Practical-8

**AIM:**

Social engineering is a term that encompasses a broad spectrum of malicious activity. Social Engineering scams are the art of deception used by evil-minded people to feed their greed for money or something else. They exploit the weakness that found in every organization, human psychology. Using phone calls and other media, these attackers trick people into handing over access to the organization’s sensitive information. (eg. phishing, spear phishing, vising, pretexting, baiting, quid pro quo and tailgating.) Reverse social engineering is a very unique form of social engineering. In most social engineering attacks, the attacker goes to the victim to obtain information. In reverse social engineering, however, the victim innocently goes to the attacker.

Practical approach to study Social Engineering and reverse social engineering to perform ethical hacking.

# THEORY:

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In cybercrime, these “human hacking” scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems. Attacks can happen online, in-person, and via other interactions.

Scams based on social engineering are built around how people think and act. As such, social engineering attacks are especially useful for manipulating a user’s behavior. Once an attacker understands what

motivates a user’s actions, they can deceive and manipulate the user effectively.

In addition, hackers try to exploit a user's lack of knowledge. Thanks to the speed of technology, many consumers and employees aren’t aware of certain threats like [drive-by downloads](https://www.kaspersky.co.in/resource-center/definitions/drive-by-download). Users also may not realize the full value of personal data, like their phone number. As a result, many users are unsure how to best protect themselves and their information.

Generally, social engineering attackers have one of two goals:

1. Sabotage: Disrupting or corrupting data to cause harm or inconvenience.
2. Theft: Obtaining valuables like information, access, or money.

In this practical we are going to use setoolkit to understand how hackers perform social enginnering.

When a social engineering attack is performed, the weakest link in the chain is not the computer system, the firewall, services or apps. It’s us, the humans behind those technologies.

**SETOOLKIT**:

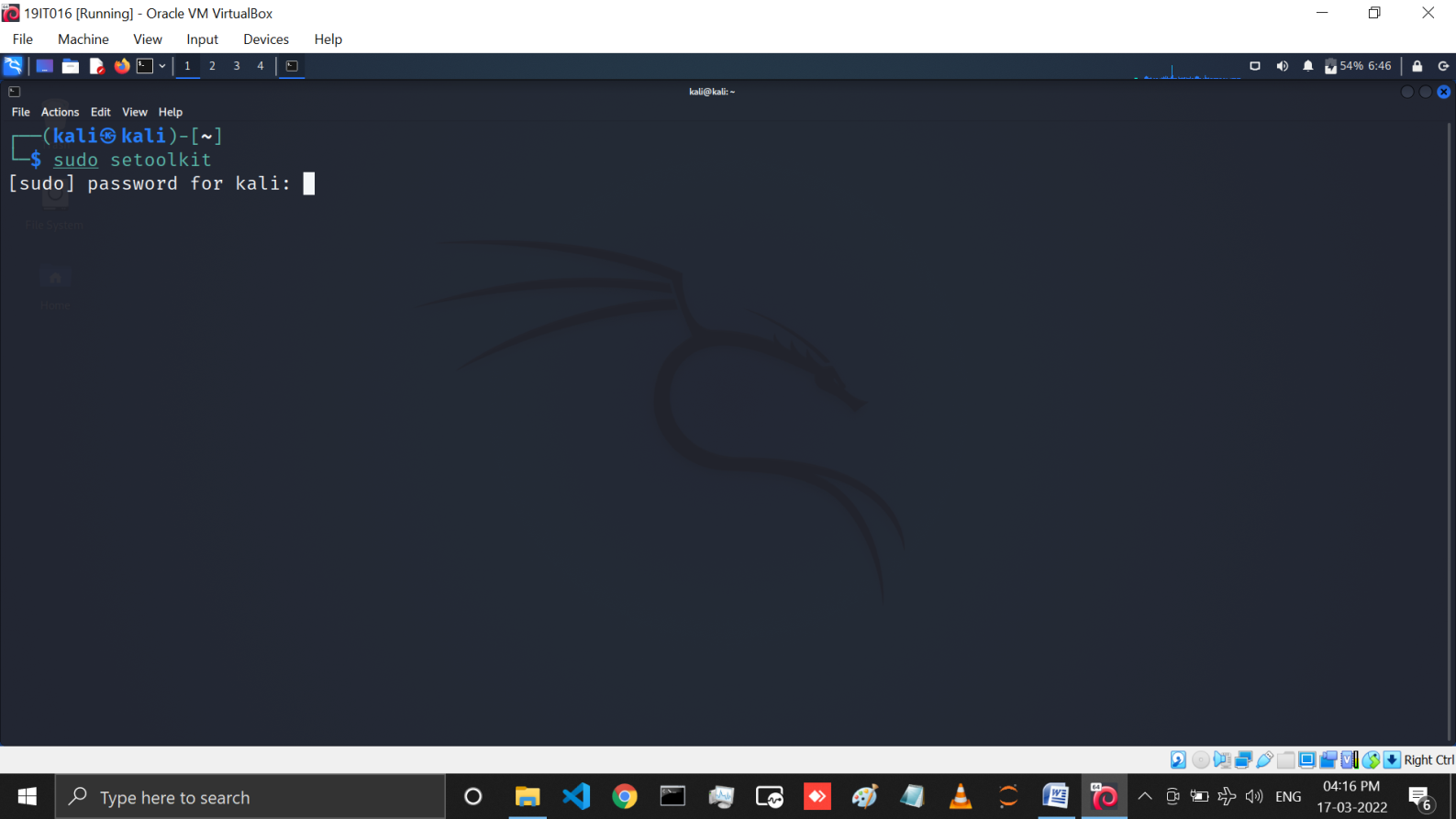
The Social-Engineer Toolkit (SET) is an open-source penetration testing framework designed for social engineering. SET has a number of custom attack vectors that allow you to make a believable attack in a fraction of time. These kind of tools use human behaviors to trick them to the attack vectors.

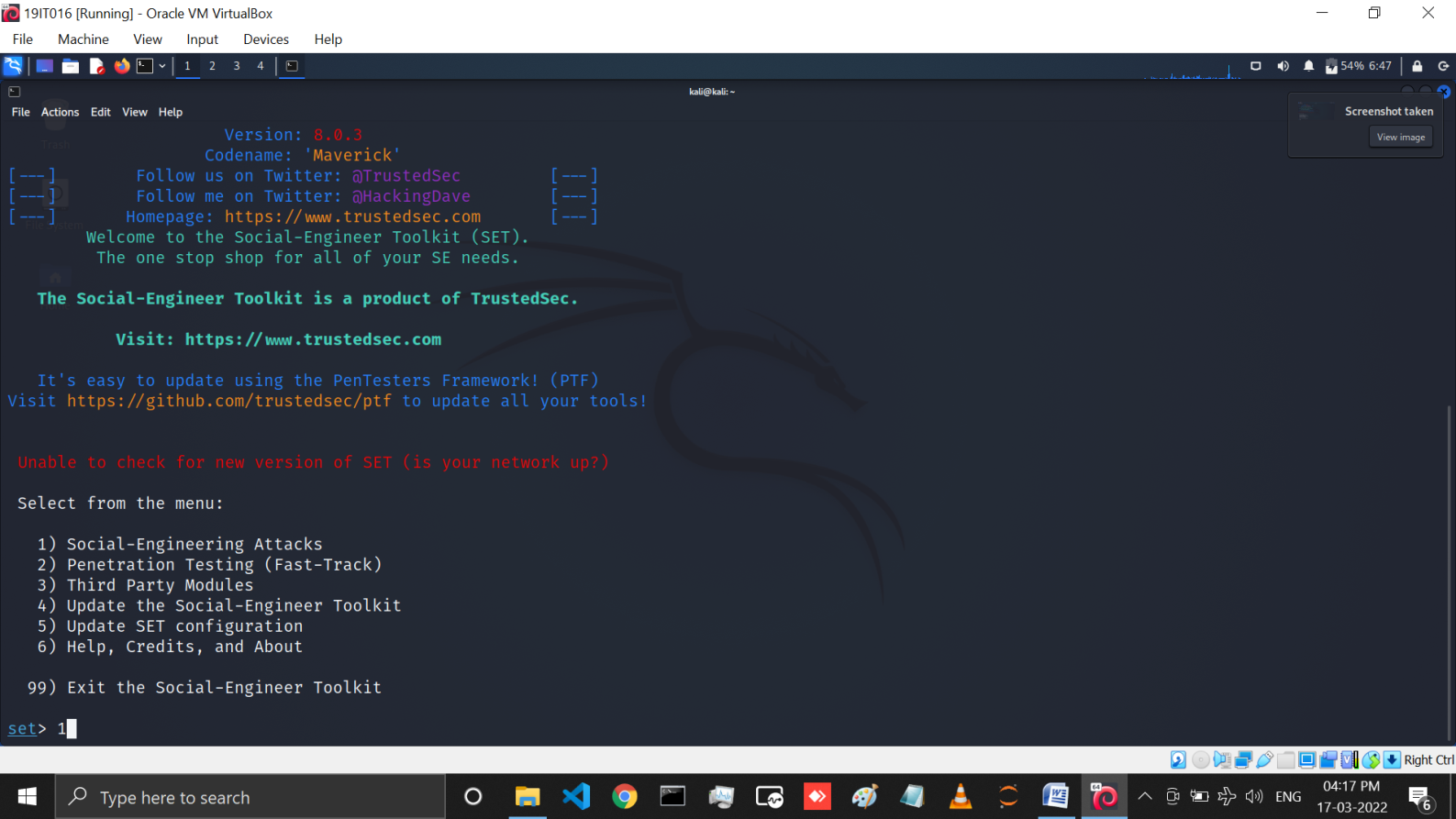
It offers many brilliant features, including faking phone numbers, sending SMS, or helping to create a phishing page by instantly cloning the original.

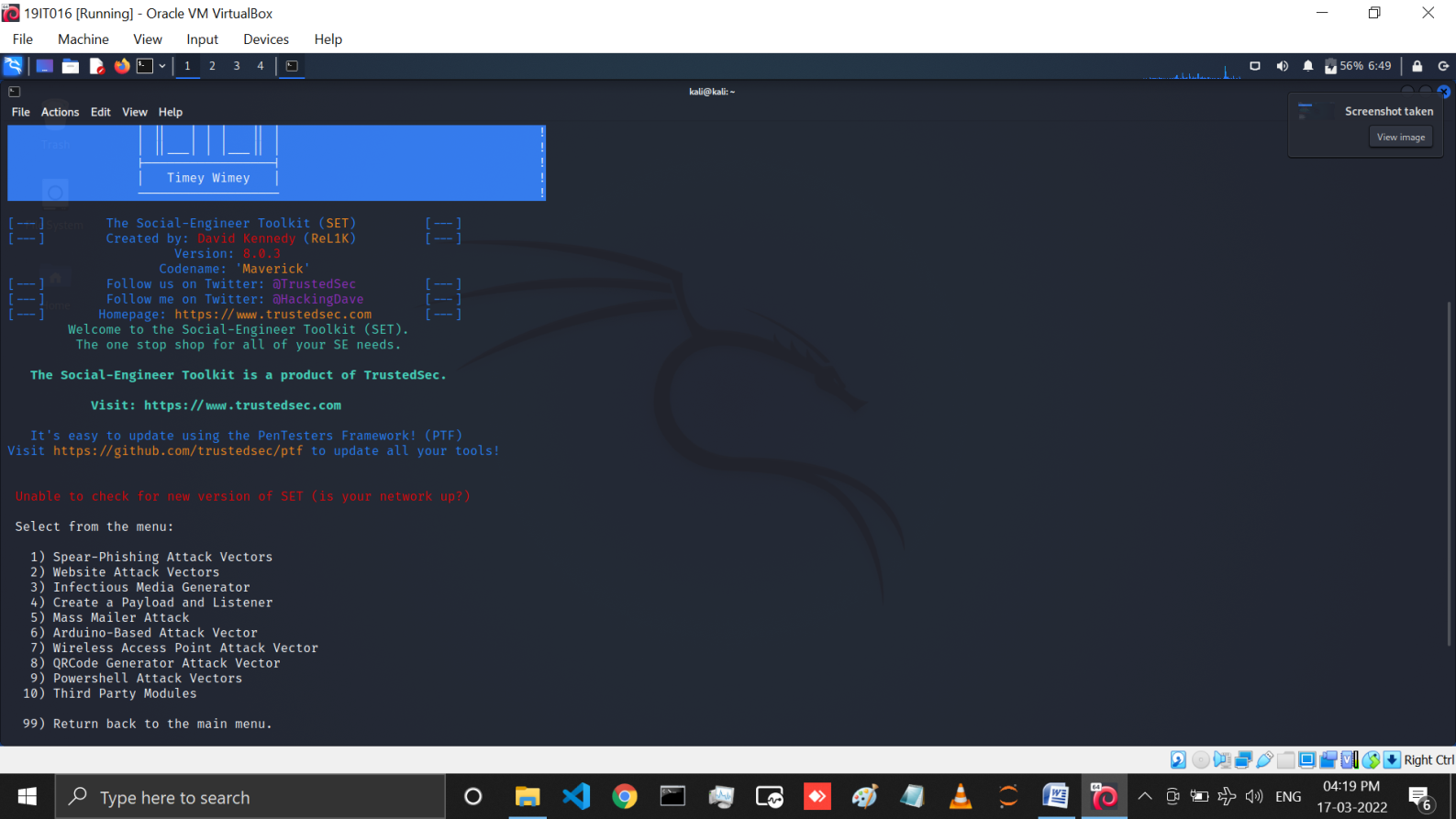
# CODE:

sudo setoolkit

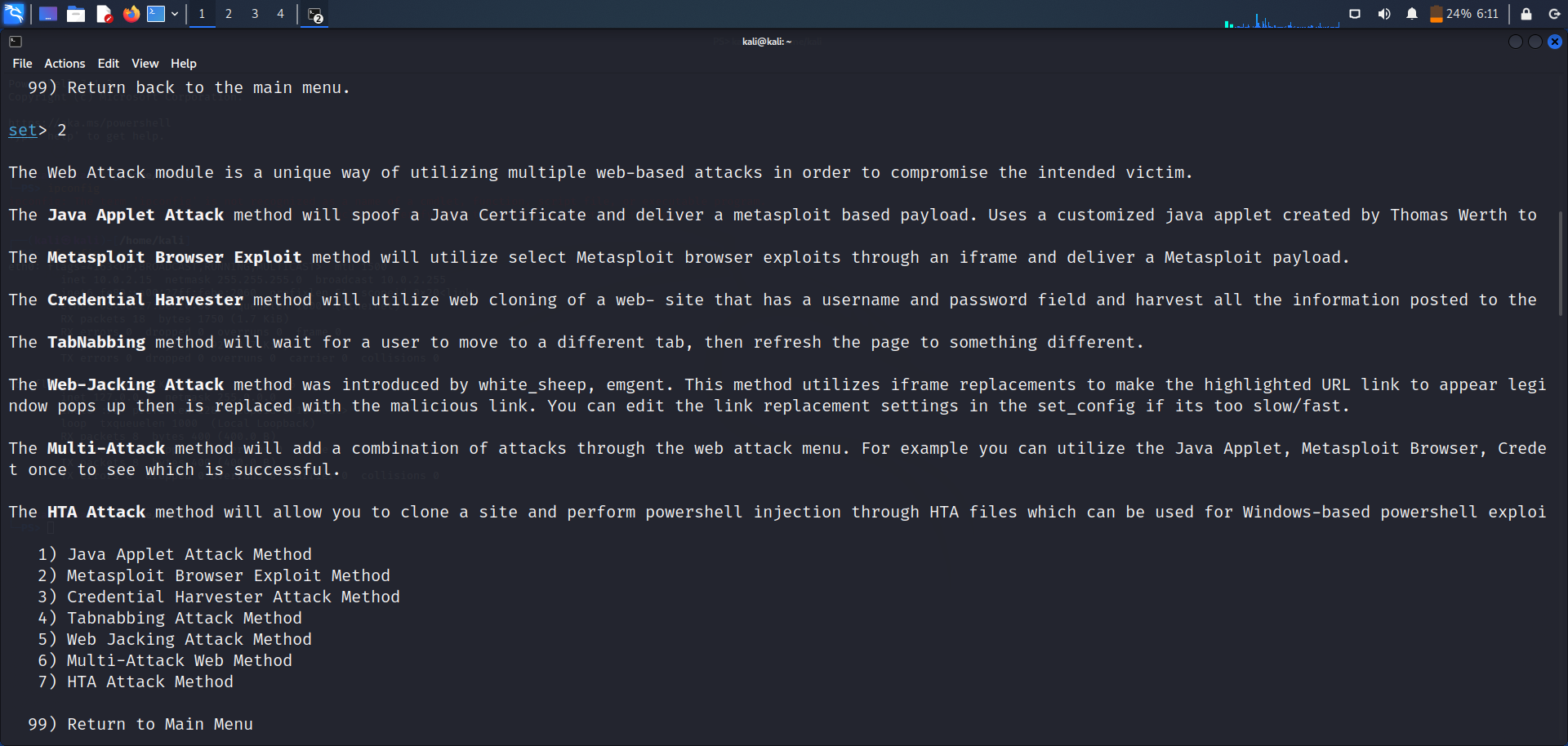
**OUTPUT:**

****

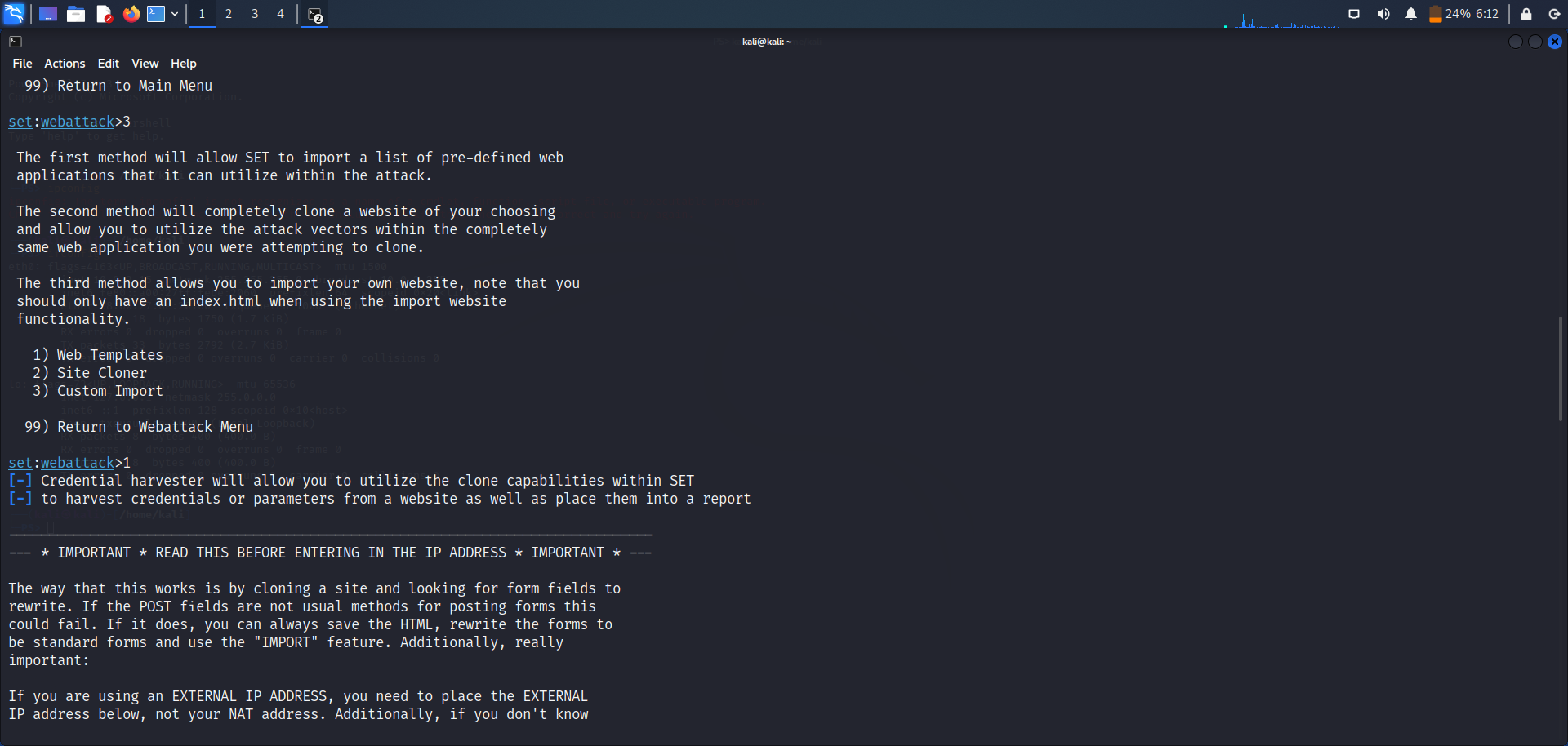
Below you can see the different types of attacks but we have to select social engineering attack for that enter 1.



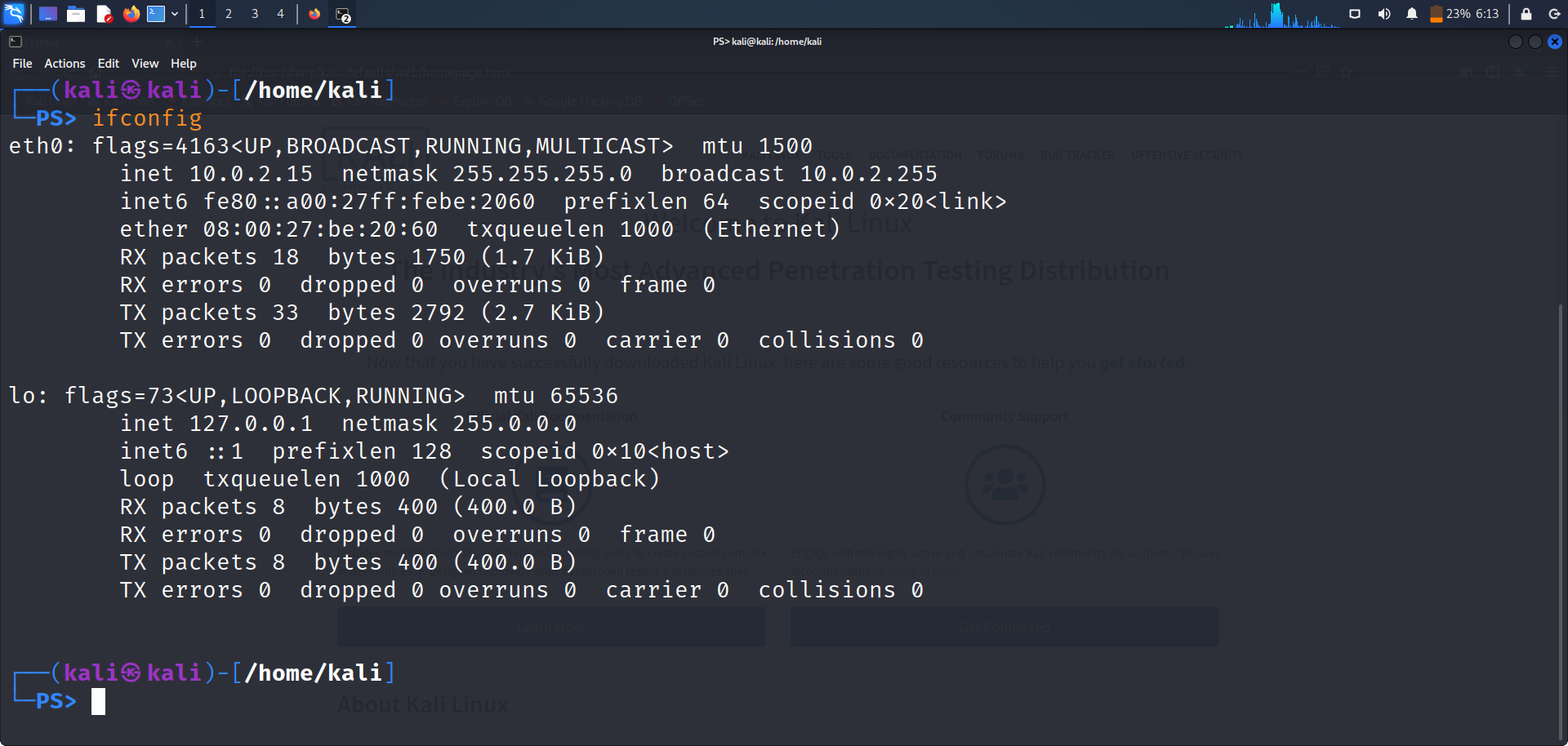
Below In Social engineering there are many attacks but we will perform website attack vectors .So select 2 and press enter to continue.

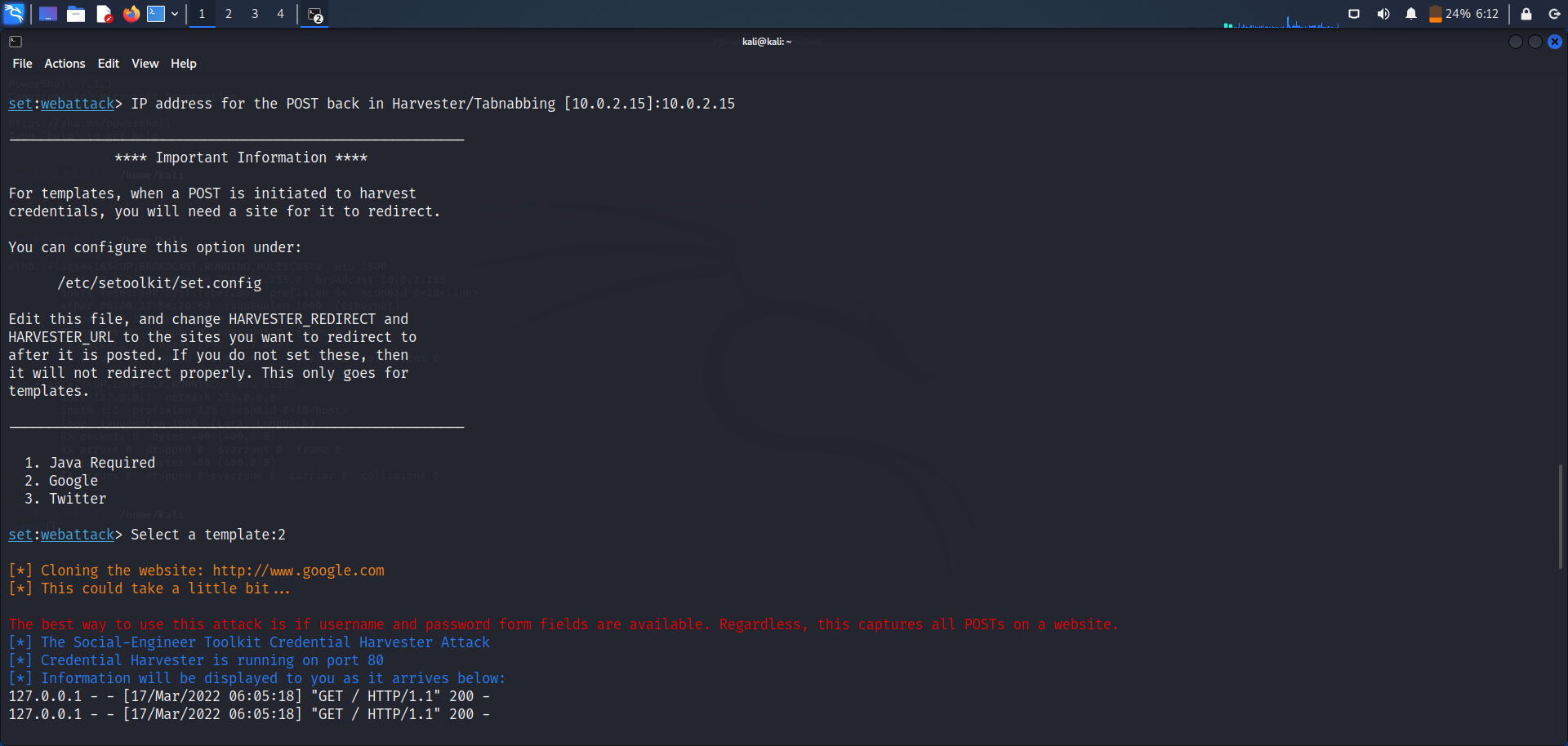


Below we are going to perform **credential harvester attack** which is used to get credentials from user by launching the popular sites like Google and twitter's login page .So select 3 for it. then select 1 and press enter to create web template for phishing.

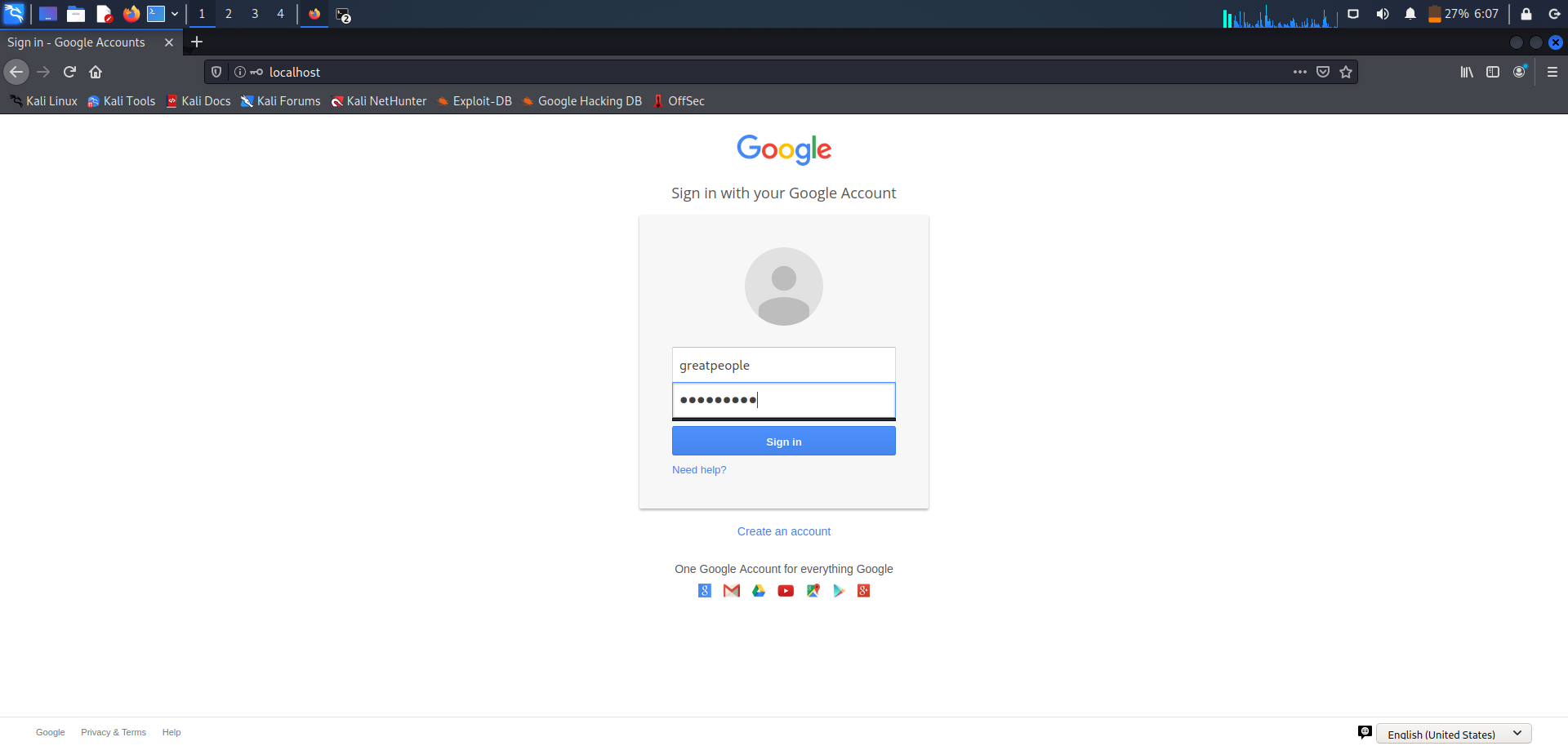


Below select IP address of your pc to get victim's credentials to your terminal. And then select the template of website you want to clone here we are selecting Google.

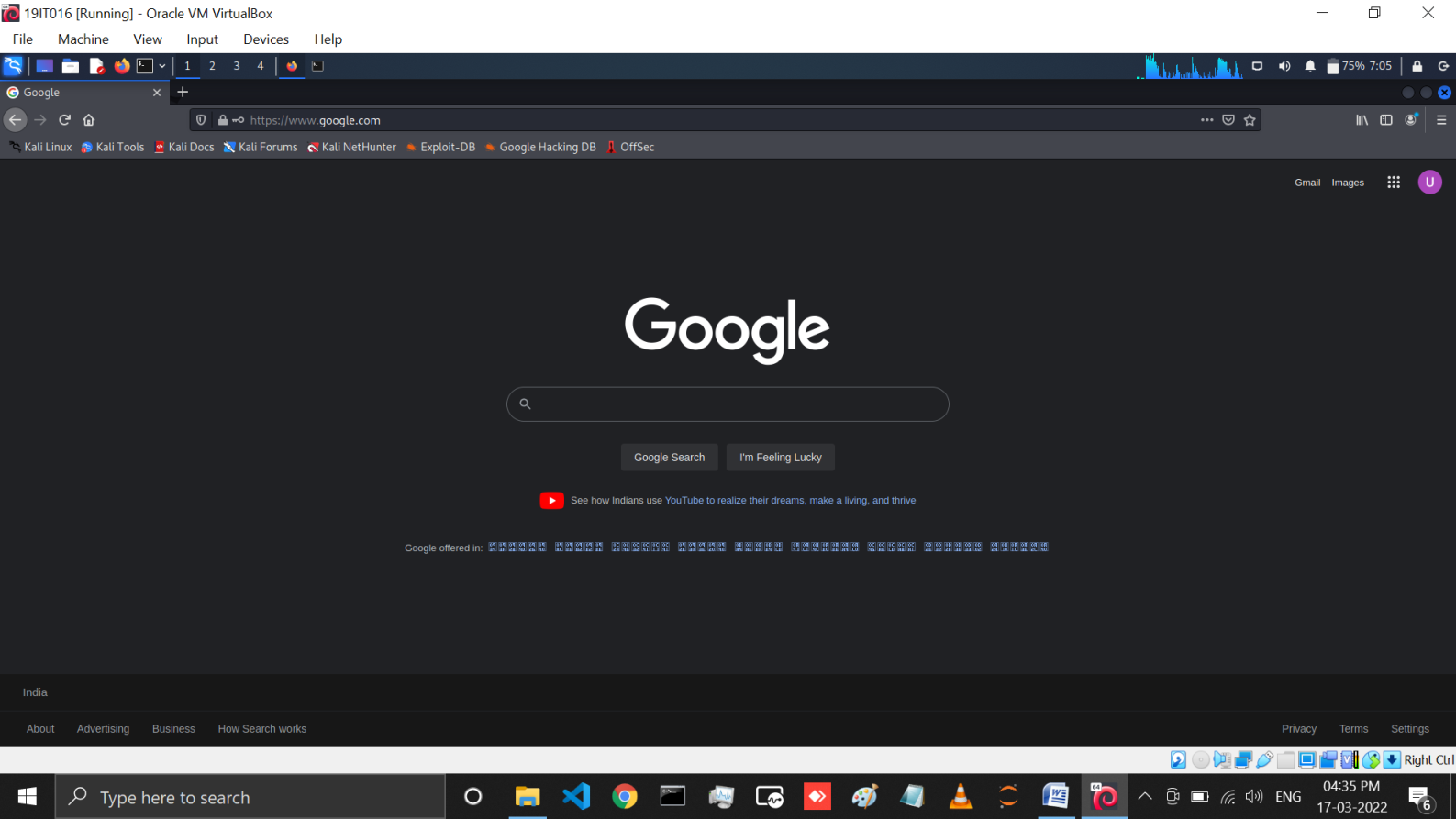




Below enter the IP address of your machine to browser and press enter you will see the Google login page. Then we have entered information for login.



Below we can see, after pressing enter original Google login page will open and victim will think like there may be error because of low internet.



Below we can see, whenever victim will enter it's email id and password, it's credentials will be shown in our terminal.



# LATEST APPLICATIONS:

* Multi-platform: It can run on Linux, Unix and Windows.
* Supports integration with third party modules.
* Allows multiple tweaks from the configuration menu.
* Includes access to the Fast-Track Penetration Testing platform
* Social engineering attack options such as Spear-Phishing Attacks, Website Attacks, Infection Media Generator, Mass Mailing, Arduino-Based Attack, QRCode Attacks, Powershell Attack Vectors, and much more.

# LEARNING OUTCOME:

In this practical we learned what is social engineering and how hacker’s use it to theft the personal information of victims.Then we learned about kali linux’s tool named ‘setoolkit’ which has many features and attacks like social engineering attacks,penetration testing,and many more.Then we performed credential harvesting attack and demonstrated how this attack works.

# REFERENCES:

1. Social Engineering Attack Demo - Kali Linux setoolkit - Cybersecurity - CSE4003 - YouTube