VULNERABILITY ASSESSMENT AND PENETRATION TESTING

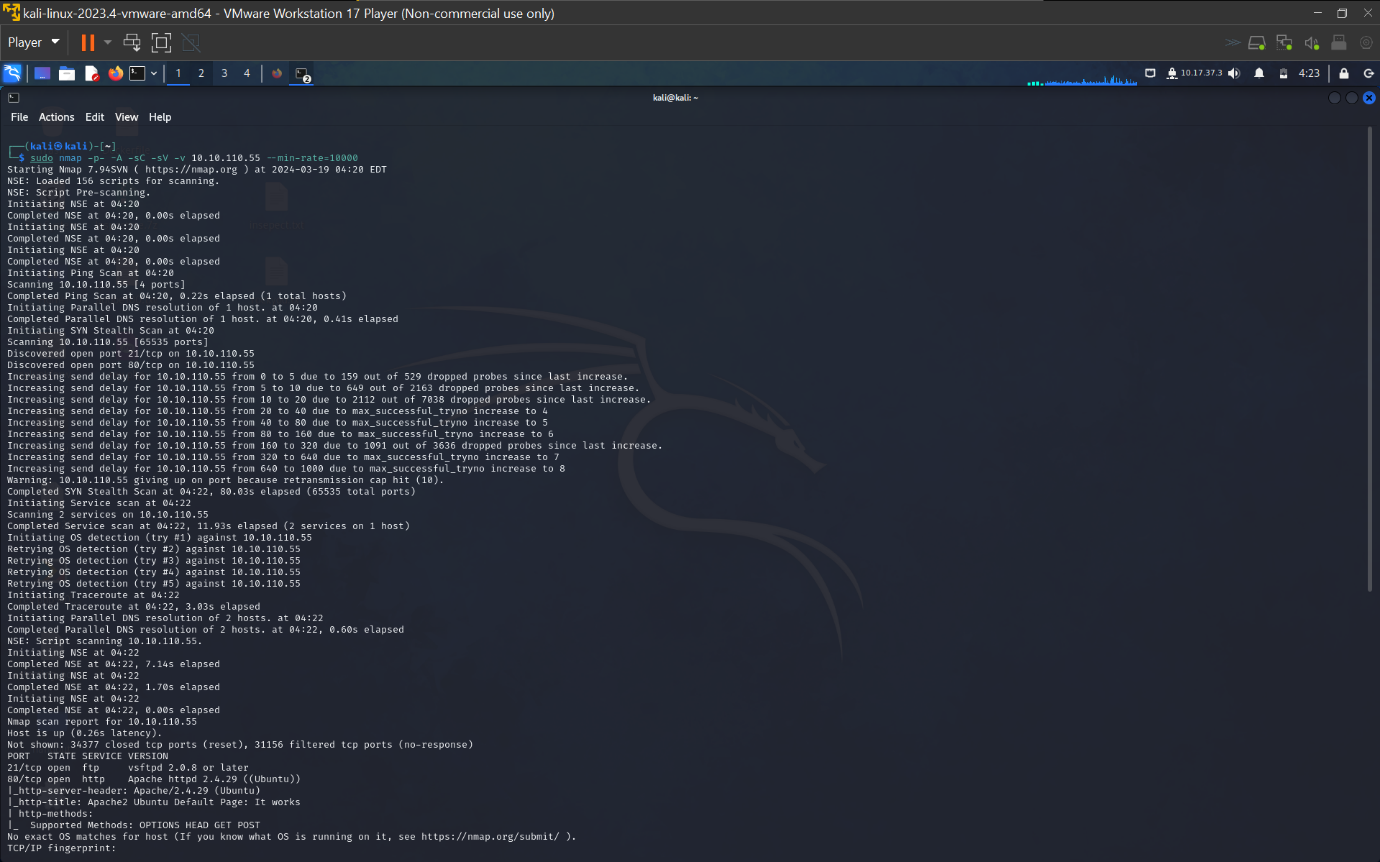
# PROCESS:

***Following the pervious lab exercise, we got the username is jenny.***

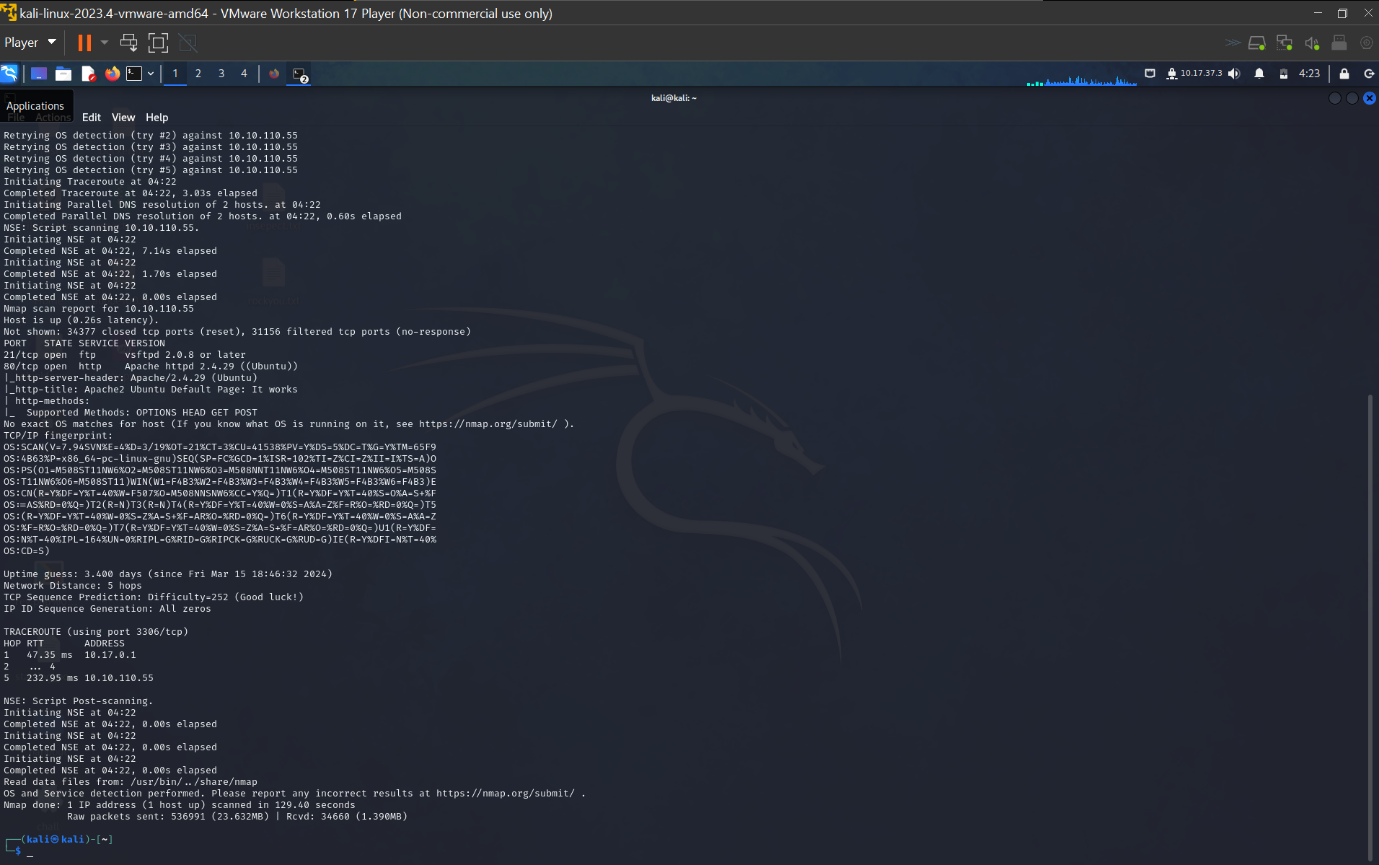
**Scanning the target is the first step that we must do to know more about the target system. We need to scan the target to find any open ports or vulnerabilities. Lets use the ‘nmap’ for this**

* **“Sudo nmap -p- -sC -sV -A -v <target\_ip> --min-rate=1000” (here ip is tryhackme machine ipaddr).**

**there are 3 open ports available in this machine.**

****

**The ports are ftp/21 and http/80.**

****

**As we know the username that is ‘jenny’ and we need password of it.**

**Lets use “hydra” to crack the password of the user ‘jenny’, using the command**

* **“hydra -l jenny -P rockyou.txt <target\_ip> ftp” (note: ‘rockyou.txt’ is text file that contains the most commonly used passwords).we download it from github.**

****

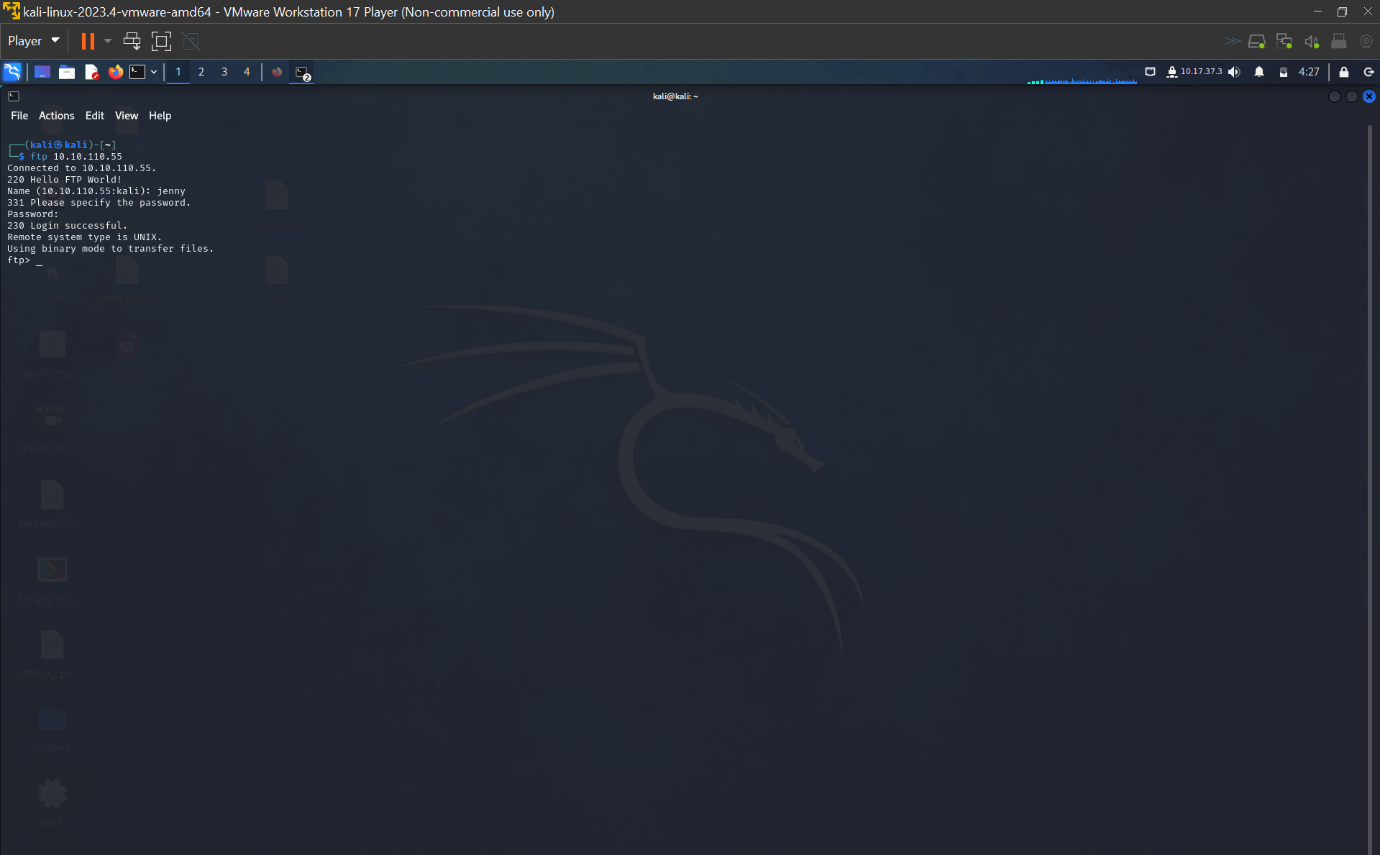
**We got ftp the password from hydra as “987654321”.**

**Lets start the ftp service.**

**As ftp port is open and the we know the username as “jenny” and it password from the hydra.**

**Login into ftp, using command on the terminal.**

* **ftp <target\_ip>**

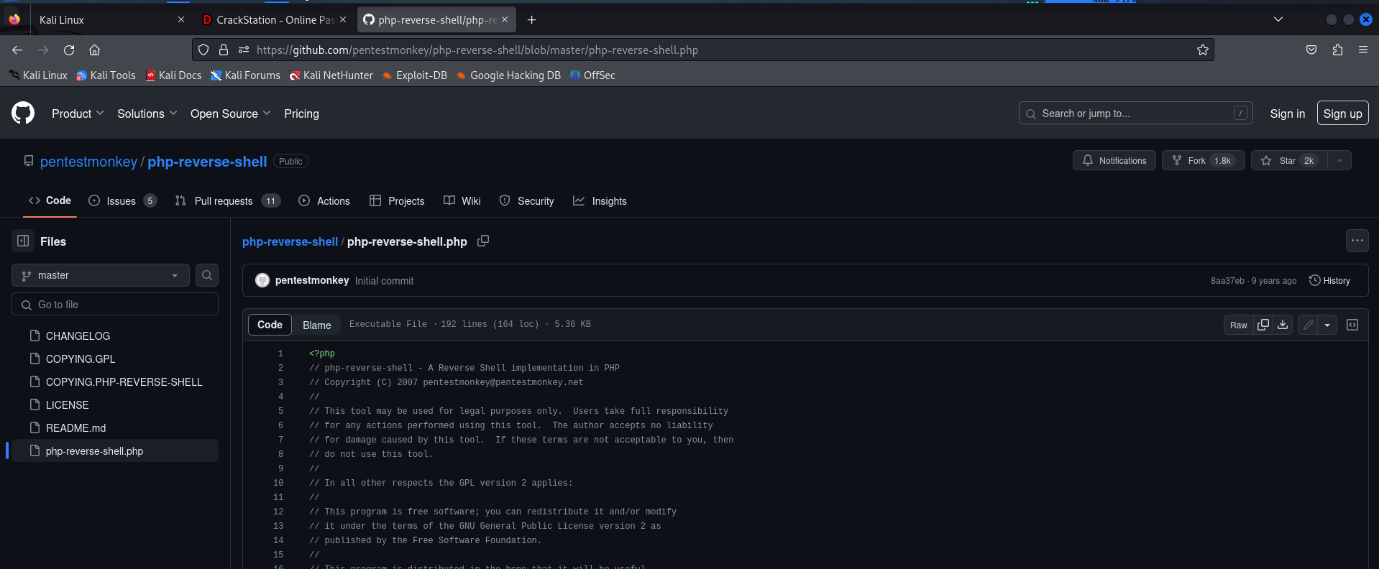
****

**We now need to upload a reverse shell into it to gain access of root user.**

**So lets download reverse file from github or revshells. Download the**

* **Pentestmonkey/php-reverse-shell/**

[**https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php**](https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php)

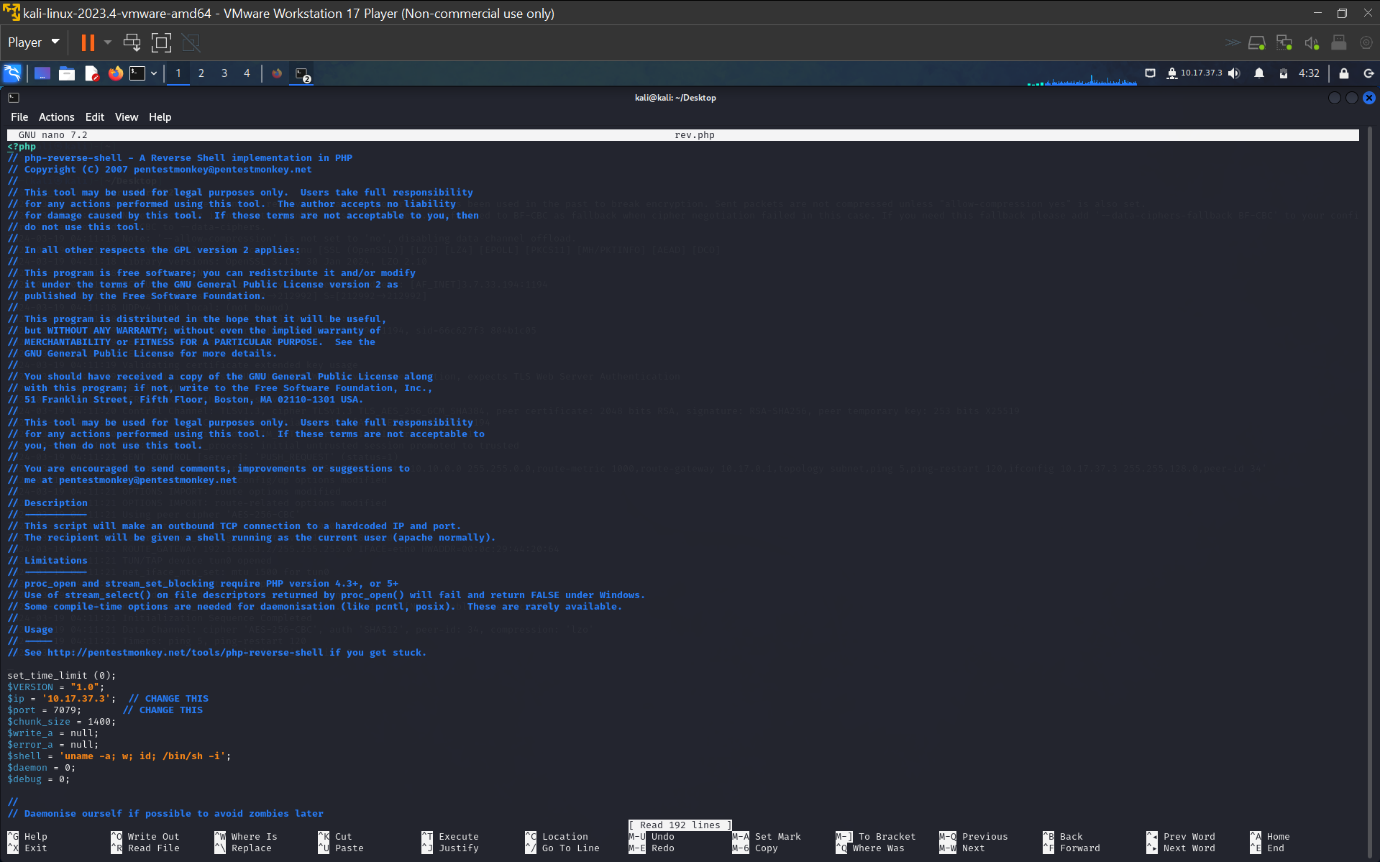
****

**Using the nano command access the file and change the ip addr and port no. to**

**the listener ip addr and port according to the choice and above 2ooo .**

* **Here the ip addr is the tun0 ip and port no = 7079.**

**Now save the reverse shell.php file on the desktop.**

****

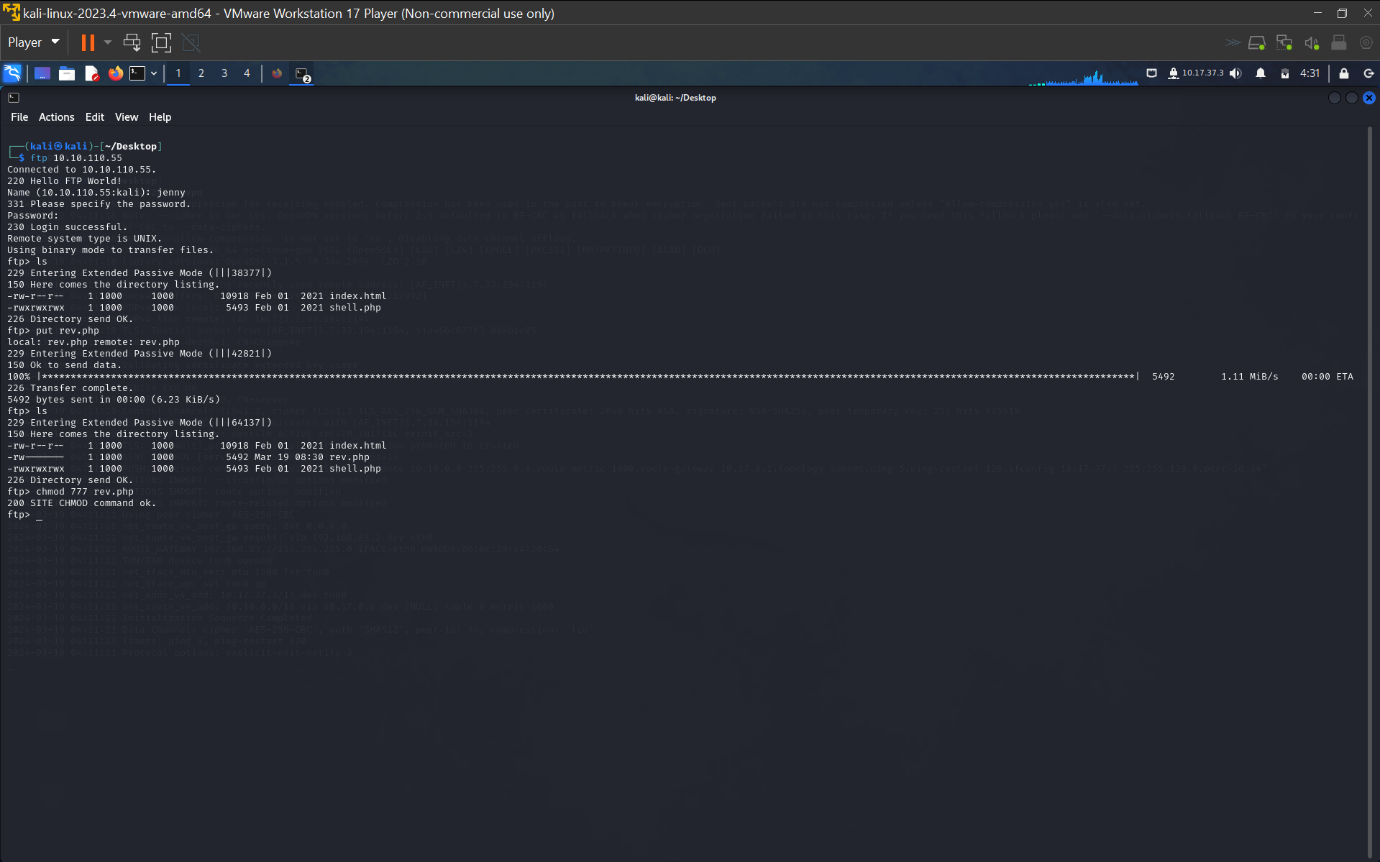
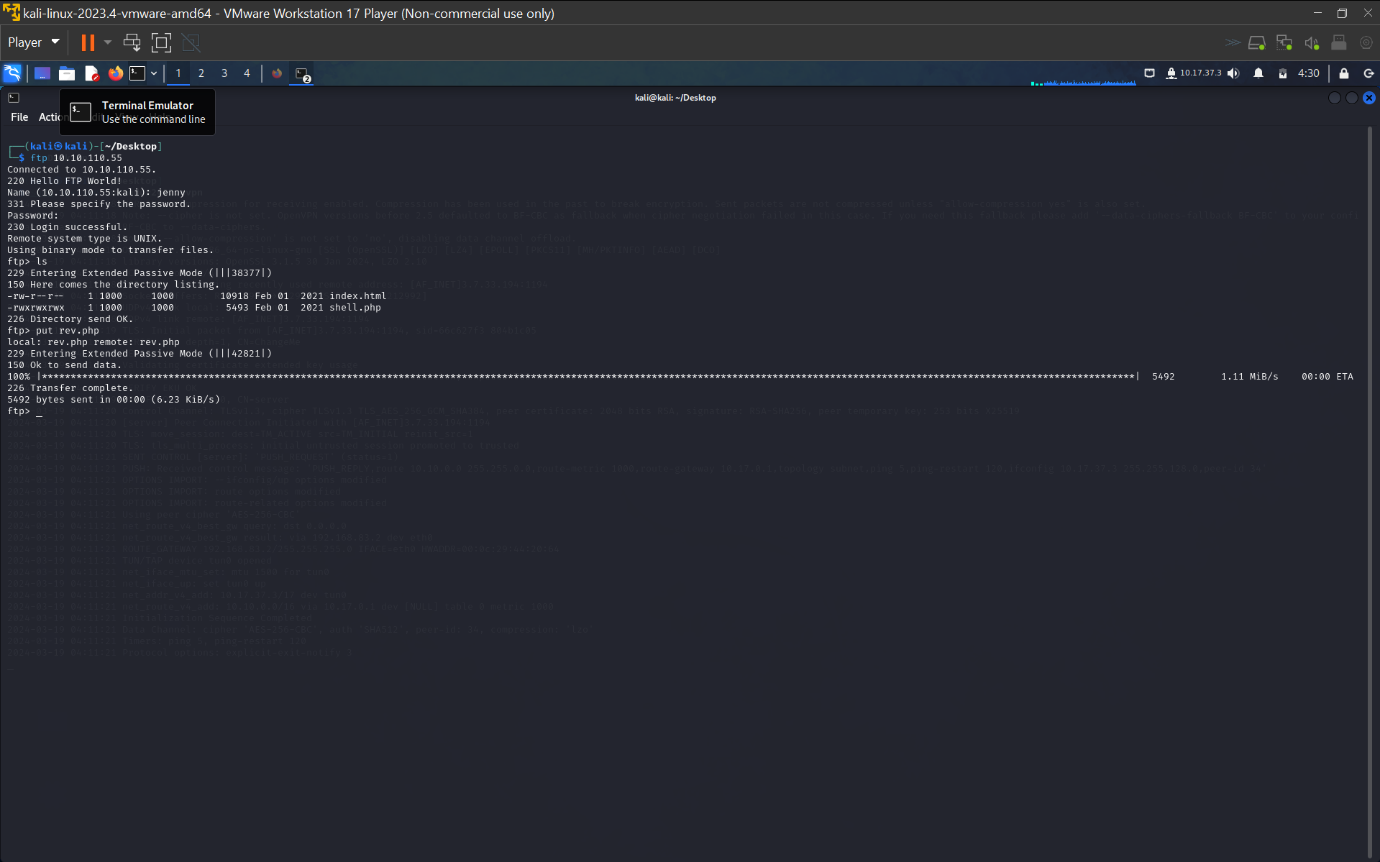
**After getting the php file and making the changes and As we have gained ftp access. now lets upload the php file into the ftp. Using the “put” command in ftp.**

* **Put <file\_name>(eg: put revshell.php)**

**After uploading the php file lets check for the file permissions, as it need execute file permission to run reverse shell. Use “ls -l”.**

* **The permissions will only be ‘-rw-------' change it to ‘-rwxrwxrwx’ permission. Using the command**
* **“Chmod 777 <file\_name>” or “chmod 755 <file\_name>”**

**After doing that check once and exit the ftp , just type “exit”.**

****

**Now that php file uploaded and given all permissions lets start the listener and**

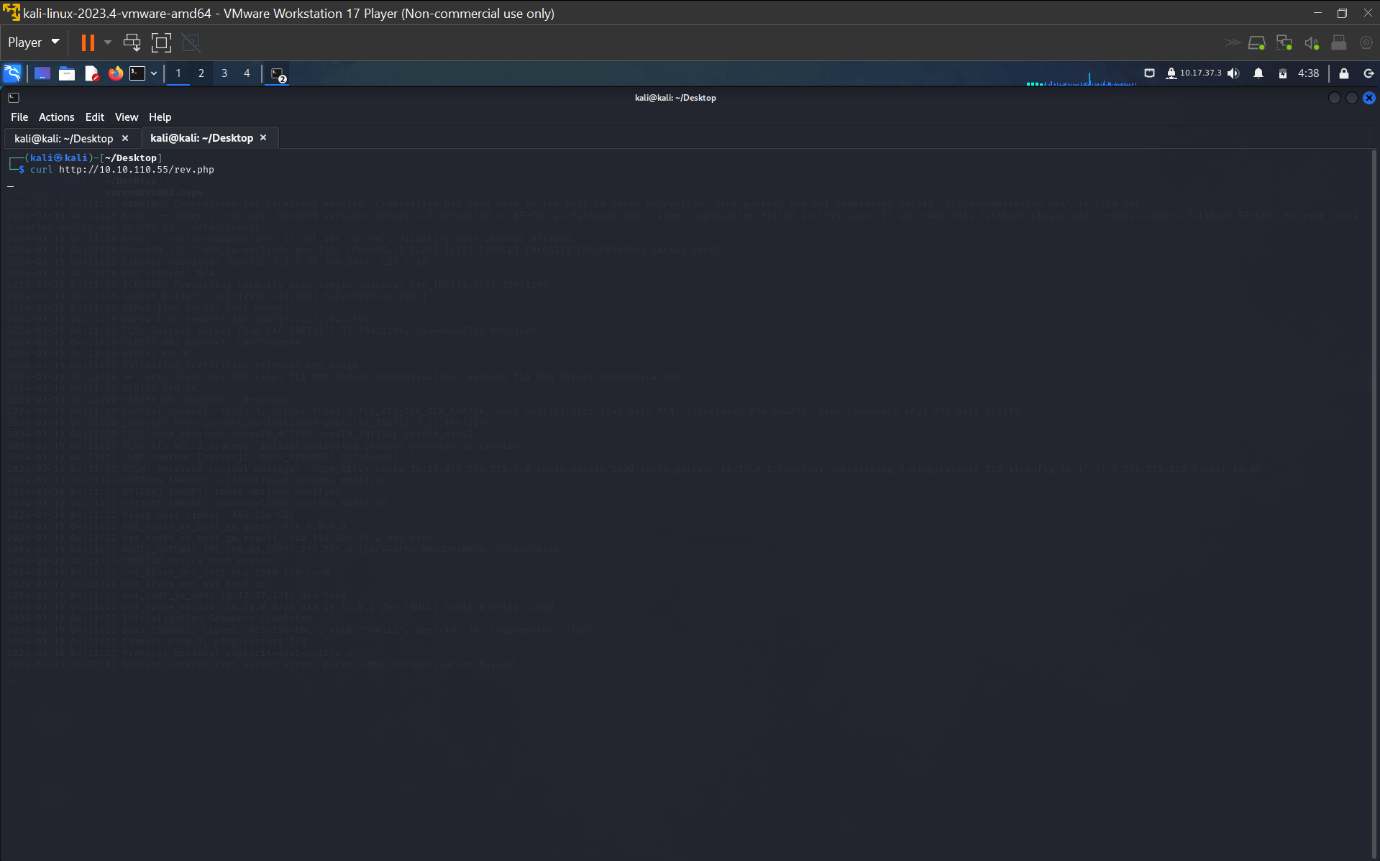
**Execute the reverse-shell file.**

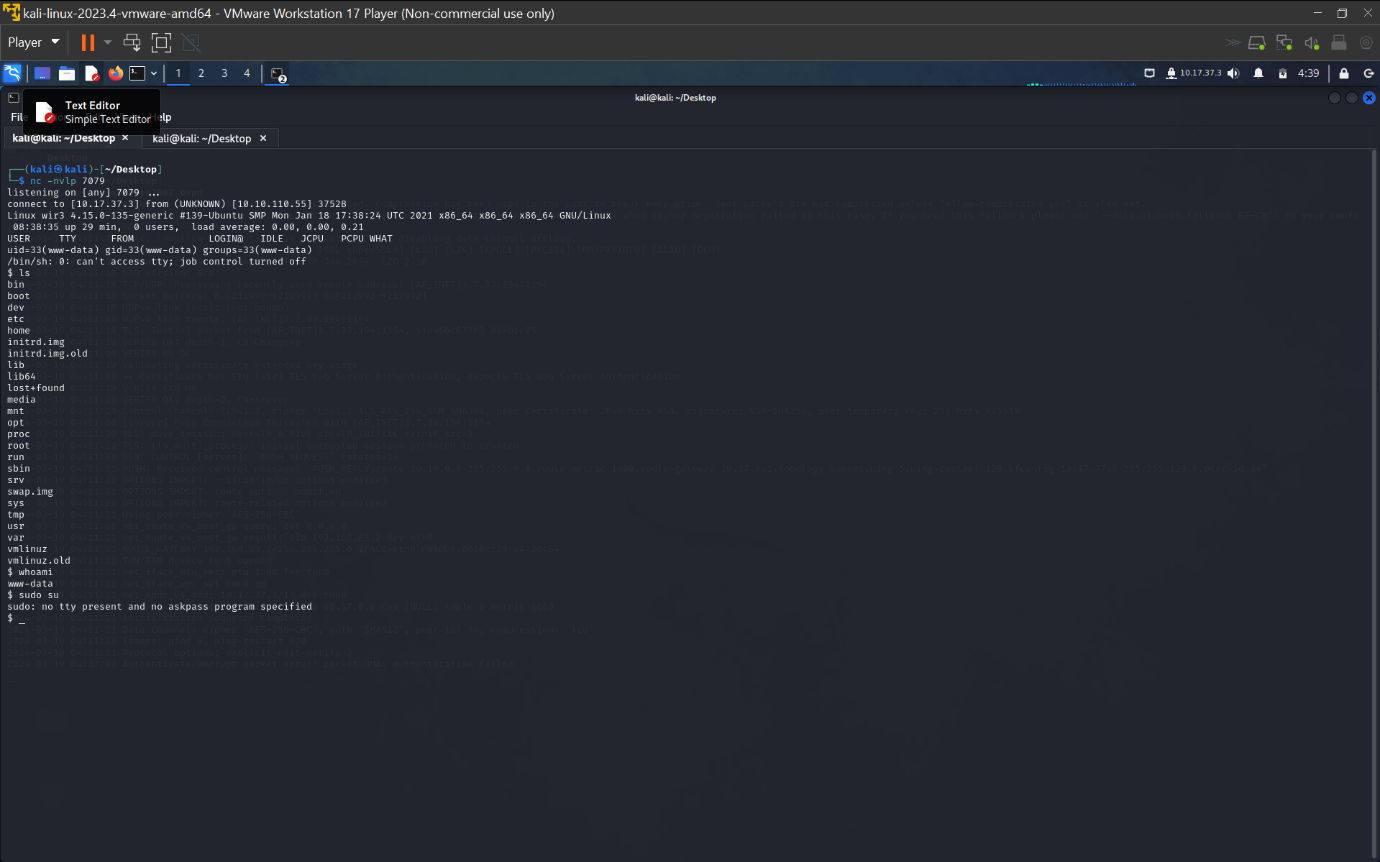
* **“nc -nvlp <portno.>” (here the portno. is 7079)**

**To run the ‘rev.php’(reverse-shell file) in ftp we can run 2 commands,**

* **“http://<target\_ip>/rev.php/” ( run this in the browser).**
* **“curl http://<target\_ip>/rev.php/” (run in a new terminal).**

**After the rev.php starts running , the listener will also start.**

****

**Lets check the username with “whoami”, ‘www-data’. **

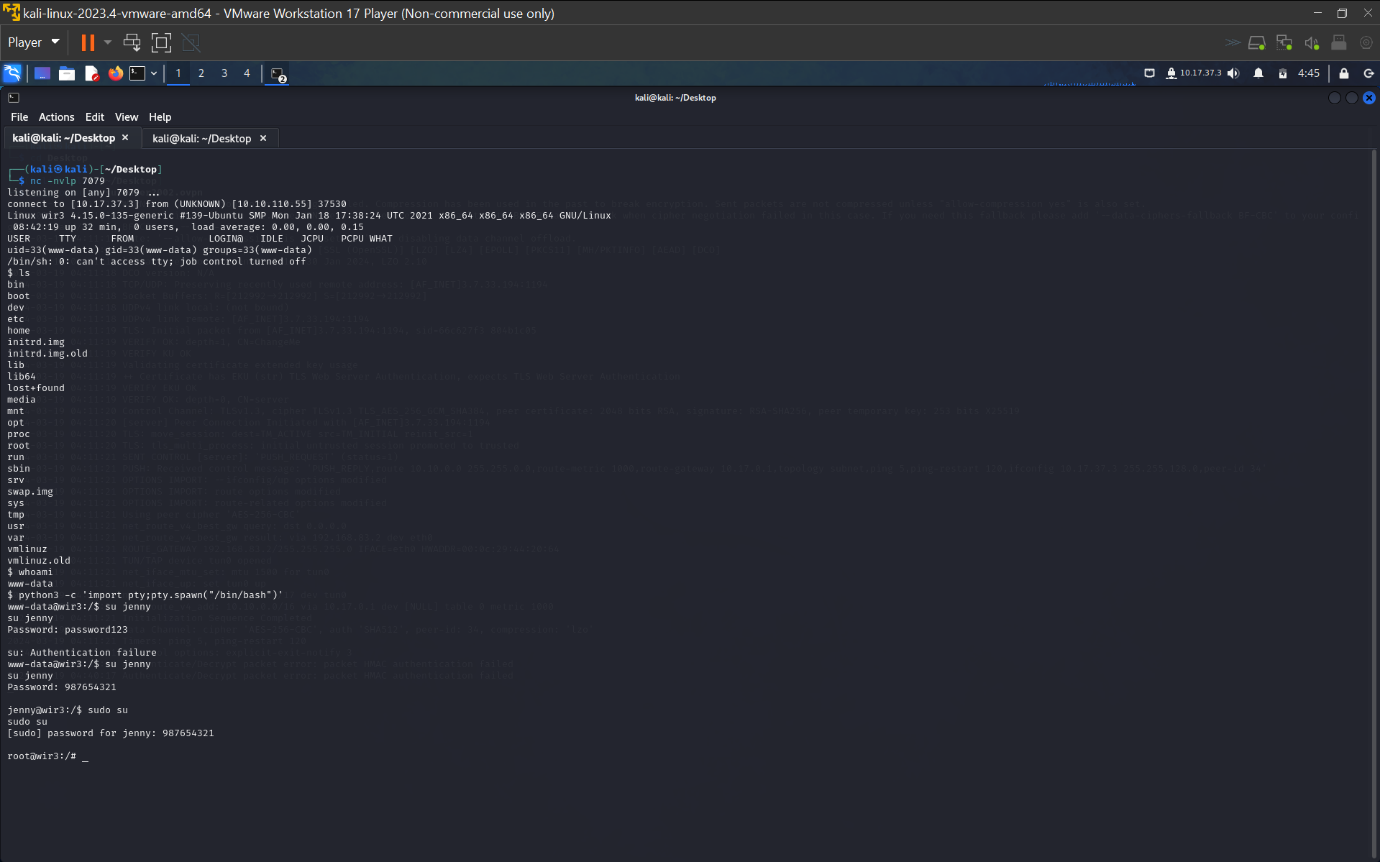
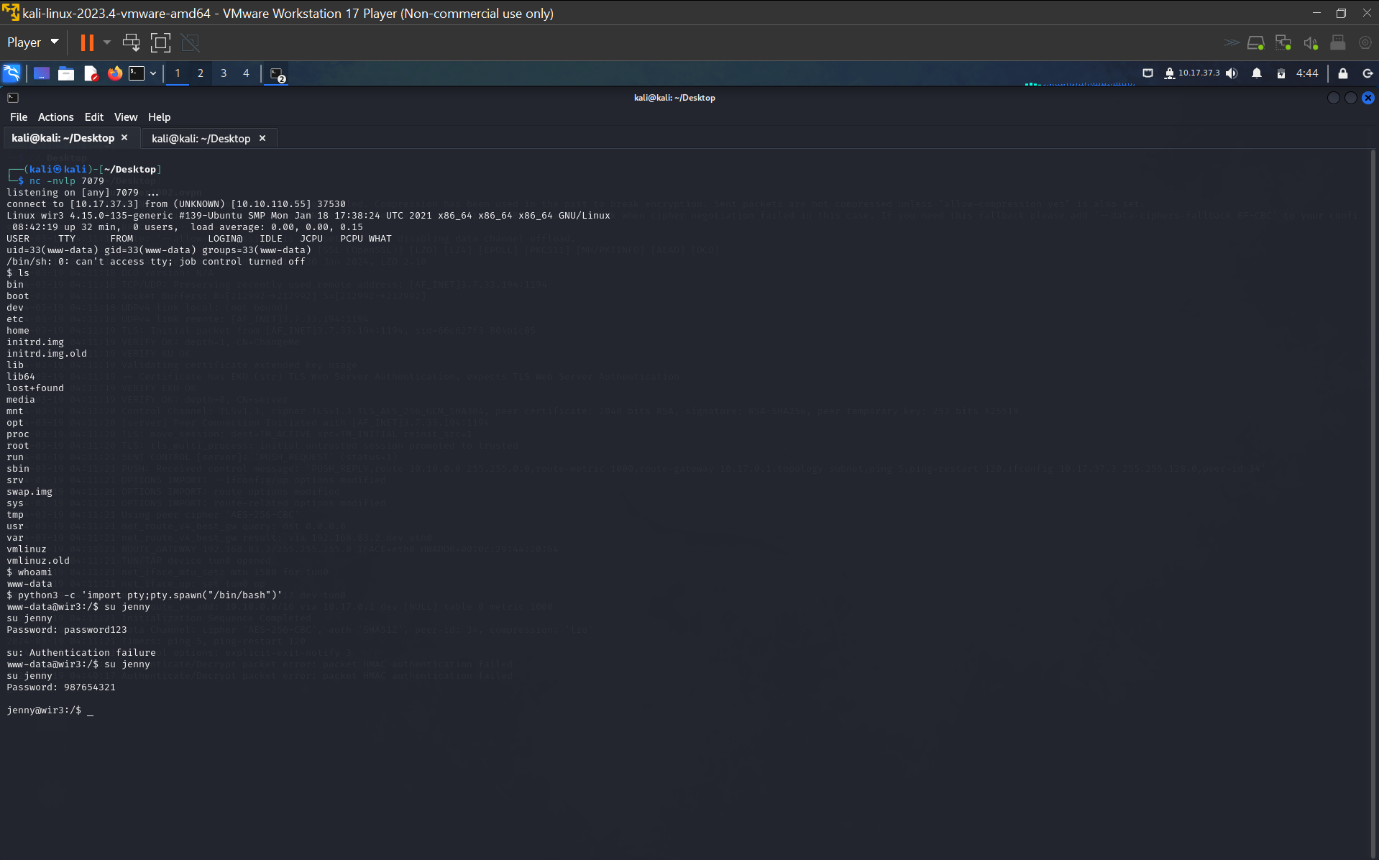
**Put it doesn’t have any sudo privileges to it, so lets give sudo privilege. Using the command ,**

* **“ python3 -c ‘import pty;pty.spawn(“/bin/bash”)’ ”**

**Now we have the sudo control , lets change the user to ‘jenny’.**

* **“ Su jenny ”(enter the jenny’s password).**

**Then again change to the root directory “sudo su”.**

****

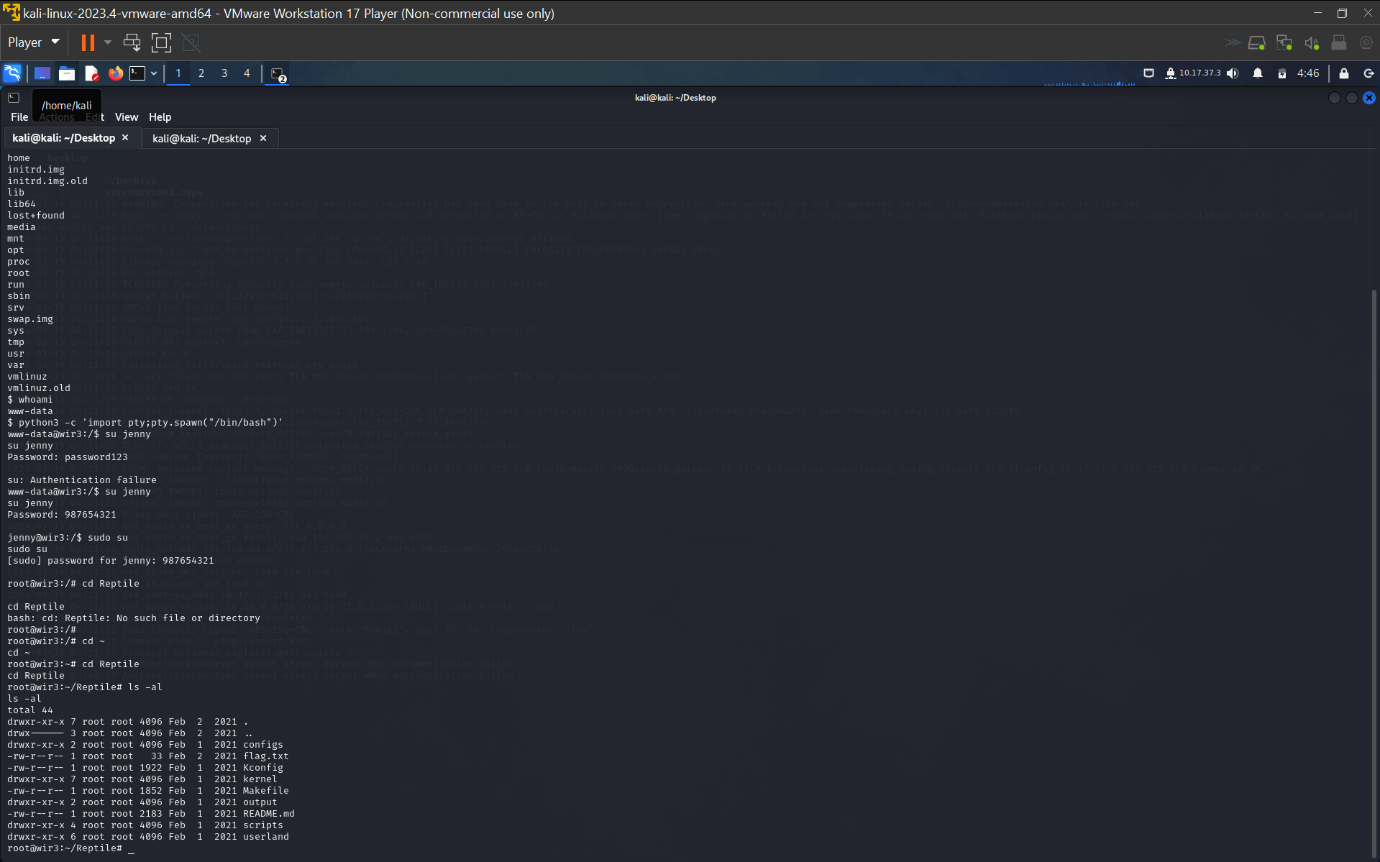
**Now that we have root access, lets find the flag.txt file from the system.**

**We can use the find command,**

* **“find / -iname <file\_name> 2>/dev/null”**

**Change the directory to the ‘Reptile’ with “cd Reptile”**

**And after the directory changed , doing “ls -al” we can list all the files and directories in the current directory.**

****

**As got the list of files the directory, we can now see the flag.txt file.**

**Lets extract the hash from it, use the “cat <file\_name>” to do so.**

****

**RESULT:**

**The pentesting of the company revealed that their system is vulnerable and can be exploited in the following way the outcome of the exploit revealed that an attacker can become the root controller of the system and run as a root user ,**

**Which leads to full access of the system to the attacker and compromises the users system and possess a high risk on the users sensitive information.**