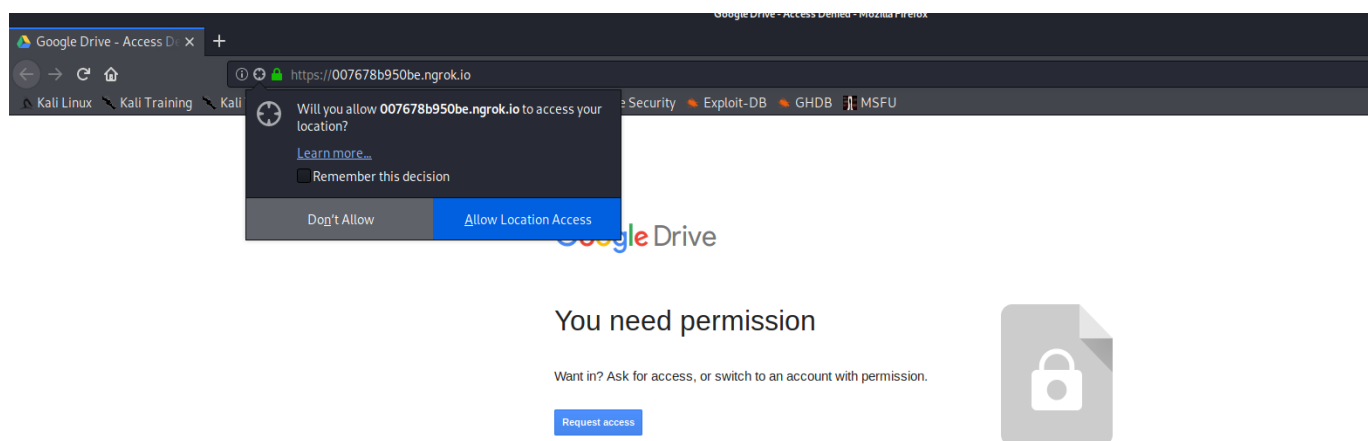
Along with this one can even use phishing pages to steal location of the victim. Since we have already learned on how to create a phishing page, to show this demonstration we will be using a pre-existing tool named seeker. The tool basically generates a URL and when the victim uses the URL, it opens the webpage and fetches the location of the victim.



The image shows two terminal windows side-by-side. The left window is titled 'ShellNo.1' and shows the output of the 'ngrok by @inconsheveable' command. It displays session status (online), account information (vighneshsalgaonkar.vs@gmail.com), version (2.3.35), region (United States (us)), web interface URL (http://127.0.0.1:4040), forwarding URL (http://007678b950be.ngrok.io → http://localhost:8080), and a table of connections.

Connections	t1	opn	rt1	rt5	p50	p90
0	0	0.00	0.00	0.00	0.00	

The right window is also titled 'ShellNo.1' and shows the output of the 'seeker' tool. It displays a ASCII art logo, version information (Created By : thewhite4t, Version : 1.2.5), and a list of templates (NearYou, Google Drive, WhatsApp, Telegram). It shows the selection of the Google Drive template, the loading of the template, the entry of the Google Drive file URL, the port (8080), and the starting of the PHP server.



This is how one can create or use pre-existing scripts to fetch the details of the target.

Preventive measures from phishing:

- One should always check the URL of the page he / she is using.
- One should always try to type the searches by their own rather than accessing the links directly.
- When you come across any shortened URL, makes sure that you pass the link through online URL detectors which will determine whether the link is malicious or not.
- Always keep on changing your password once in a while so that even if you have come across a phishing link, the user won't be able to access your account.
- In case of website prompts make sure that you are not accessing any random site and allow the prompts only if the site is trusted and reputed
- One should also try to avoid http sites and should always prefer https site.

Chapter 4

Conclusion

Thus, I conclude that I have learned about how phishing works, how can one create phishing pages and what are the preventive measures one should take to keep his/her identity and credentials secured from the exploiters.

Project files:

The files on which I have worked during this mini-project are available on as git repositories and are accessible to everyone for verification.

Link: <https://github.com/vighnesh111/DCE-Project>