
# Project Report

## DEMONSTRATION OF THE CYBER SECURITY ATTACKS

MODULE TITLE: COMPUTER SYSTEMS SECURITY

MODULE CODE: B9IS103

GROUP MEMBERS:

SINGUPURAM NAVIN KUMAR | 10612366

DIGVIJAY JATKAR | 10508676

FEBIN BABU SKARIYA | 10563025

MODULE LEADER: PETE CASSIDY

# TABLE OF CONTENTS





# TABLE OF FIGURES





## 1. SUMMARY

The practice of simulating various sorts of cyber assaults to highlight weaknesses in computer systems and networks is referred to as a cyber security attack demonstration. This presentation is frequently carried out by ethical hackers or security professionals who utilize their knowledge and experience to uncover and exploit vulnerabilities in security systems to highlight possible security breaches.

The goal of such demos is to educate computer users about the risks and implications of cyber assaults, as well as the best methods for safeguarding their systems and data. It also assists enterprises in identifying weaknesses in their systems and strengthening their security procedures.

Social engineering, phishing, malware assaults, denial-of-service (DoS) attacks, and other tactics may be used in cyber security demonstrations. These demos are often conducted in a controlled environment, employing a combination of real-world situations and simulated attacks to demonstrate the possible impact of cyber attacks on an organization's operations, data, and reputation.

Ultimately, the purpose of cyber security attack demos is to assist individuals and organizations in remaining aware and proactive in their attempts to defend themselves from cyber-attacks.

## 2. INTRODUCTION

A cyber-attack is any attempt to obtain an unauthorized personal computer, system software, or computer system to cause harm. A cyber-attack aims to change, block, delete, alter, or steal data from a computer system as well as to disable, disrupt, destroy, or seize control of it.

- The cause of 95% of cybersecurity breaches is human mistakes. (World Economic Forum).
- The global market for information security is projected to reach $366.1 billion in 2028 by Forbes Business Insights.
- More than any other country in 2020, the U.S. was the target of 46% of cyberattacks.
- About 40% of breaches in 2021 involved phishing, 11% involved malware, and 22% involved hacking. (Verizon)
- The number of data breaches increased in 2021, from 1,506 in 2017 to 1,862.

Two distinct but related types of illegal behavior are referred to as "cybercrime."



Purely technological cybercrimes relate to illegal actions that can only be carried out through computer systems, computer networks, or other kinds of information and communications technology (ICT). These crimes are impossible to perform without the use of technology, and they frequently entail the exploitation of flaws in computer systems, networks, or digital devices.
Hacking, distributed denial-of-service (DDoS) assaults, virus attacks, identity theft, and phishing are all examples of pure cybercrime. These cybercrimes employ technology to gain access to or modify data or systems, steal personal information, or disrupt digital activities.
These consist of:

- Unauthorized entry into networks and network hacking.
- The transmission of viruses and other infections that cause computers to cease working as a result of DDoS attacks.

In this report, we'll talk about a few cyberattacks and show you how to carry them out using the tools provided below. For demonstration reasons, we'll simulate attacks on a second virtual system using Kali with the ip of DVWA.

## 3. SETUP

Required software:

1. Oracle VirtualBox Hypervisor
2. Kali Linux Operating System machine
3. DVWA machine

We must build fresh Kali and DVWA instances and images as part of the initial stage. The steps involved in setting up both machines are similar.



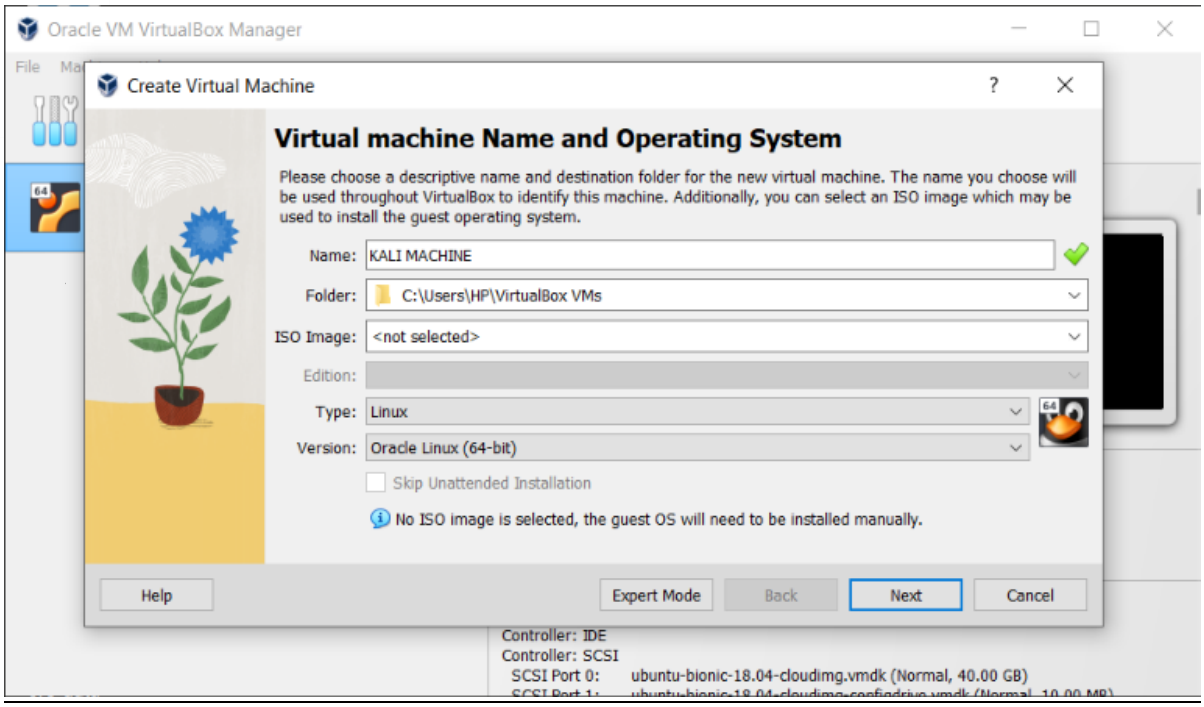



**Figure 1: Choosing the VM name and version**

Both virtual machines use Linux as their operating system (OS), with Kali based on Debian and DVWA on Ubuntu. As a result, it is critical to pick the proper operating system versions for each virtual machine.

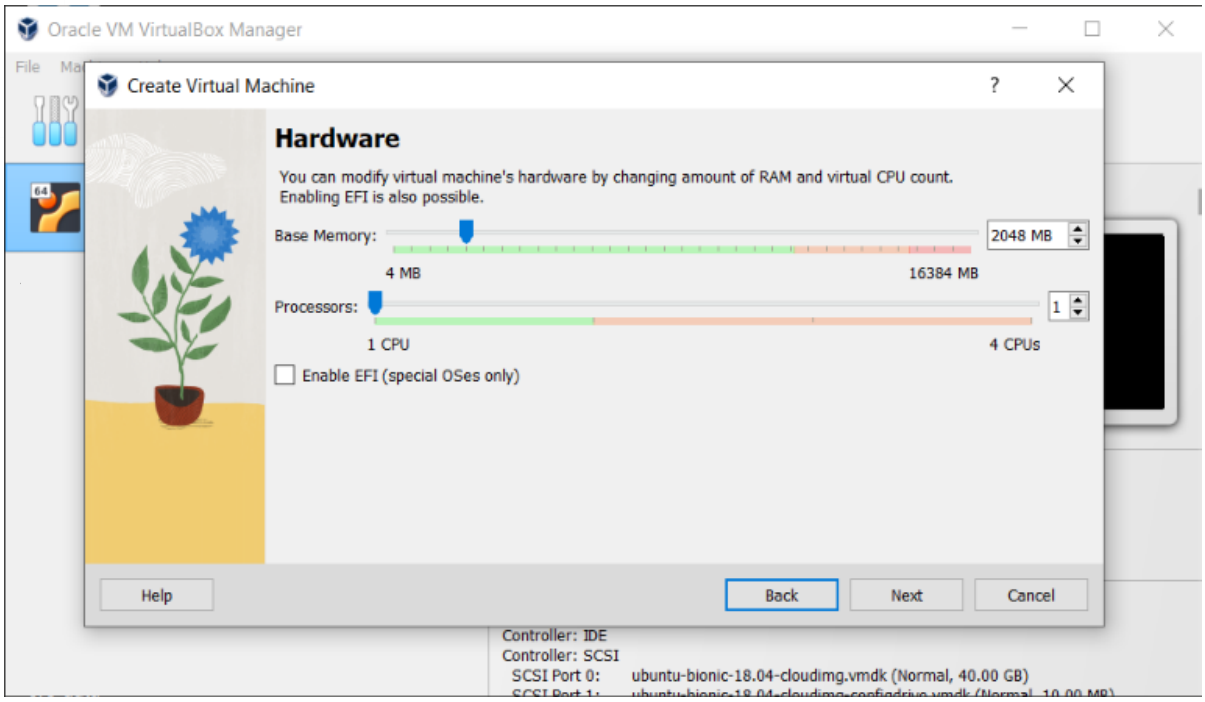



**Figure 2: Base Memory and Processors**

Set the system to at least one gigabyte of RAM.

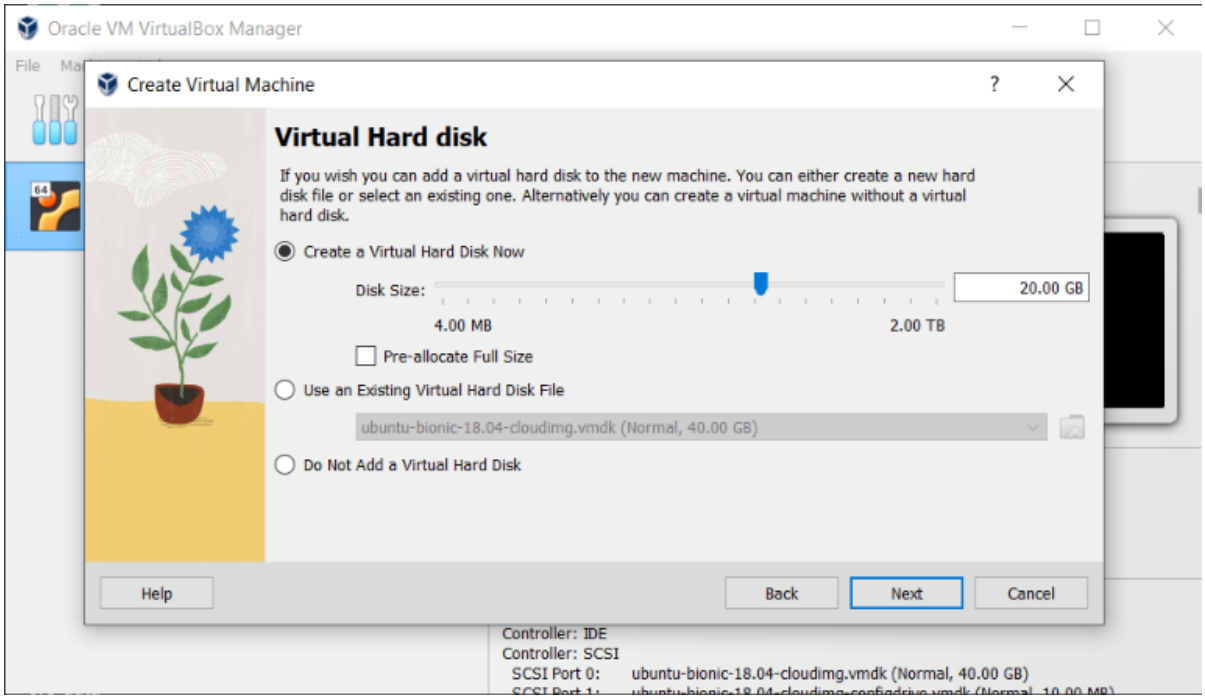



**Figure 3: Choosing Virtual Hard Disk**

In the case of configuring new machines, select generating a hard disk. Choose a virtual hard drive that is already set up on the host system if not.

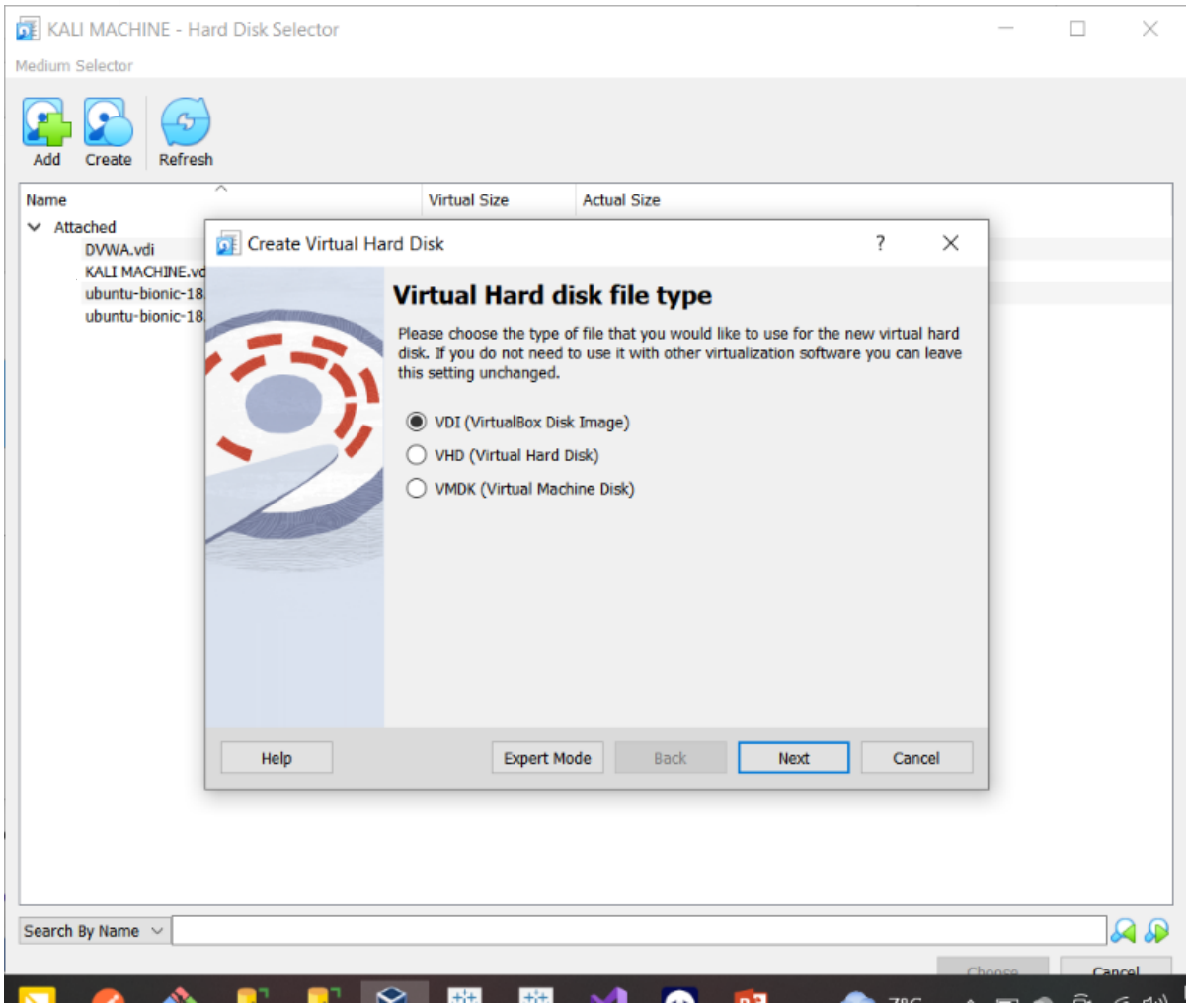



**Figure 4: VDI file**

Dynamic disk allocation assigns only the amount of disk space that the guest machine is currently consuming, and this amount increases as more data is stored on the virtual machine's disk.

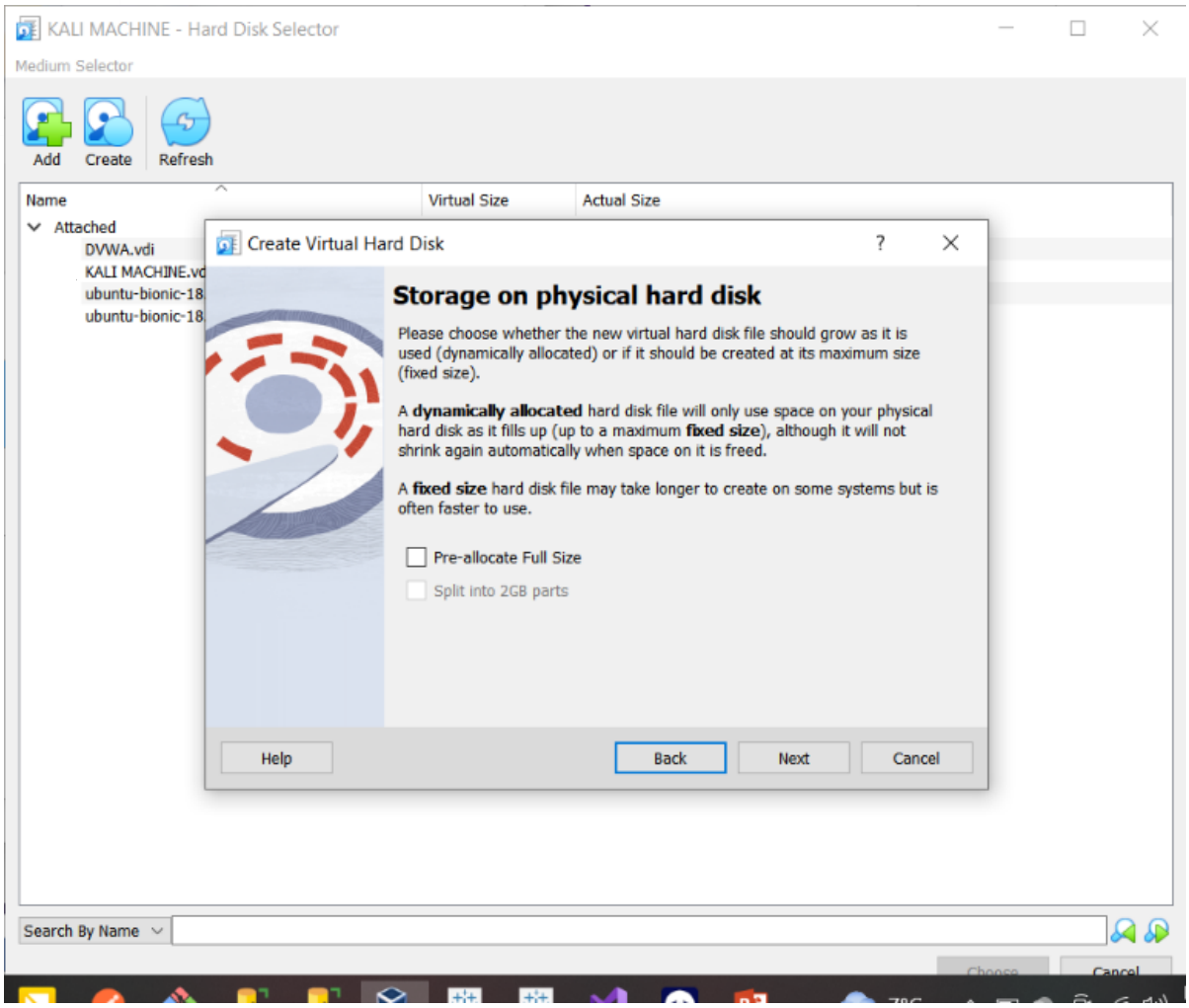



**Figure 5: Storage type**

Summary for the new configuration of the new virtual machine.

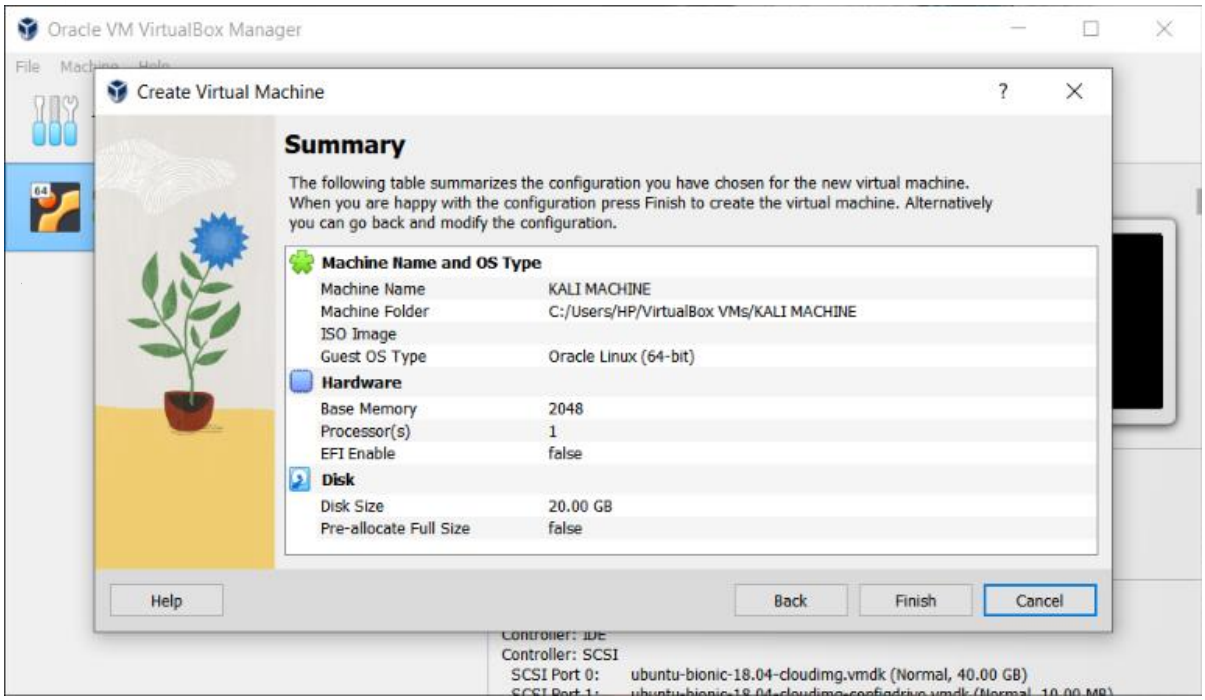



**Figure 6: Configuration Summary**

Allowing bidirectional data flow will greatly simplify processes like transferring files and text between the host and guest computers.

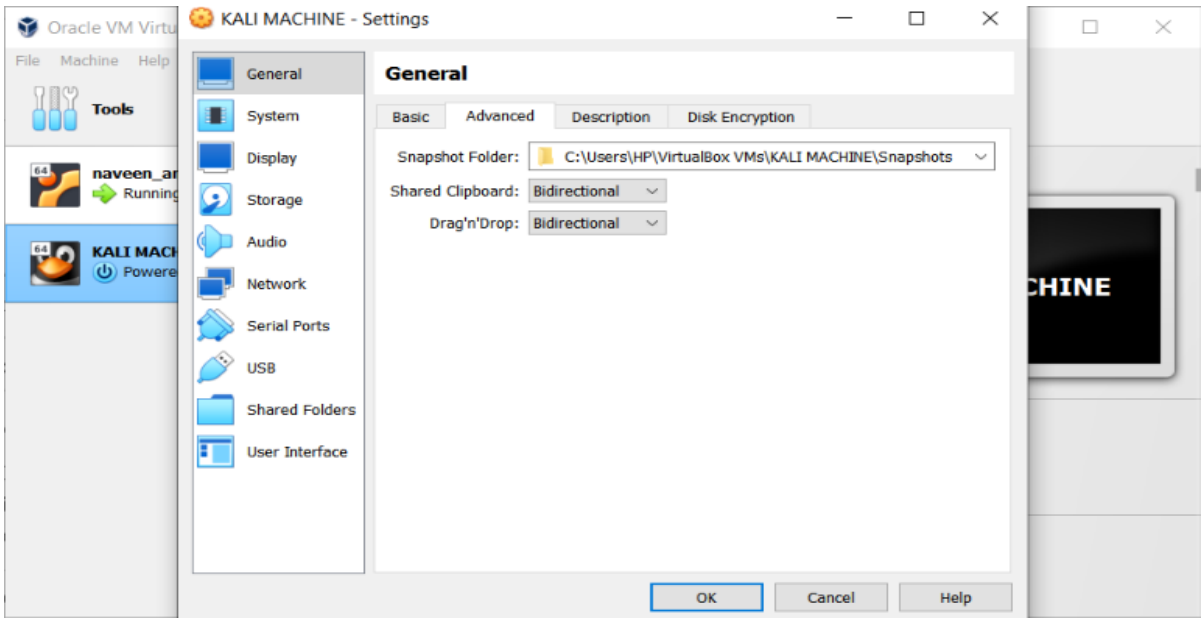



**Figure 7: Allowing Data Flow**

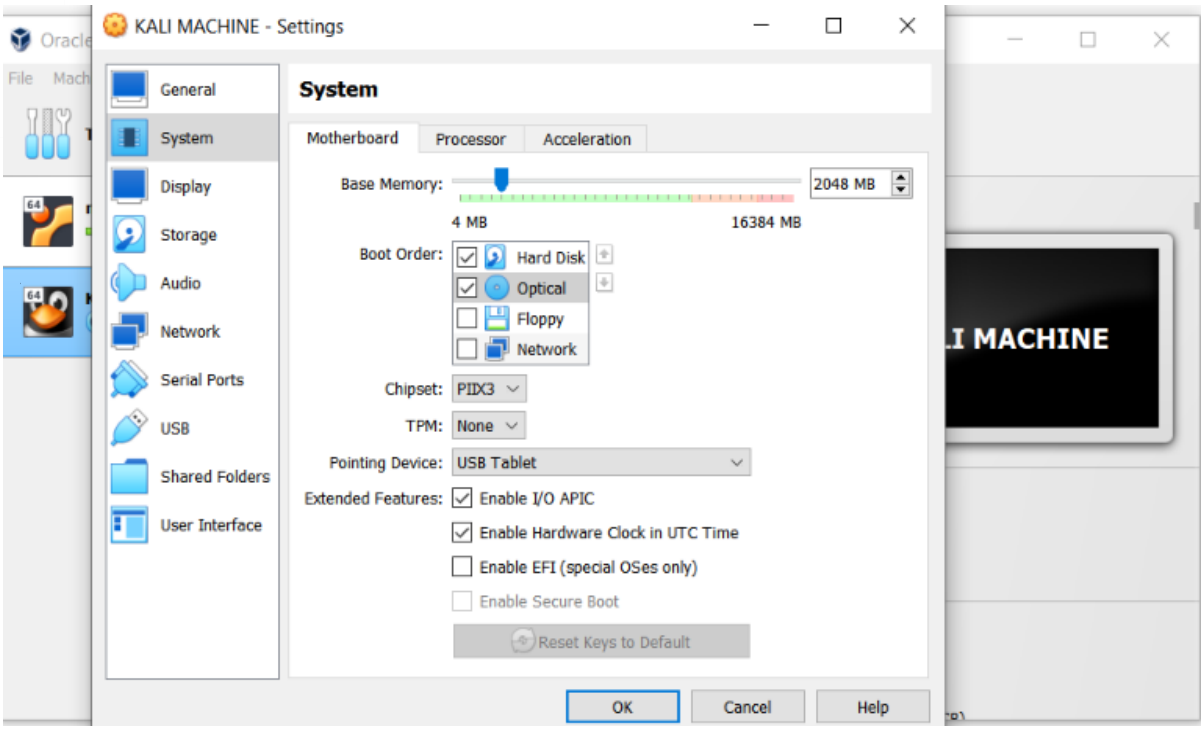



**Figure 8: Boot Order and Pointing Device**

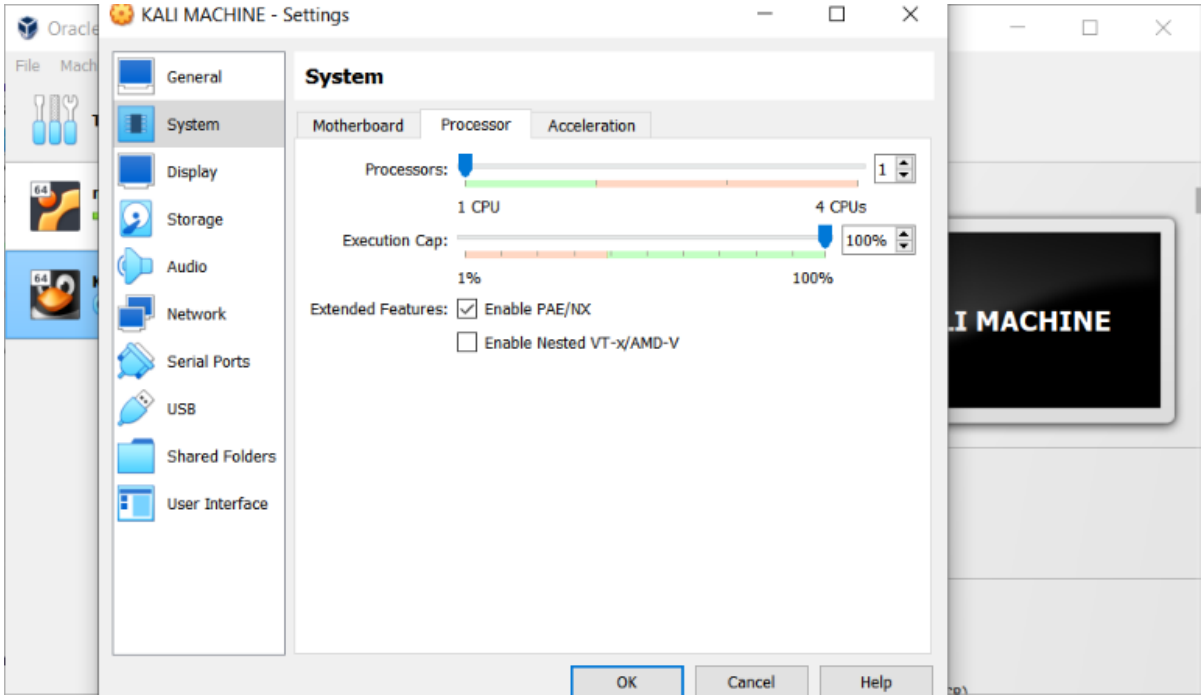



**Figure 9: System Processors and featurs**

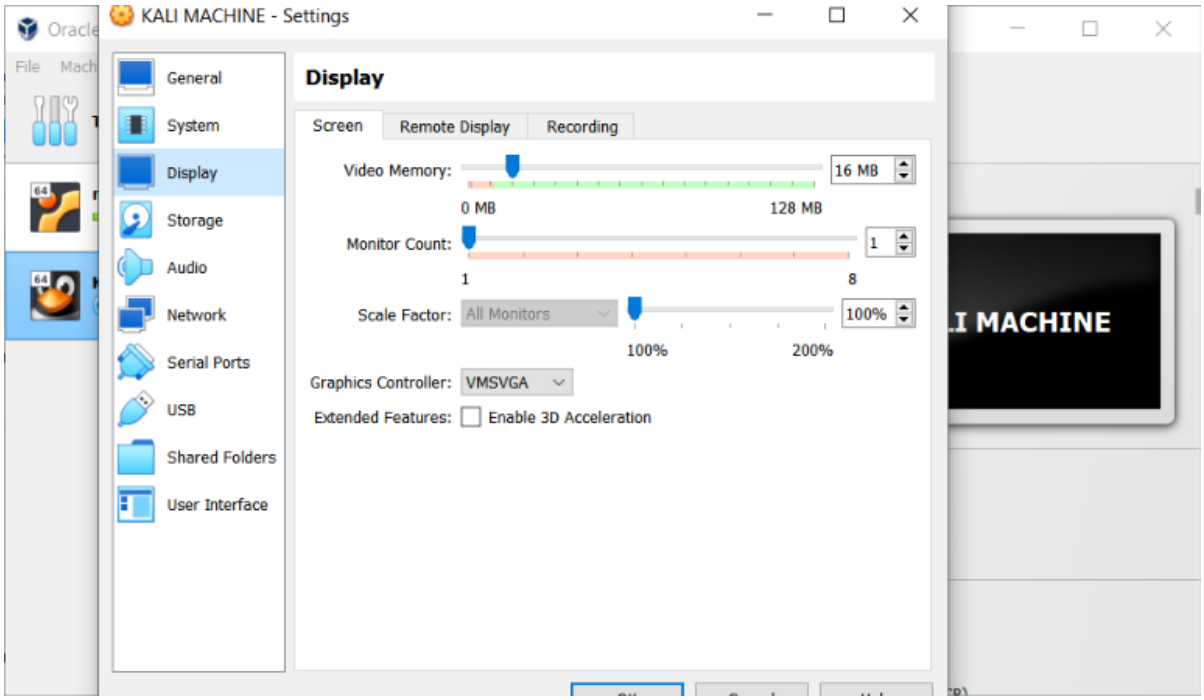



Figure 10: Display Configuration

The two virtual computers must be configured to be in the same virtual network to enable communication. To accomplish this, connect both virtual machines to a host-only network adapter.

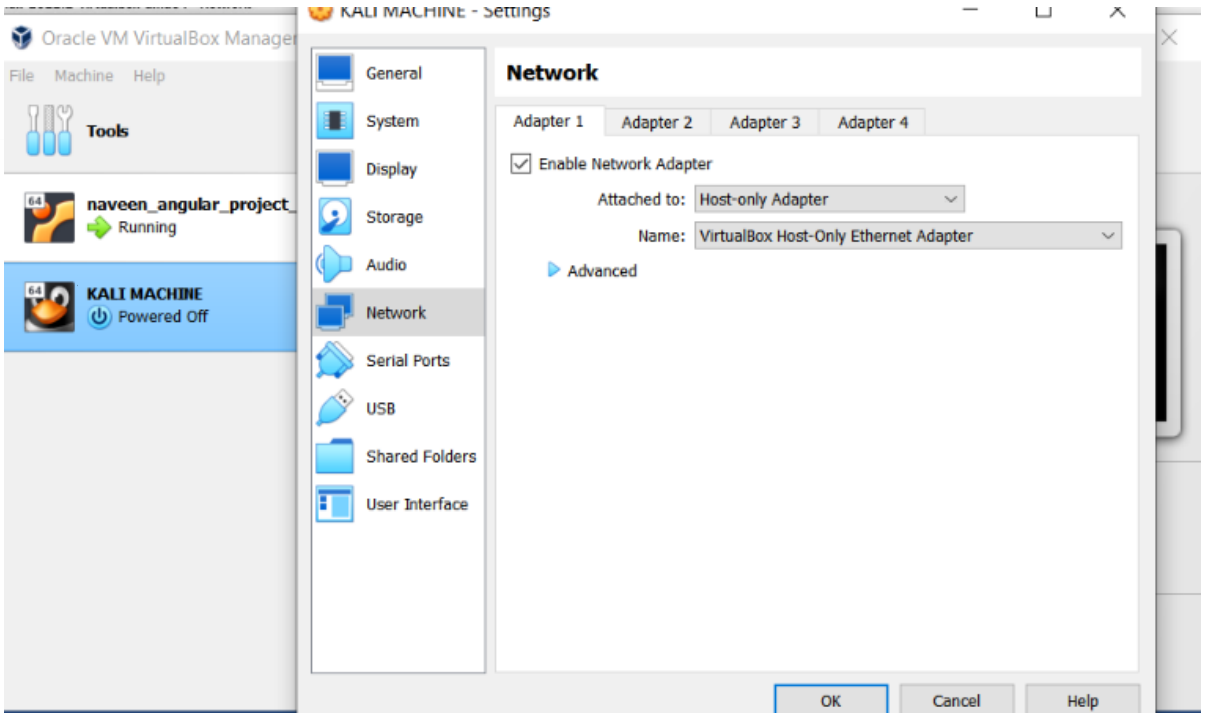



**Figure 11: Network Adaptor**

After pressing the start button, both virtual machines will start up, and we can test their connectivity by pinging them from each freshly constructed virtual machine.

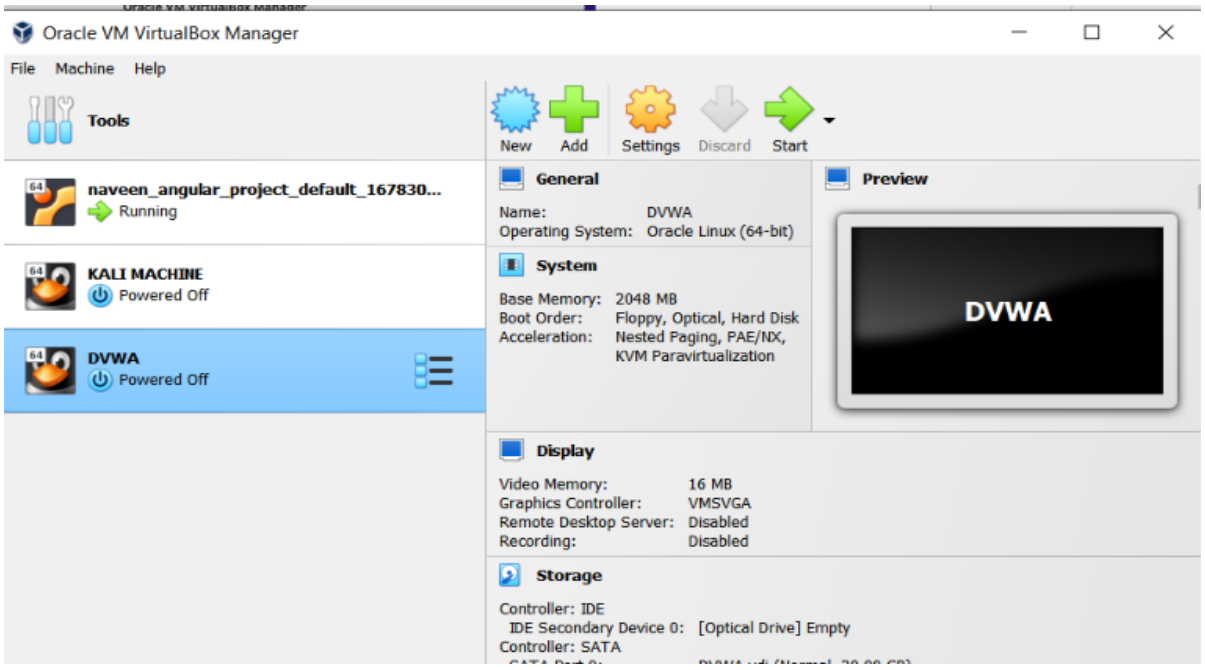



**Figure 12: Starting System**

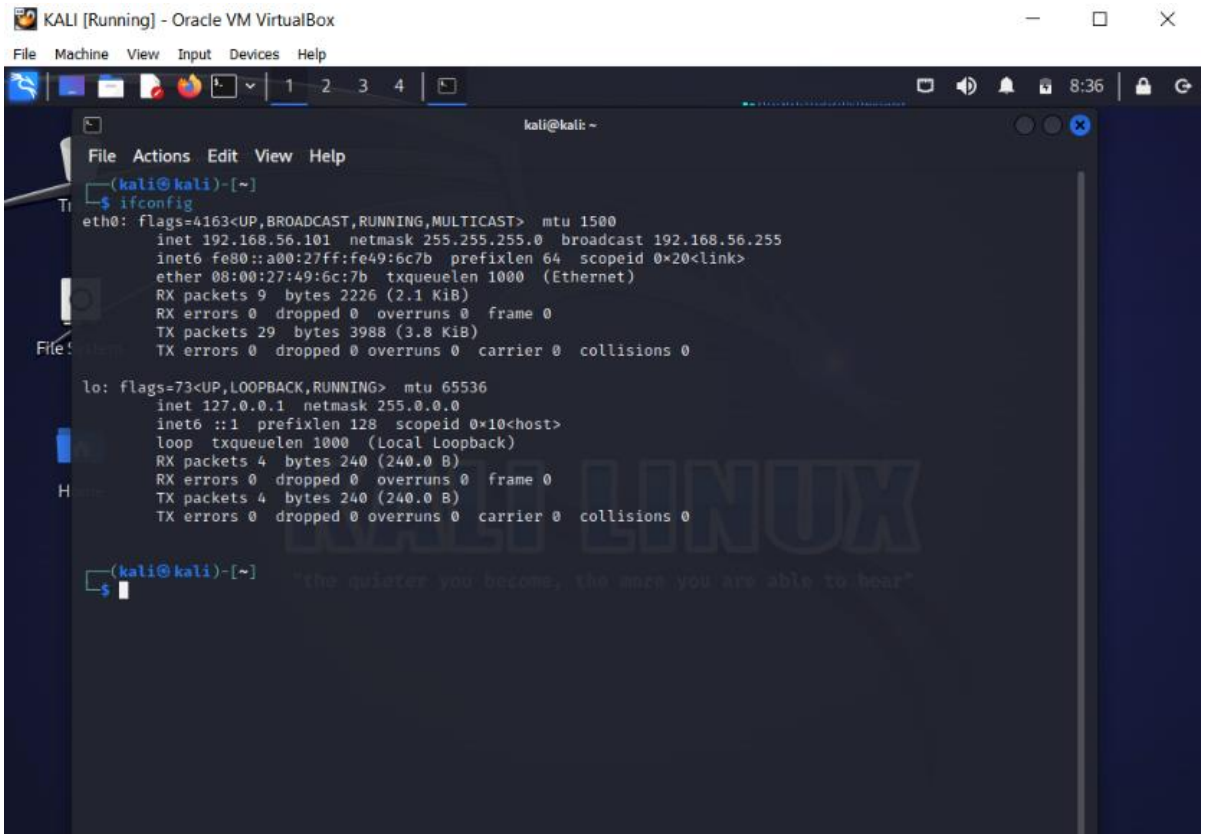



**Figure 13: Kali Linux System Testing**

We can obtain the IP address of the current virtual machine by using the "ifconfig" command, which we can then use to test it using ping.



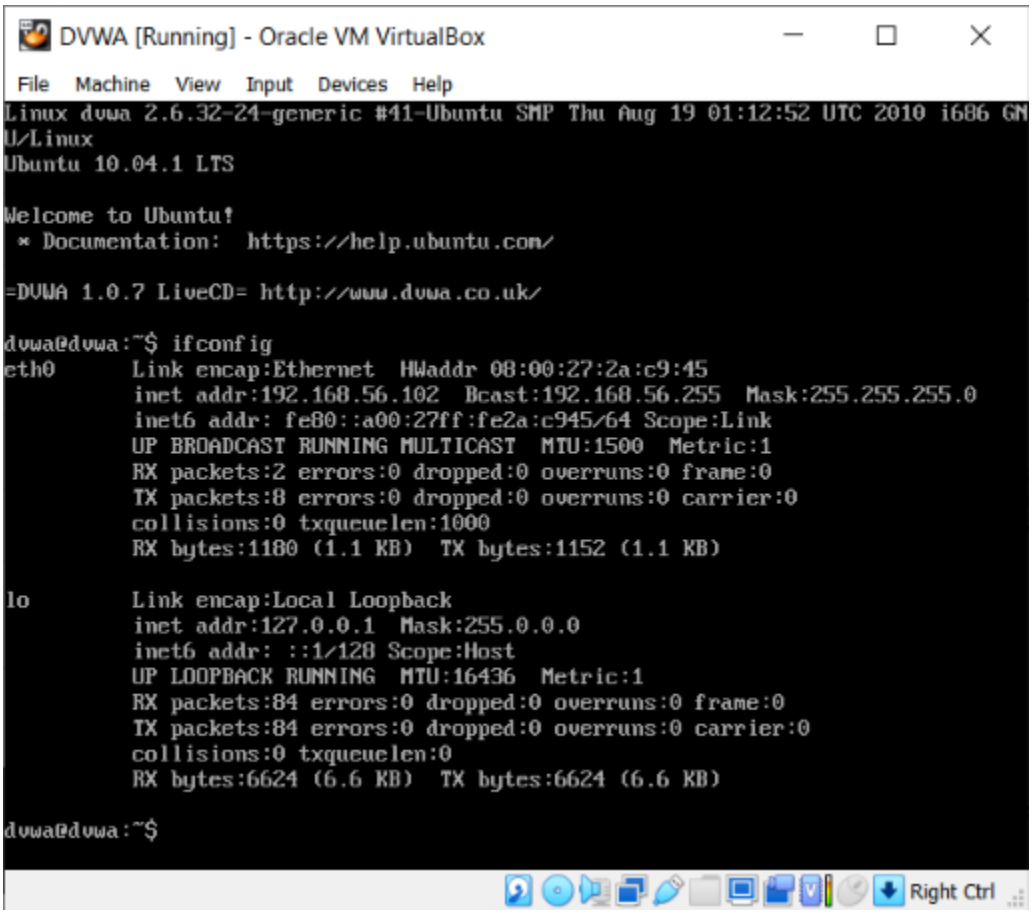



**Figure 14: Testing on DVWA**

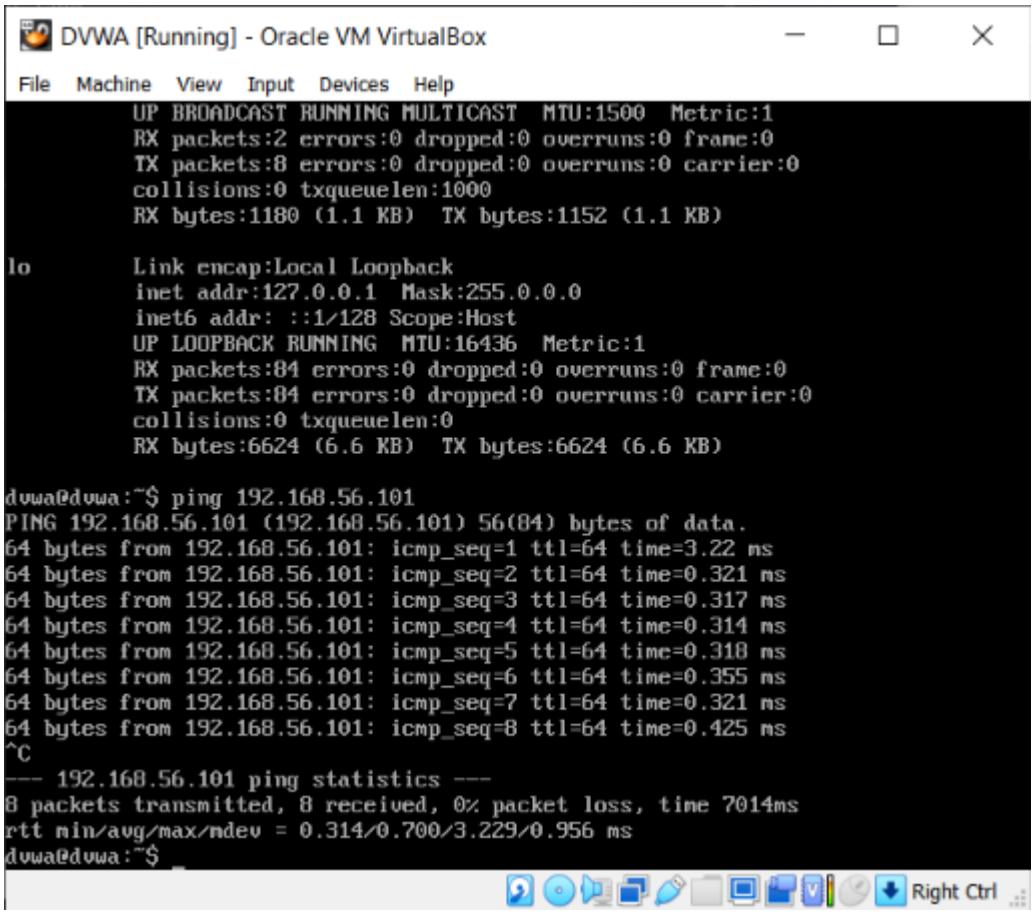



**Figure 15: Pinging Kali from DVWA**

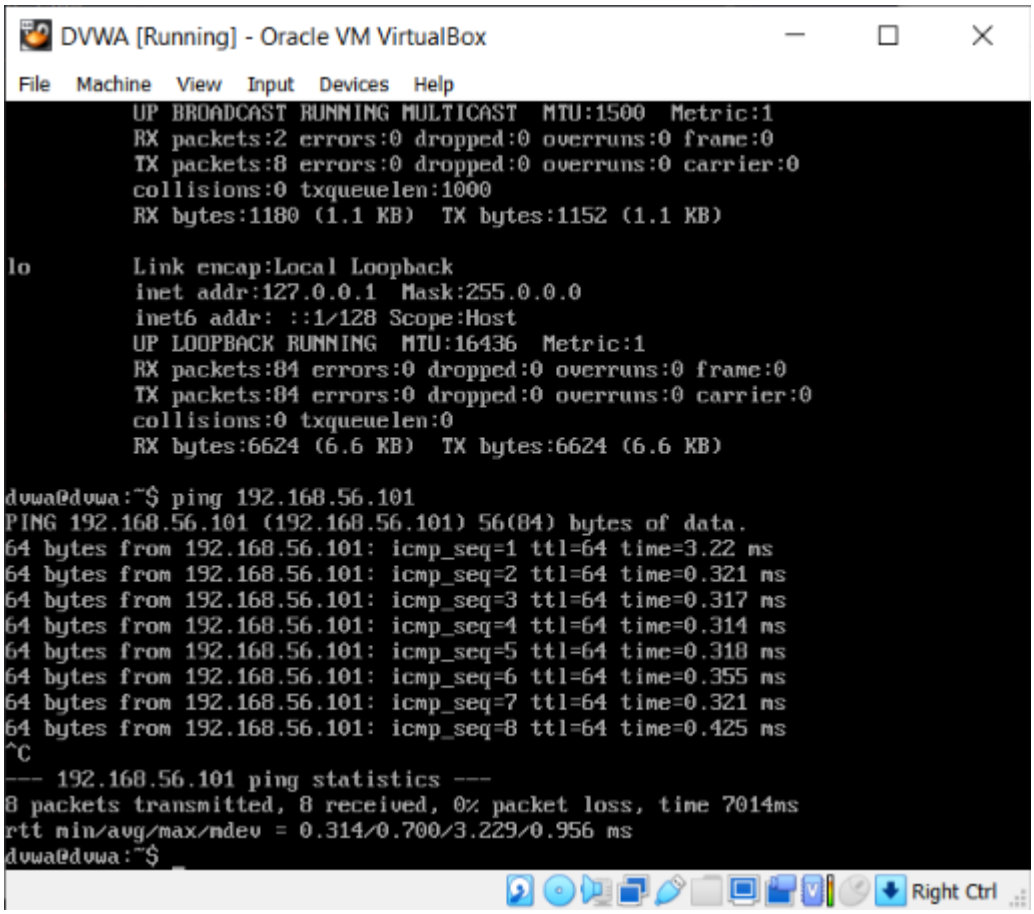



**Figure 16: Pinging DVWA from Kali**

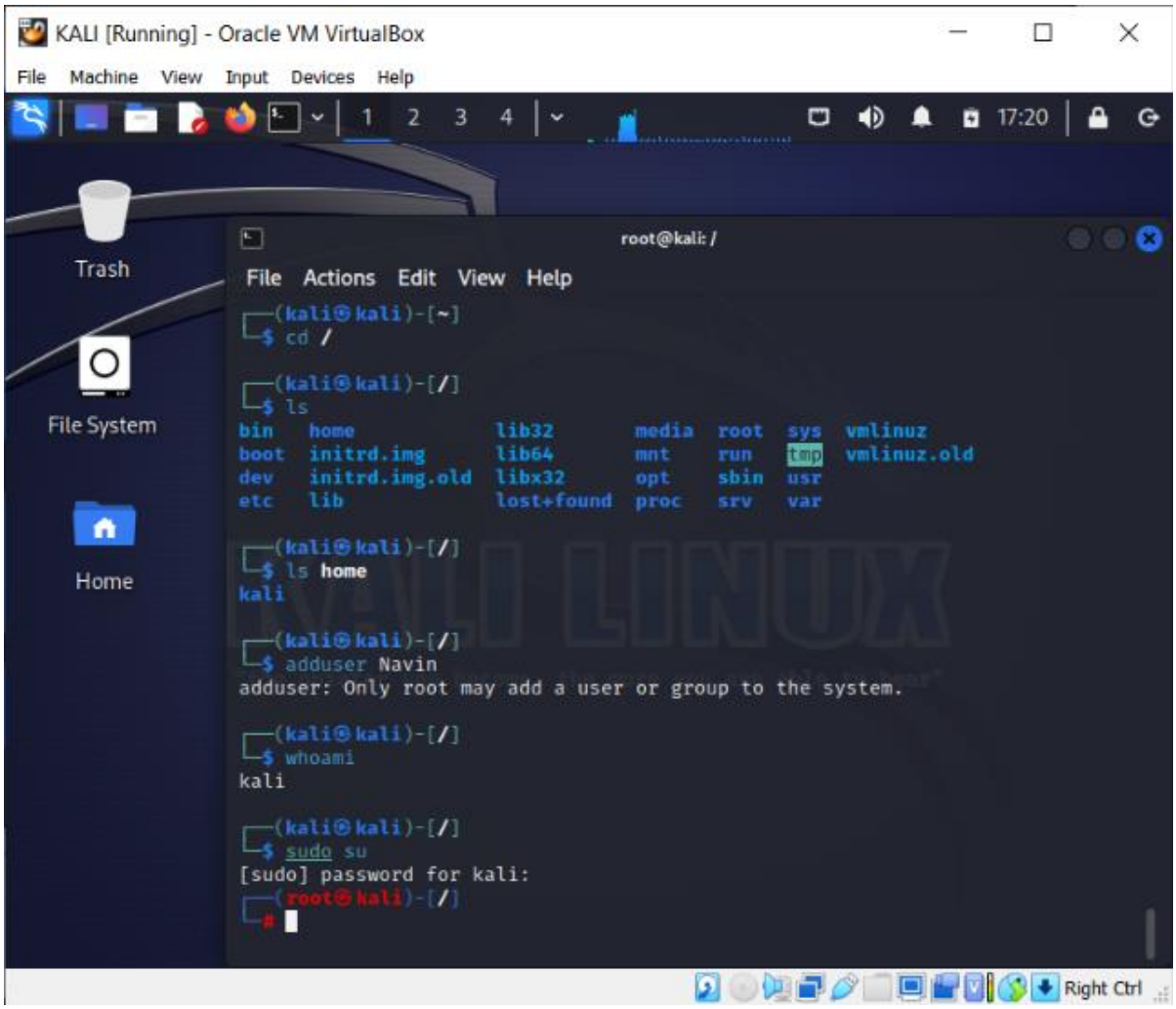



**Figure 17: Switching to Root in Kali to add a new username**



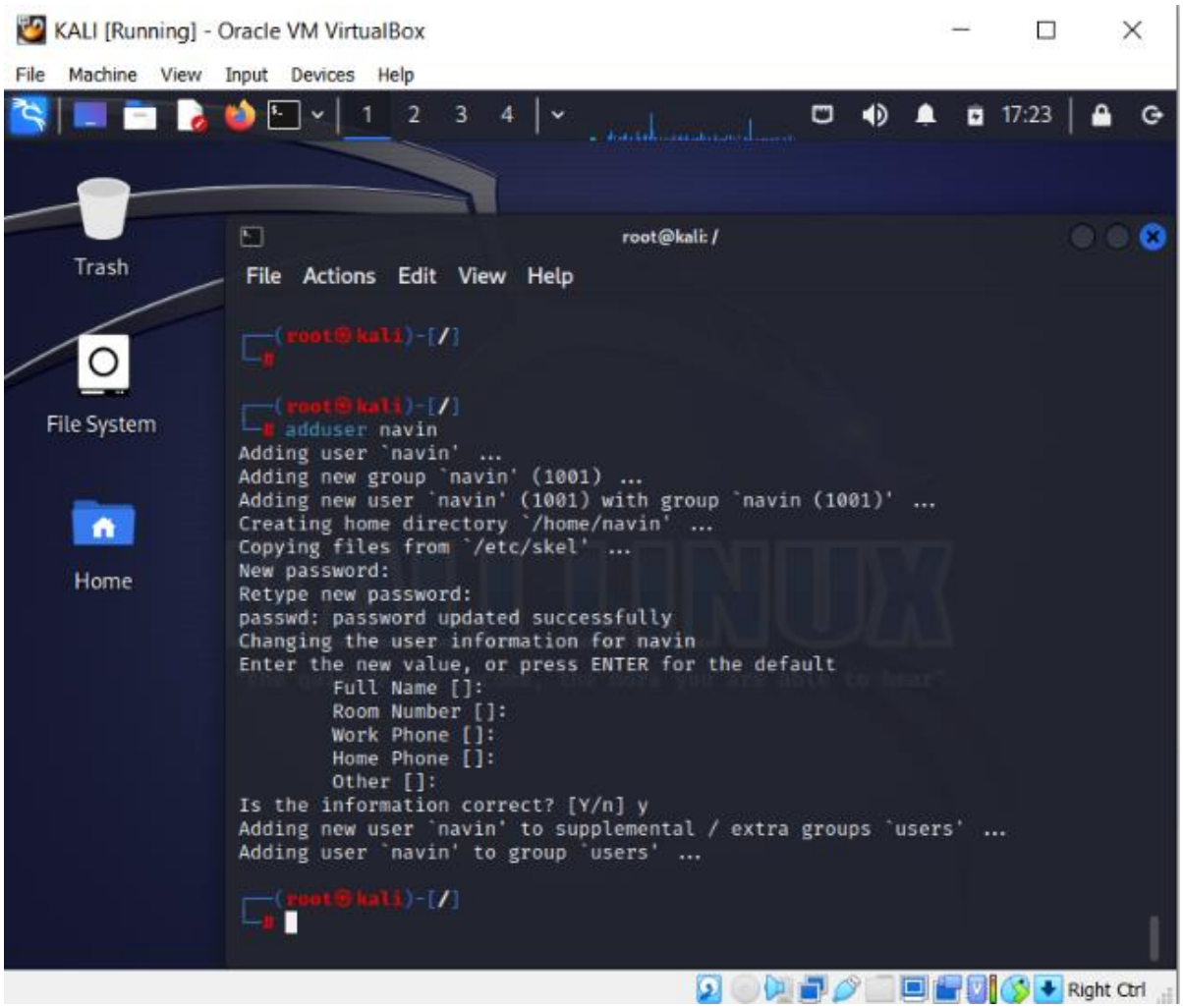



**Figure 18: Added username and new password**

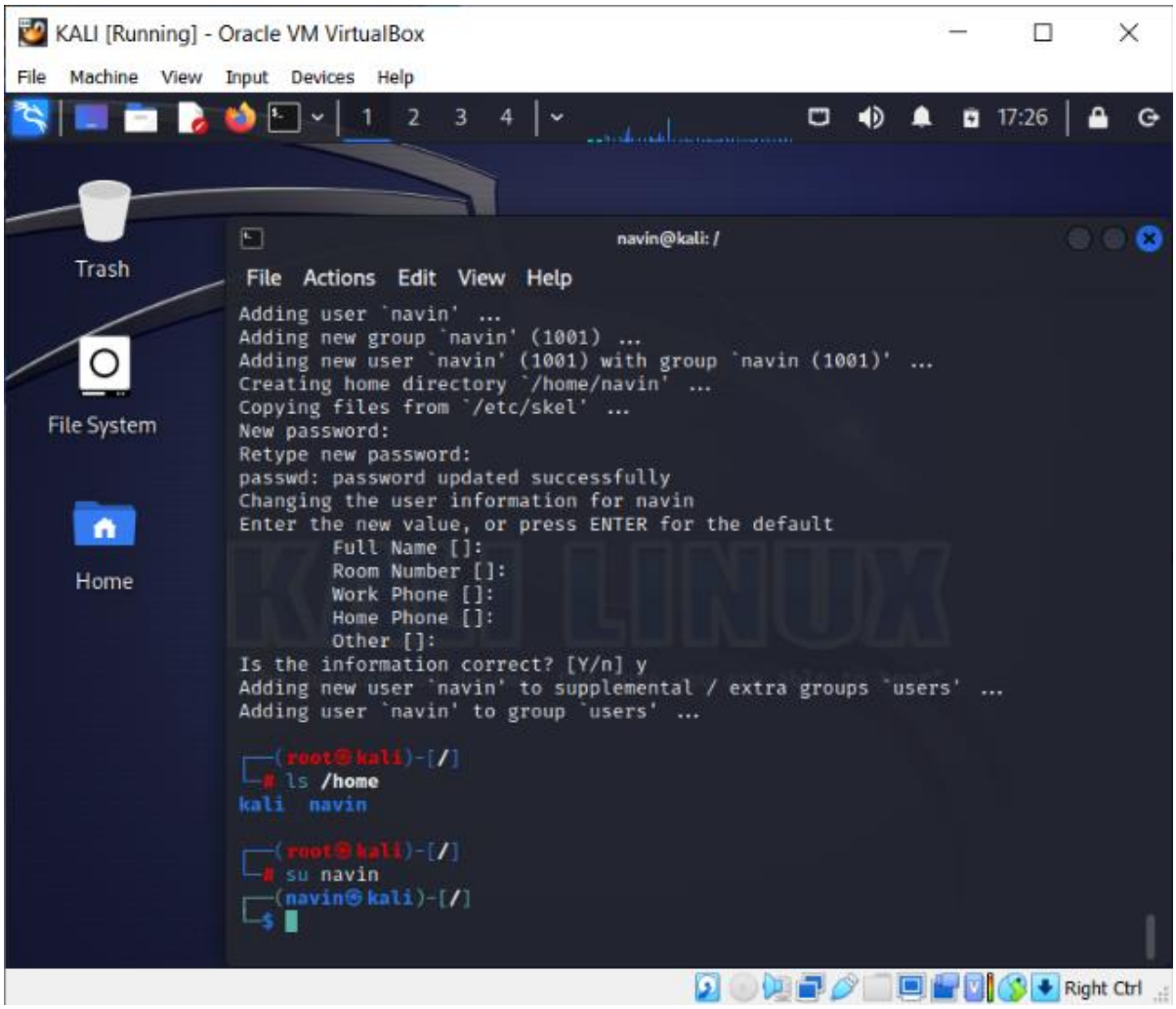



**Figure 19: Switched to the created user**


**Figure 20: Executed the "date", "hostname" and "whoami"**

## 4. DVWA VULNERABILITIES

The DVWA and main goal of this pen-testing playground is to assist security specialists in testing their knowledge and technologies.

If you want to work in security, you need to have expertise in finding bugs and vulnerabilities in web applications. By using your expertise, you can always advance professionally and at work. Before entering the professional field, newbies should test their understanding of the procedures and tactics for protecting web apps. You can determine where you stand and where you need to make the greatest progress by demonstrating how things are done.

## 5. BRUTE FORCE ATTACK

An automated procedure of testing every conceivable combination of characters or passwords until the proper one is identified is used in this sort of attack. It is a time-consuming technique based on the premise that the target's password is weak or easily guessable. This technique is known as brute force cracking. Brute force attacks are

simple and dependable. Attackers pass this task off to a machine, which may test a variety of username and password combinations before settling on one that works. Since attackers are harder to stop after they have internet connectivity, the best defense is to thwart a brute force attack as it is happening.

The two most prevalent uses of brute force assaults are to crack passwords and encryption keys (keep reading to learn more about encryption keys). Brute-force attacks commonly target SSH logins and API keys. Login pages of websites are often targeted by scripts or bots that attempt to carry out brute-force password attacks.

Brute force attacks have the advantage of being relatively easy to execute, and if given enough time and in the absence of any targeted security measures, they will eventually succeed. However, brute force attacks can be time-consuming as they must attempt every possible combination before succeeding.

Let's explore how to launch an attack on the system. Kali Linux comes equipped with various built-in tools for penetration testing and intrusion detection, including Burp Suite which can be used for application security testing.

Before we can start, we have to set the security settings on the Kali machine. There are several security settings that need to be lowered to proceed with the attack.

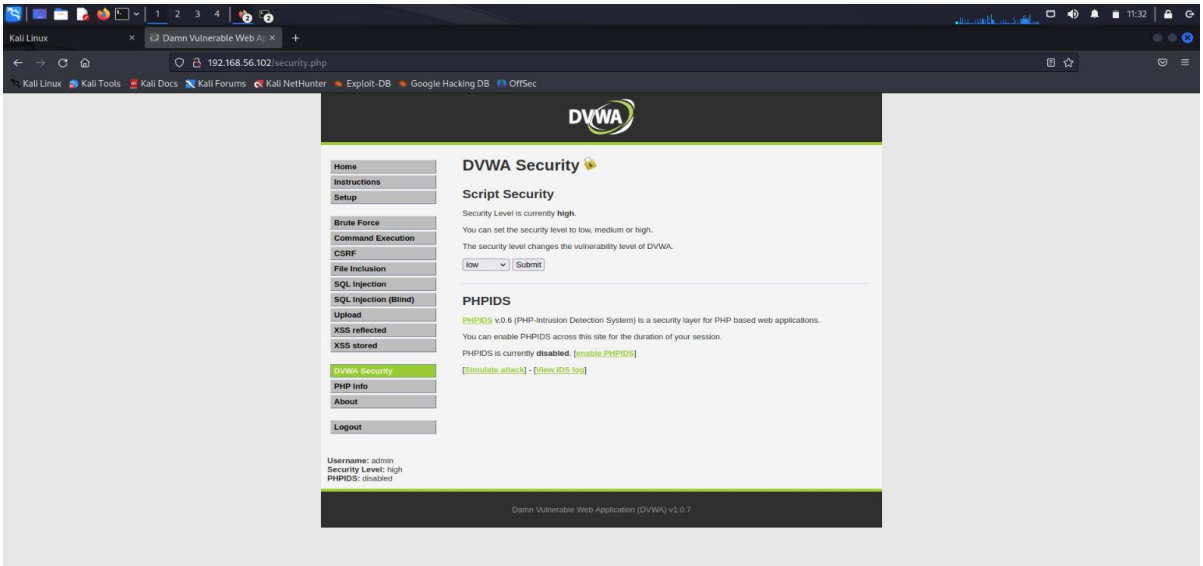



**Figure 21: DVWA Security Settings**

Burp is designed to work in tandem with your browser. Burp, which acts as an HTTP proxy server, processes all HTTP/S communication from your browser. To ensure that Burp's proxy listener is active, go to the Proxy tab and enable Intercept.

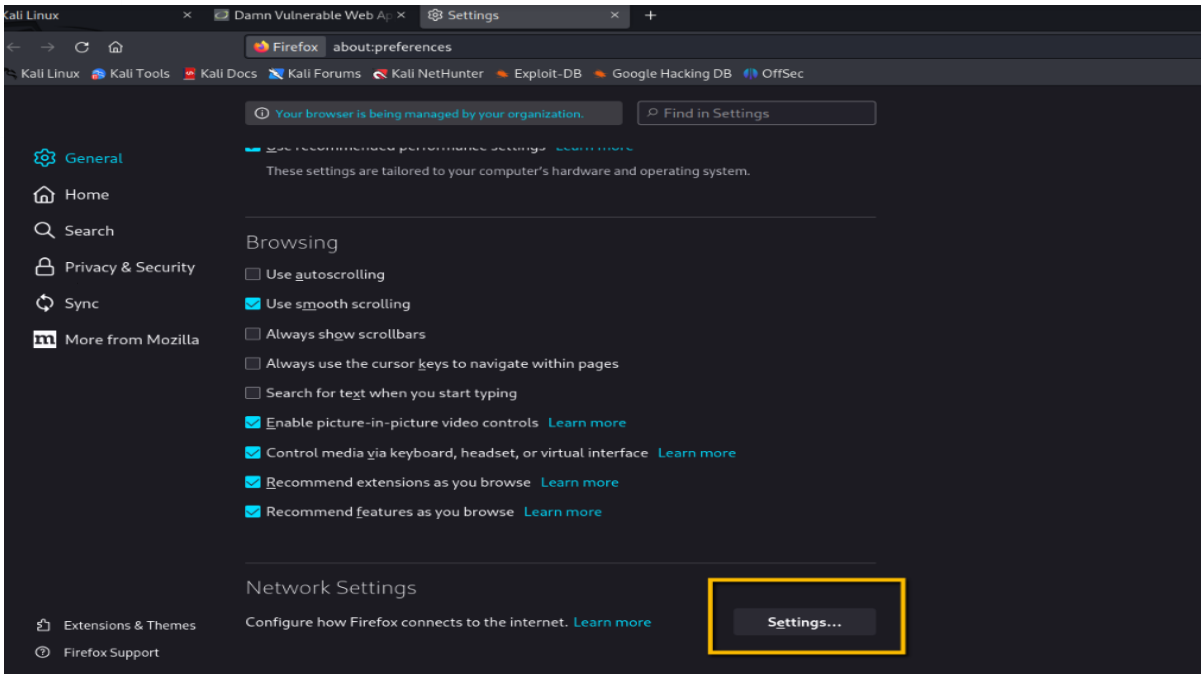



**Figure 22: Setting Browser Proxy Setting**

To use Burp Proxy as the HTTP proxy server for your browser, you need to configure your browser's proxy settings. Set the proxy host address to 127.0.0.1 and the port to 8080 for both HTTP and HTTPS. If you are using Firefox, Kali's default browser, launch it and go to Preferences. Click on Advanced, then on Network, and finally on Settings, as shown in the illustration below.



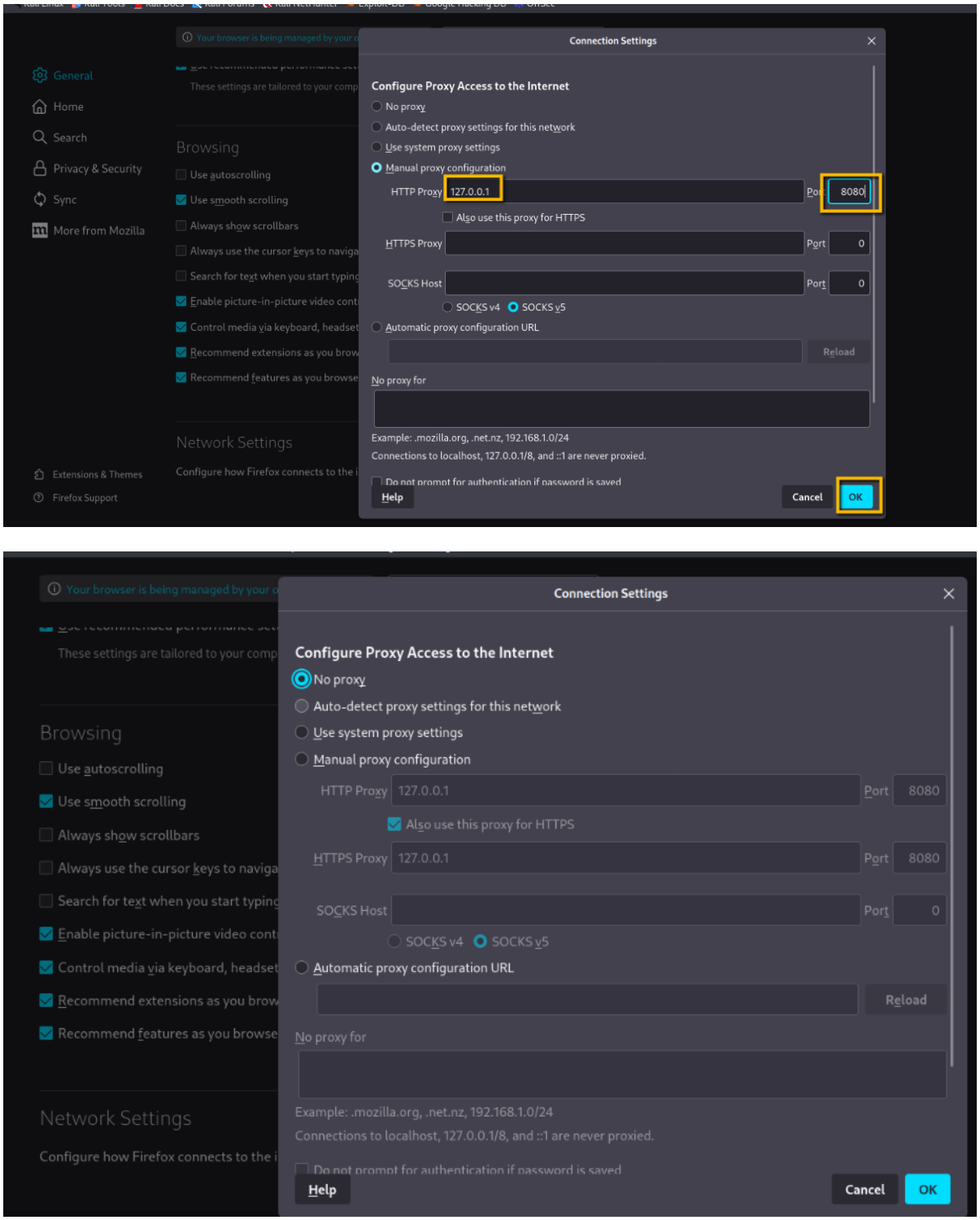



**Figure 23: Browser Proxy Settings**

Assuming that the configuration is correct, Burp should now be able to handle all HTTP/S traffic. When a website is visited, theBurp will hold the request until a decision is made on how to proceed with it. The intercept feature is currently disabled, so it should only be enabled when necessary.

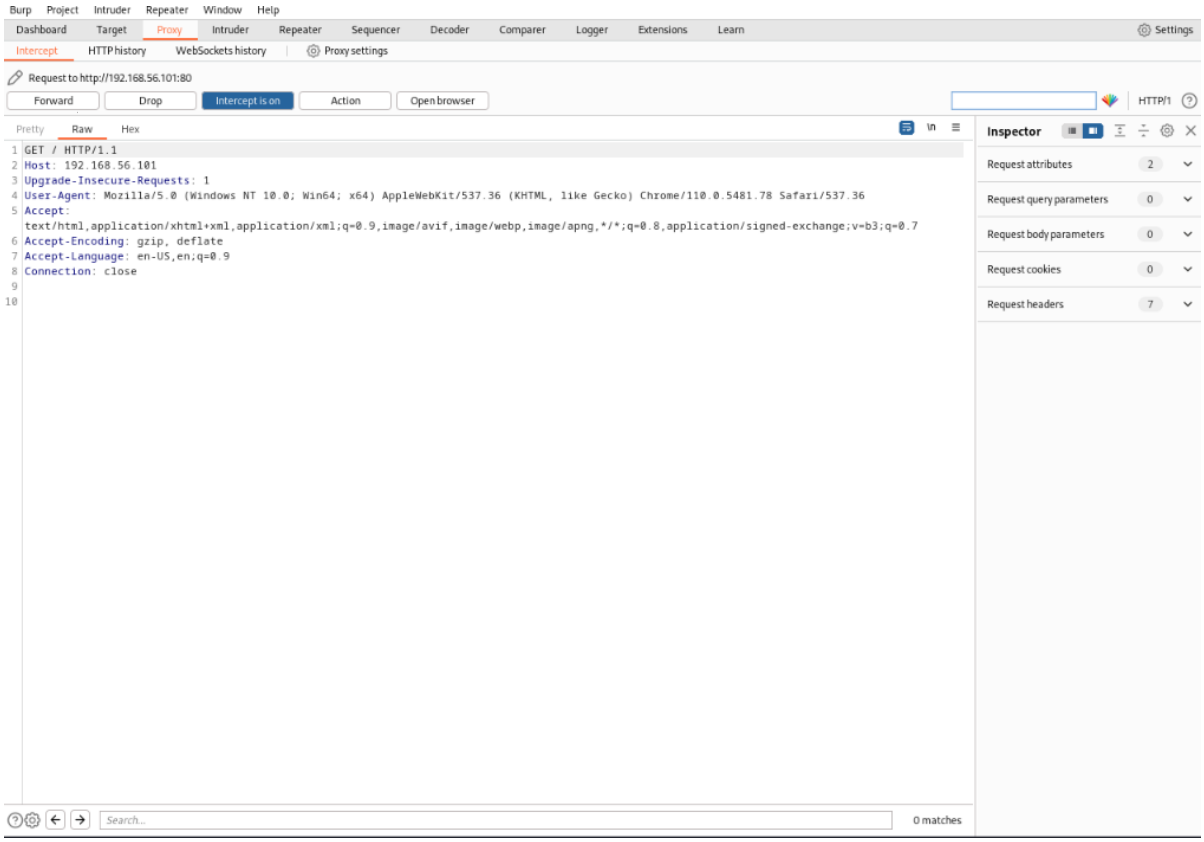



**Figure 24: Proxy Tab**

During a penetration test of a client's website, it's important to keep in mind that gaining access to the admin account through a brute force attack would provide complete control over the website. To initiate a brute force attack on the login page, first open Burp and

ensure that the intercept feature is enabled.

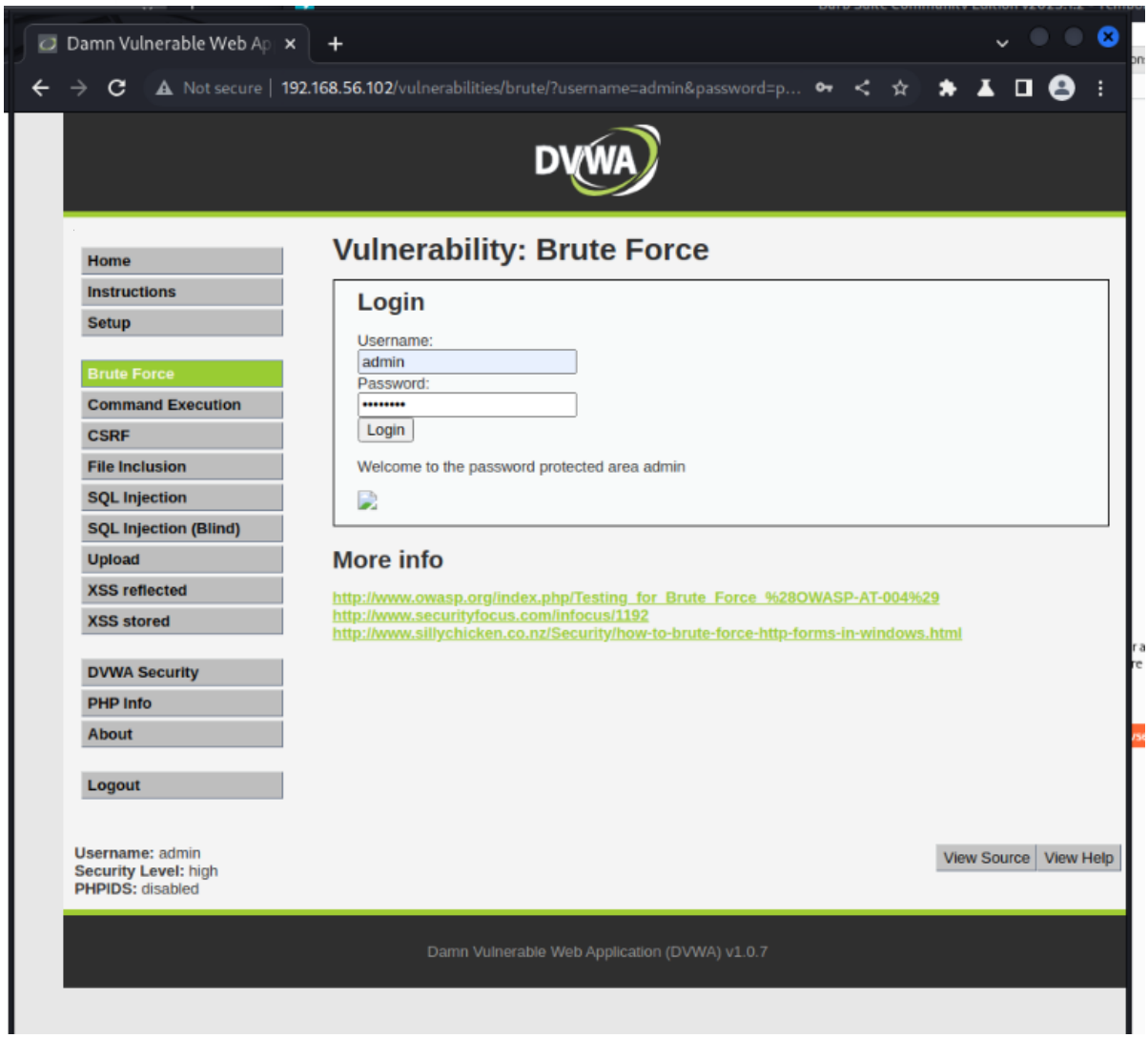



**Figure 25: Brute - Log In**

After a successful login, the program displays "*Welcome to the password-protected area admin.*" Because it was included in the HTTP response sent as a consequence of successfully signing in, this phrase may be used to filter out successful login attempts. The screenshot of the BurpSuite login request is displayed below.

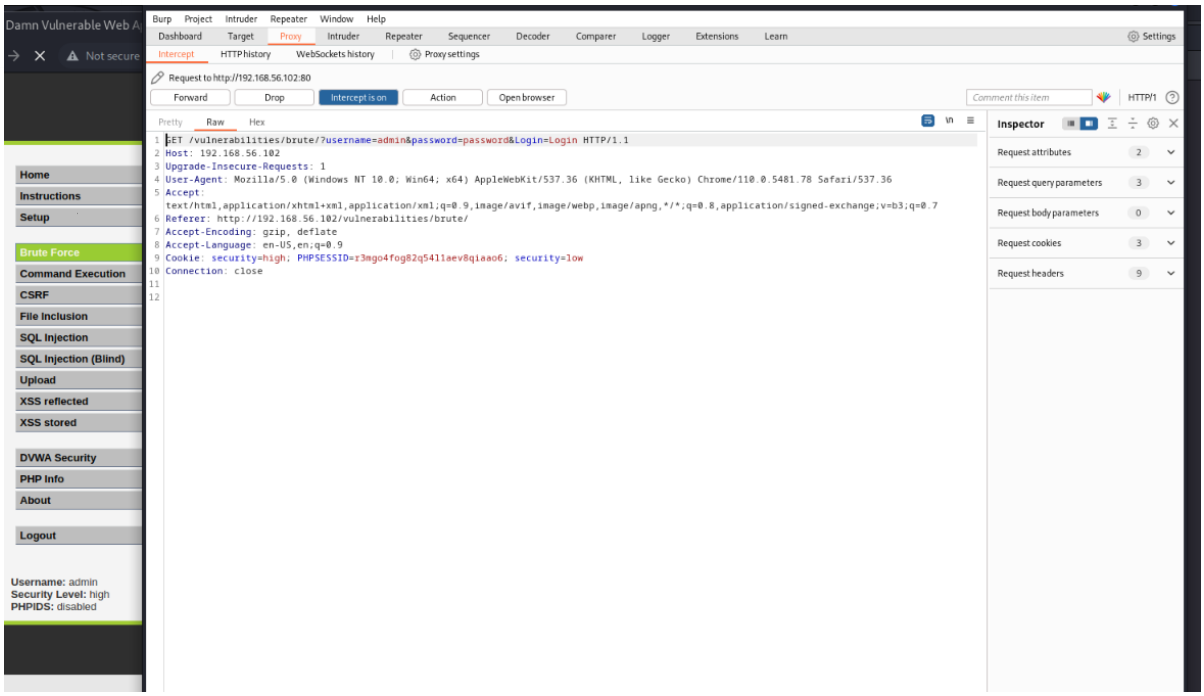



**Figure 26: Log-in Req Interception**

After the intruder tab receive the request and we can use it to develop the brute attack.

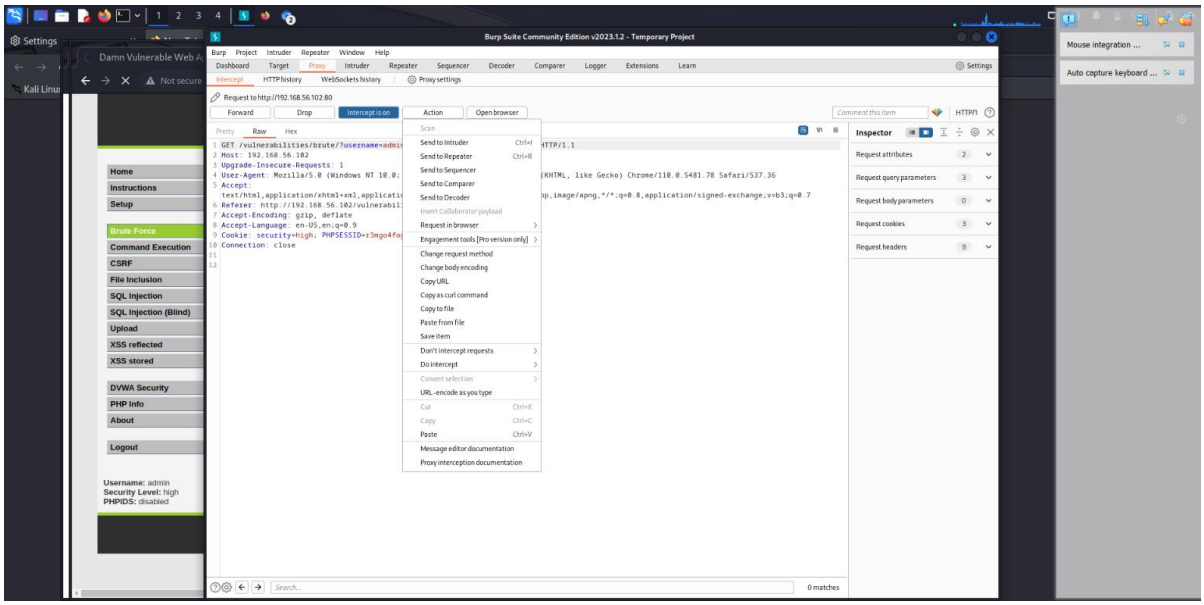



**Figure 27: Action for Interception**

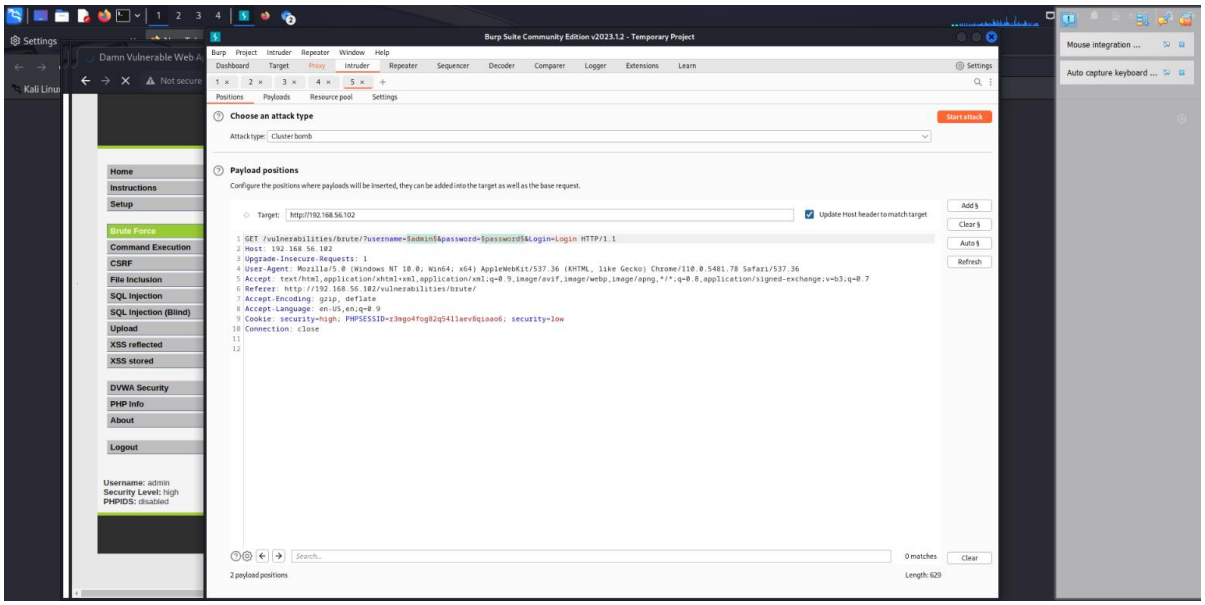



**Figure 28: Positions - Attack Target**

Since brute force attacks rely on trial-and-error methods, such as request interception, we need to modify the request variables for each attempt. To define the parameters for adding our attempted parameters (known as a payload) under the Positions tab, we can include the "username" argument from the URL noted above.

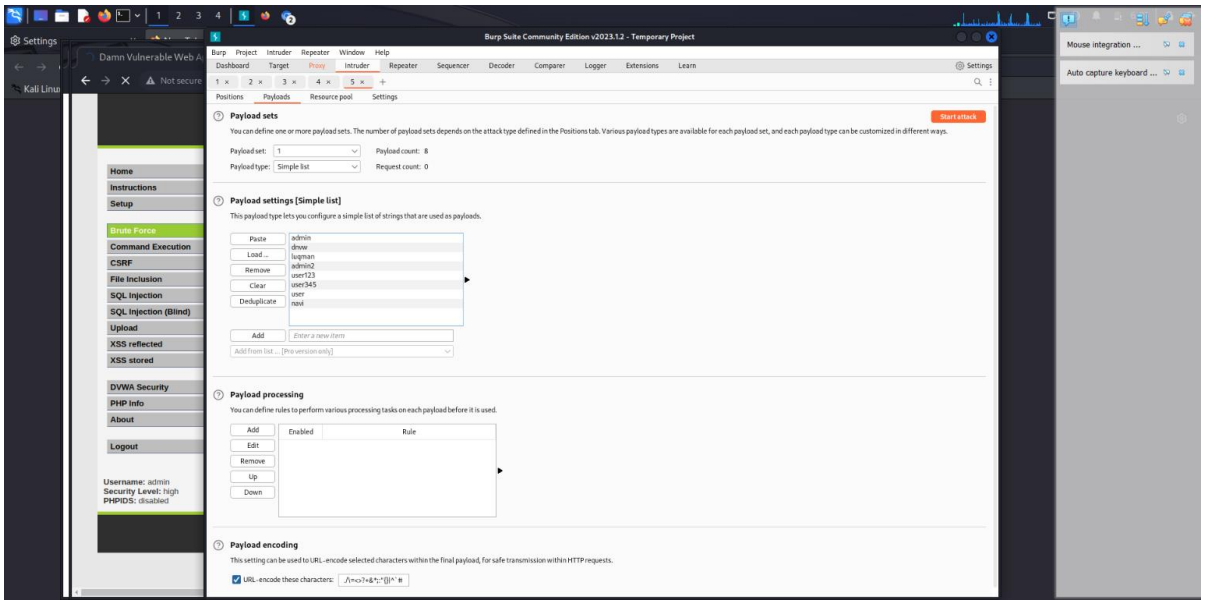



**Figure 29: Payload Simple List 1 Username**

Since brute force attacks rely on trial-and-error methods, such as request interception, we need to modify the request variables for each attempt. Under the Payload tab, we can define

the parameters for the simple list 2 and can be used the "password" by adding the list of the arugument or text.

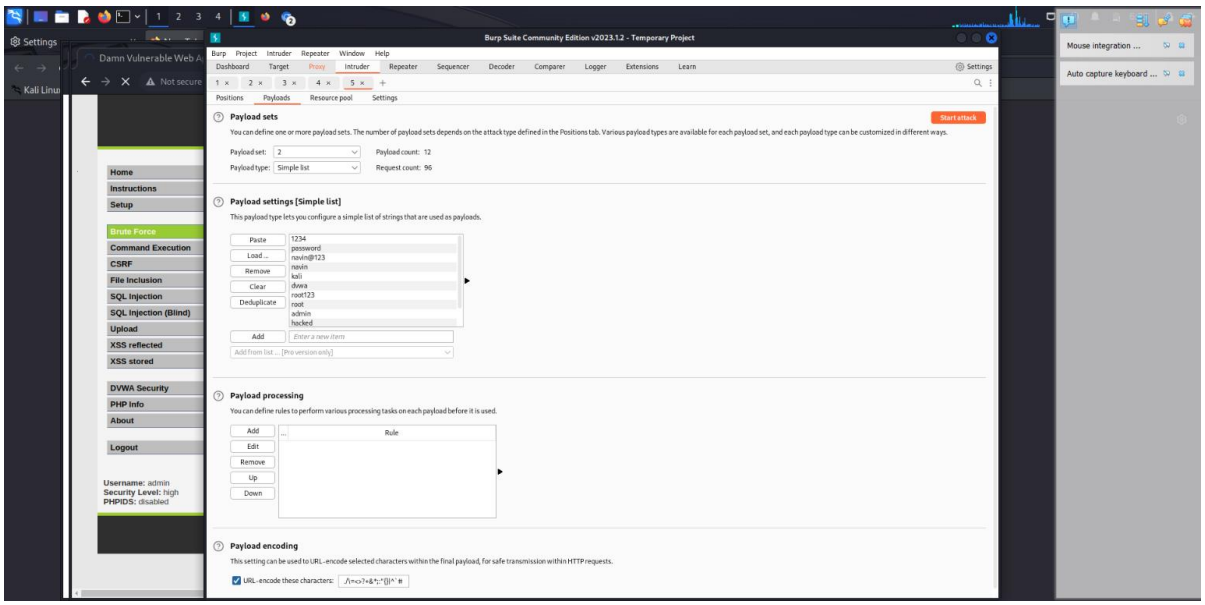



**Figure 30: Payload Simple List 2**

We'll use the “password” argument from the URL noted above.

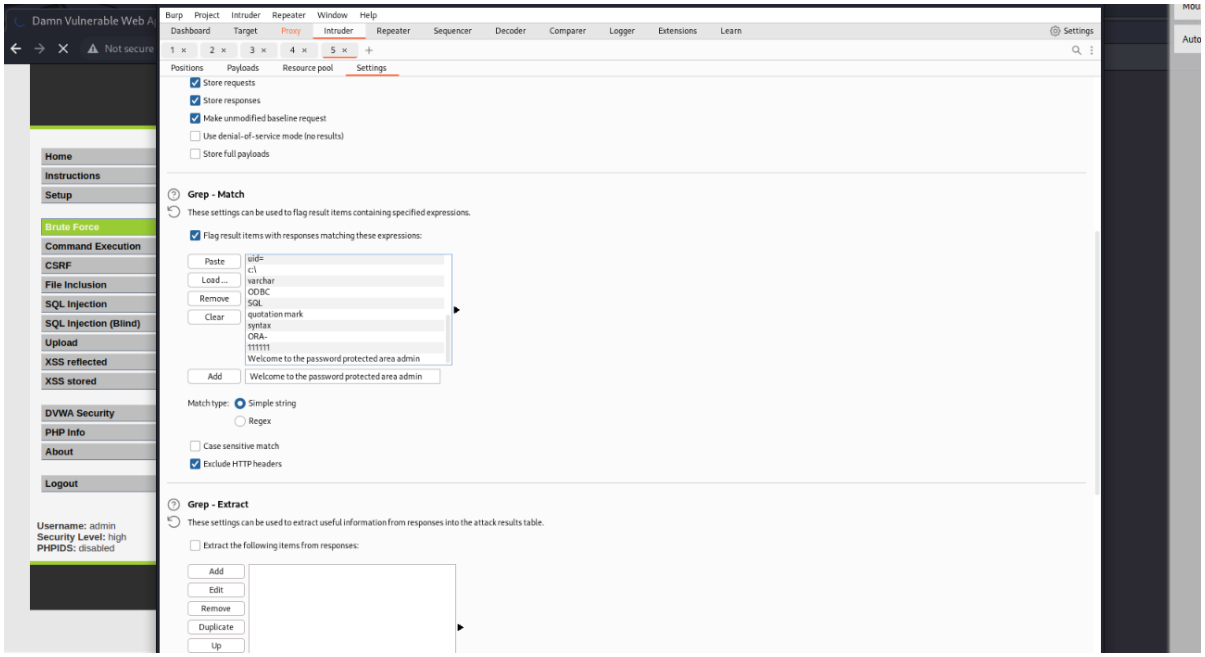



**Figure 31: Grep Match setting**

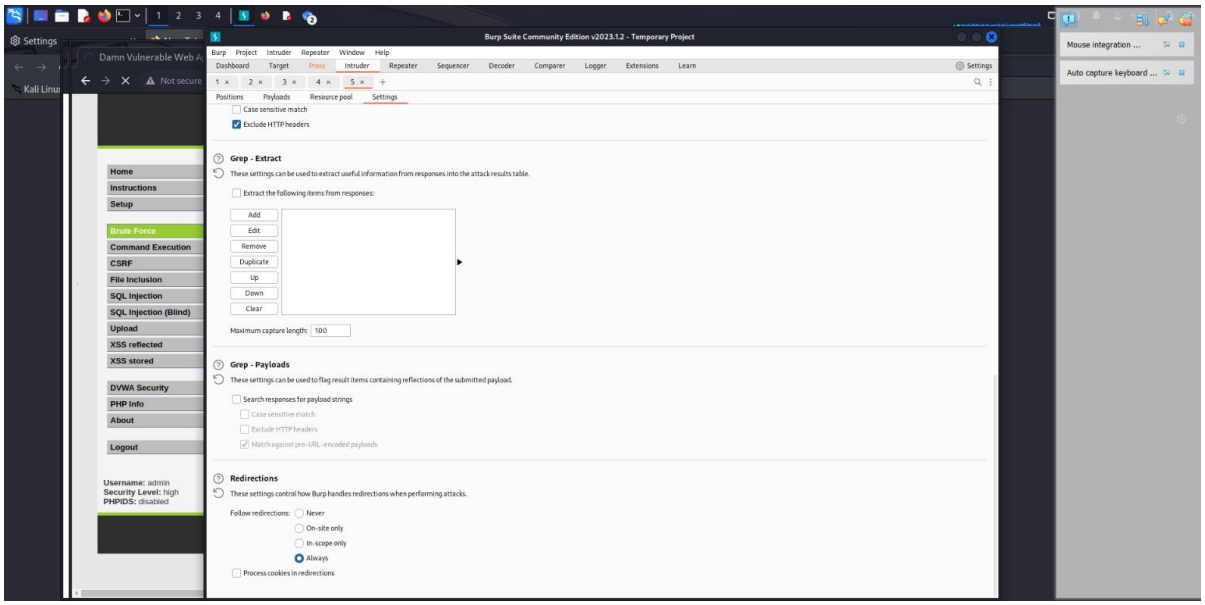



**Figure 32: Change in the redirection settings**

Any successful brute force attack can be understood by the complex decryption of user information.Options tab to discard successful brute force attempts.

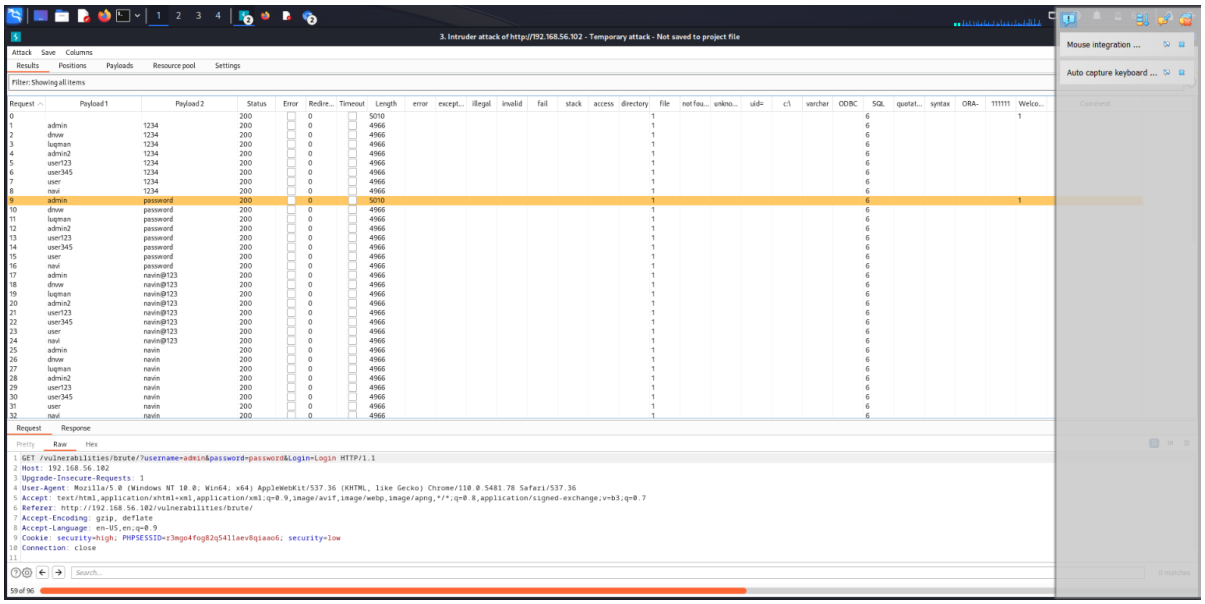



**Figure 33: Brute Force - Successful Attack**

Under the "Raw" tab, you can view the "HTTP GET" request submitted to the Systemconf server.

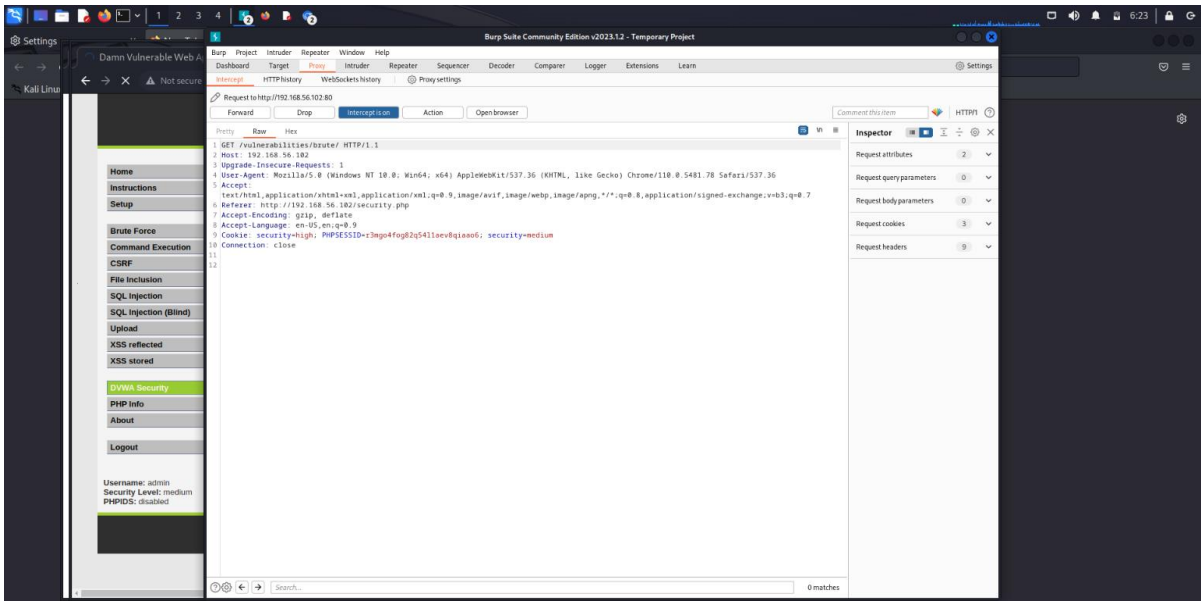



**Figure 34: Medium Settings – RAW data**

Under the "Proxy -> HTTP history" area, we can see our request history from Burp's inception.

Furthermore, we may show information such as the request's address, type (POST, GET, and so on), request status code (HTTP request status code), request duration, and so on.

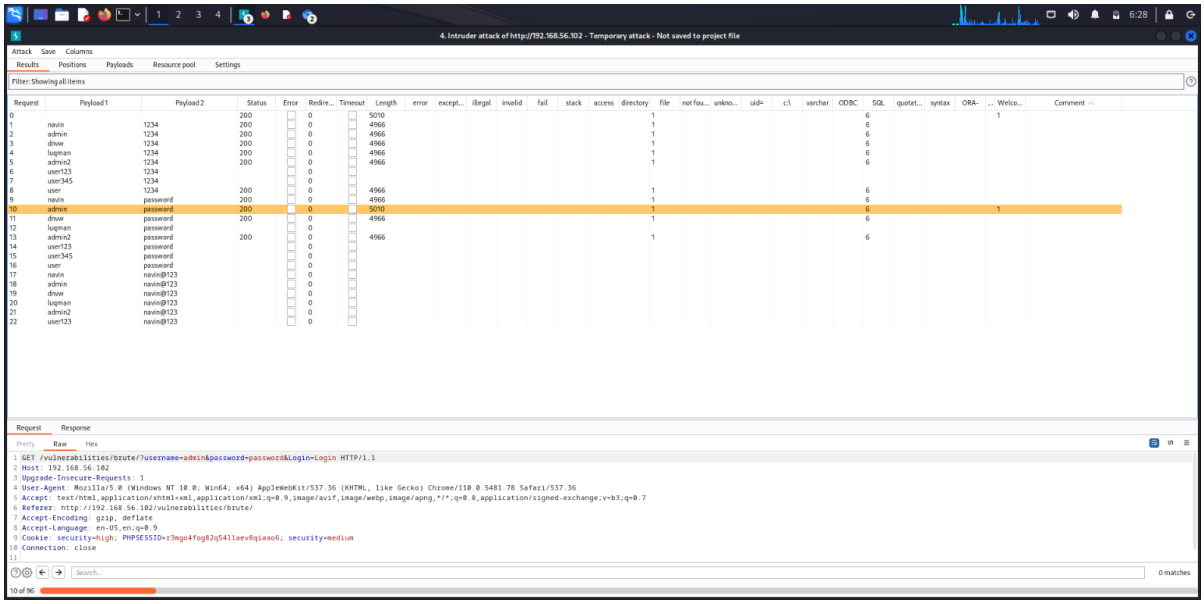



**Figure 35: Medium Settings - Successful Attack**

When it was sent, the request was removed from the "Intercept" section. If we want to try many identities and passwords, we may use Burp's "Repeater" module. This module allows you to regularly send changes to the Request.

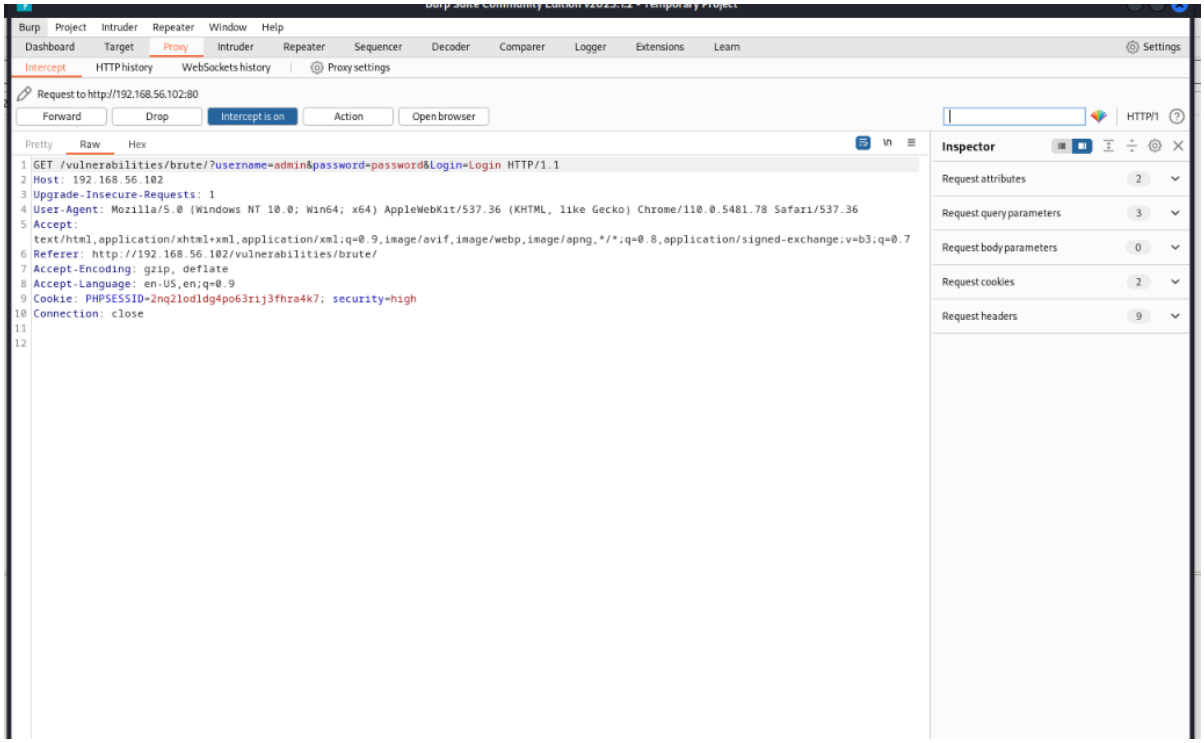



**Figure 36: High Settings –Interception**

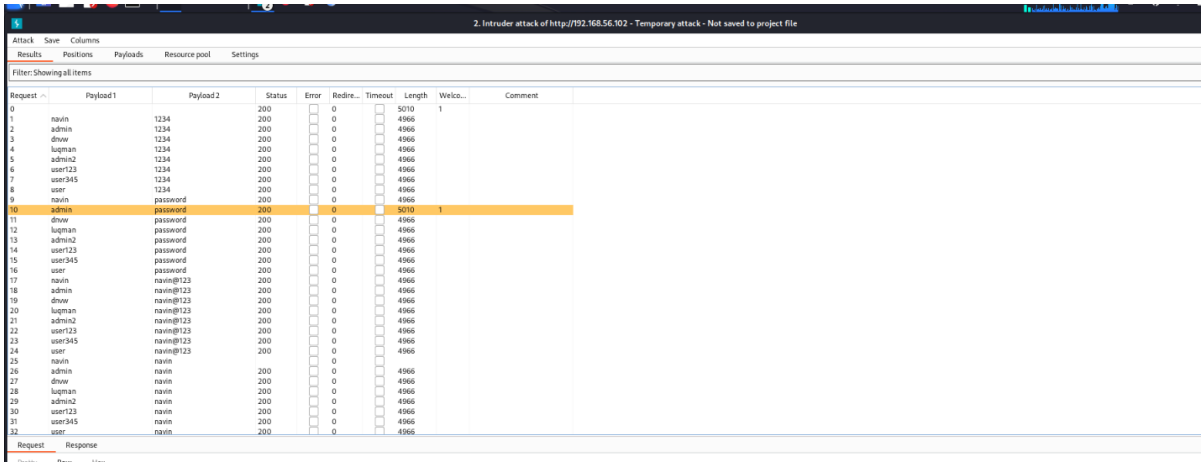



**Figure 37: High Settings - Successful**

On execution of a successful brute force attack on the vulnerable system. We can be able to see the matching password is highlighted.

## 5. 1 BRUTE FORCE ATTACK PREVENTION TECHNIQUES

### Strong Password:

A strong password policy is the most effective and simple way to prevent a brute-force attack. 30% of repeated or changed passwords can be decoded in ten attempts. Make use of long passwords with special characters and spaces. Upper and lowercase characters, numerals, and symbols should all be included in your passwords.

### Monitor IP address:

Restricting login attempts from users with a specified IP address or range is important for security, especially in blended work environments or for remote employees. It is recommended to set up notifications for any login attempts from unknown IP addresses and take measures to prevent them.

### 2 Factor Authorization:

When 2FA is enabled, you will be required to confirm that you are the one attempting to access your account. To confirm your identity, a secret code will be sent to your phone, and you must enter it before you can access your account.

### Use of CAPTCHA

CAPTCHAs are used as a security measure to ensure that a real human is interacting with a website or application, rather than an automated script or bot. The tasks are designed to be simple for humans to complete, but difficult for machines to solve, such as identifying distorted text, selecting specific images, or solving simple math problems. By requiring users to complete a CAPTCHA, websites can reduce the amount of spam, bots, and automated attacks.

### Web Application Firewalls

Web Application Firewalls (WAFs) are a type of security solution that can be used to protect web applications from various attacks, including brute force attacks. WAFs can be configured to monitor incoming traffic and identify patterns of behavior that are



indicative of an attack. When such behavior is detected, the WAF can take action to block the offending traffic, such as by dropping packets or blocking the offending IP address.

In the case of brute force attacks, WAFs can be configured to detect and block repeated login attempts with incorrect credentials. This can be done by setting thresholds for the number of failed login attempts from a single IP address within a given time period. If the threshold is exceeded, the WAF can block further login attempts from that IP address.

WAFs can also be configured to detect and block brute force attacks that attempt to exploit vulnerabilities in web applications, such as SQL injection or cross-site scripting (XSS) attacks

## 6. SOCIAL ENGINEERING ATTACKS

The social engineering technique exploits human mistakes to get commodities, private information, or access.

These social engineering tactics, also known as "human hacking," are used to trick unsuspecting individuals' insensitive information, spread malware infections, or grant access to restricted systems. Such attacks can occur both in-person and online or through other means.




**Figure 38: Social Engineering Attacks**

Social engineers use a variety of online and offline strategies to deceive unsuspecting persons into compromising their security, paying money, or giving sensitive information.

Furthermore, hackers seek to exploit a user's ignorance.

Many may not realize the importance of information, such as their phone number, and may be uncertain about how to protect themselves and their data. Large-scale engineering attacks, on the other hand, depend on direct communication with their targets. Instead of using brute force methods to gain access to data, the attacker often convinces the user to divulge the information.

These attackers use a reliable method to deceive victims, known as the social engineering attack cycle, which typically involves the following steps:

1. To become more knowledgeable, you can educate yourself by learning more about yourself or the larger community to which you belong.

2. Establish trust and build rapport by initiating a dialogue and fostering a relationship..

3. After establishing trust and identifying a vulnerability, the attacker may enlist the victim to further the attack

4. Once the intended activity has been accomplished, it is crucial to disengage from the user.

The Social Engineering Toolkit, created by programmer Dave 23 Kennedy, is a free and open-source program designed for conducting social engineering attacks.

Uses of Social engineering toolkit:

1. Web Attack:

A web attack is a sort of cyber assault that targets a website or online application with the goal of gaining unauthorized access or stealing sensitive information by exploiting weaknesses in the software or infrastructure. SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and other types of web assaults are examples.

Social engineering attacks, on the other hand, relate to a collection of strategies used by cybercriminals to deceive people into disclosing sensitive information or doing actions that might lead to a security breach. Social engineering attacks can be launched by email, phone calls, text messaging, or social media, and they typically prey on human emotions, trust, or a lack of knowledge.

2. Attack Mass Mailers

Cybercriminals frequently utilize mass mailers to undertake social engineering attacks. These assaults are intended to deceive users into disclosing sensitive information or taking actions that benefit the attacker.

The phishing assault is one sort of mass mailer social engineering attack. The attacker conducts a phishing assault by sending out a huge number of emails that appear to be from a genuine source, such as a bank or a famous social networking site. The email usually contains a link that takes the receiver to a bogus website that appears to be the genuine thing. The website will then request sensitive information from the receiver, such as login credentials or credit card data, which the attacker can exploit to steal money.

3. Phishing Attacks

The Social Engineering Toolkit (SET) enables the creation of phishing pages for popular websites like Google, Facebook, and Instagram. When the target clicks on the link generated by SET, they are redirected to a genuine webpage of the legitimate website, but



with a phishing page overlay. This phishing link can then be sent to the victim via email or other means.

4. Create a Payload and Listener

   It is worth noting that while social engineering can be an effective method for penetration testing, it is only one approach and should not be relied upon exclusively. Additionally, if the target lacks open ports or other information that can be used for penetration testing, alternative methods must be employed to locate it.

   This is possible using Kali Linux. To begin, open Kali Linux's Terminal and type "setoolkit."

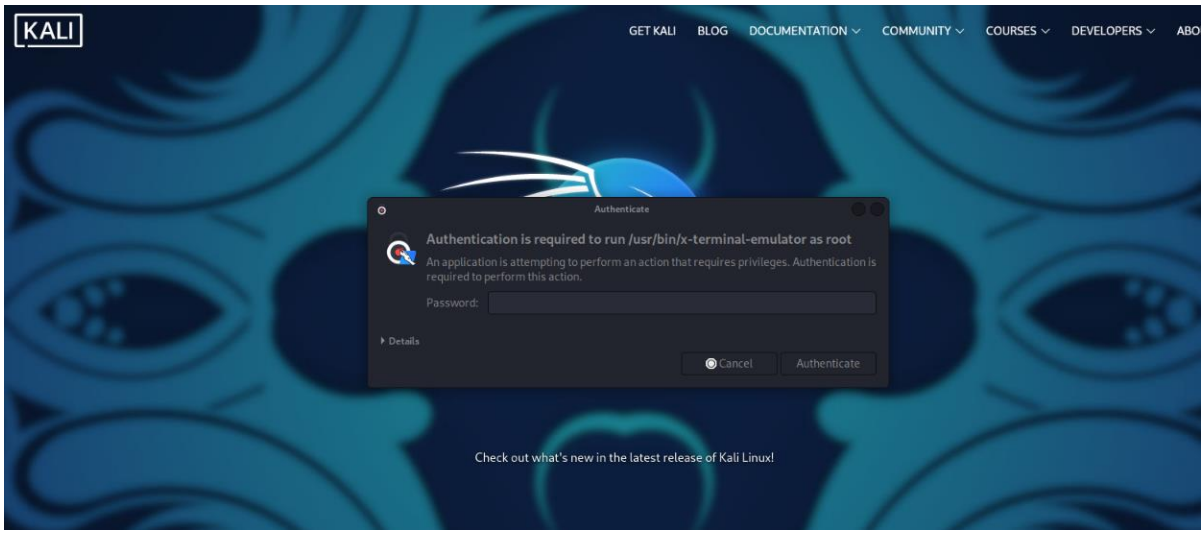



**Figure 39: Password For Root Term**

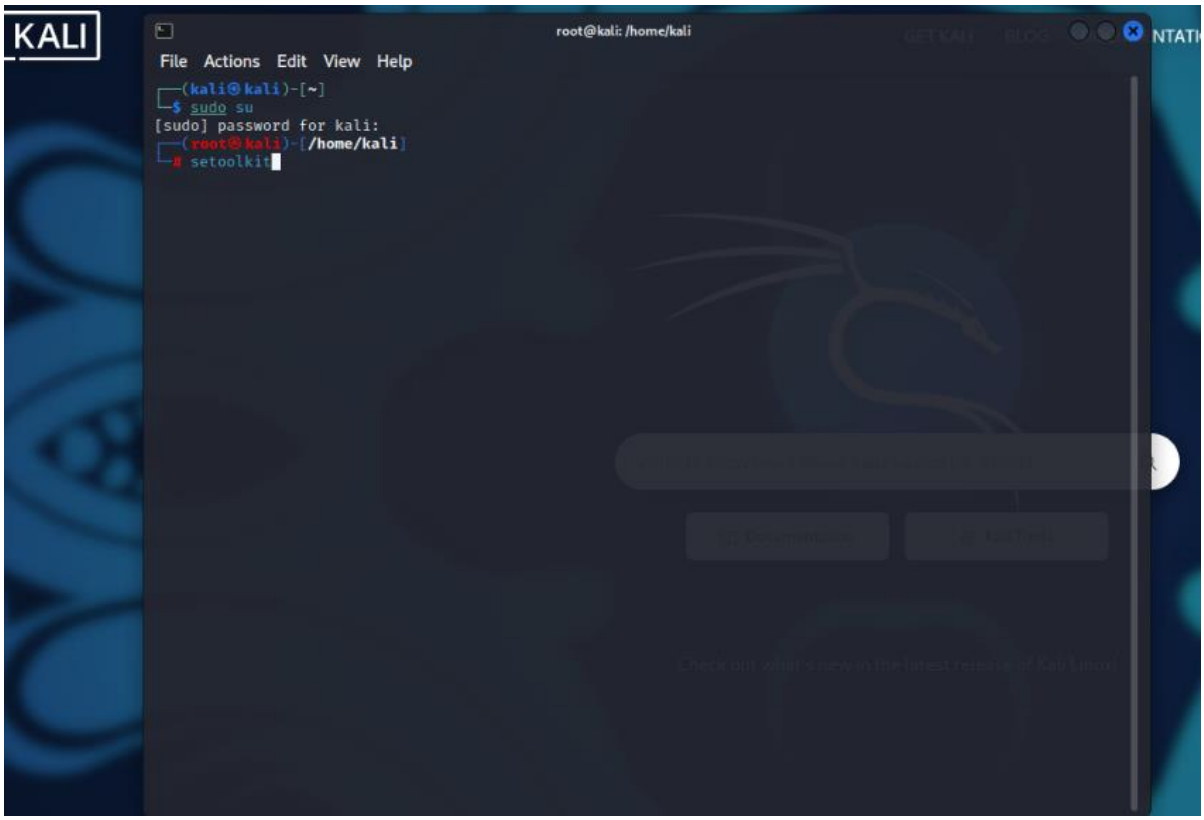



**Figure 40: Social Engineering Toolkit**

As seen below, a list will be supplied. Option "1" is for social engineering assaults.

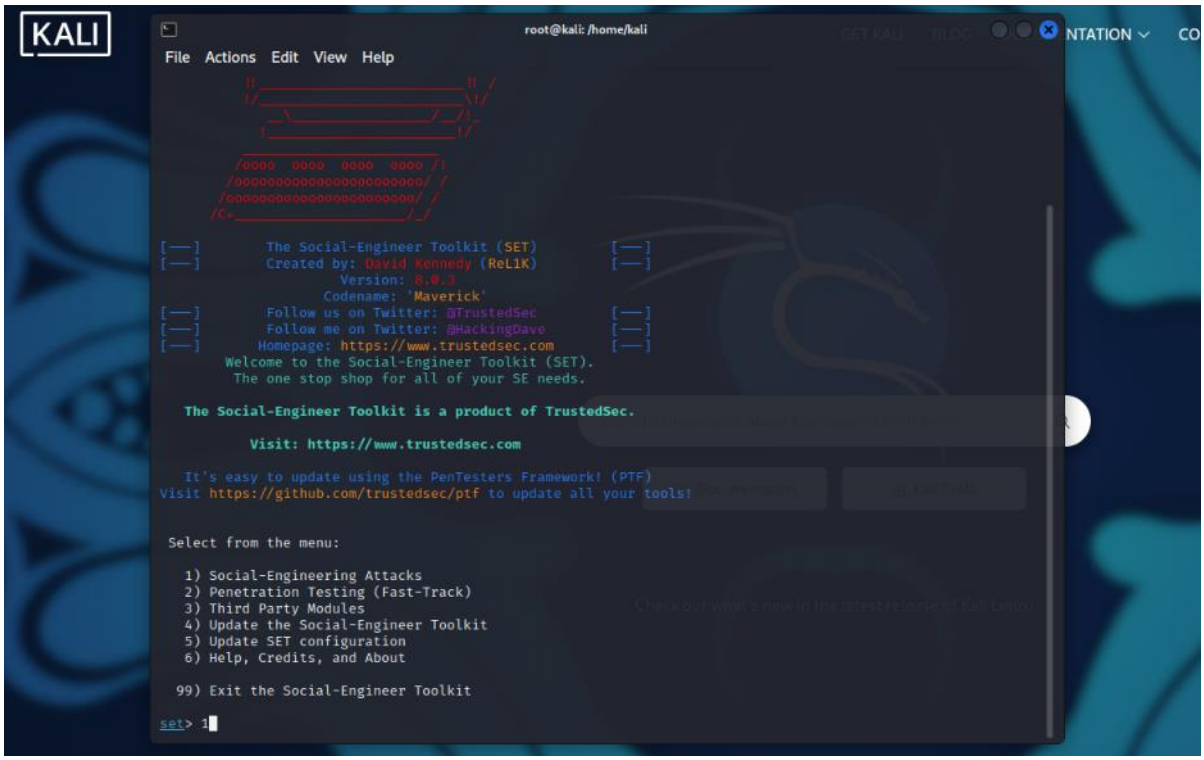



**Figure 41: Selecting Social Engineering Attack**

A list will be displayed once again. Type "2" refers to website attack vectors.


**Figure 42: Choosing Website Attack Vectors**

then select the Credential Harvester Attack Technique (option 3).

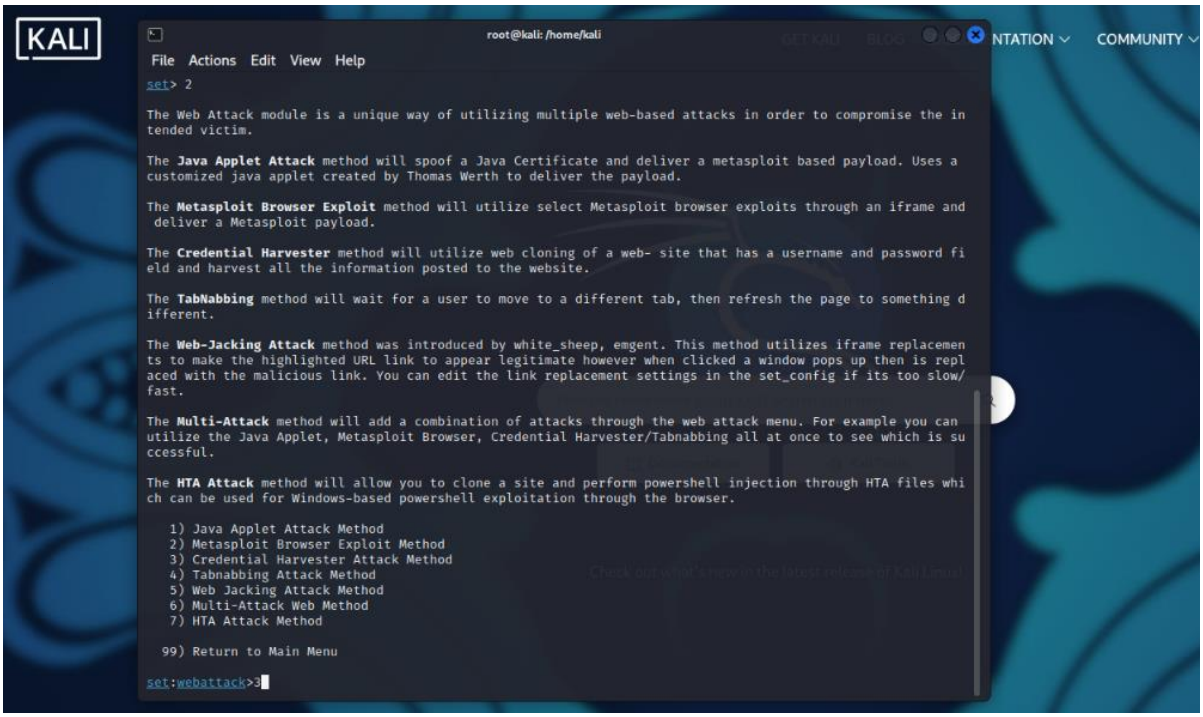



**Figure 43: Choose the Credential Harvester Attack Method**

Choose “1” to select the web templates option

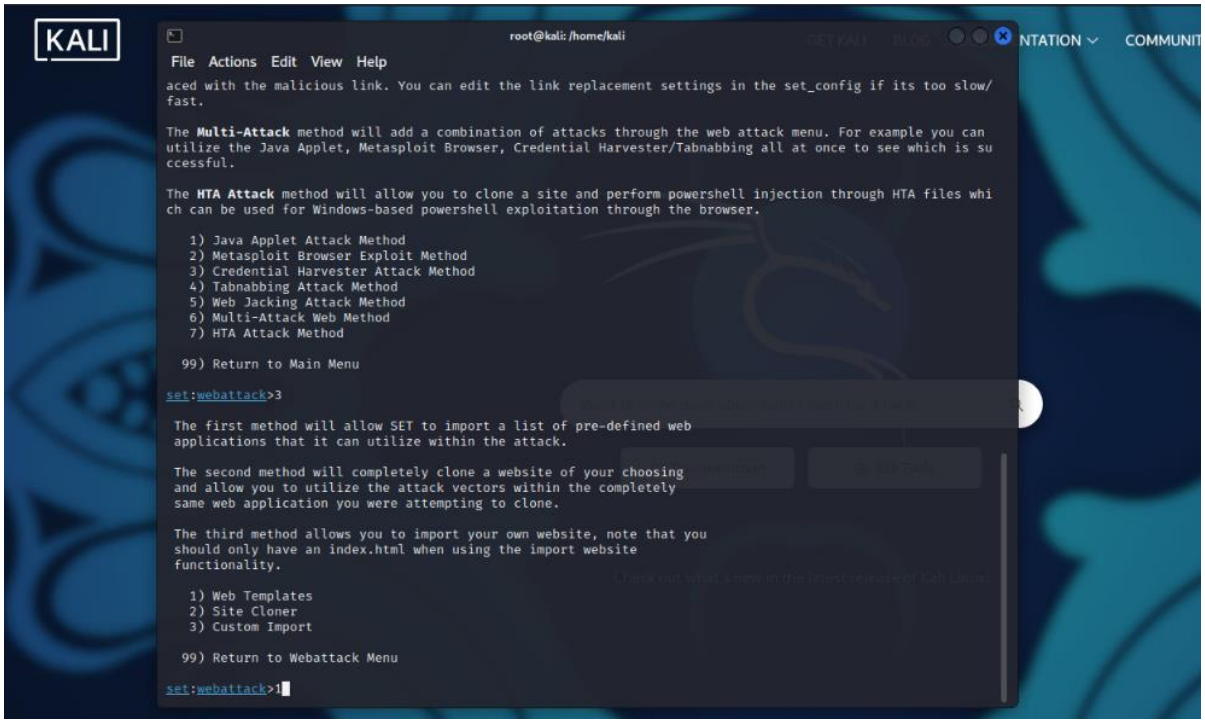



**Figure 44: Choosing Web Templates**

To conduct the attack on the test PC and Kali Linux machine within the same Wi-Fi network, it is sufficient to use the attacker's (my PC) local IP address. However, if the attack is carried out over a WAN, the external IP address must be specified.

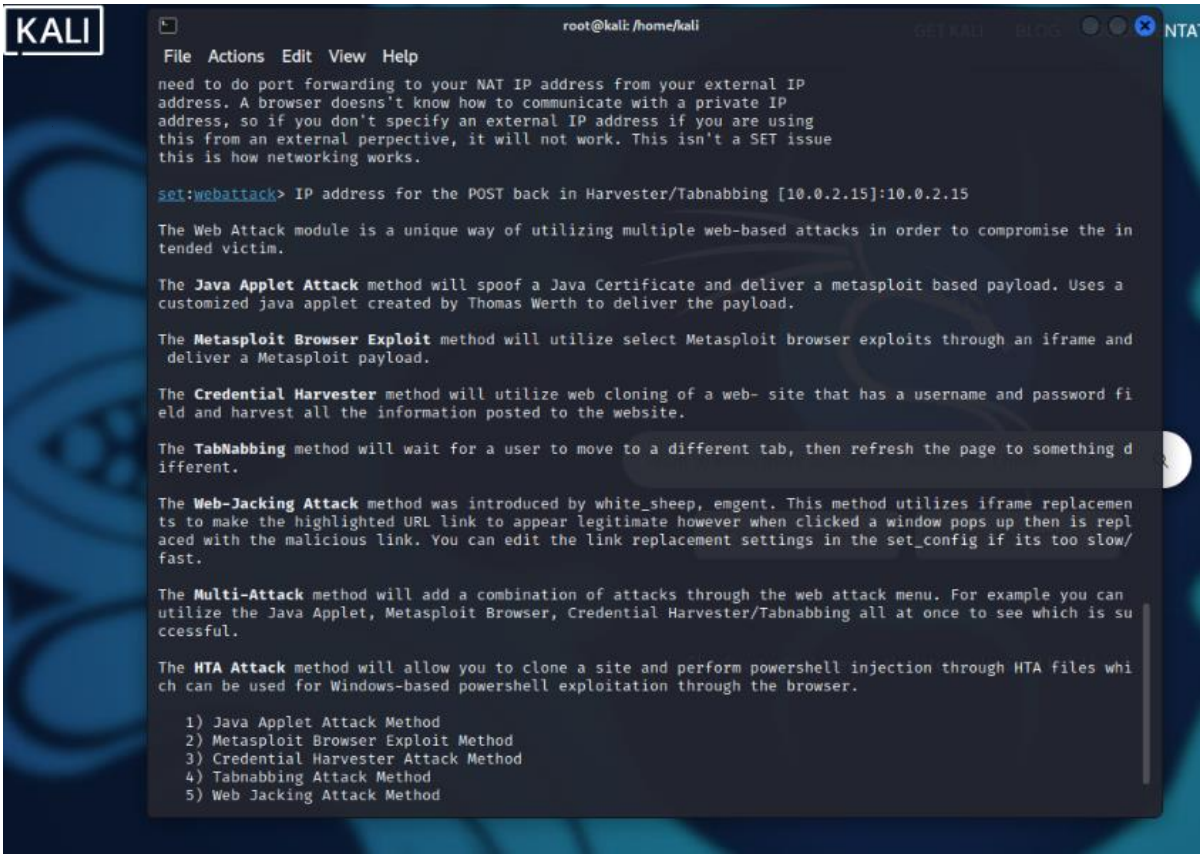



**Figure 45: IP address for Harvester**

After selecting the local or external IP address, the next step is to specify the website that will be cloned using SET. Once the website is selected, the user can then choose a suitable site template. In our case, we selected Google, which is one of the most recognizable and

widely used search engines.

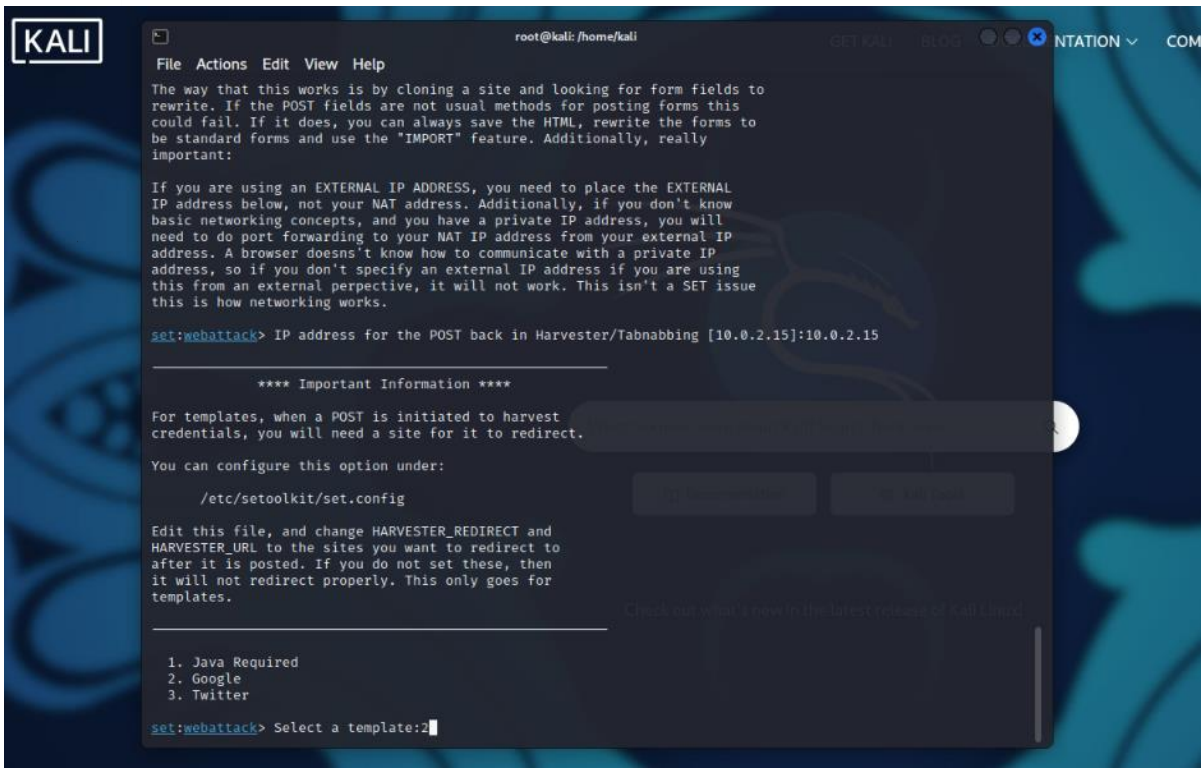



**Figure 46: Selecting Google**

Now is the moment to provide our internal IP address to users via a website. One way to do this is by sending them fake emails that appear to be from Facebook, urging them to log in

for some reason

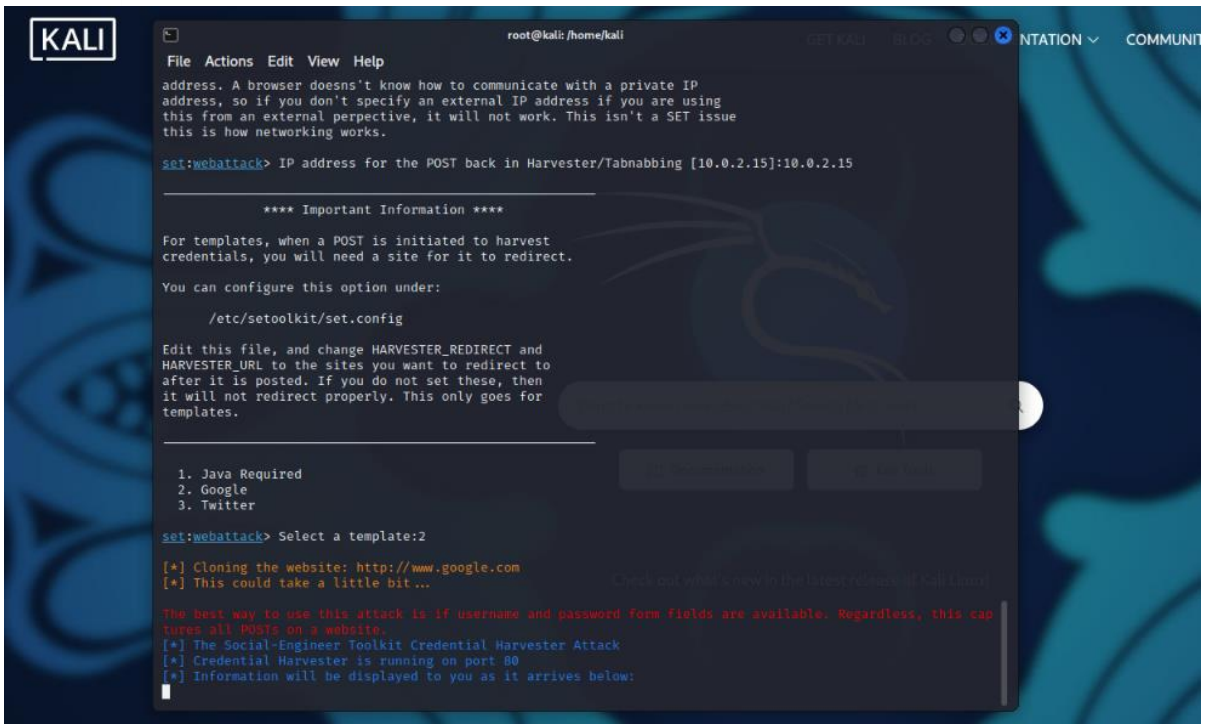



**Figure 47: SET Logs**

The recipient of the email will be redirected to a fake Google login page if they click on the link, which is actually our IP address

Let's observe what happens if the victim inputs his credentials.

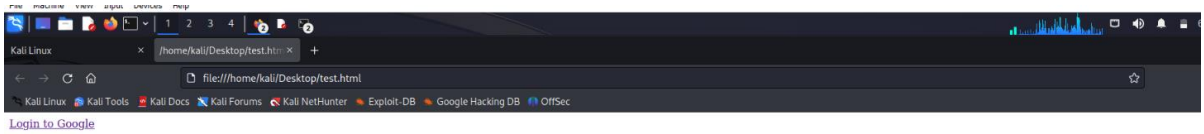



**Figure 48 : Link to open google browser**

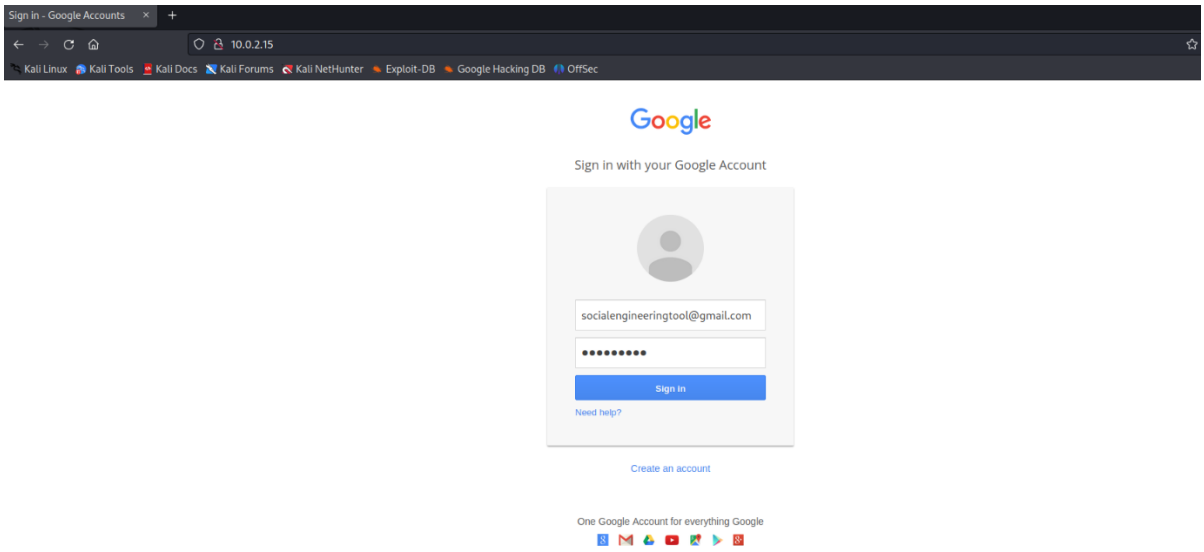



**Figure 49:Google Login screen**

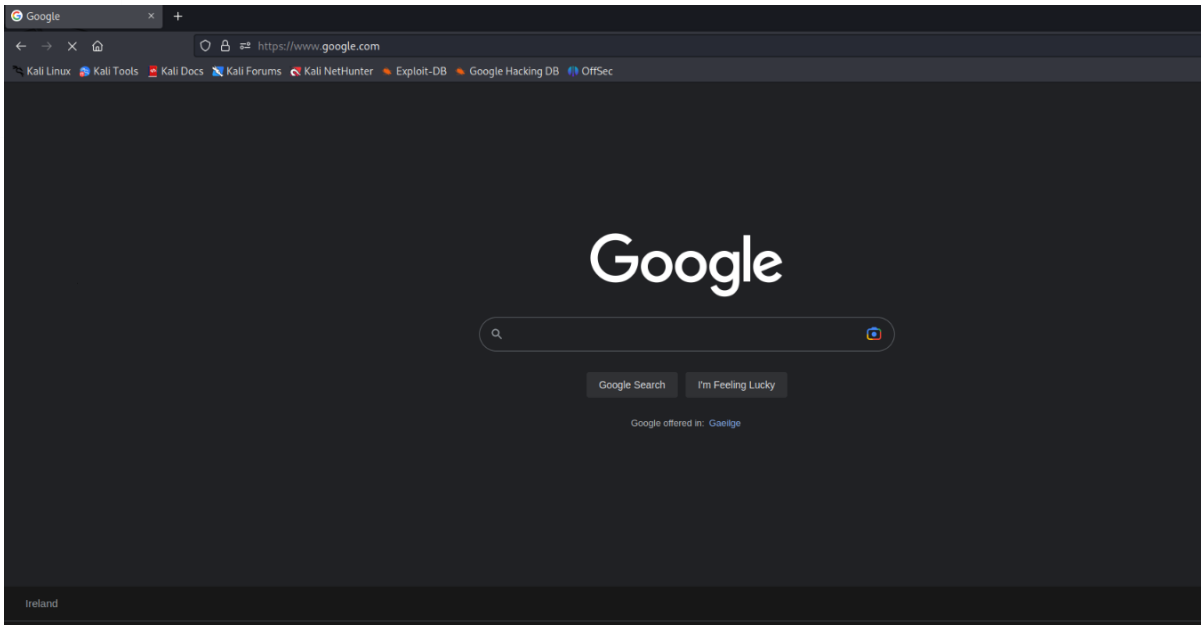



**Figure 50: Redirecting to browser Google**

As we can see, as soon as the victim inserts his credentials into the phony webpage, SET will give us his email address and password. This demonstrates the effectiveness of our offensive tactic.

If a large number of people enter their login credentials on our bogus website, we should notify our customer to examine his security policy and implement additional safeguards against such attacks.

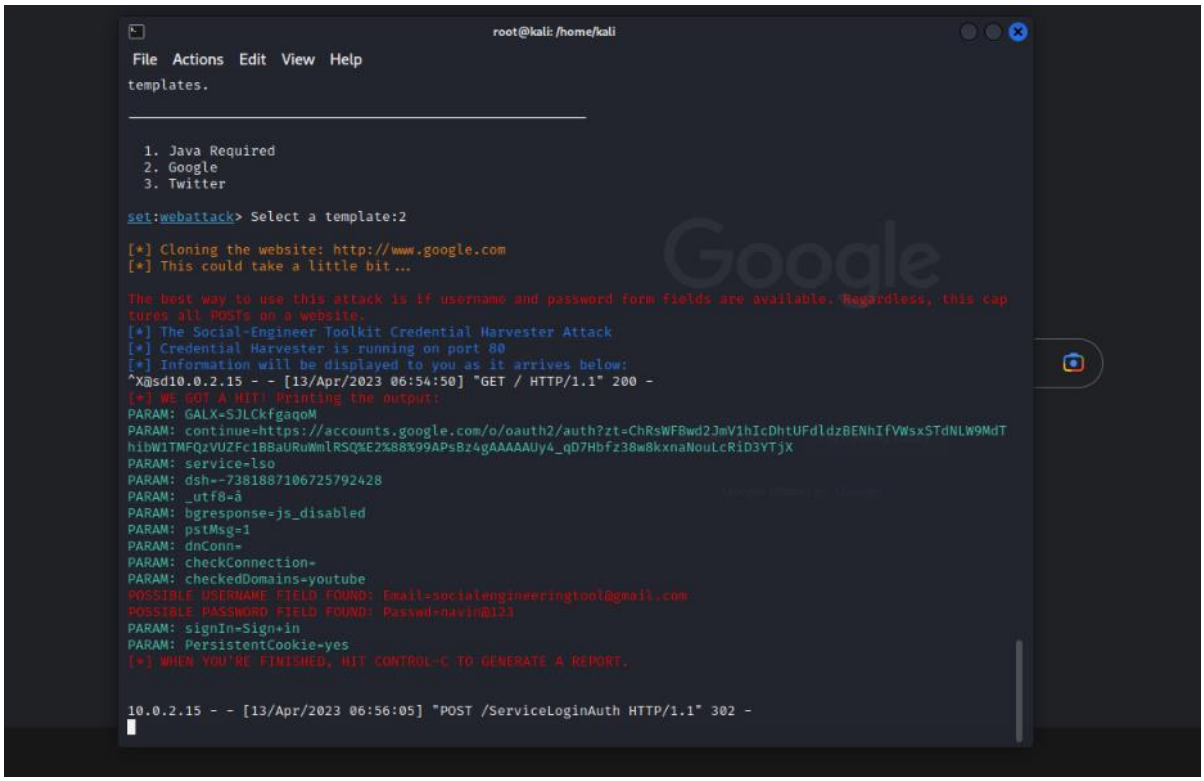



**Figure 51: Credentials in SET**

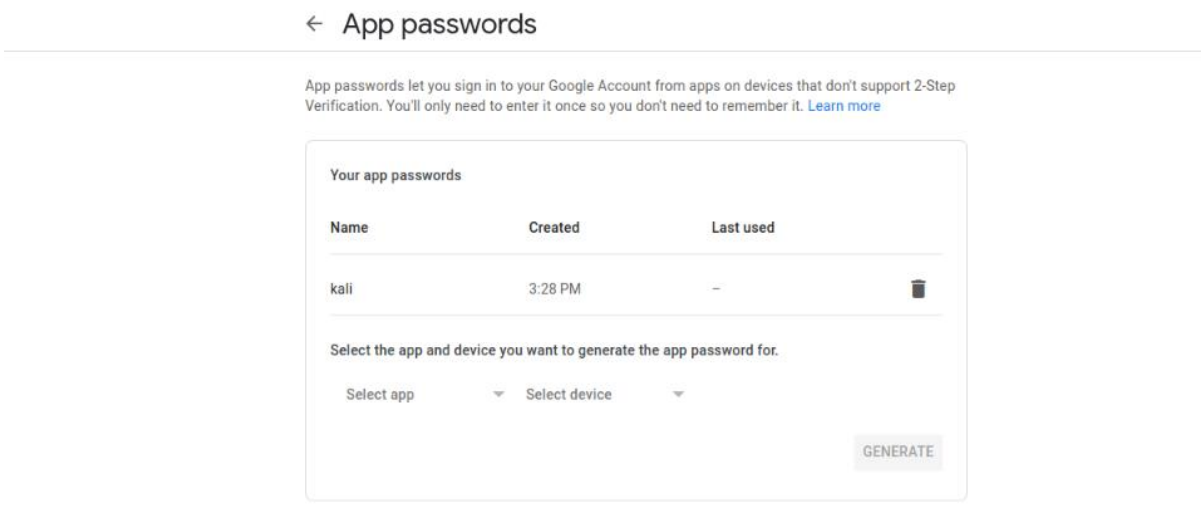
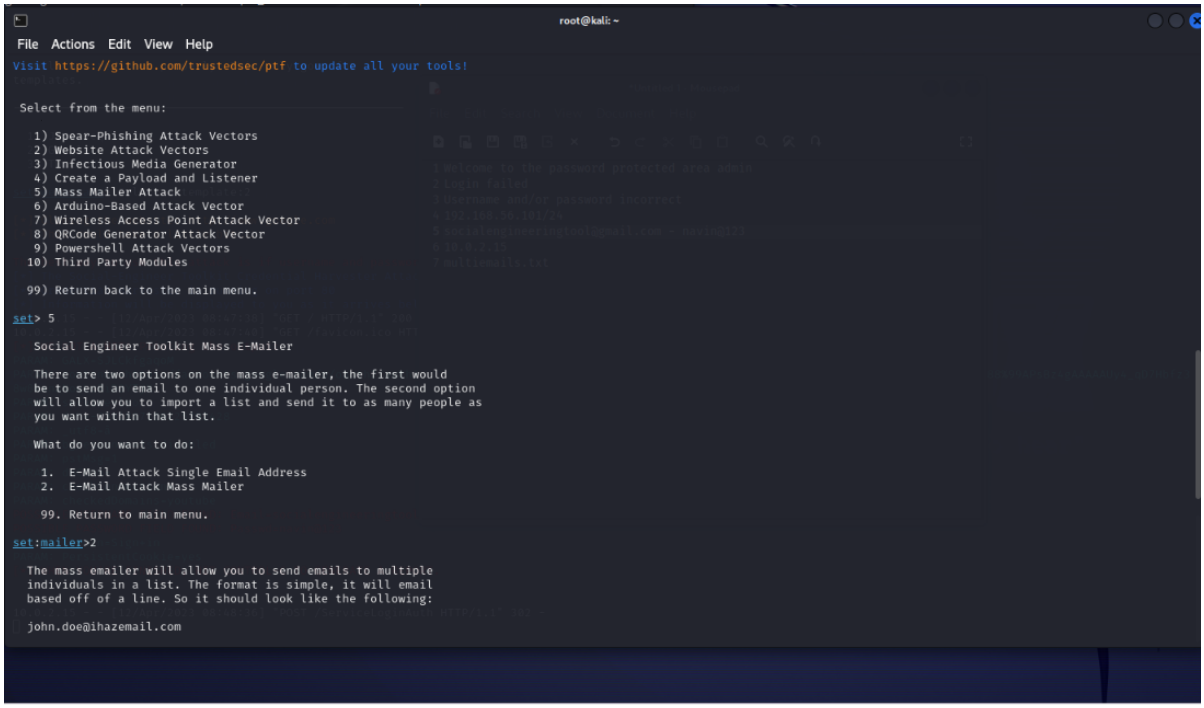



**Figure 52: Creating App Password for Mass Mailer Attack**

To use your Gmail account for these purposes, according to the latest Gmail upgrade, we should generate an app password from the  Gmail account, which can be done through the account settings.



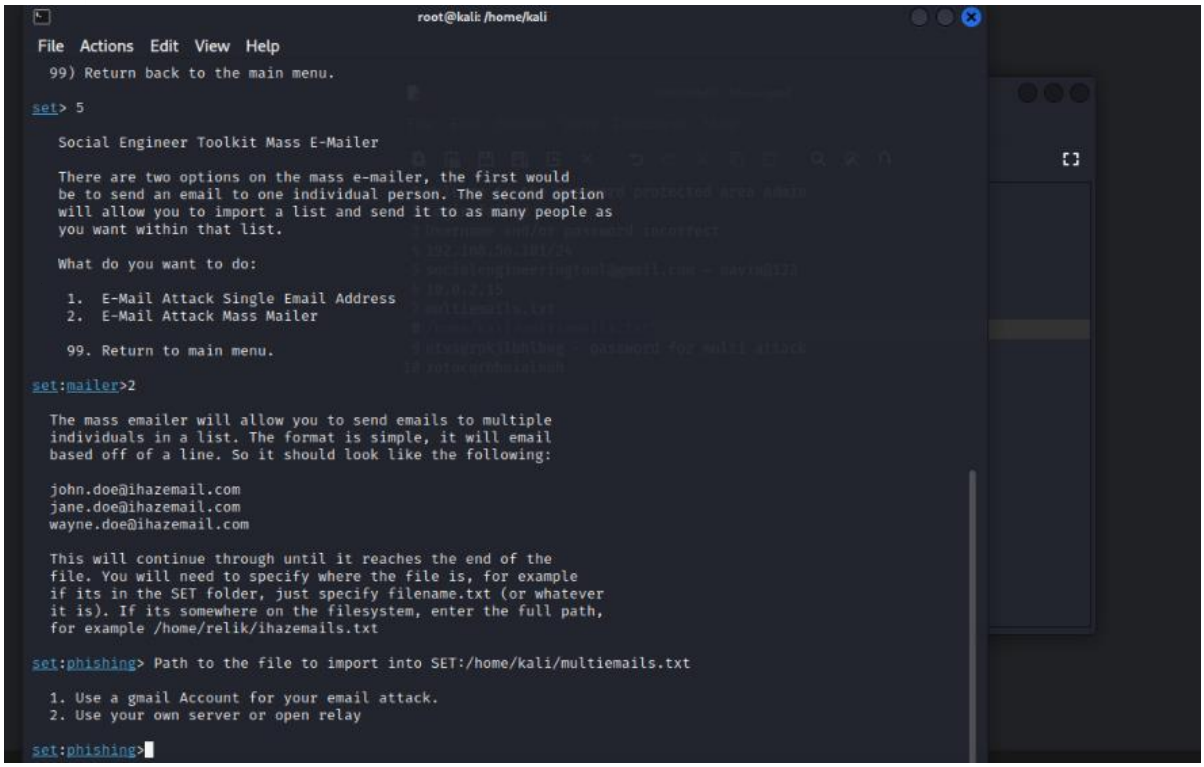



**Figure 53: Mass Mailer Attack**



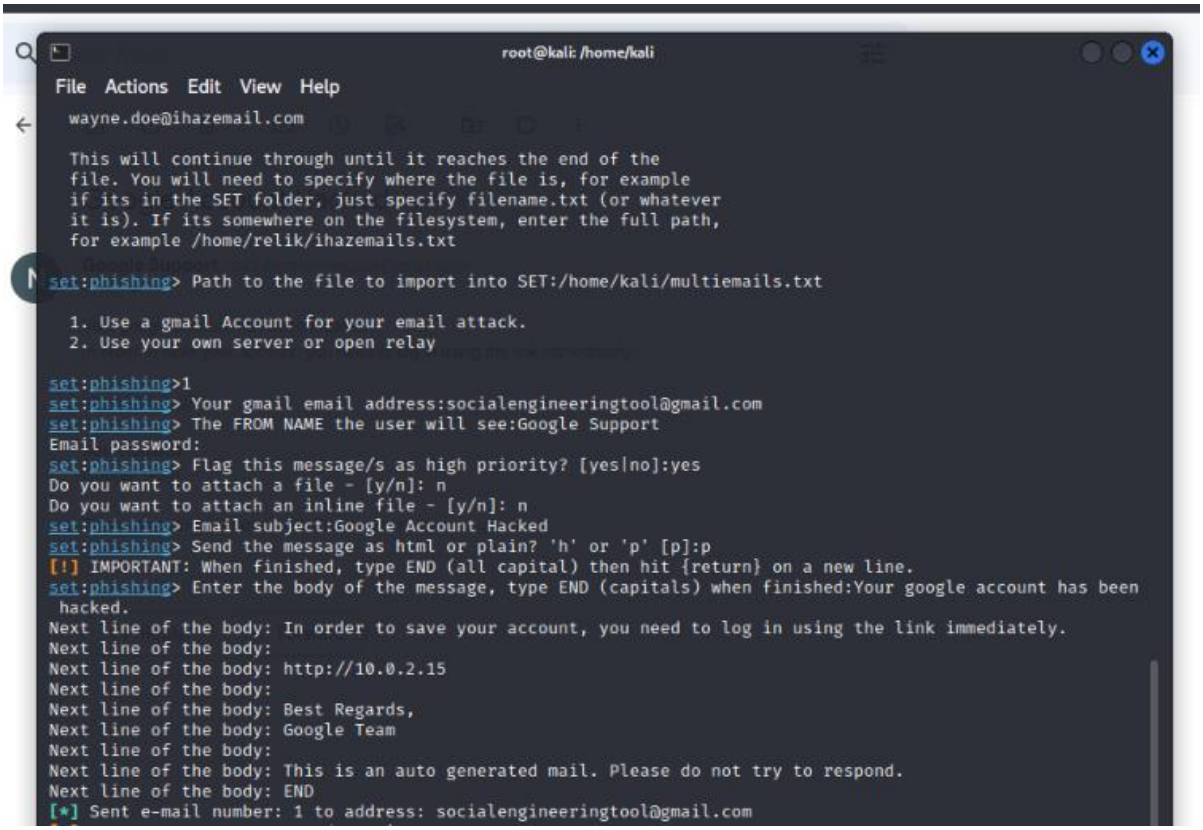



**Figure 54: Entering Option asked for Attack**

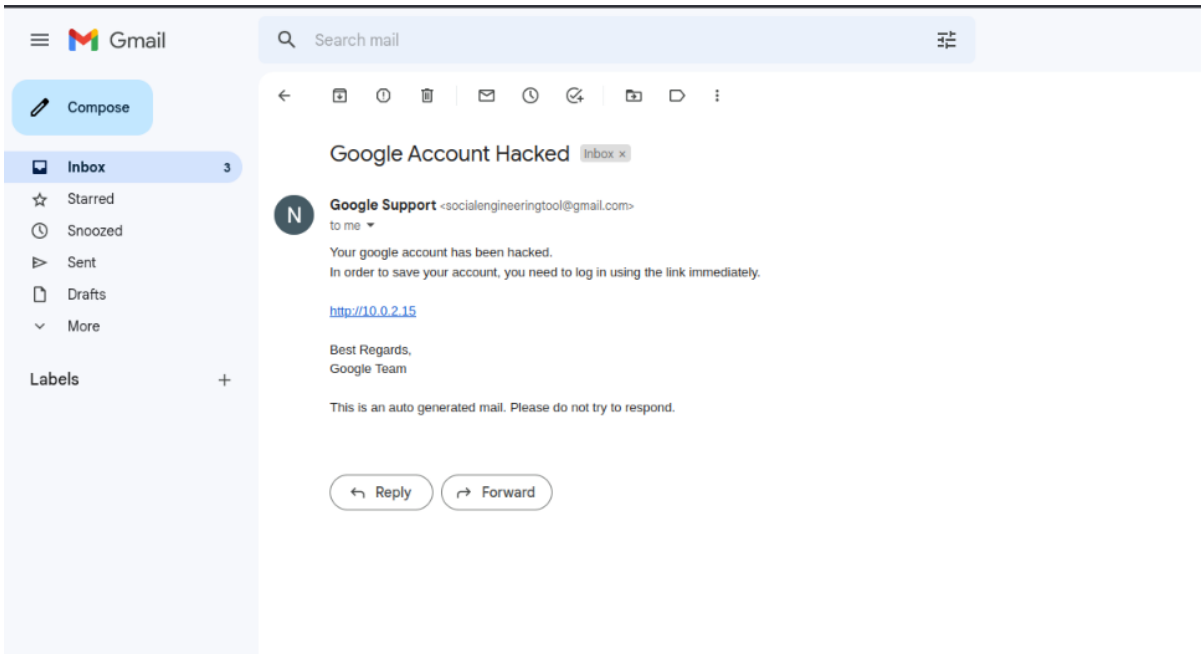



**Figure 55: Mail Sent to Victim**

Once you have completed the necessary steps, you can access your Gmail account and verify that your message has been successfully delivered to the victim.

**Figure 56: Credentials displayed in Kali**

If the victim clicks on the link and logs in, we will be able to retrieve all of their credentials through our terminal

## 7. CONCLUSION

To defend against social engineering attempts, it's important to first identify what you're trying to protect. Determine what data is most valuable to your organization, such as highly sensitive documents, critical business data, or personal information databases, and ensure that they are treated with the utmost caution. Employees who work with these files should be trained extensively and held to strict guidelines. Regular meetings, seminars, and strategies should be implemented to guard against social engineering attacks, and it's crucial to ensure that all employees are aware of and strictly adhere to these measures.

Exceedingly sensitive documents, data that is critical to commercial initiatives, personal information databases, and so on. These files should always be treated with extreme caution. Workers that interact with them will very certainly be required to take extra measures, receive additional training, and follow guidelines.

## 8. BIBLIOGRAPHY

1. 15 Burpsuite Intruder - YouTube (no date). Available at: https://www.youtube.com/watch?v=pX_aG8D5r3A (Accessed: 13 April 2023).

2. A Brute-Force Black-Box Method to Attack Machine Learning-Based Systems in Cybersecurity | IEEE Journals & Magazine | IEEE Xplore (no date). Available at: https://ieeexplore.ieee.org/abstract/document/9138418 (Accessed: 13 April 2023).

3. Analysis of Cyber Security Attacks using Kali Linux | IEEE Conference Publication | IEEE Xplore (no date). Available at:

https://ieeexplore.ieee.org/abstract/document/9793164 (Accessed: 13 April 2023).

4. Create App Passwords to use Gmail account for less secure Apps (2022). Available at: https://www.youtube.com/watch?v=pAPWBHxnFHM (Accessed: 13 April 2023).

5. Kali Linux: Social Engineering Toolkit (no date). Available at: https://linuxhint.com/kali-linux-set/ (Accessed: 13 April 2023).

6. Mass Mailer Attack using Social Engineering Toolkit (2022). Available at: https://www.youtube.com/watch?v=XsGavtm8448 (Accessed: 13 April 2023).

7. How to open damn vulnerability page in kali - Google Search (no date). Available at: https://www.google.com/search?q=how+to+open+damn+vulnerability+page+in+kali&rlz=1C1ONGR_enIN1040IN1040&oq=how+to+open+damn+vulnerability+page+in+kali&aqs=chrome..69i57j33i160.33606j0j7&sourceid=chrome&ie=UTF-8#fpstate=ive&vld=cid:2e4d6480,vid:6zj30jEahgU (Accessed: 13 April 2023).

8. Kore, A. et al. (2022) 'Burp Suite Extension for Script based Attacks for Web Applications', in 2022 6th International Conference on Electronics, Communication and Aerospace Technology. 2022 6th International Conference on Electronics, Communication and Aerospace Technology, pp. 651–657. Available at: https://doi.org/10.1109/ICECA55336.2022.10009116.