**Name: Vidya Solanki**

**CFSS CYBER SECURITY & ETHICAL HACKING PROJECT**

**Q1. Explain the concept of steganography, its benefits, and a practical example. Specifically, could you demonstrate how to perform image steganography, hiding text within an image using tool like Stegosuite in Kali Linux.**

* Steganography:
* It is practice of hiding one piece of information or data within another in such a way that it is difficult to detect.
* It often involves hiding a message or file within another file, like hiding text within an image or audio file.
* The goal is to conceal the existence of the hidden data, making it hard fir anyone to realize that there is a secret message embedded within the apparent carrier file.
* Benefits:

Here are some key benefits of steganography:

* Convert Communication
* Security Enhancement
* Data Concealment
* Prevention of Data Tampering
* Invisible Communication Channels
* Watermarking and Copyright Protection
* Reduced Susceptibility to Attacks
* Military and Intelligence Applications
* Enhanced Privacy

Practical Example:

Image Steganography using Stegosuite

Stegosuite is a tool designed for various steganographic techniques, and it can be used to hide text within images.

Steps:

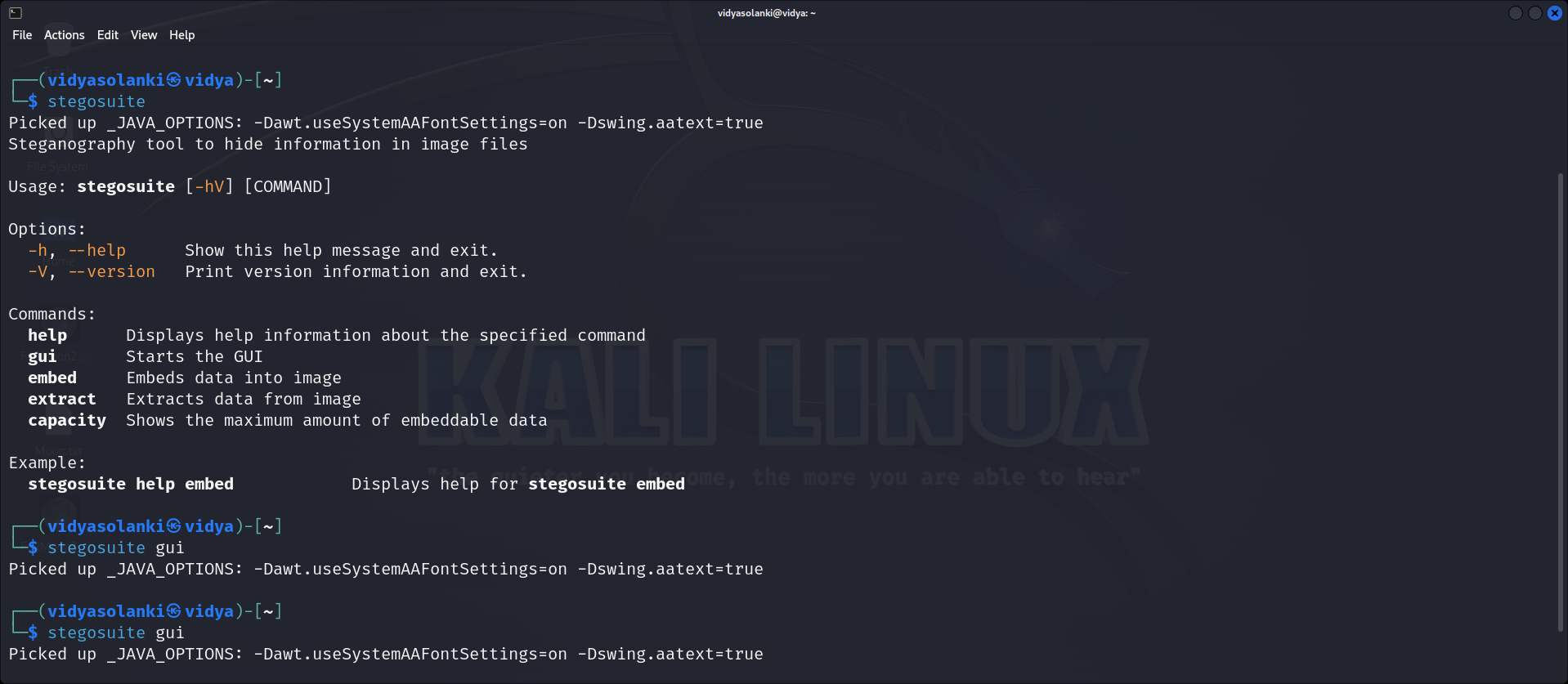
1.Install Stegosuite

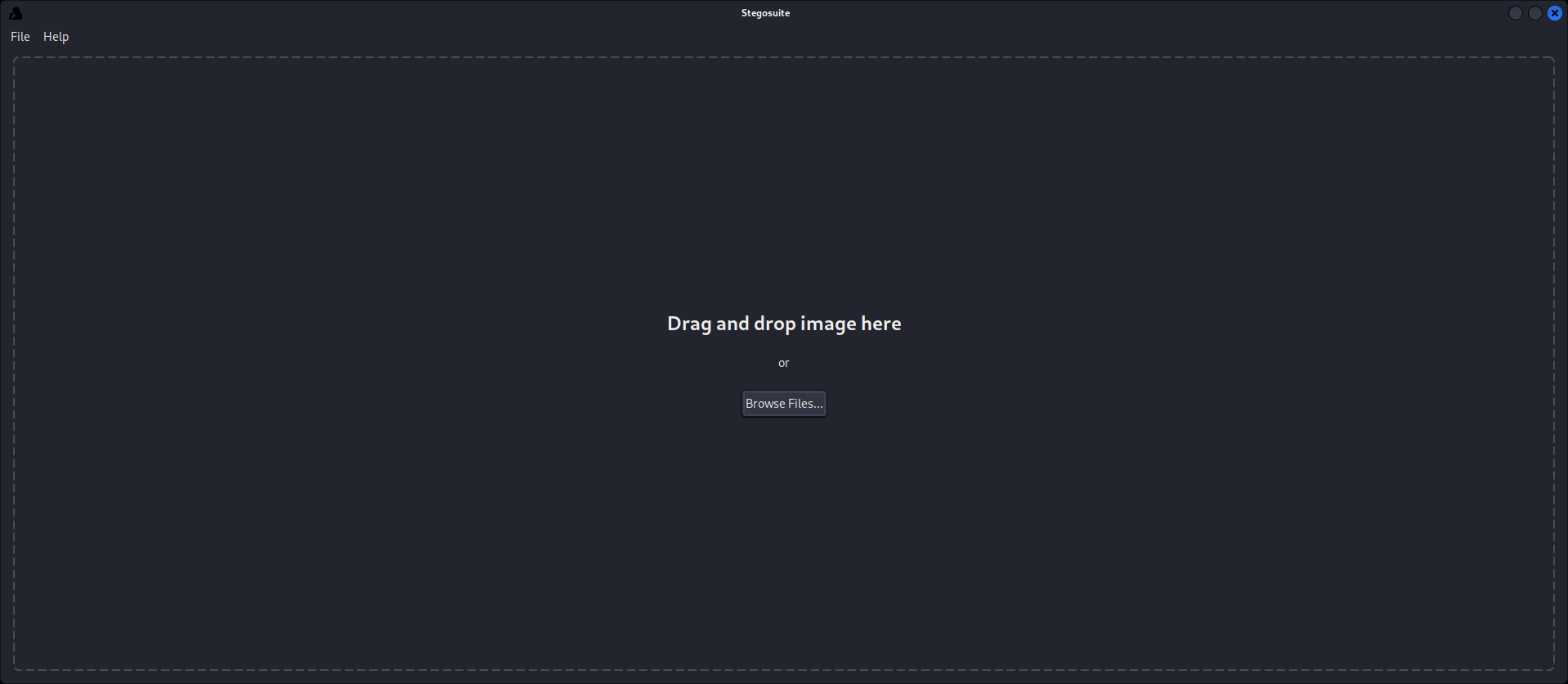
On Kali Linux terminal use this “sudo apt install stegosuite” command to install Stegosuite tool. As Shown in Figure



2.Open Stegosuite

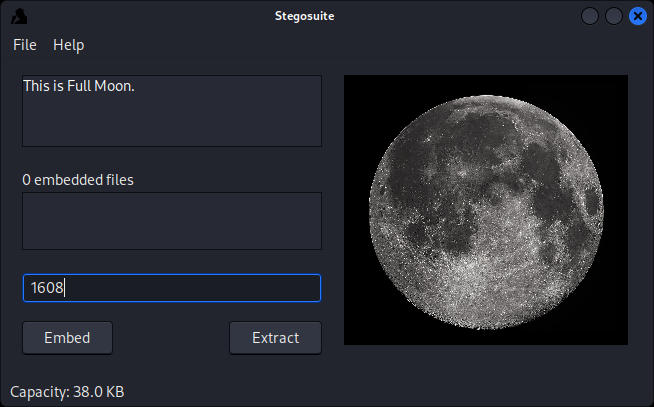
Launch stegosuite from the terminal or application menu.





3. Choose Image and Text

Select an image file to be the carrier and input the text message you want to hide.



4. Embed the Text

Click on Embed button to Embed the text.

5. Open Embed File

Open the embed.jpg file to see the Secret text.

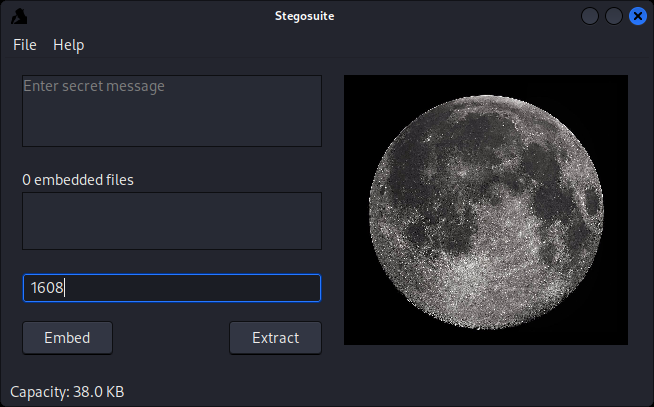


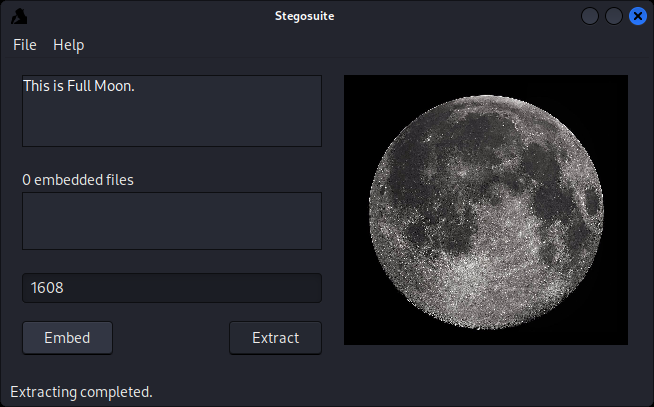
6. Extract Secret Message

Enter the password and click on Extract button.

7. Resulting Image

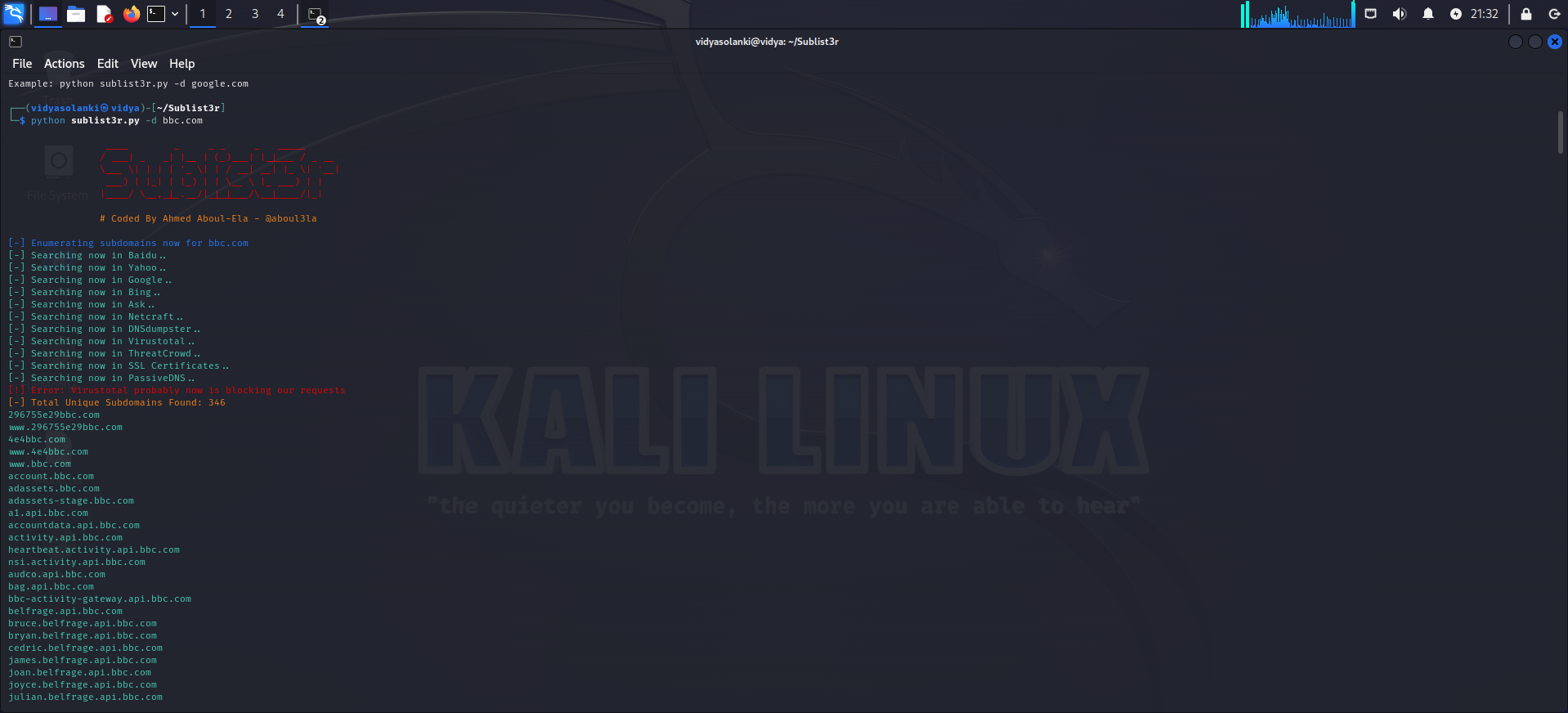
Now this image file contains secret message.





**Q2. Utilize various tools such as Sublist3r and Maltego, along with the search engine Netcraft, to discover subdomains of the target ‘bbc.com’.**

* Sublist3r:
* It is tool designed in python and uses OSINT in order to enumerate subdomains of websites.
* It helps pen-testers in collecting and gathering subdomains for a domain which is their targets.
* To fetch accurate results, it uses many search engines like Google, Yahoo and even tools like Netcraft, Virustoral, etc.
* Maltego:
* It is powerful OSINT and data visualization tool that helps investigators and security professionals gather and analyze information about individuals, organization, and relationships.
* It provides a graphical interface to link and correlate diverse information from various sources on the internet.
* The focus of maltego is analyzing real world relationships between information that is publicly accessible on the Internet.



**Q3. Explain what the Wayback machine is how it functions. Describe the process of retrieving sensitive data from the Wayback Machine. Provide a screenshot of how the website ‘bbc.com’ appeared in 2010, obtained from the Wayback Machine.**

* It refers to the Internet Archive’s Web archive service, which allows users to view past versions of websites as they appeared at various points in the past.
* The Internet Archive is a non-profit digital library that aims to preserve and provide access to historical collections of digital content, including websites.
* The Way back Machine crawls and save snapshots of web pages at different points in time.
* Users can enter a specific URL and select a date to see how a particular website looked in the past.
* This service is valuable for researchers, historians and anyone interested in tracking the evolution of websites and online content over time.
* The availability of historical snapshots may vary depending on factors like the website’s popularity and the frequency of updates.
* It is useful tool for exploring the history of the web and understanding how websites have evolved.
* Retrieving data from the Way back Machine is straightforward process.

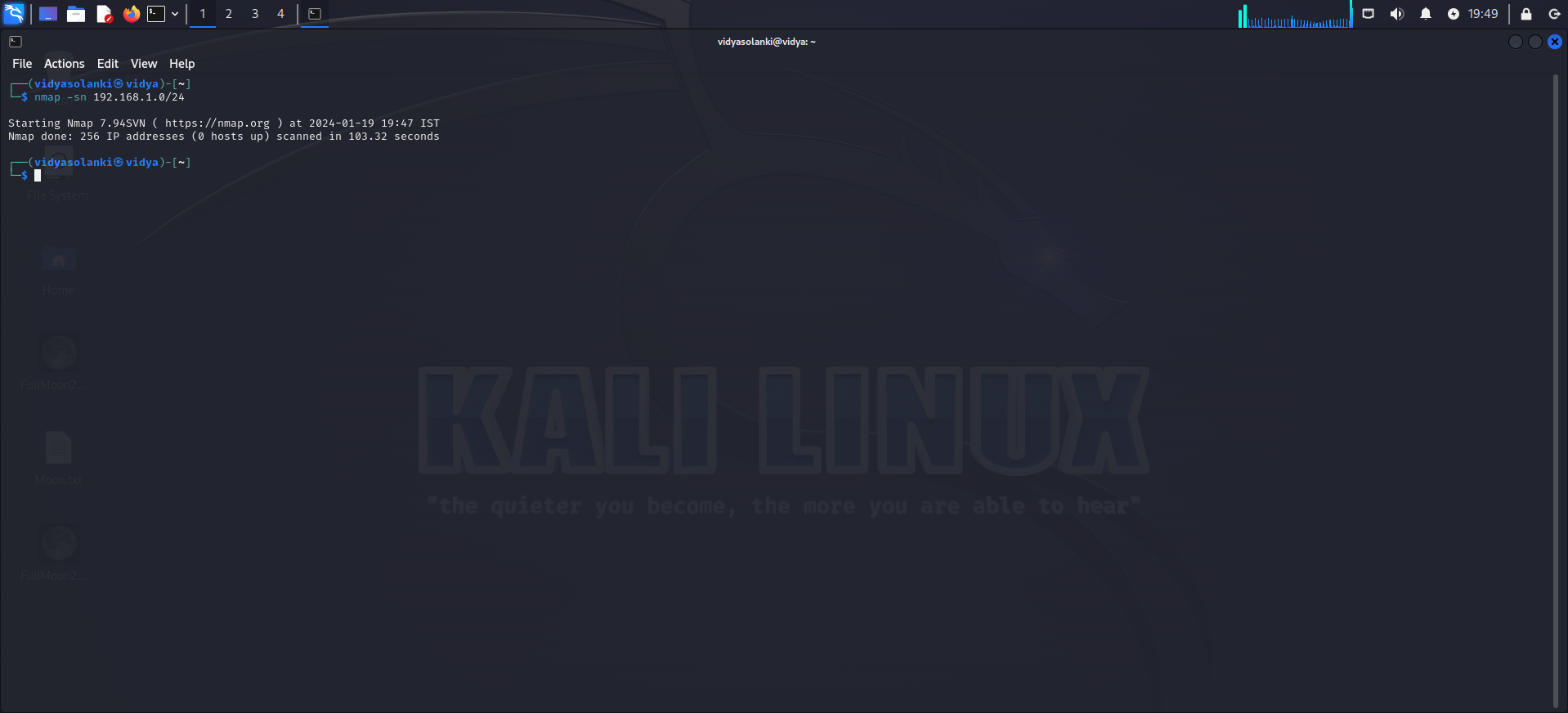
1. Visit the wayback machine website
2. Enter the URL
3. Select a Date
4. View Snapshot
5. Navigate the archived Website
6. Accessing specific content
7. Save the Snapshots

**Q4. Establish a connection to a local area network (LAN) via Wi-fi. Utilize the NMAP tool to determine the number of devices currently connected to the LAN. Show the results.**

* “Network Mapper” (Nmap) is a powerful open-source network scanning tool.
* It is used for Discovering hosts and services on a computer network, creating a map of the network, and finding open ports.
* It is widely used by network administrator and security professionals for various purposes, including network inventory, managing service upgrade schedules, and monitoring host or service uptime.
* Some common features of Nmap:

1. Host Discovery
2. Port Scanning
3. Service version Detection
4. OS Detection
5. Firewall Evasion techniques
6. Output Formats
7. Scripting Engine

* Now we use following command to discover hosts on the network.
* This command performs a ping scan(-sn) on all IP address in the specified range (192.168.1.0/24).



**Q5. Perform privilege escalation on the Metasploitable machine and provide a detailed description of the process you used to achieve this. Explain how you gained elevated privileges.**

* To perform privilege escalation on the Metasploitable machine, follow these steps:

1. Find a way into the system: Look for a vulnerability, like a flaw in the SMB service running on port 445. This can be exploited using a module in Metasploit.
2. Exploit the vulnerability: Use the Metasploit module to exploit the vulnerability, which will give you a shell on the system with low privileges.
3. Look for more vulnerabilities: Use Metasploit's 'enum\_patches' module to find missing patches on the system.
4. Identify privilege escalation vulnerabilities: Based on the missing patches, search for known privilege escalation vulnerabilities.
5. Exploit the privilege escalation vulnerability: Use a Metasploit module to exploit the identified privilege escalation vulnerability, which will elevate your privileges to the highest level.
6. Verify elevated privileges: Check your privileges using a command like 'who am i /all' to confirm that you have elevated privileges.
7. By following these steps, you can perform privilege escalation on the Metasploitable machine and gain higher access levels. Note that the specific vulnerabilities and exploits used may differ depending on the version and configuration of the Metasploitable machine.

**Q6. Employ a password cracking tool such as John the Ripper or Hydra to illustrate how a week password can be compromised. Provide a detailed explanation of the step-by-step process you followed to achieve this.**

* John the Ripper is an open-source password cracking tool that helps assess the strength of passwords on a system.
* It uses techniques like dictionary attacks and brute-force attacks to identify weak passwords.
* The tool supports various password hash algorithms, allows customization, and is optimized for performance.
* Steps to use John on Kali Linux and Cracking Password.

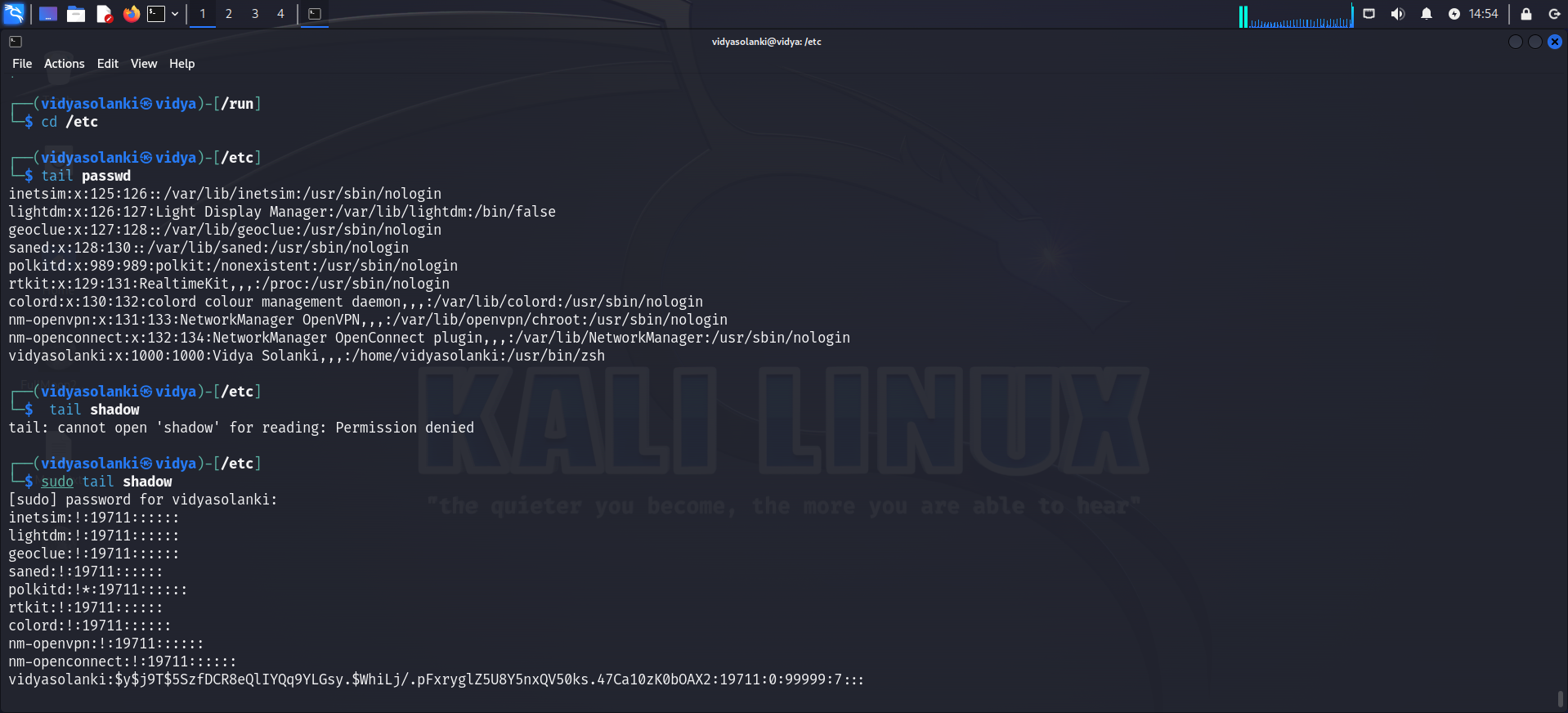
1. Install John



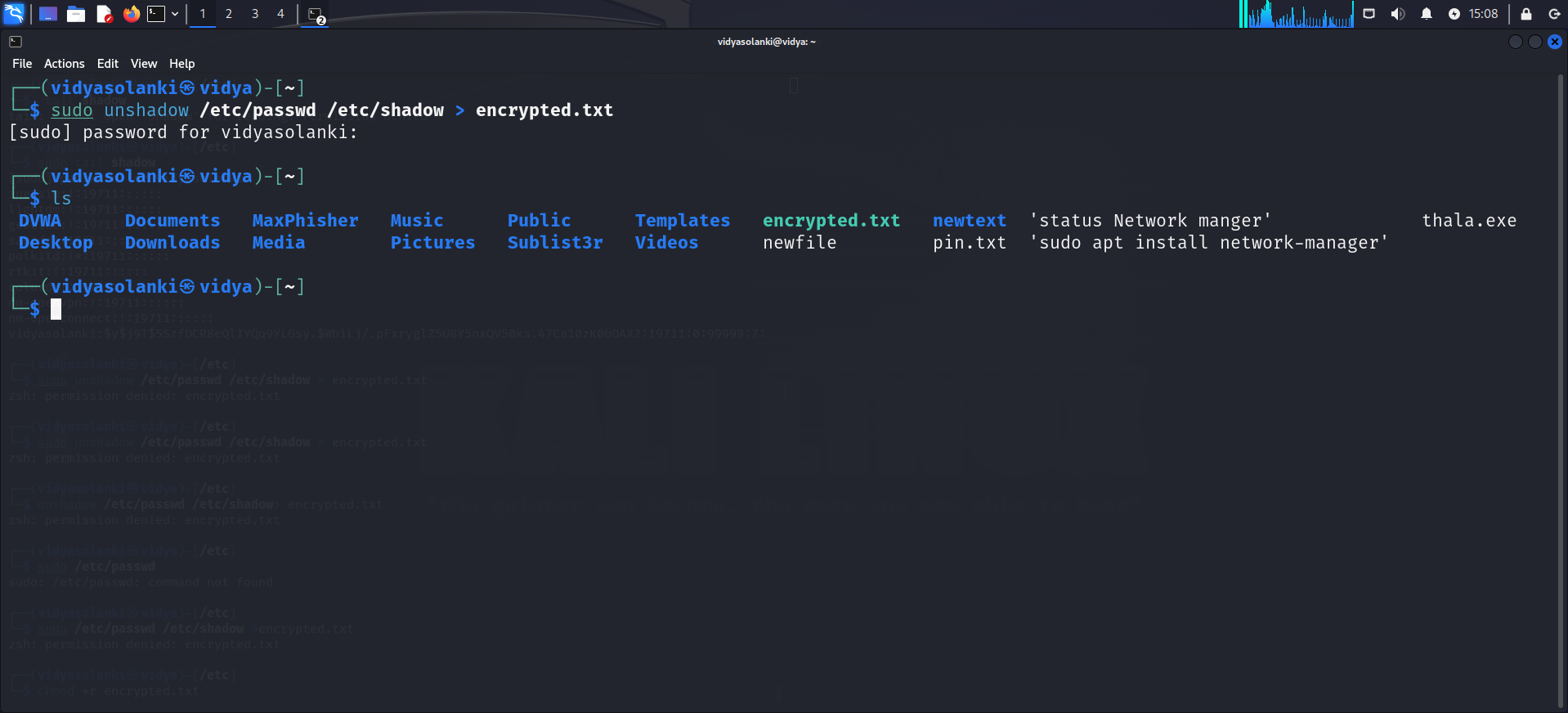
1. Now we have to go and check its operations and we have to enter in run directory.Top of Form



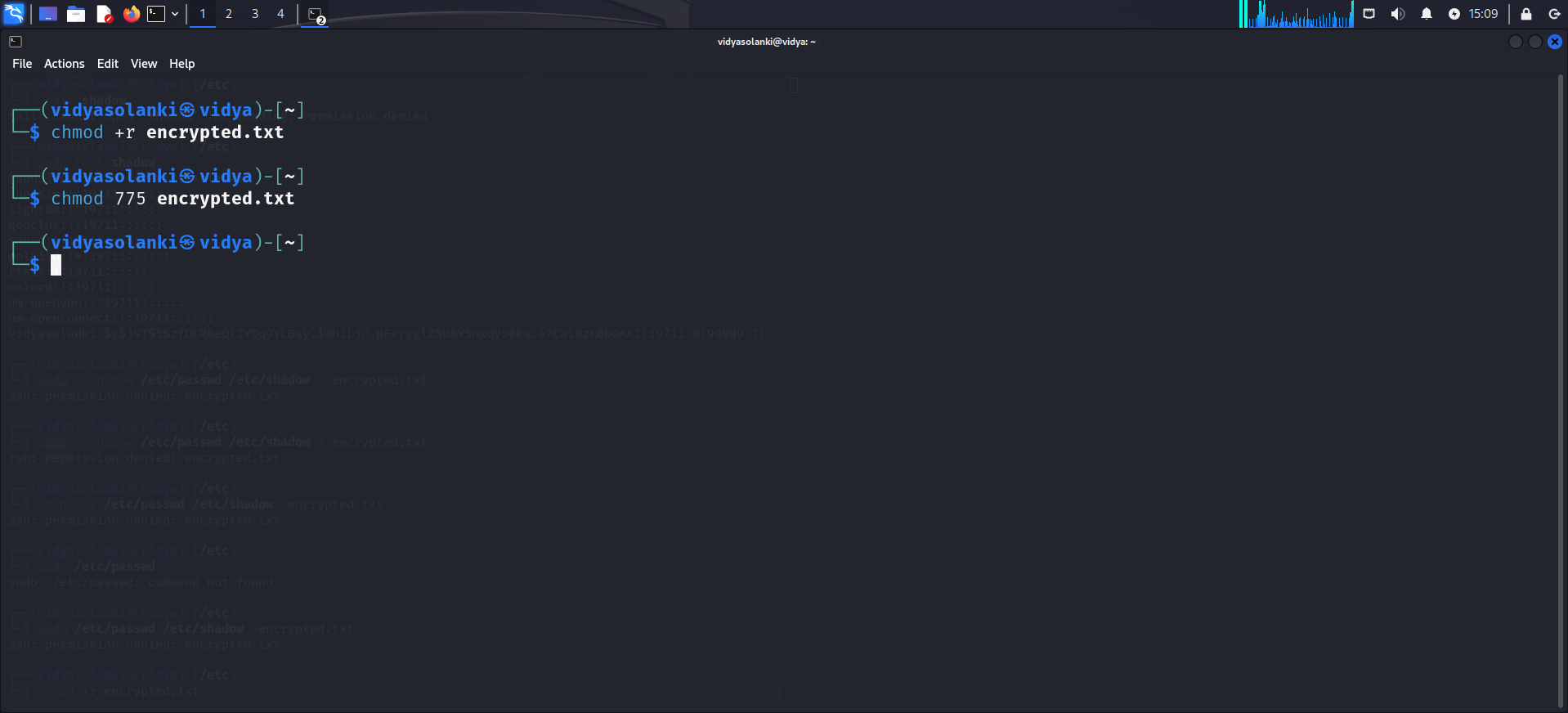
3. We have tested the John and now we have to look at two files that are in the etc directory, etc passwd, etc shadow.



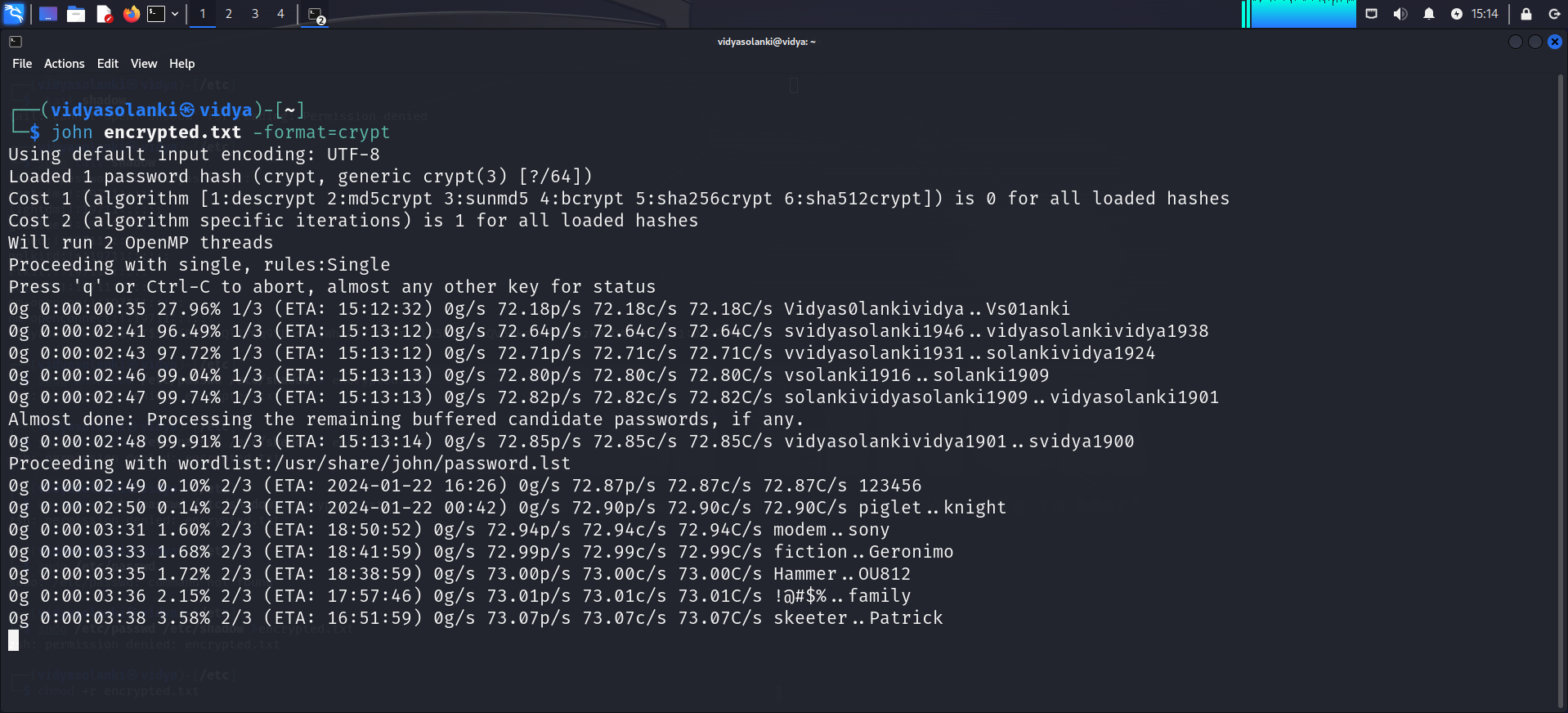
4.Now we will write following command.



5. Give read permissions



6. Now we are going to start the process with the John and we are going to decrypt the password and now it is making all the passwords which are decrypted.



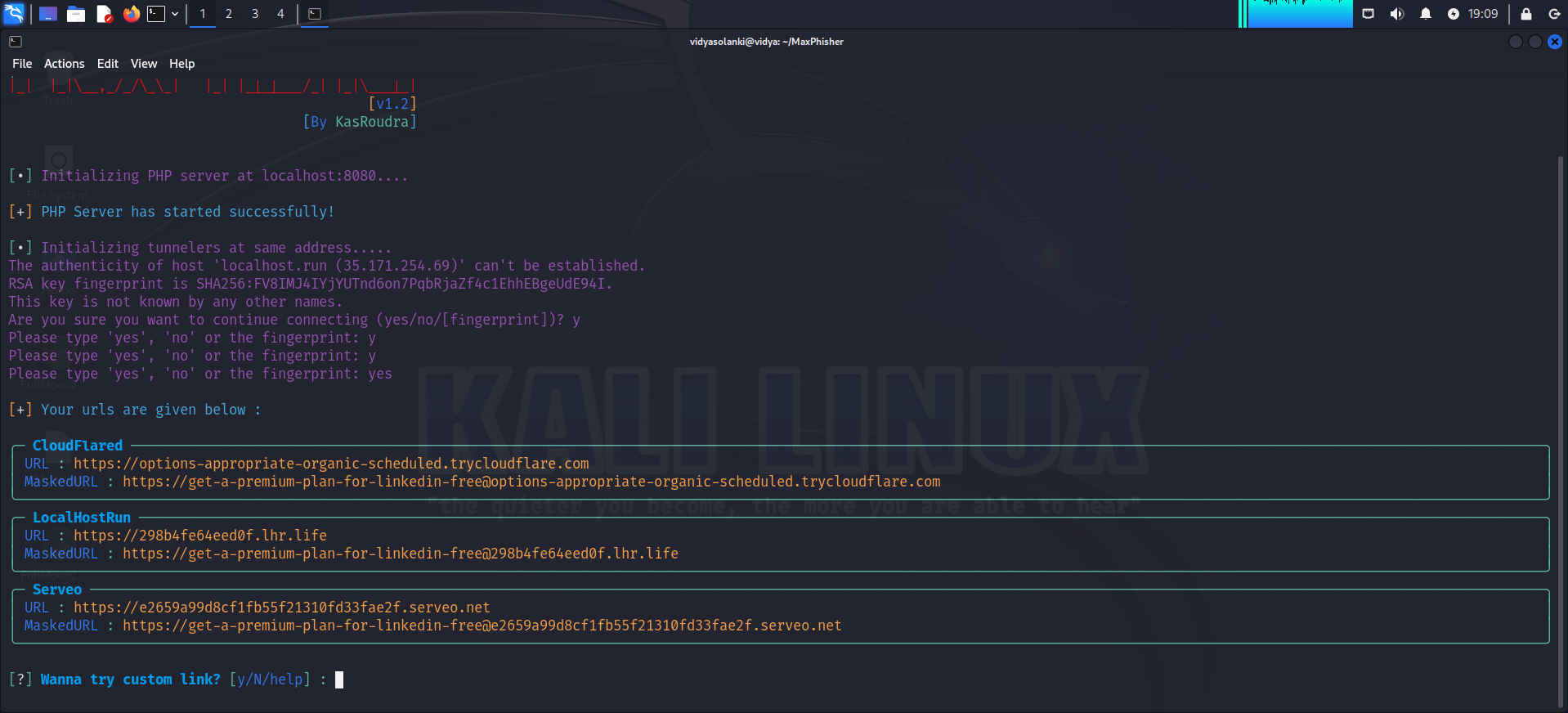
**Q7. Conduct a simulated phishing attack in a wide area network WAN environment using any suitable tool to demonstrate potential risk, specifically focusing on accessing webcams. Provide a detailed account of the steps you took during the simulation.**

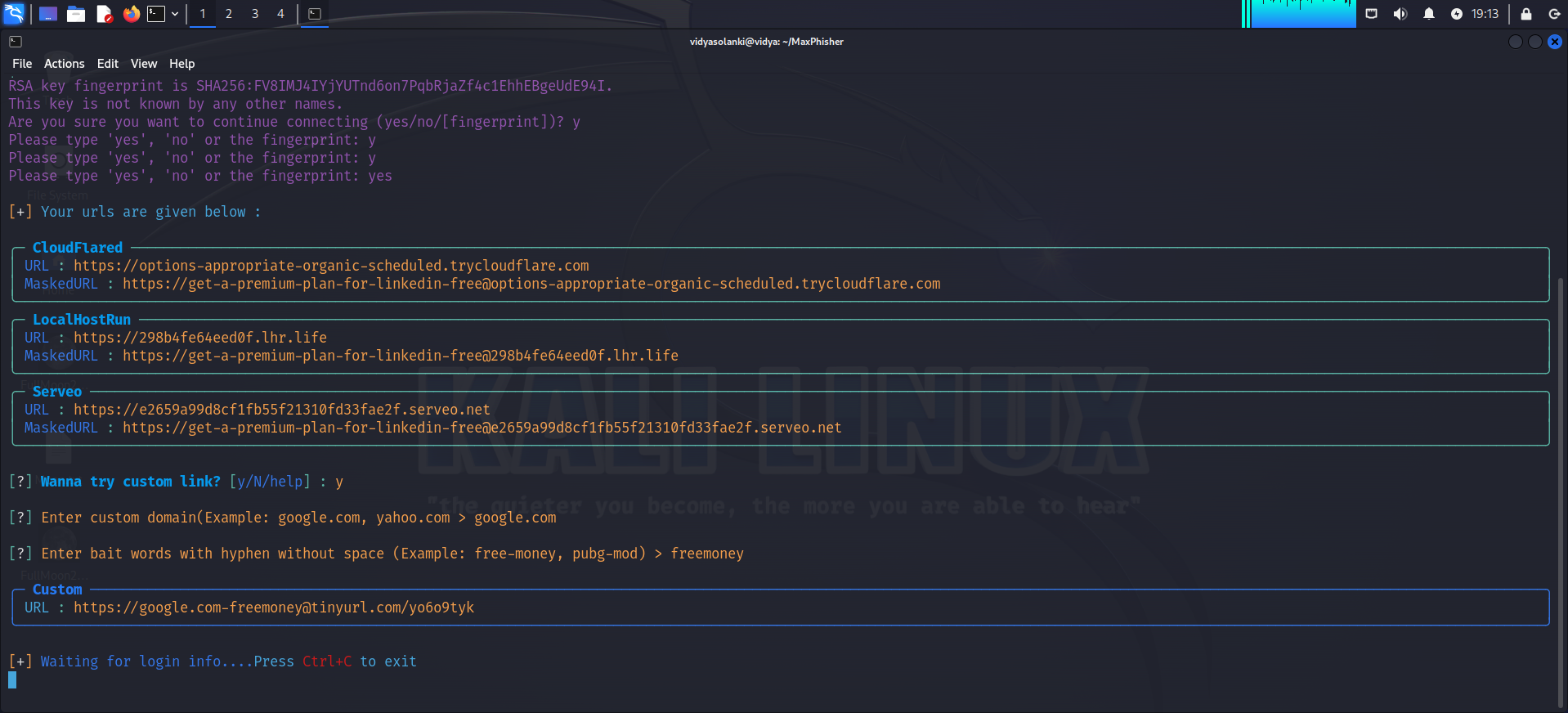
* Phishing is a type of social engineering attack that aims to deceive users into divulging sensitive information or installing malware.
* It can be conducted through emails, voice calls, SMS messages, or by modifying DNS settings.
* Max Phisher is a phishing attack simulation and testing tool designed to help organizations assess their susceptibility to phishing attacks.
* It can be used to create and launch phishing campaigns, mimicking real-world phishing attacks.
* By using Max Phisher, organizations can simulate and test their susceptibility to phishing attacks, helping them identify vulnerabilities and areas for improvement in their security posture.
* This in turn can help organizations improve their overall cybersecurity defenses and reduce the risks and potential impact of phishing attacks.
* To use Max Phisher for conducting phishing follow these steps:











**Q9. Provide an in-depth explanation of the distinctions between WEP, WPA, WPA2 and WPA3 in the context of wireless networking. Additionally, share your recommendation for the most secure option among them and elucidate the reasons behind your choice.**

* Wireless networking security protocols, such as WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA2, and WPA3 are designed to secure data transmission over wireless networks.

1. WEP

Security level is low.

Uses a static 64 or 128-bit key for encryption.

It is highly insecure and easily crack able. Weak key management and vulnerabilities in its encryption algorithm make it susceptible to attacks.

1. WPA

Security level is Moderate.

It utilizes TKIP for encryption.

It also provides stronger key management through the use of dynamic keys.

1. WPA2

Security level is High.

It uses AES for encryption, which is a robust and widely accepted encryption algo.

It also enhances the authentication process through the use of a 4-way handshake.

It is generally secure, it had faces vulnerabilities such as KRACK.

1. WPA3

Security level is very high.

It is most secure wireless security protocol.

It uses SAE protocol, also known as Dragonfly, for key establishment.

It provides enhanced protection against offline dictionary attacks and improves security for open Wi-Fi networks.

It considered as robust.

* Recommendation:
* Given the security levels and vulnerabilities associated with each protocol, the recommendation is to use WPA3 for the highest level of security.
* WPA3 addresses many of the vulnerabilities present in WEP, WPA, and even WPA2.
* Its use of the SAE protocol for key establishment enhances security, making it resistant to various attacks.
* Always ensure that both your Wi-Fi router and client devices support the chosen security protocol.
* Additionally, regularly update firmware and software to patch any newly discovered vulnerabilities.
* Keep in mind that the security landscape evolves, so staying informed about the latest developments is crucial for maintaining a secure wireless network.

**Q10. Can you provide insight into the methods for accessing a CCTV camera without authorization? If so, kindly describe the process. If not, please elucidate the challenges and difficulties you encounter in attempting to gain unauthorized access.**

That being said, here are some common methods used by malicious actors to attempt to gain unauthorized access to CCTV cameras:

1. Default Credentials:

Many CCTV cameras come with default login credentials, such as "admin" for both the username and password. Attackers can use these default credentials to attempt to gain unauthorized access to the cameras.

1. Brute-Force Attacks:

Attackers can use automated tools to attempt to guess the correct login credentials by trying out various combinations of usernames and passwords.

1. Exploiting Known Vulnerabilities:

Attackers can search for and exploit any known security vulnerabilities in the CCTV camera's firmware or software. This can allow them to gain unauthorized access to the camera.

1. Social Engineering:

Attackers can use various social engineering tactics, such as phishing emails or vishing phone calls, to trick employees or other authorized users into revealing their login credentials for the CCTV camera.

1. Physical Access:

In some cases, attackers may attempt to gain physical access to the CCTV camera itself. This can allow them to tamper with the camera, modify its settings, or even replace the camera with a malicious device.