**ETHICAL HACKING LAB PROJECT**

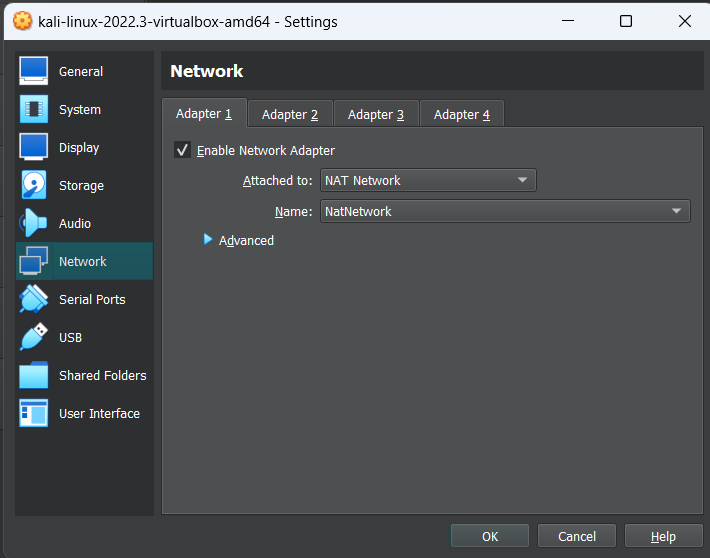
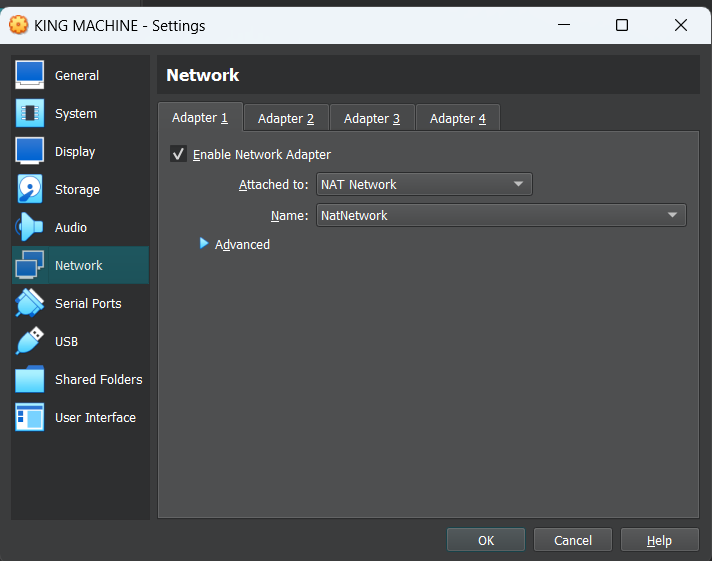
**VULNERABLE BOX CREATION AND EXPLOITATION**

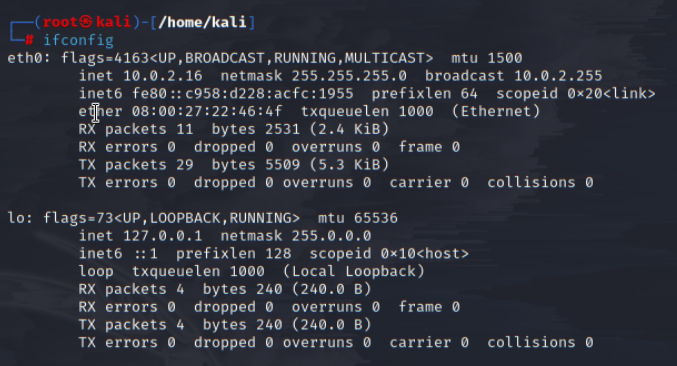
21PC15-HARSHAD KRISHNA B S

21PC33-SHANJU SHREE A

**KING BOX WRITEUP:**

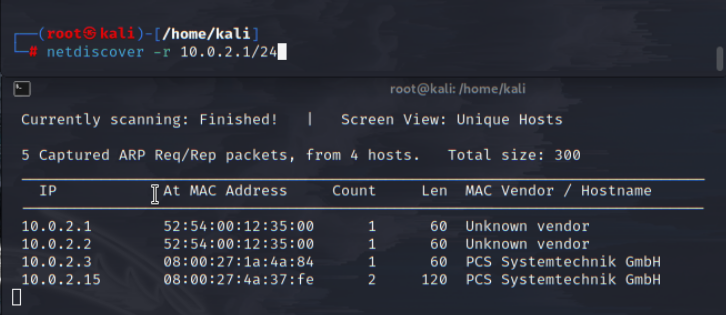
* This machine was tested with network adapter **NAT Network**.
* Both Attacker machine and the victim machine are connected to same **NAT Network**.

**** ****

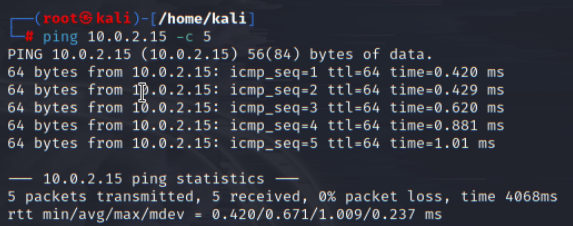


**Reconnaissance:**

* Start the netdiscover to find victim machine IP.

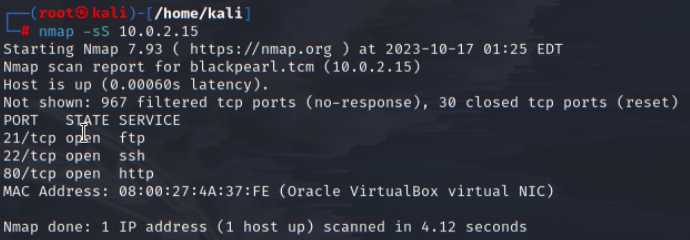


* Here you can see the IP 10.0.2.15, which could be the possible IP of the victim machine.
* Ping and see if the host is reachable or not.



**Scanning:**

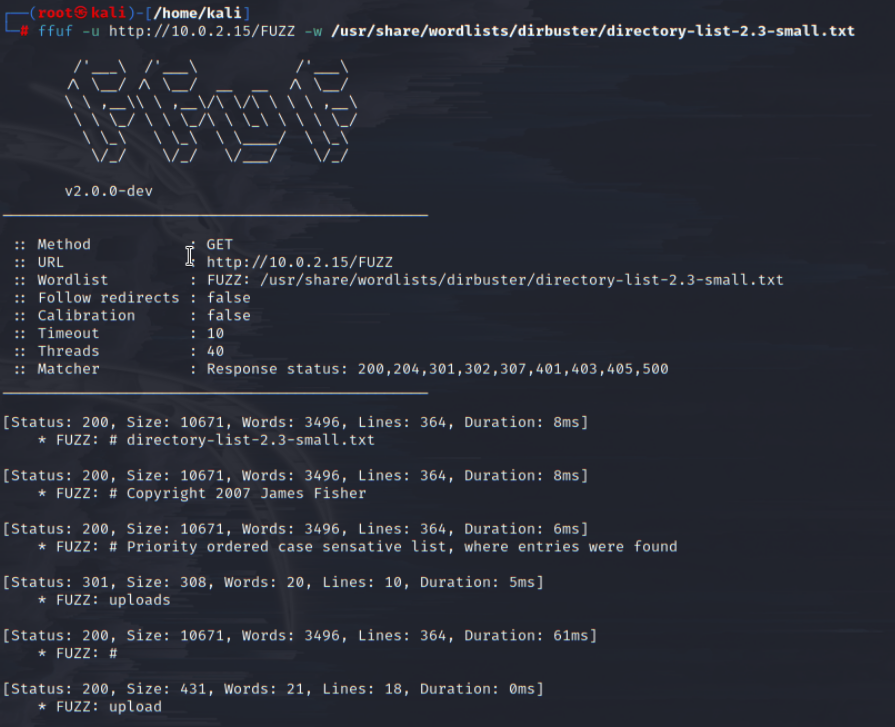
* Start the nmap scan to find the open ports in the machine.
* You can add more options if needed, like making a scan to all ports by “-p-” option or running all the scripts with option “-A” and finding the OS of the machine.

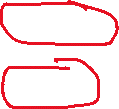


* As the port 80(http) is open we can see a html page from our browser.

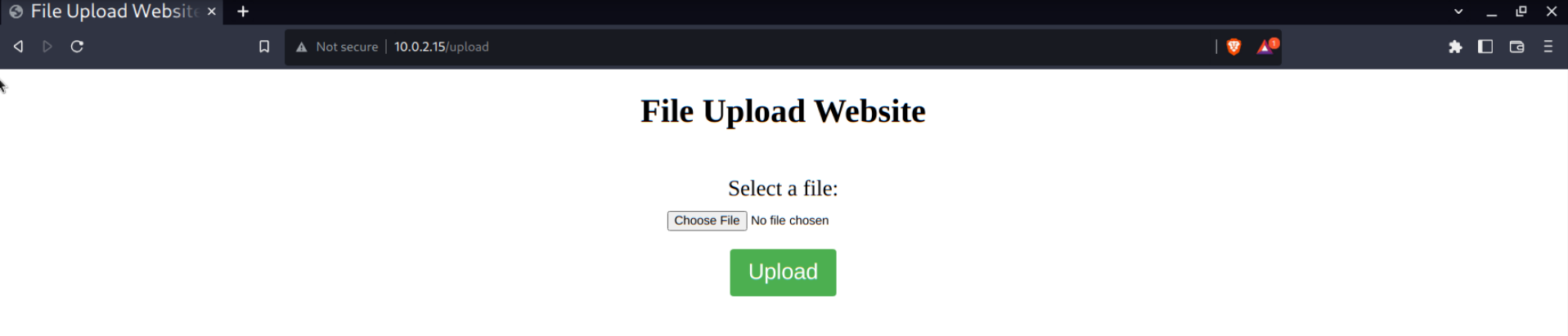


* Now scan for hidden directories using FFUF tool or any other directory Brute-forcing tools.



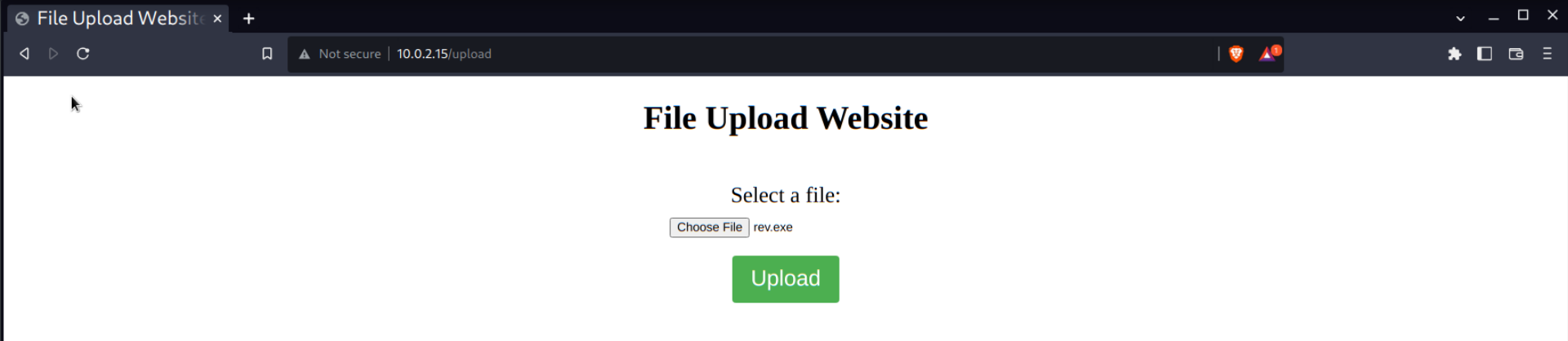


* We found the directories upload and uploads hosted on the victim’s machine.



**Exploitation:**

* Now, we will try uploading rev.exe reverse shell to the website.
* Here we can see it only accepts .jpg, .jpeg, .png.gif. This shows that there is a filter in the upload.php and now we can also conclude that the website runs on php.



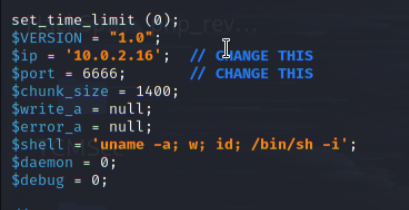




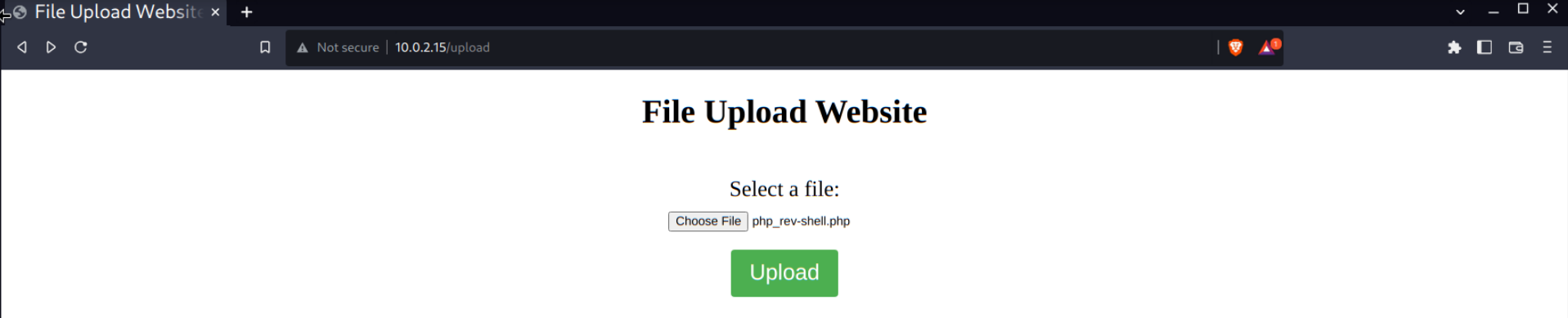
* Let’s try uploading a php reverse shell from the below resource link.

<http://pentestmonkey.net/tools/php-reverse-shell>

* Make sure you change the IP and port number of the shell code.

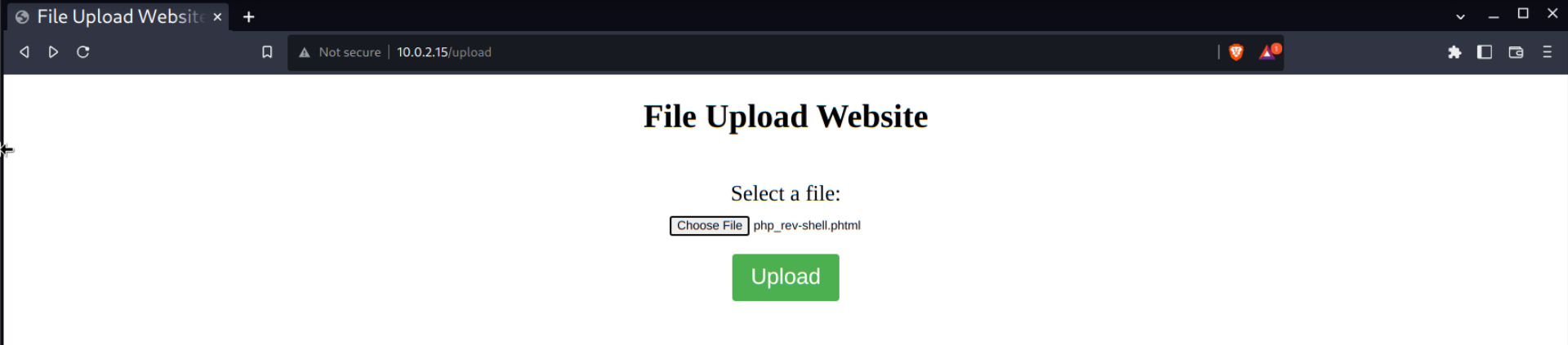


* Now we can see the webpage does not allow .php files also.

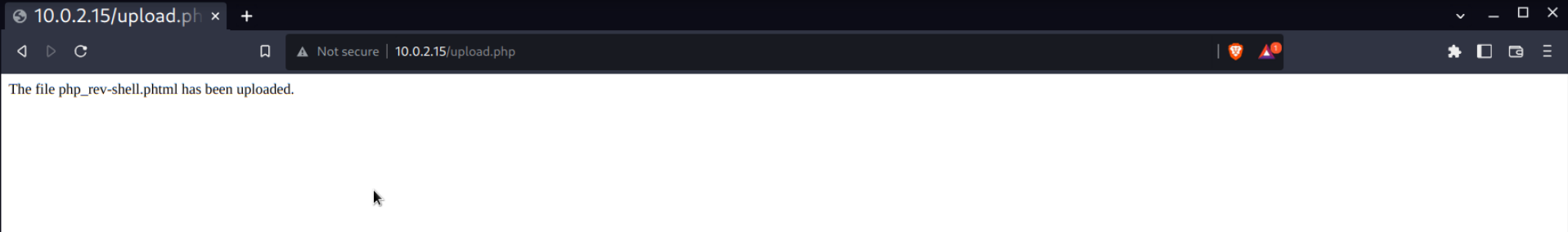




* Therefore, let’s try uploading .phtml file to the webpage.



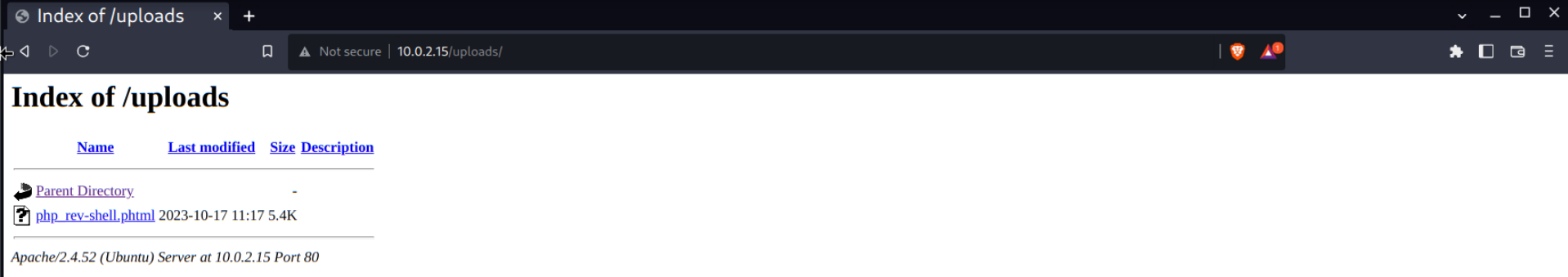
* Now the .phtml file is been uploaded.

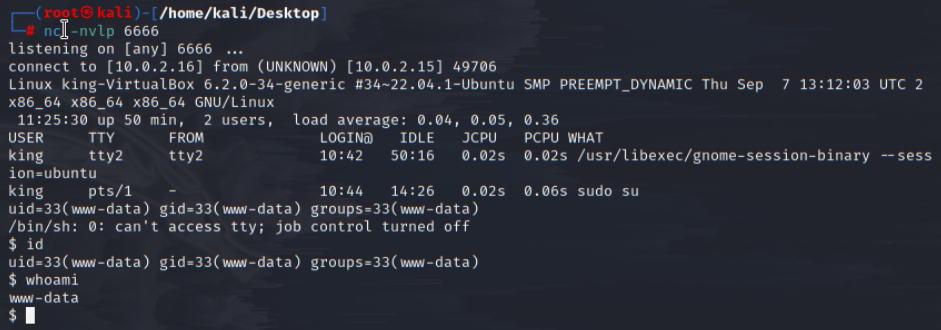


* Set up a netcat listener to listen for the incoming reverse shell connection from file we uploaded. **Note:** Enter the correct port number same as the one mention you mentioned in the reverse shell file



* Now run the .phtml file by just clicking the file in the uploads directory.

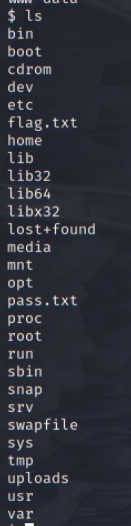




* Now you got the shell for the victim machine. But the shell belongs to the user www-data, we should try escalating the privilege to any other user.



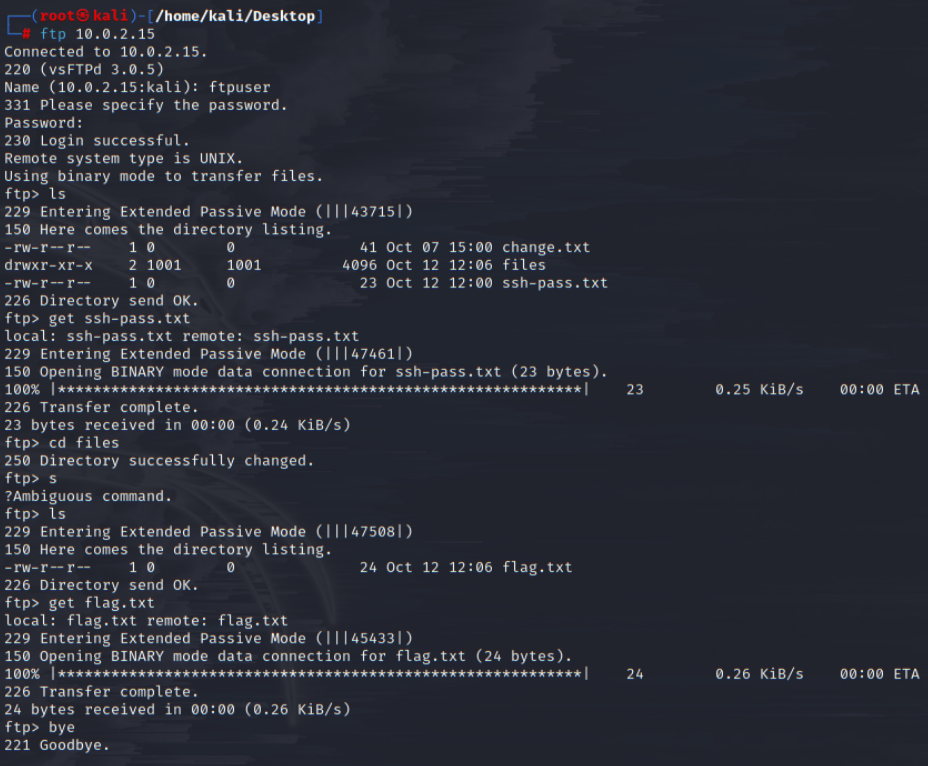
* From the listed files you can see the file, flag.txt and pass.txt.

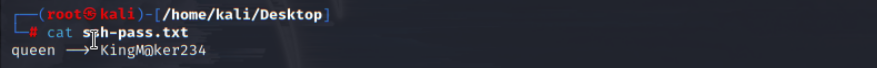


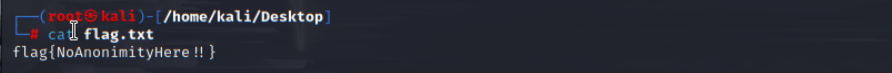
flag{F1leUploader$uck3d}



* We can see a file named pass.txt, which contains username password for the ftp server. Now we shall try connecting to the ftp of the victim machine.

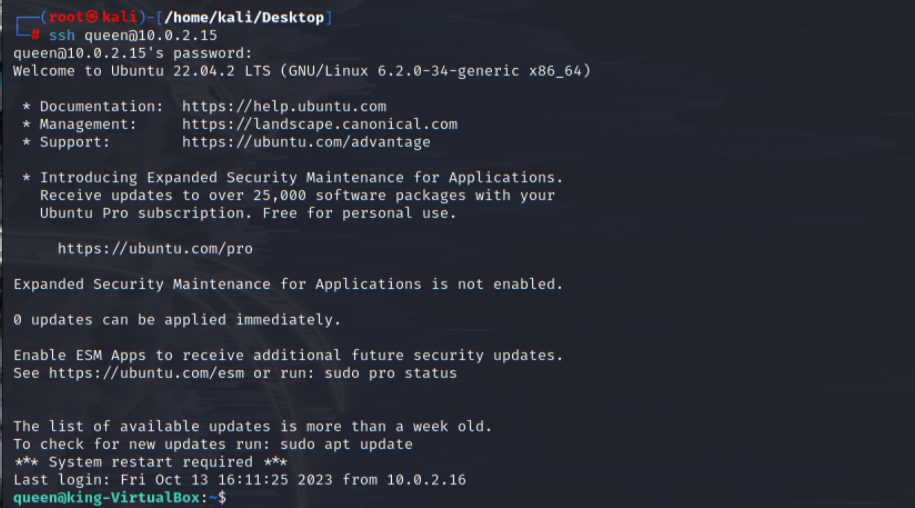


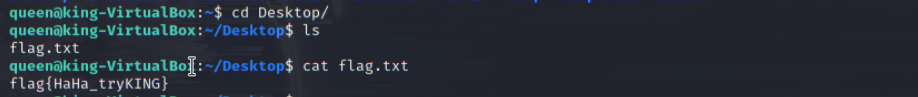




flag{NoAnonimityHere!!}

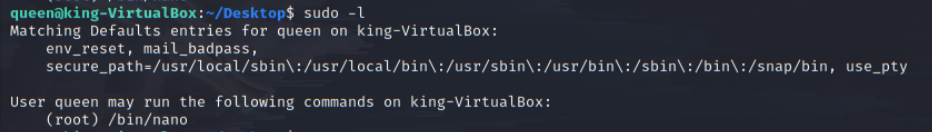
**Privilege Escalation:**

* Now we got the SSH credentials for the user queen now we will try logging in to that machine.
* We can find the flag in the Desktop of the Queen



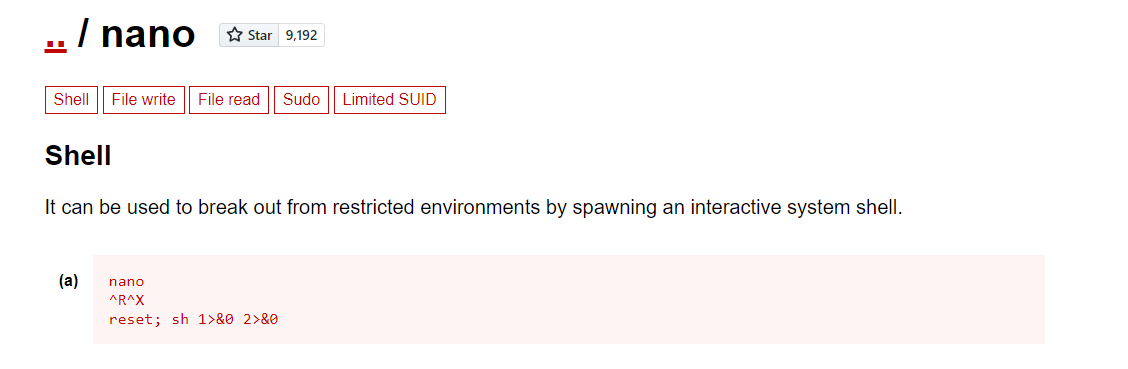
flag{HaHa\_tryKING}

* Let us try escalating our privileges from here, try running the sudo command and find the binaries which we can run as a sudo user.

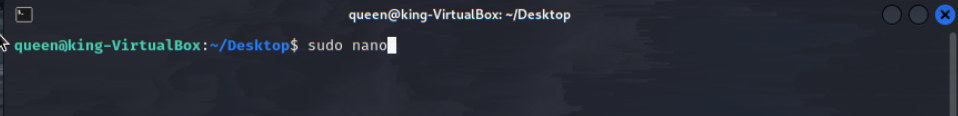


* Here we can see that the binary “nano” can be run by the queen as the super user in this machine.
* Let’s now find a way to escalate using the commands given in the GTFObins.  
  **Note:** Read the article to find new ways to escalate using the nano binary.

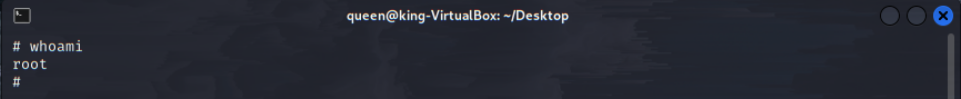
<https://gtfobins.github.io/gtfobins/nano/>



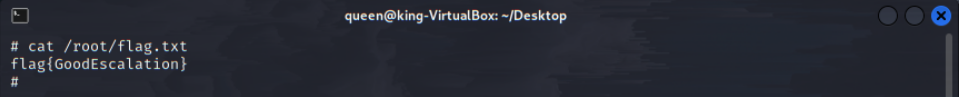
* Try entering the commands to spawn the root shell.







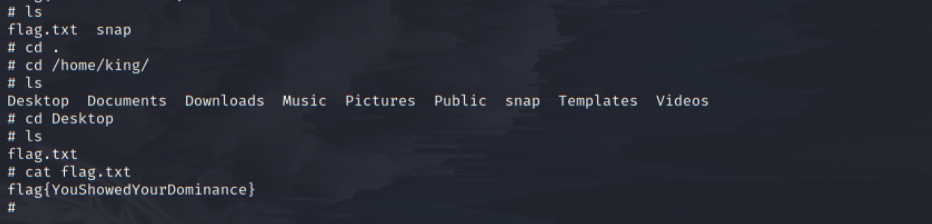
* Now we spawned a root shell for the victim machine. This shows that the KING box is fully conquered.



* You can go into /root directory for the flag.

flag{GoodEscalation}

* And /home/king/Desktop for the other flag.

flag{YouShowedYourDominance}

**Credentials :**

**KING - rul1ng@123**

**ftpuser - FTPisM1n3%%%**

**QUEEN - KingM@ker234**

**Flags :**

**flag{F1leUploader$uck3d}**

**flag{NoAnonimityHere!!}**

**flag{HaHa\_tryKING}**

**flag{GoodEscalation}**

**flag{YouShowedYourDominance}**