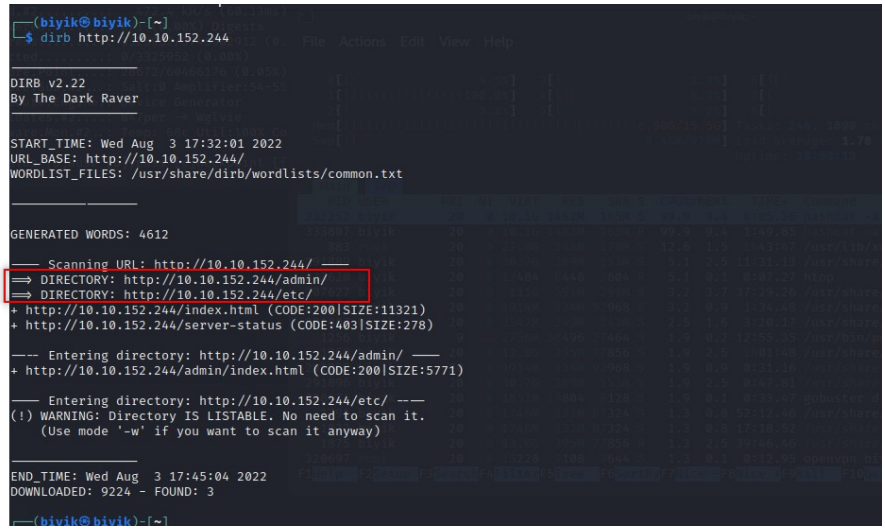
we need information for server and web pages etc.

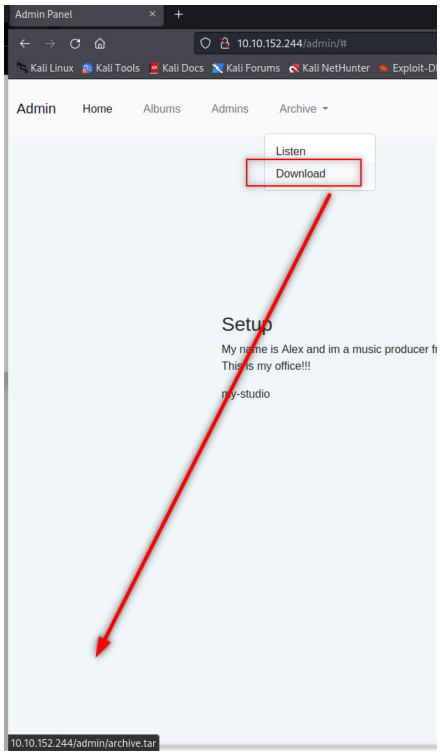
We used the following list of tools:
- Nmap
- gobuster
- dirb
their command list is here
-dirb http://machine_IP
- sudo nmap -A -sV -O -p- 10.10.152.244
- gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt -u http://machine_ip

we take results.

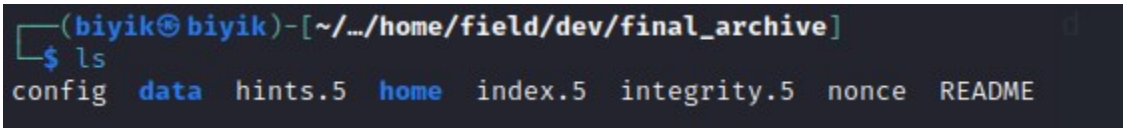


The results we got from the “dirb” command were /admin and /etc page.

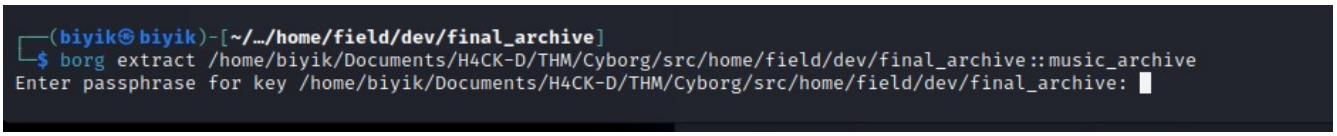
The admin page is.



- 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,



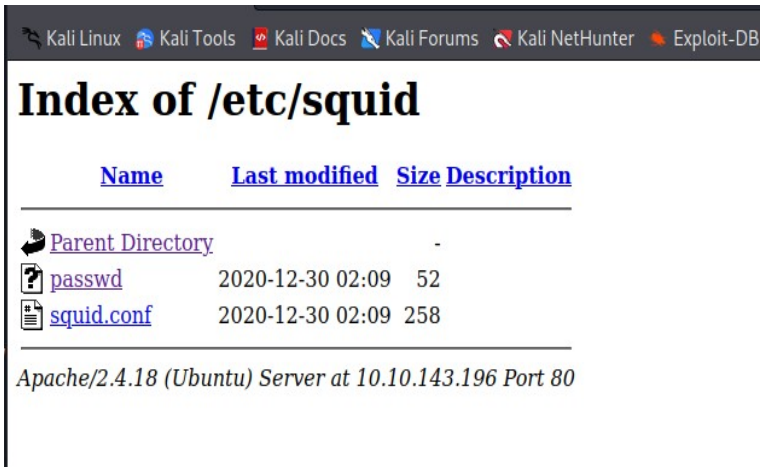
If you mind want open to all file you can learn some information for ctf. However we open the only main subject documents. So I am run that command “cat README” on terminal and I see borgbackup github and I installed on my machine. “borg extract path/to/final_archive::music_archive”



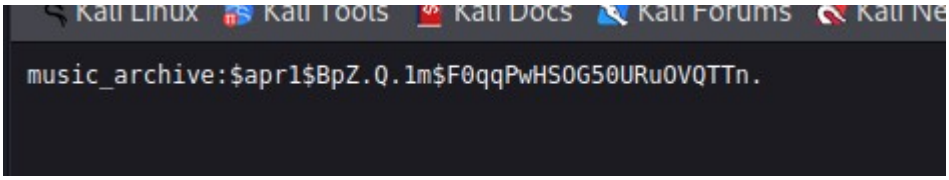
$apr1$BpZ.Q.1m$F0qqPwHSOG50URuOVQTTn.

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

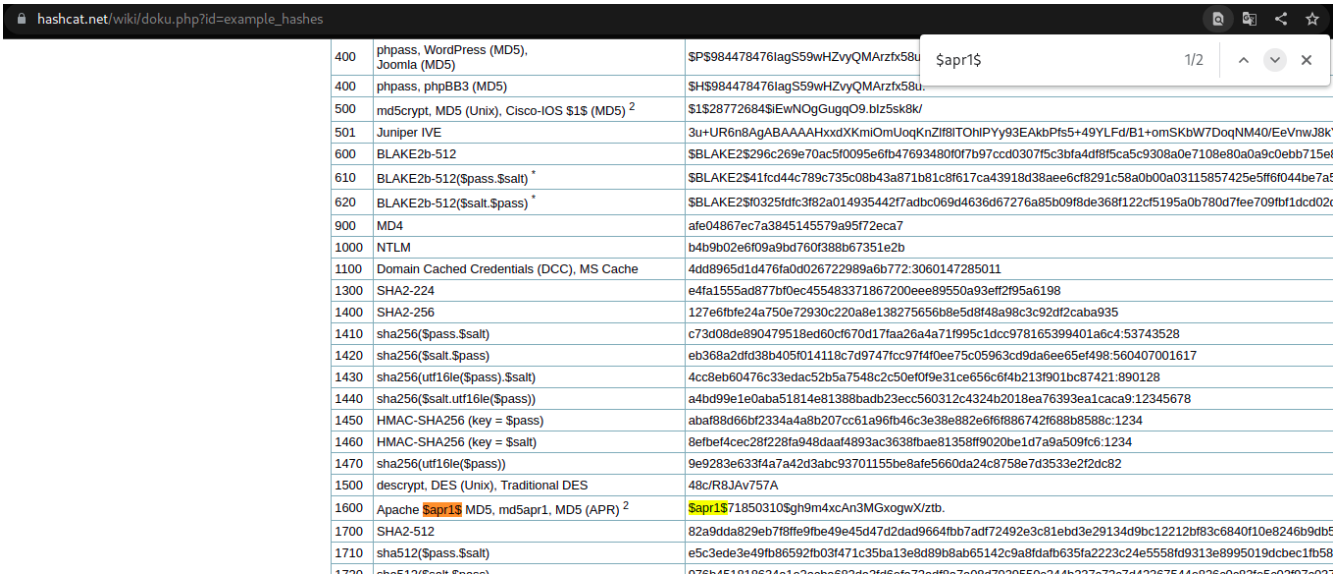
The etc page is



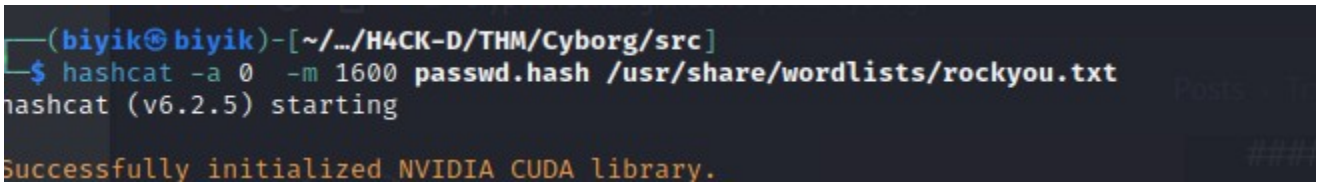
click to passwd and see that:



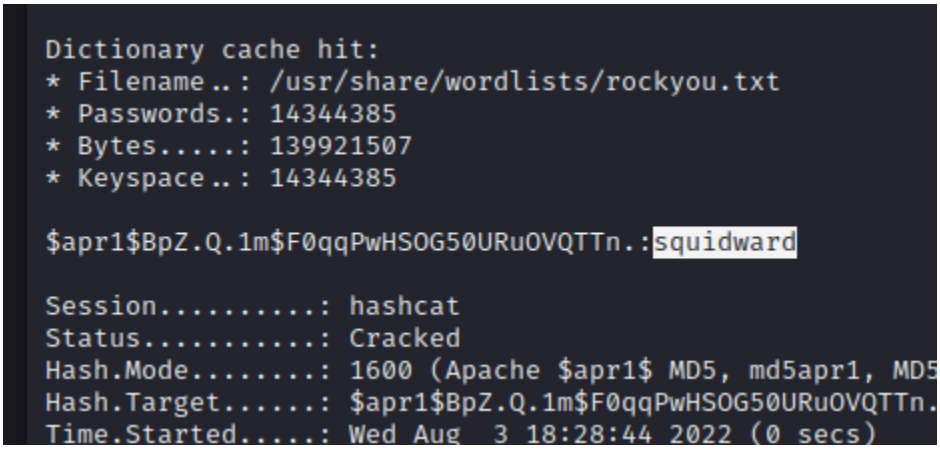
we search to hashcat example list on



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

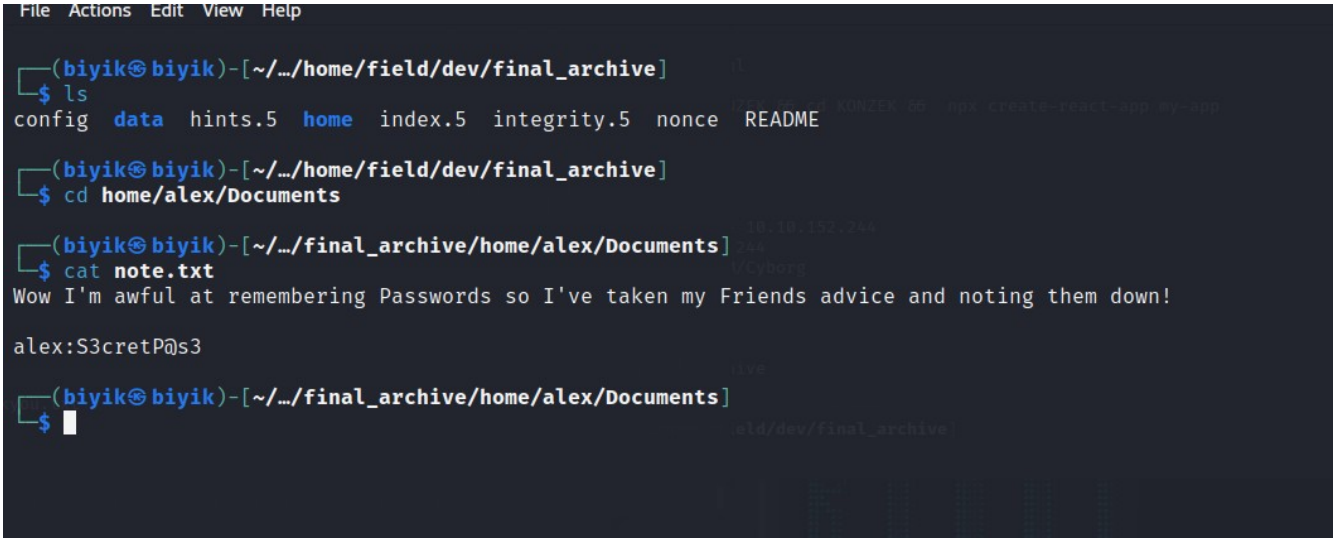


And I got this result.



-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 S3cretP@g3 and login.

“Cat user.txt” we found user flag.

---- Root flag -----

We run the “sudo -l” 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.