**Cybersecurity 401**

**Module 3 - Security Operations**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

# **OPS Challenge 15 - Brute Force Attacks**

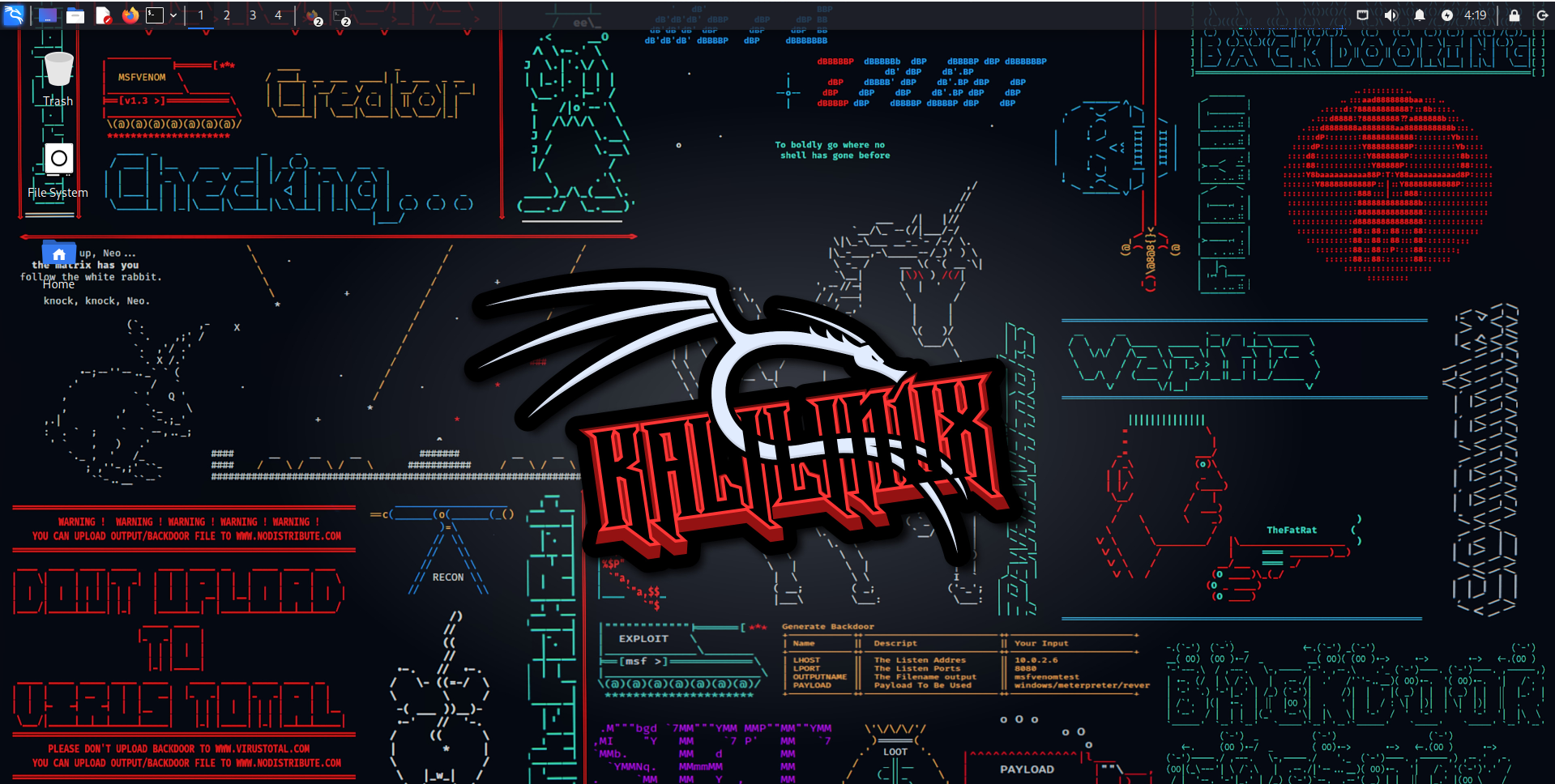


**| Rodrigo Brasil 11/2023 |**

## Part 1: Staging



**Metasploitable VM**



**Kali VM**

## 

### Creating a new user and installing ipcalc



In the **Metasploitable VM** we will create a new user the will serve has the victim for for the brute force attack

Using the command “**sudo adduser victim**” we will create a new user called “**victim**”



because we are using admin privileges it will ask for the sudo password.

after entering the sudo password it will create the user and ask for a new password for the user. For the purpose of this exercise we will use a very weak password.

The password is “**password123**”.



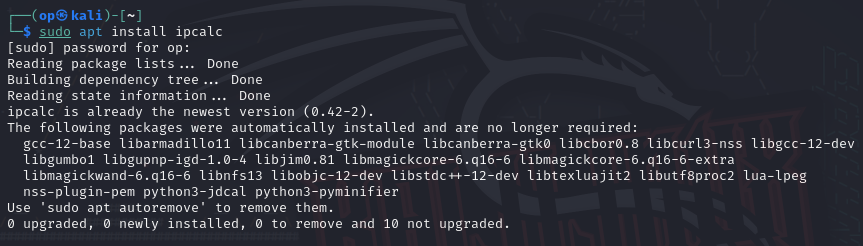
After introducing the password it will ask to reenter it.

after doing so it will start asking for information for the user like the full name, phone number, etc.

This is optional and we will skip this by clicking ENTER on everything.

at the end it will ask if the information is correct (even though there is no information) we type y for yes.

Now we will jump to the **kali VM**



In kali we will open up the terminal and install ipcalc

To install it we will type the following command “**sudo apt install ipcalc -y**”

**“sudo”** for admin privileges

**“ap**t” for the package manager

**“install”** to install the package

**“ipcalc”** the name of the package

**“-y”** so doesn't ask if we are sure we want to install

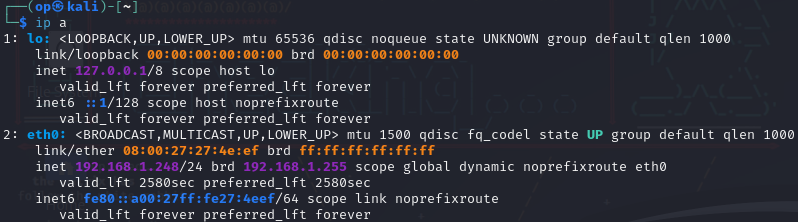
## 

## Part 2: Scouting with Nmap

### information from **kali VM** machine ip

So we will pretend we don't know the victim’s username, we only know we are inside the same network as the victim.

So to find out we will need to do some reconnaissance.

First we will get some information from our **kali VM** machine

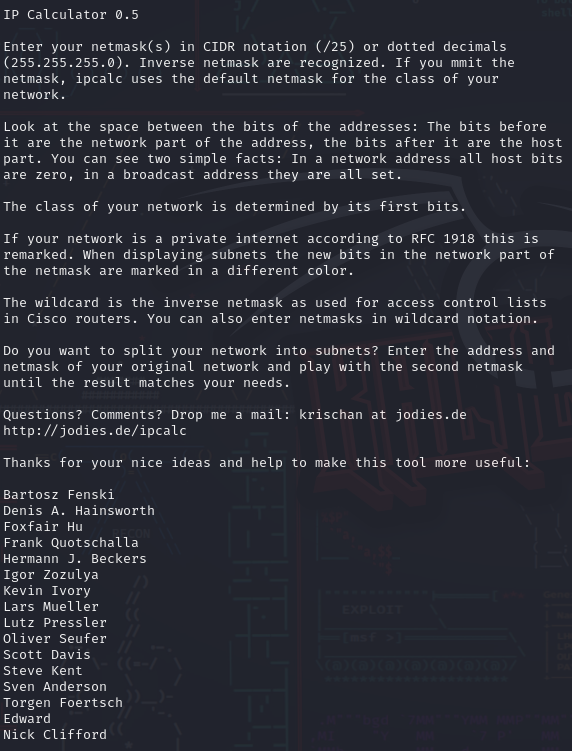
On the terminal we will type the command “**ip a**”to find out our ip

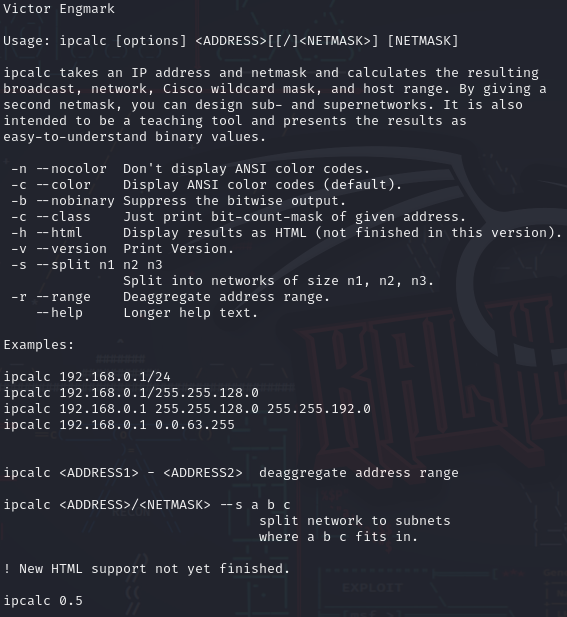
it seem that on our NIC eth0 our ip is “**192.168.1.250”**



Now we will use the previous tool installed called ipcalc.

We never used the tool so to start, on the terminal we will type the command “ipcalc -h”





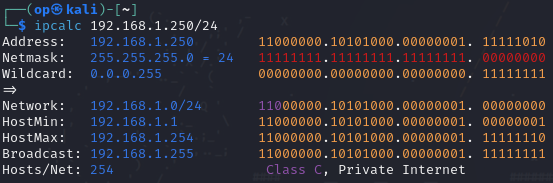
As we can see it gave us a big output with some messages from the developer, explaining what the tool does and how we can use it.

We can see in the examples some ways that we are able to use it.

We will use the first example.



So type the command “**ipcalc 192.168.56.107/24**”



The output will give ups a lot of information about our ip

### Scanning with nmap

Now to find the victim machine we will do a network scan using our ip with the tool nmap.

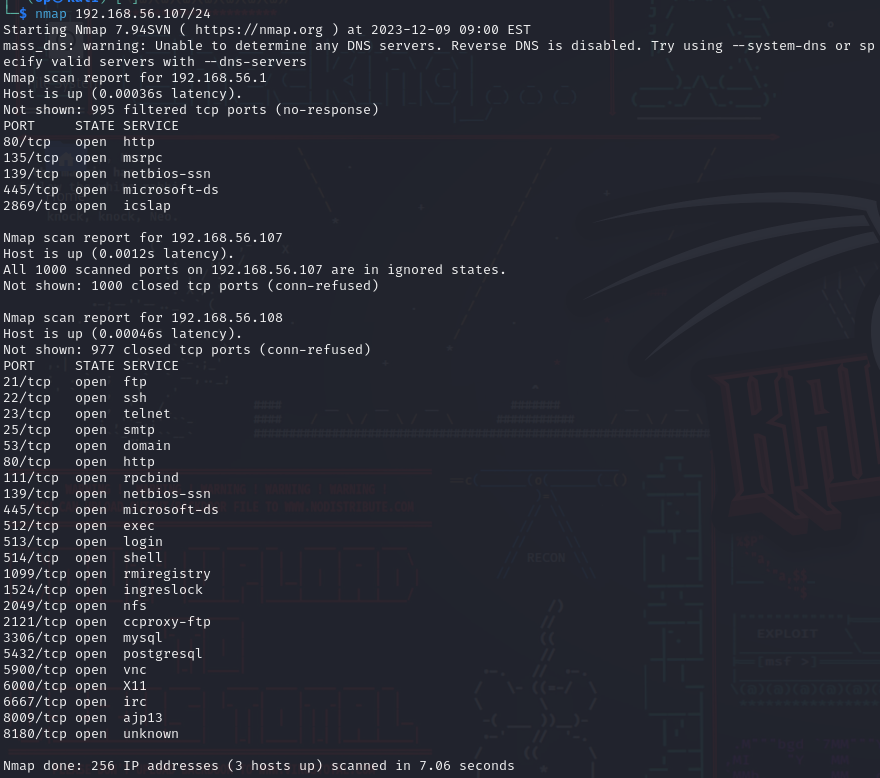
nmap is already installed on kali by default.



type the following command “**nmap 192.168.1.250/24**”

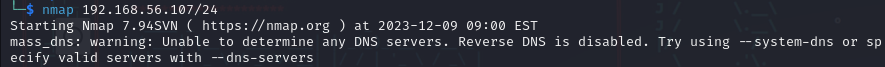
This command serves to simply scan the network for other hosts.

This can take awhile depending on the devices connected to the network

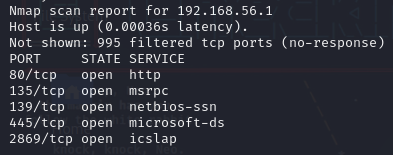


After entering the command we can see a big output.

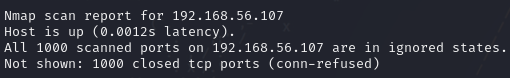
We will dissect it slowly from top to bottom.



The first block we can see its giving a warning that it wasnt able to find any dns server so a Reverse DNS is disabled. we dont know what that is. so we will leave it to the side.



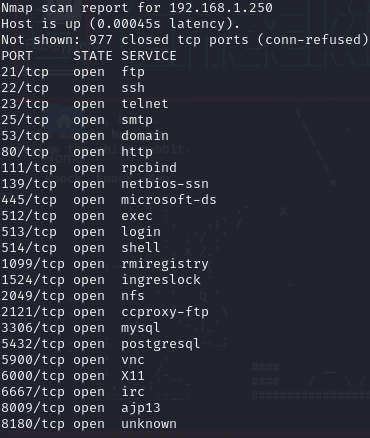
The second block we can see information about the ip “**192.168.1.1**”. This ip we can safely assume is the router. And there are some standard ports open.



The third block shows the **kali VM** IP

It shows that all **1000 common ports** are **closed**.

That does not mean there are no **open ports**, that just means that the common 1000 are but there are a lot more.



Now who is this??

This seems very interesting.

there are ALOT of **open ports** on this host

we can identify its ip is “**192.168.1.250**”.

also we can identify that the **port 22** for **ssh** is **open**!

## 

### Finding the user with enum4linux

Before we attack this ip, first we need to find a user

for this we are going to install **enum4linux**

****

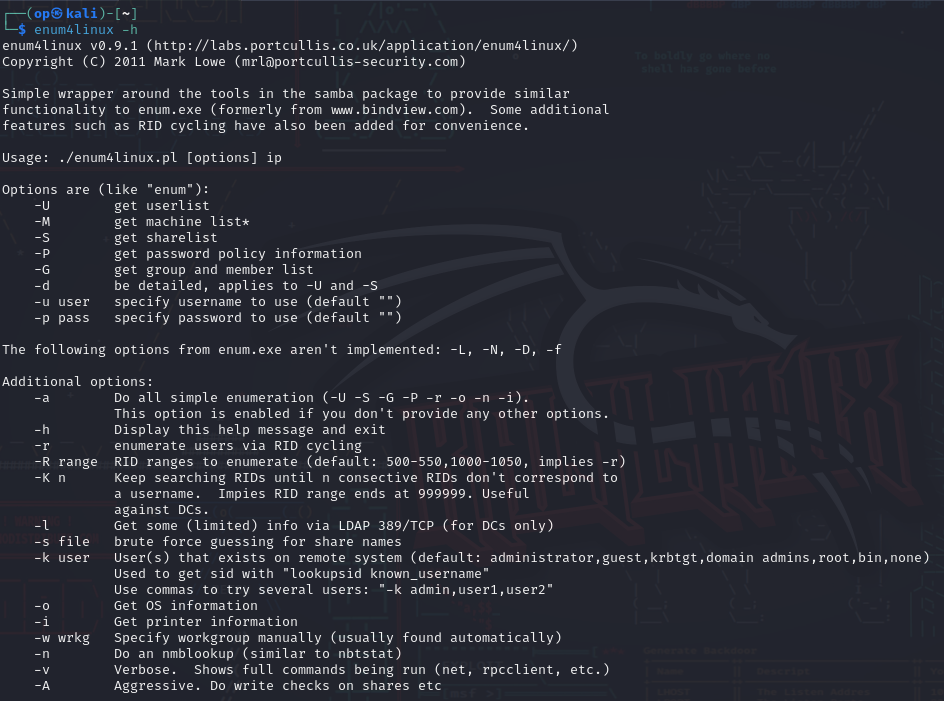
To install we are going to type the command “**sudo apt install enum4linux**”

in my case its already installed

Like before we have no idea how to use this tool so let's look at its manual



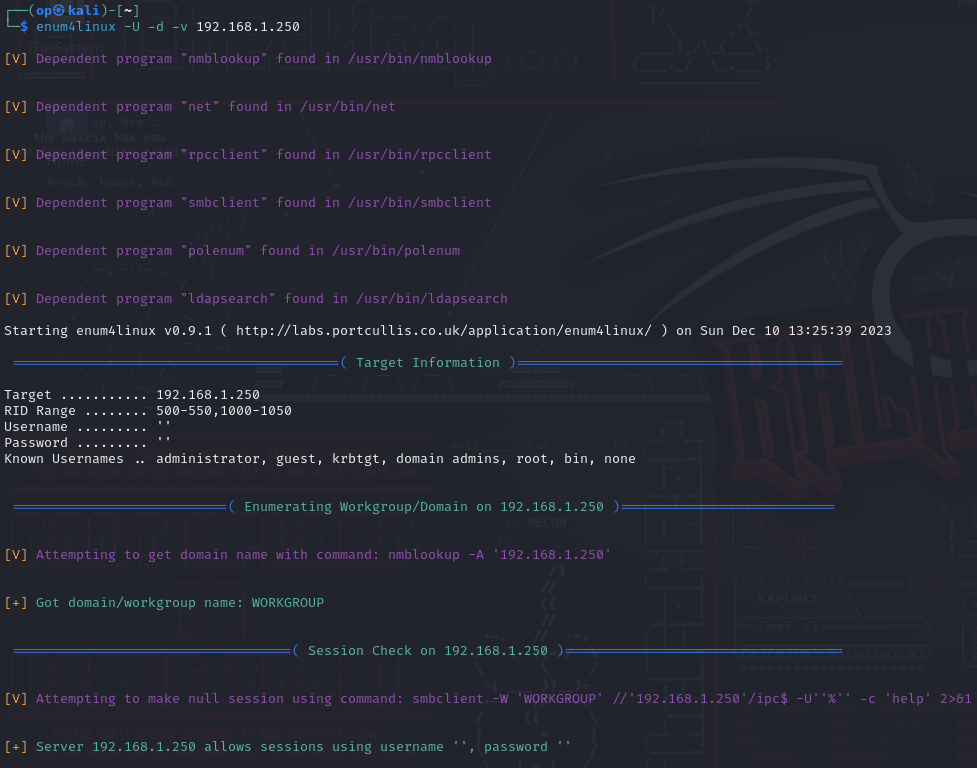
type “**enum4linux -h**” -h stands for help



it will give us this big output and can see alot of options we can use with this tool, but we want to find the user so we are going to use -U to get the userlist, with -d for the output to be more detailed and -v for verbose for easier readability



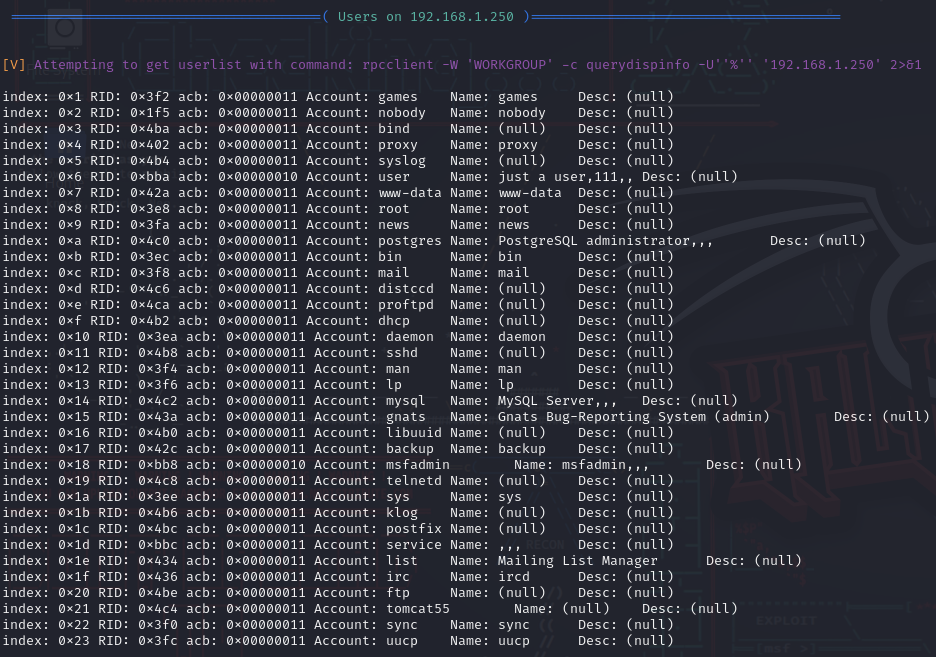
So let's type the command “**enum4linux -U -d -v 192.168.1.250**”



After clicking ENTER there will be an enormous amount of information on our output

Don't be afraid to dig into this information, we will look at it slowly searching for users

  
Scroll a bit down until you find a section of users



In this section we can see a lot of “users” which they are not, they are “fake users” created by the programs installed on the machine.

Now let's observe them, what can we see that stands out?

If we look closely at the last digits on the acb (0x00000011) we can see that most of them end in **11** but 2 of the users end in **10**

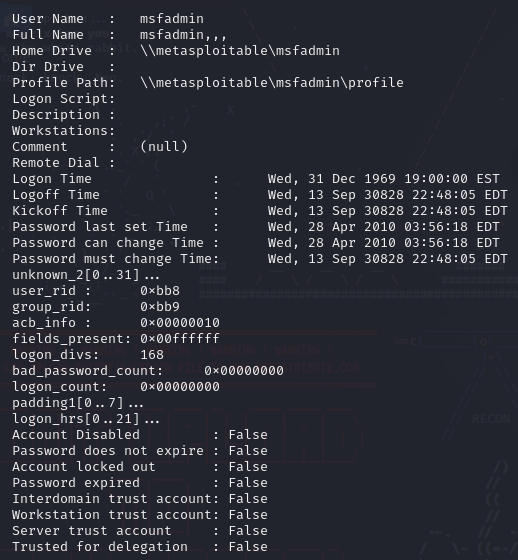
those users are: **user** and **msfadmin**

msfadmin looks like an admin user

and user looks like a simple user

we can see that the user **Name** says “just a user” how convenient!

so we found 2 users but lets scroll a bit more down and lets try to find msfadmin and user while observing the other ones as well to compare differences



So we found msfadmin, if you observed the other users we can see that there is a detail that stands out

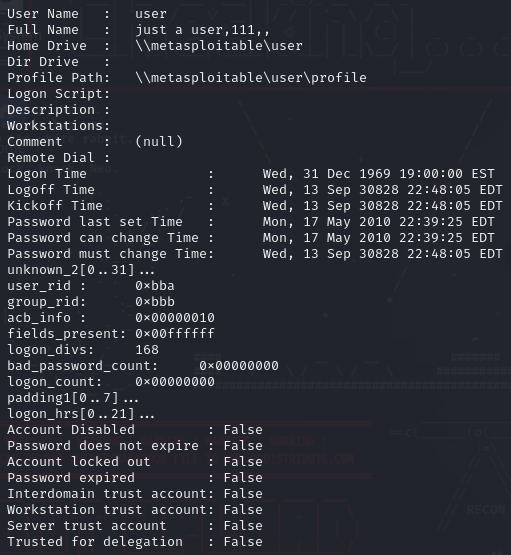


If you observed the other accounts there is a detail that stands out

The parameter “**Account Disabled”** in msfadmin is false while the other ones are true

This means this account is enabled. we can probably log into it.

what about user? if we scroll down a bit more



We found the user and it has the same parameter.

Let’s target this user for the bruteforce attack!

## 

## 

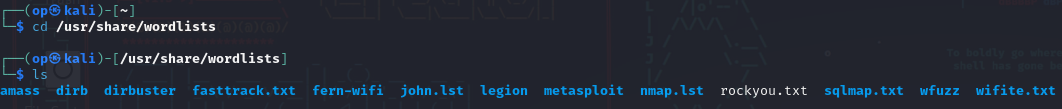
## 

## Part 3: Attack SSH using Brute Force

Now that we have the IP and the user we are going to need a password list

fortunately for us kali already comes with some lists pre-packaged with it

for this exercise we are going to use the gigantic list that is **rockyou**

****

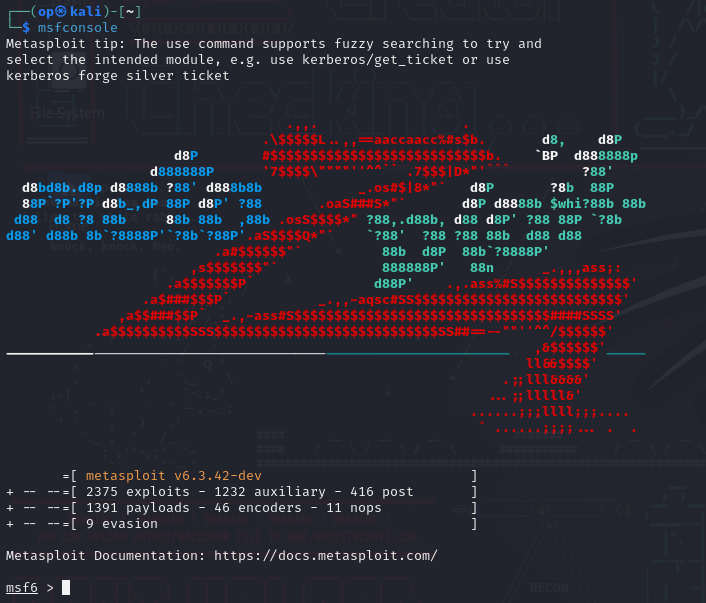
****

This list can be found in **/usr/share/wordlists**

So for this attack we are going to use the tool “**metasploit**”



To prepare the ssh attack, in the terminal we will start the tool by typing the command “**msfconsole**”



When started it will look like this.

Now we are going to prepare **metasploit** for the attack.



where it says “**msf6 >**” we are going to type the following command:

“**use auxiliary/scanner/ssh/ssh\_login**”



after hitting ENTER it will look like this.

This is a script inside metasploit for our brute force attack

Now this script needs some parameters.

The first parameter is going to be the IP of the target machine

****

So we are going to type the command: “**set RHOST 192.168.1.250**”  
It will give us and output saying the RHOST now is the target IP

Next is the user



Type the command: “set USERNAME user”

It will give an output saying the USERNAME now is user

now we will give it the password list to use for the attack



Type the command: “**set PASS\_FILE /usr/share/wordlists/rockyou.txt**”

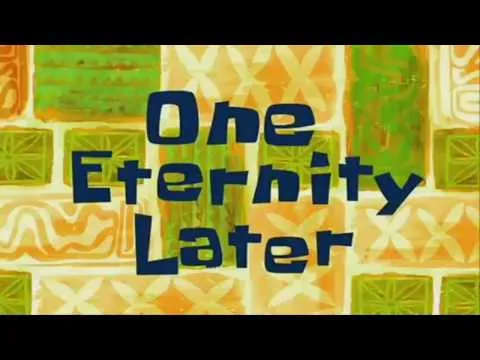


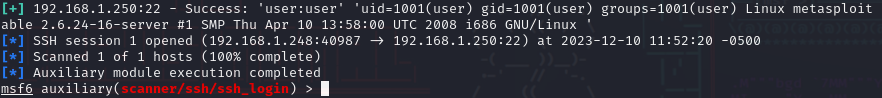
Now to simply start the brute force attack type “**run**”



The brute force attack is now running!

note that this can take a while so grab a snack do, take a walk and relax until it is done.





Sucess!

As we can see the password was found!



We can see in this line the “**user:user**” user being the username and user being the password!

Now all we have to do is ssh to the target machine using these credentials!



open a new terminal and type the command: “**ssh user@192.168.1.250**”



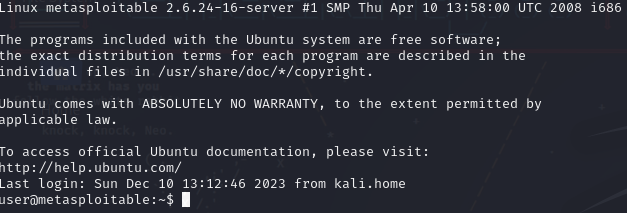
If you find this error when trying to login



Use the following command: ”**ssh -oHostKeyAlgorithms=ssh-rsa -oPubkeyAcceptedKeyTypes=+ssh-rsa user@192.168.1.250**”



It will ask for a password which we now have muahaha



And we are in Neo!



## Part 4: Reporting

Time to recap and summarize each of your tests. For each test:

* Describe the advantages and disadvantages of using this tool.
* How many authentication attempts did your tool make against the SSH server?
* Share a screenshot of a successful attack you made today and include your thoughts on the tool in a Slack post to the class Slack channel.