BIOS PENTESTING

**VulnSphere Task**

Write-up

horizontal line

# 

***-Flag1:ftp***

*1.Used* ***NMAP*** *tools and found out the open ports and their port numbers.*

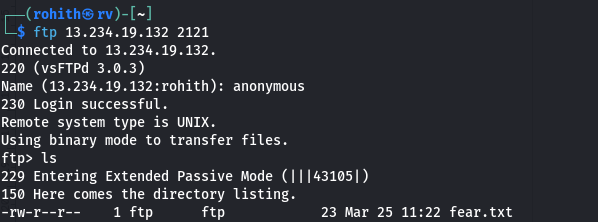
*2.For this flag,I found out the ftp port number i.e shown ccproxy-ftp open at port 2121.*

*3.After that opened fear.txt by downloading it to my local machine by using*

*>get fear.txt*

***flag{fe4r\_1s\_n0t\_3v1L}***

*Ref:*[*https://thefluffy007.com/category/boot2root*](https://thefluffy007.com/category/boot2root/)

**

***-Flag2:http***

*1.Checked the* ***NMAP*** *for the http open port which is shown as http-alt is open at port 8000.*

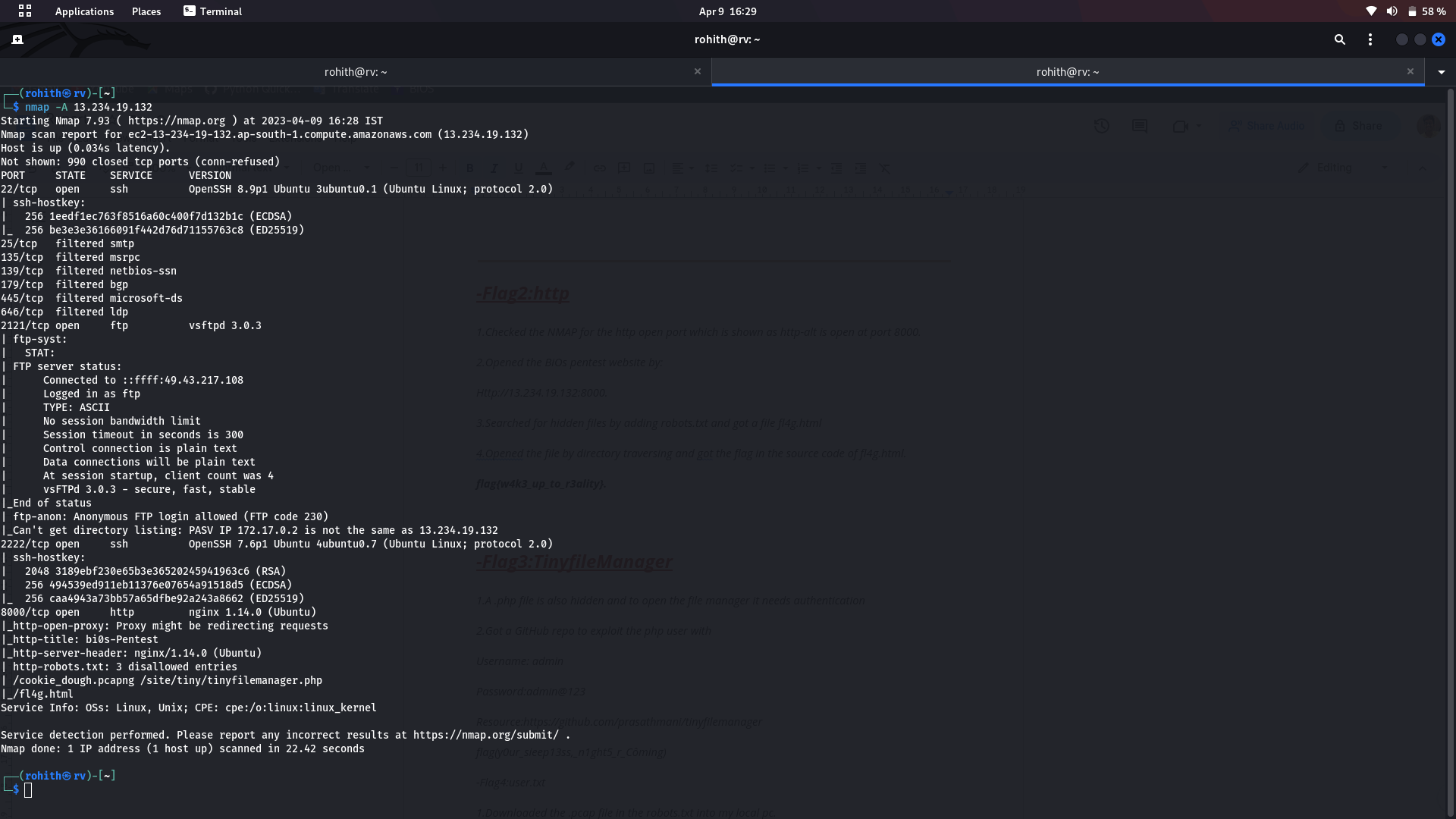
*2.Opened the BiOs pentest website by:*

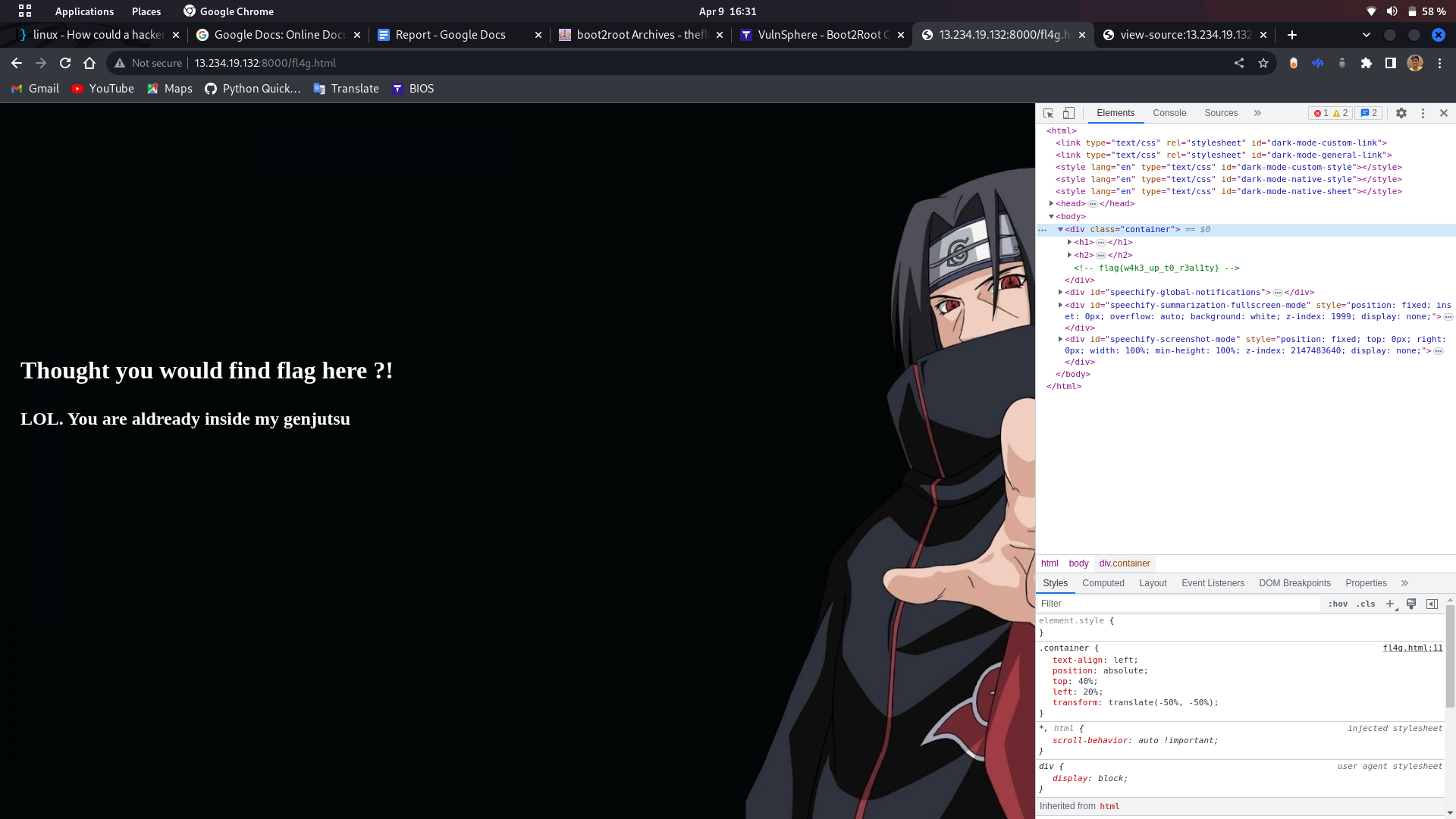
***http://13.234.19.132:8000.***

*3.Searched for hidden files by adding robots.txt and got a file fl4g.html*

*4.Opened the file by directory traversing and got the flag in the source code of fl4g.html.*

***Flag{w4k3\_up\_to\_r3ality}.***

******

******

***-Flag3:TinyfileManager***

*1.A .php file is also hidden and to open the file manager it needs authentication*

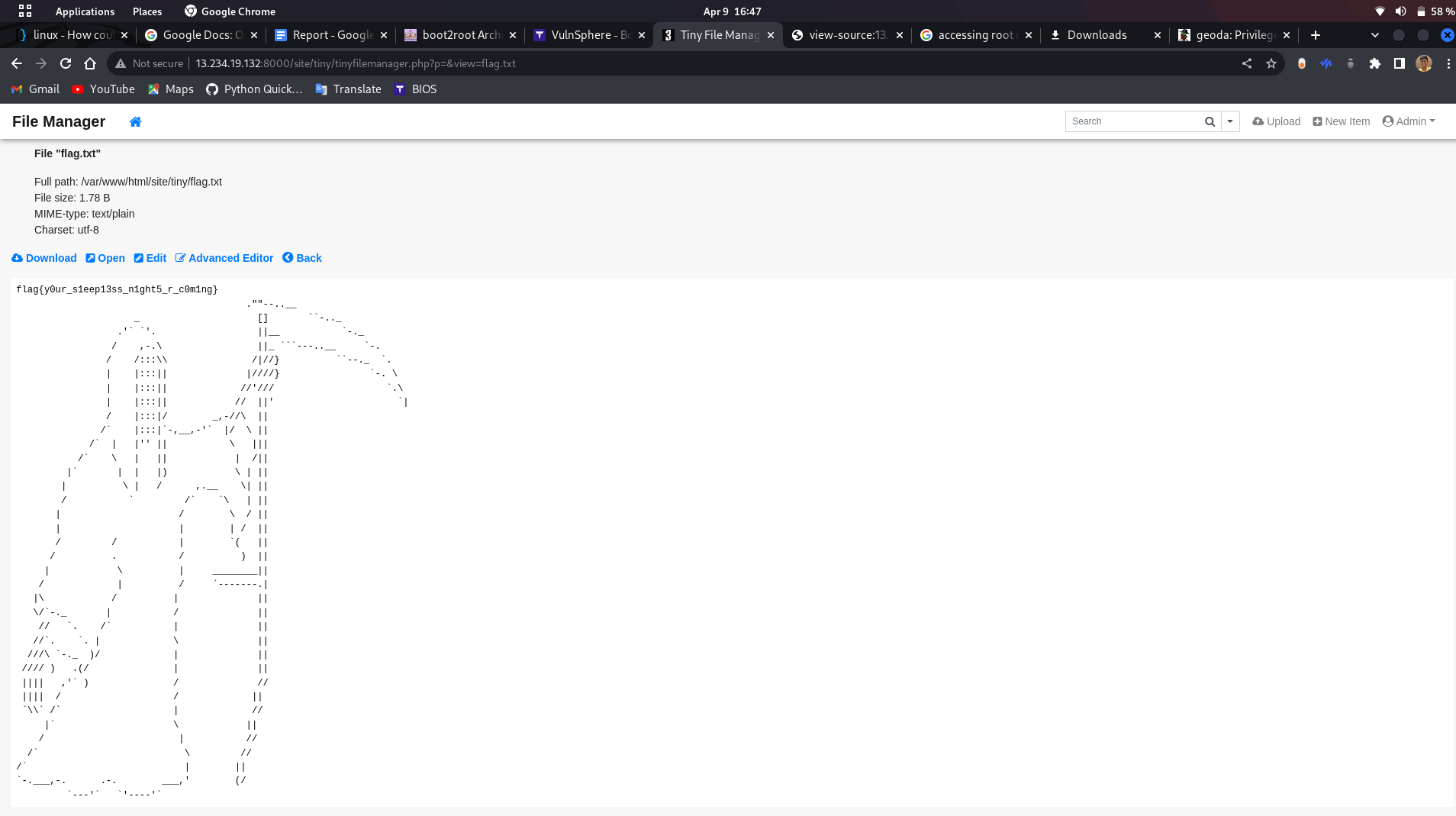
*2.Got a GitHub repo to exploit the php user with*

*Username: admin*

*Password:admin@123*

***flag{y0ur\_s1eep13ss,\_n1ght5\_r\_C0m1ng}***

***Ref:https://github.com/prasathmani/tinyfilemanager***

******

***-Flag4:user.txt***

*1.Downloaded the .pcap file in the robots.txt into my local pc.*

*2.Opened the file in wireshark.*

*3.Used http filter.*

*4.And analyzed by following tcp protocol to get the username and pass for ssh login.*

***Ref:https://unit42.paloaltonetworks.com/using-wireshark-identifying-hosts-and-users/***

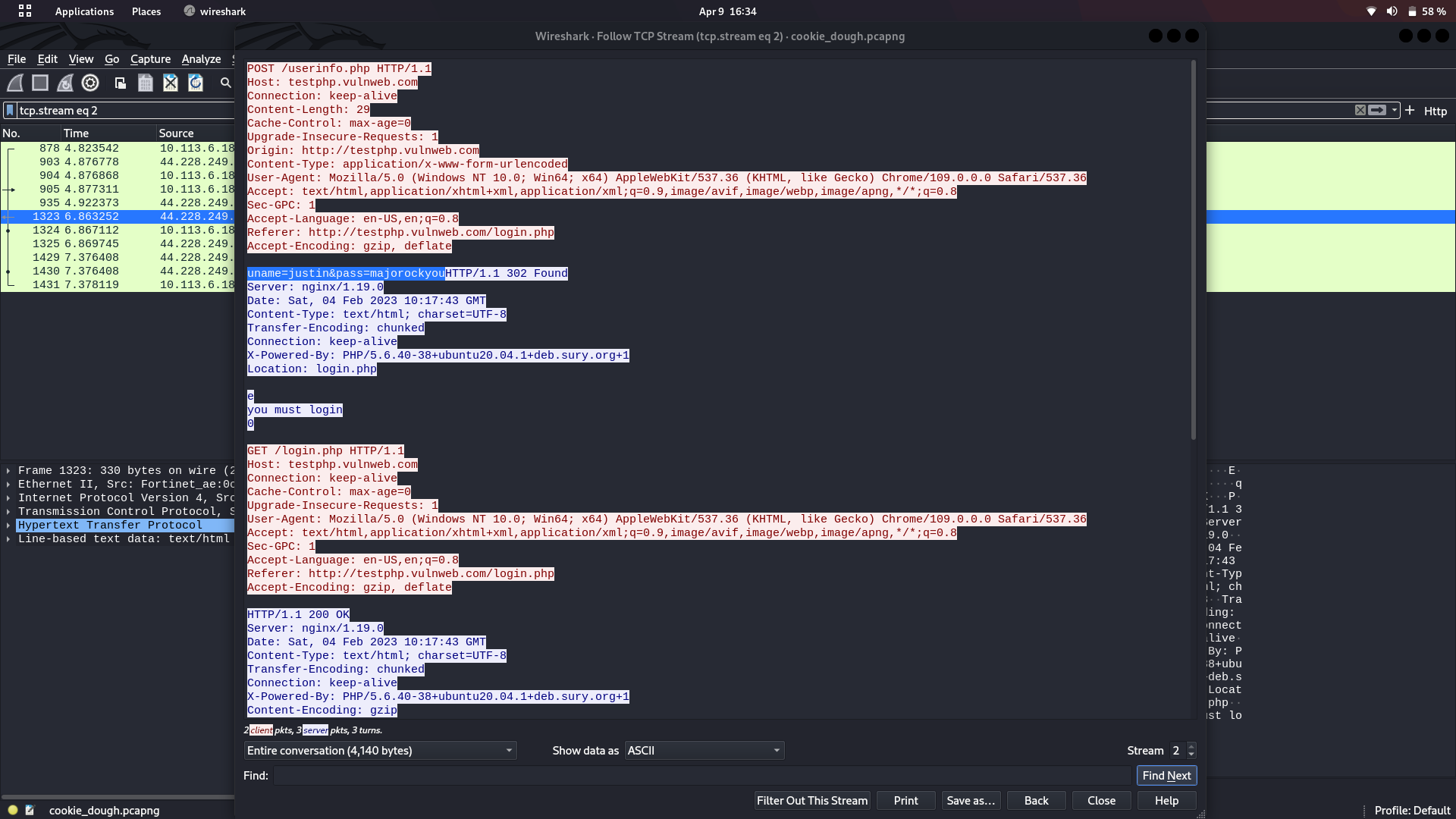
***>ssh justin@13.234.19.132 -p 2222***

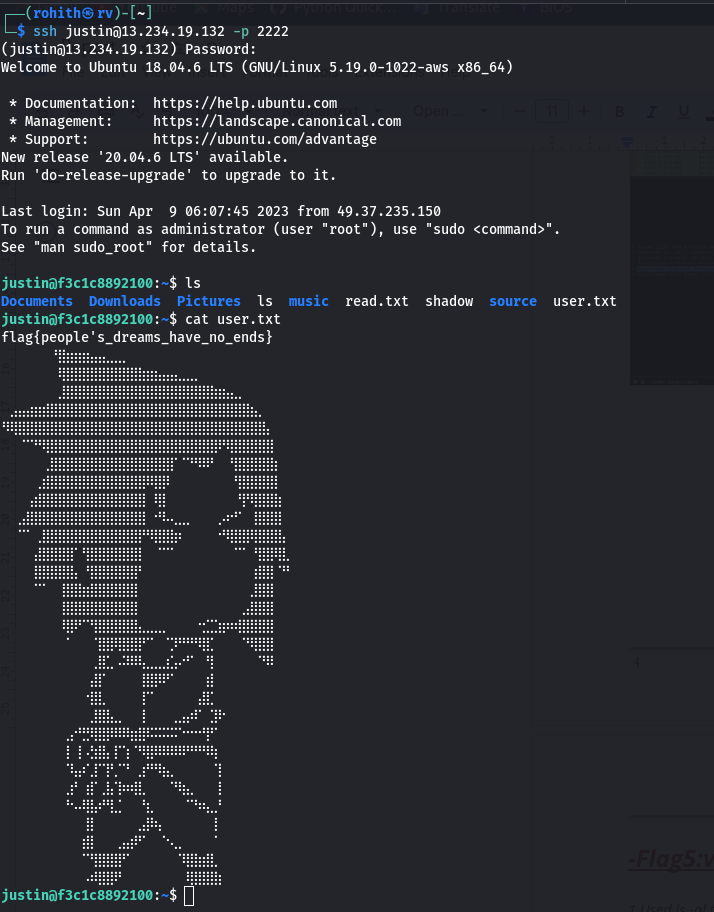
***password:majorockyou***

*5.Used ls to list all the files/Directories.*

*6.User.txt has the user flag.*

***flag{people's dreams\_have\_no\_ends}.***

******

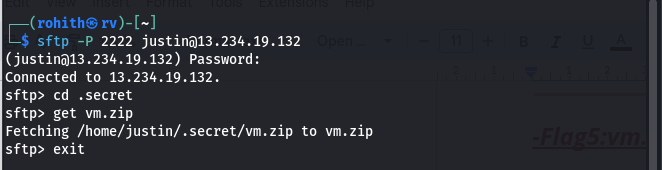
**

***-Flag5:vm.zip***

*1.Used ls -al to long list all the hidden files and found a .secret directory*

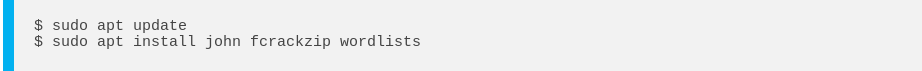
*2.Traversed into the directory by using cd and found a zip file in it which was unable to unzip in the server.*

*3.So used* ***sftp*** *and downloaded the zip file into my local computer.*

**

*4.While unzipping it asked for authentication to unzip.*

*5.Cracked the password by running John ripper it automatically uses its word list to find the password.*

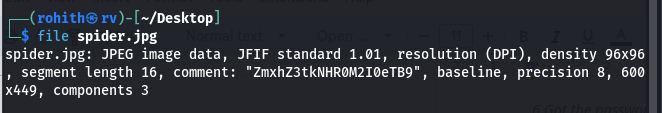
**

*6.Got the password as* ***qwretyio.***

*7.Searched for hidden info inside a jpg in Google and got a blog related.*

*8.Used file spider.jpg and then got a code in comment section.*

*9.When the code is pasted in a cipher analyser it shows it is* ***base64 encoded*** *then decoded it and got the flag.*

**

***flag{d4tt3b4y0}***

***ref:***[***https://linuxconfig.org/how-to-crack-zip-password-on-kali-linux***](https://linuxconfig.org/how-to-crack-zip-password-on-kali-linux)

***-Flag6:root.txt***

*1.Found a blog about exploiting privilege of user and learned about /etc folder.*

*2.Shadow contains hashes of the passwords of the users.*

*3.Hash code is a one way function so instead overwritten the shadow by* ***cat > /etc/shadow***

*Changed the hash of root to same as justin.*

*4.Logged into root by su command and listed the total files in which root.txt file consists of the flag.*

***flag{one\_piece\_does\_exist!!)***

***Ref:***[***https://blog.geoda-security.com/2019/02/privilege-escalation-exploiting-write.html***](https://blog.geoda-security.com/2019/02/privilege-escalation-exploiting-write.html)

### 

### 

### ROHITH VARMA DATLA

### rohithvarmadatla12@gmail.com