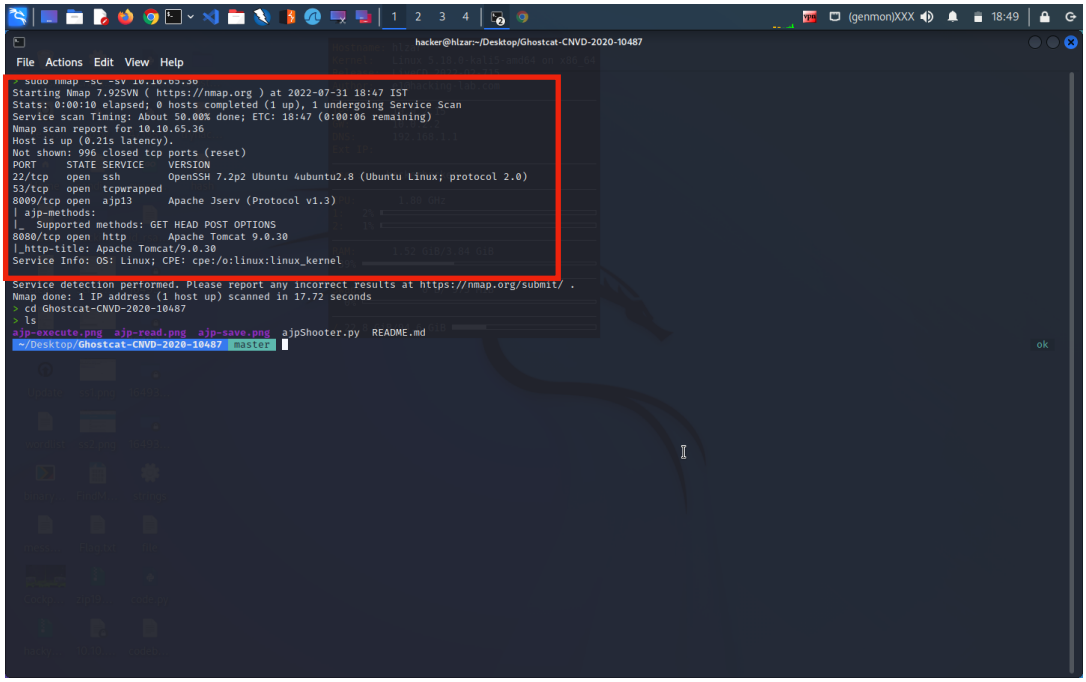
TomGhost Writeup

By Sandip Banerjee

Hi this is a beautiful box given by Tryhackme this box type is boot2root box there has many interesting steps like

1.Information Gathering
2.Enamuretion
3.Exploitetion

Step1:

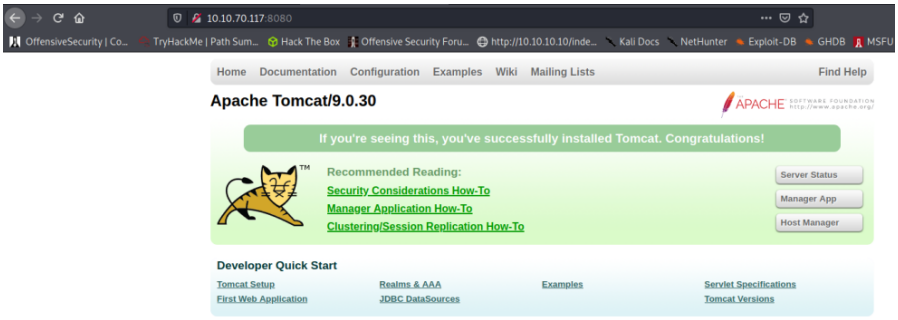


I gather information about the given ip address with the Nmap tool the command is-

- nmap -sC -sV <IP_ADDR>

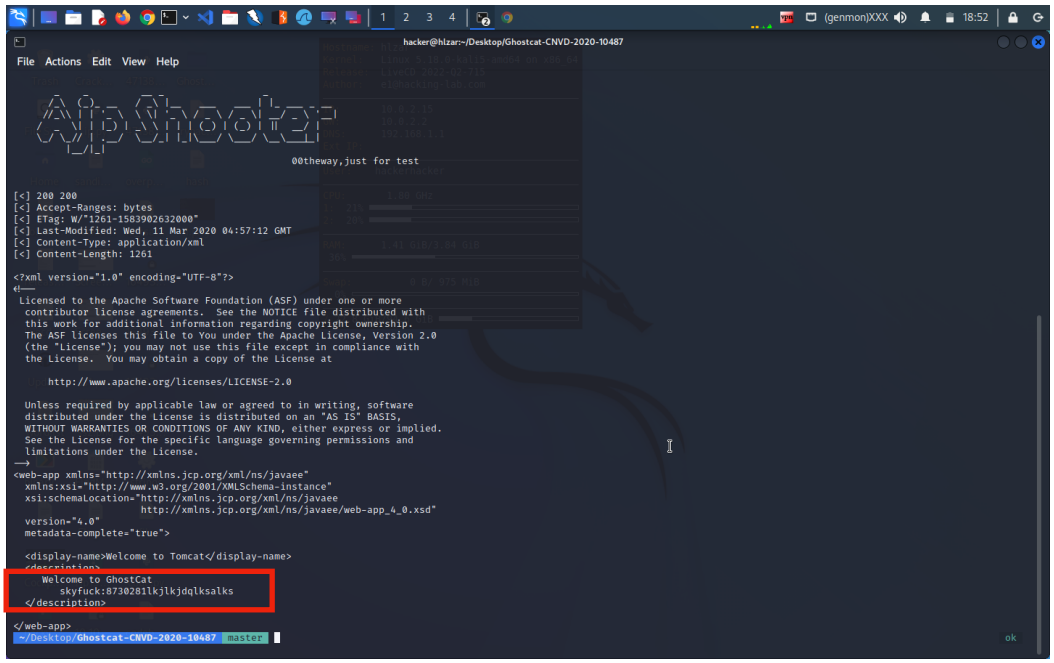
We get the 3 ports are open and 3 services are running in the 3 ports in port 22 ssh, in port 8009 ajp13 and in port 8080 http are open so now our clean target is to exploit the ssh port so we need the password and username for the ssh port.

The http page is



Step2:

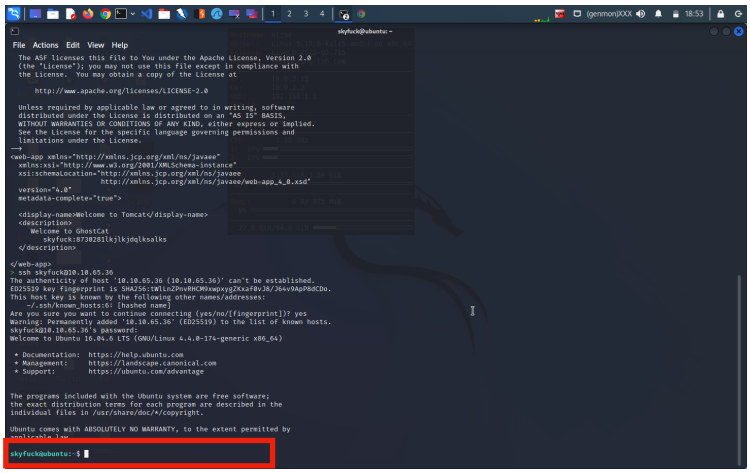
In this step 2 firstly I use a tool named ajpshooter Witten in python and take the information about the service also in the process we found the username and the password of the ssh server machine.



In the process we found the tool from GitHub and we use the following command-

- python3 ajpshooter.py http://<ip:port> 8009 /WEB-INF/web.xml read

Here we see the id and password skyjack:<password> at the marked place



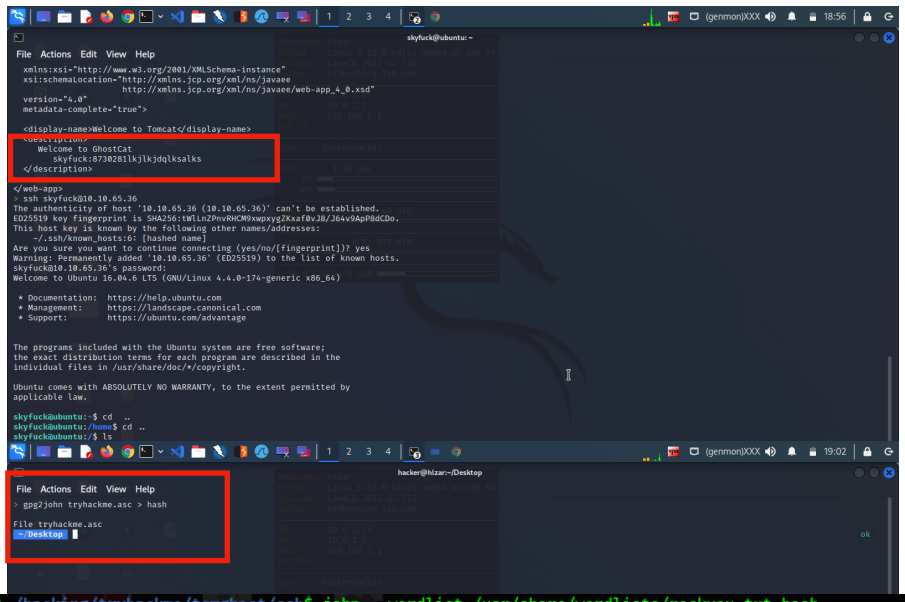
Step3:

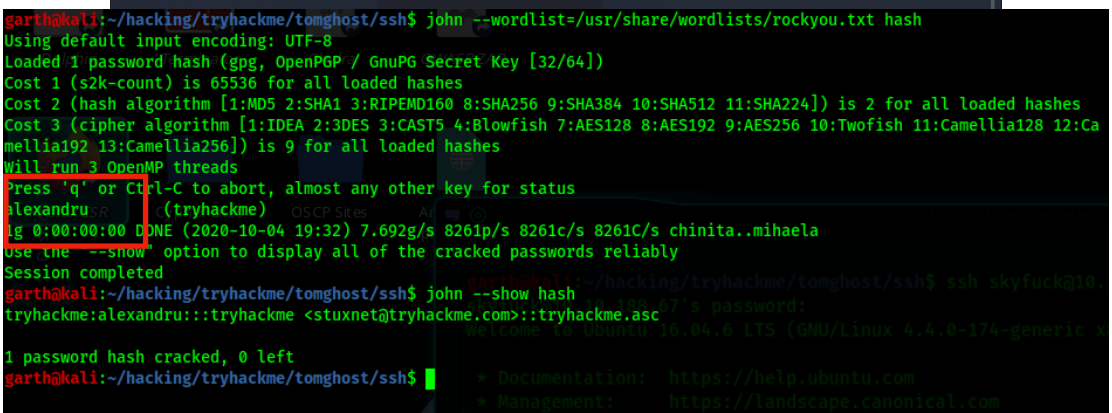
Now we login to the machine with the login credentials which is skyfuck an the <password> the login command is

- ssh skyfuck@<IP>
- Yes
- <password>

Step4:

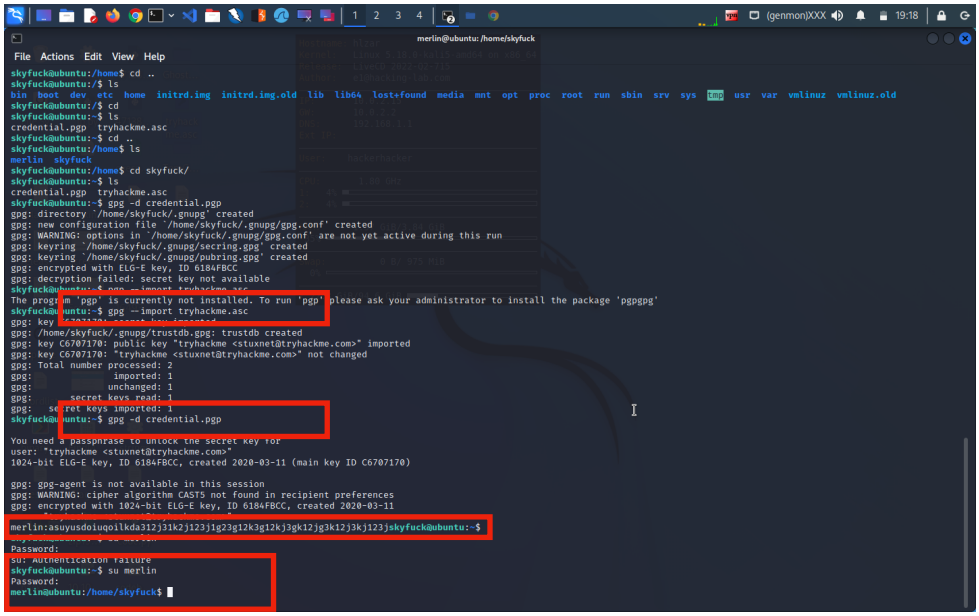
We found two files in the user with ls command we can see the file in the user and the file extensions are .asc and .pgp so we se in the tryhackme.asc file a big code types then we coy the file and make a hash file with john2pgp tool and try to crack the hash





Step4:

After getting access to the ssh server and find out the passphrase or decode the password we go for the ssh server and find the another user called merlin and try to find out the merlin password
Firstly we try to import the credentials and then try to decrypt the .pgp file after decoding the file with gpg command we found the ssh name called merlin and the password.

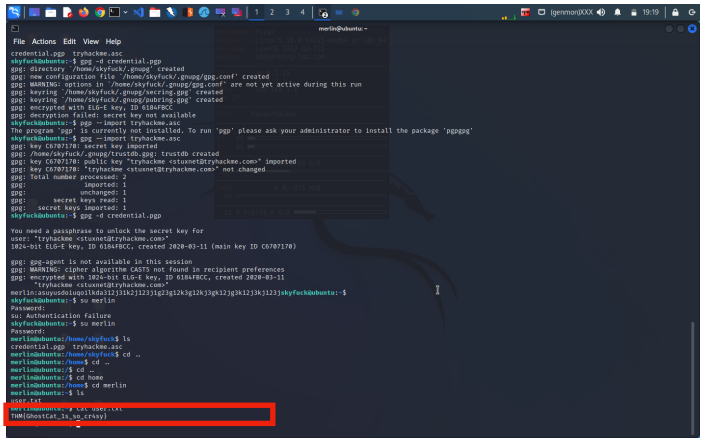


Command 1:
gpg —import tryhackme.asc

Command 2:
gpg -d credential.pgp

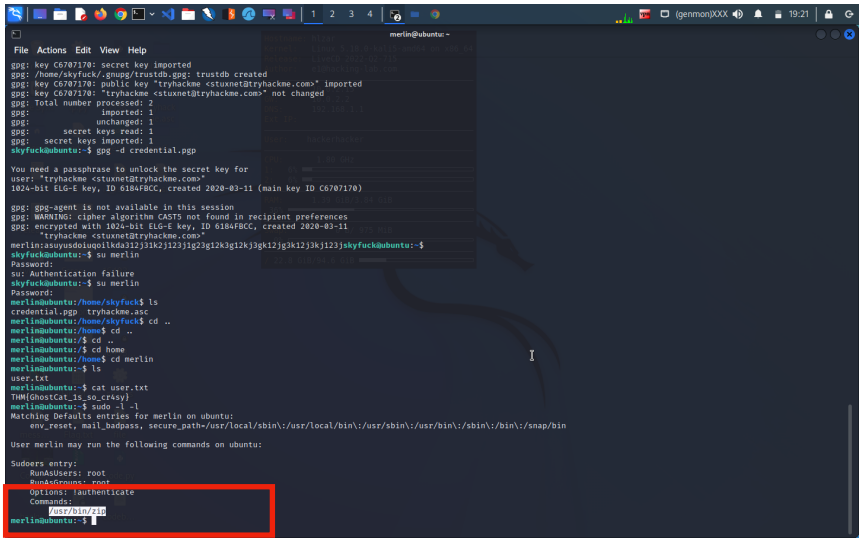
Command 3:
su merlin
Password: <pass>

//User merlin is now on//
// Now we se in the home/merlin directory and BOOM the user.txt is the user flag//

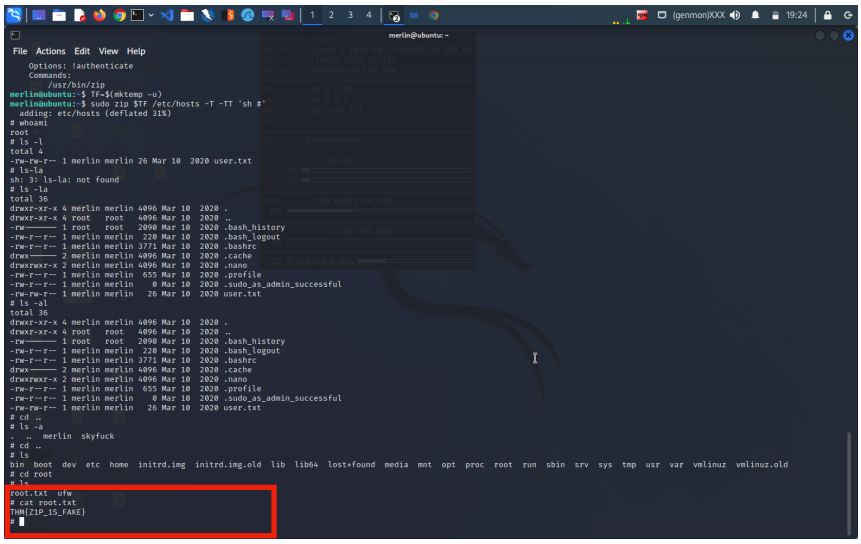


Step 5:

Next we try to make the root access for the root user for the machine by using a vulnerable zip file we see the zip vulnerability with the help of “sudo -l -l” command



And then we try to exploit the vulnerability with the help of $TF and we enter into the root in the root folder the root.txt is our root flag



Hurreeeyyy the flagg is overrrr and the box is complete!!!!!!!!!!!!!!!!!!