

# Enumerando NetBIOS/SMB no Windows

+ Situação em que estamos dentro de uma máquina Windows e só podemos usar o prompt de cmd

+ Como o smb e o netbios usam as portas 139 e 445, para mapear os hosts com essas portas abertas podemos executar

```
nmap -v -sV -p 139,445 -Pn --open 172.16.1.0/24
```

+ No prompt windows, podemos usar o **nbtstat**, pois mostra estatísticas do protocolo usando tcp/ip

```
nbtstat -R
```

→ limpa o cacher

```
nbtstat -c
```

→ mostra todos os hosts q ele já conectou

```
nbtstat -a <nome da máquina>
```

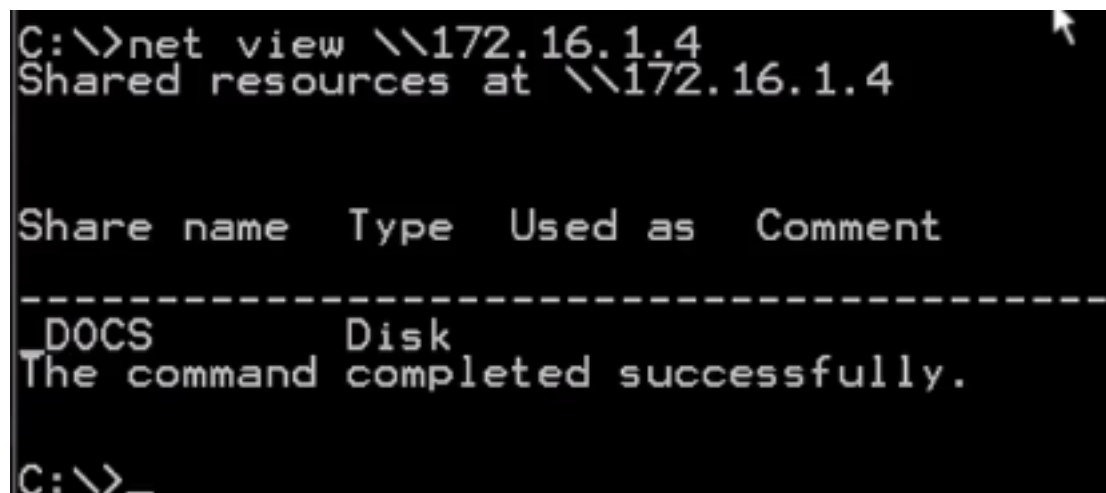
→ traz info sobre a máquina

```
nbtstat -A 172.16.1.4
```

→ traz info sobre o host

+ Podemos usar o **net view** para visualizar info sobre um determinado host:

```
net view \\172.16.1.4
```



```
C:\>net view \\172.16.1.4
Shared resources at \\172.16.1.4

Share name  Type  Used as  Comment
-----
DOCS        Disk
The command completed successfully.

C:\>
```

+ Podemos também estabelecer o null session, que é estabelecer uma sessão sem usuario e sem senha

```
net use \\172.16.1.5 "" /u:""
```

→ as primeiras aspas são a senha e a segunda o usuário

→ se for bem sucedido, poderemos usar agora o net view

+ Para estabelecer a comunicação com o diretório opt (ou outro qqer)

```
net use h: \\172.16.1.5\opt
```

+ Para desmontar a conexão:

```
net use h: /delete
```

+ Para encerrar a sessão:

```
net sue \\172.16.1.5 /delete
```

+ Para montar um diretório encontrado no meu computador,

```
net use x: \\172.16.1.4\_DOCS
```

→ eaí podemos acessar com nossas interfaces gráficas :)

→