Enumerando Network File Sistem - NFS

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

NFS - Porta 2049

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

+ Protocolo desenvolvido para compartilhamento de sistemas em rede local
+ Compartilhamento de arquivos normalmente em redes linux

+ Procurando hosts com essa porta aberta:

```
nmap --open -sS -p 2849 -Pn 17.16.1.0/24
```

+ Para verificar quais versões são suportadas do protocolo, executamos:

```
rpcinfo -p 172.16.1.5 | grep "nfs"
```

+ Para ver mais detalhes sobre o host:

```
showmount -e 172.16.1.5
```

vai mostrar quais diretórios foram compartilhados

+ Para conseguirmos nos conectar aos diretórios, devemos montá-lo na nossa máquina

```
mkdir /tmp/nfs
```

```
mount -t nfs -o nfsvers=2 172.16.1.5:/ /tmp/nfs
```

→ Com isso, já temos acesso à raiz

+ Uma ideia é habilitar as authorized_keys do ssh