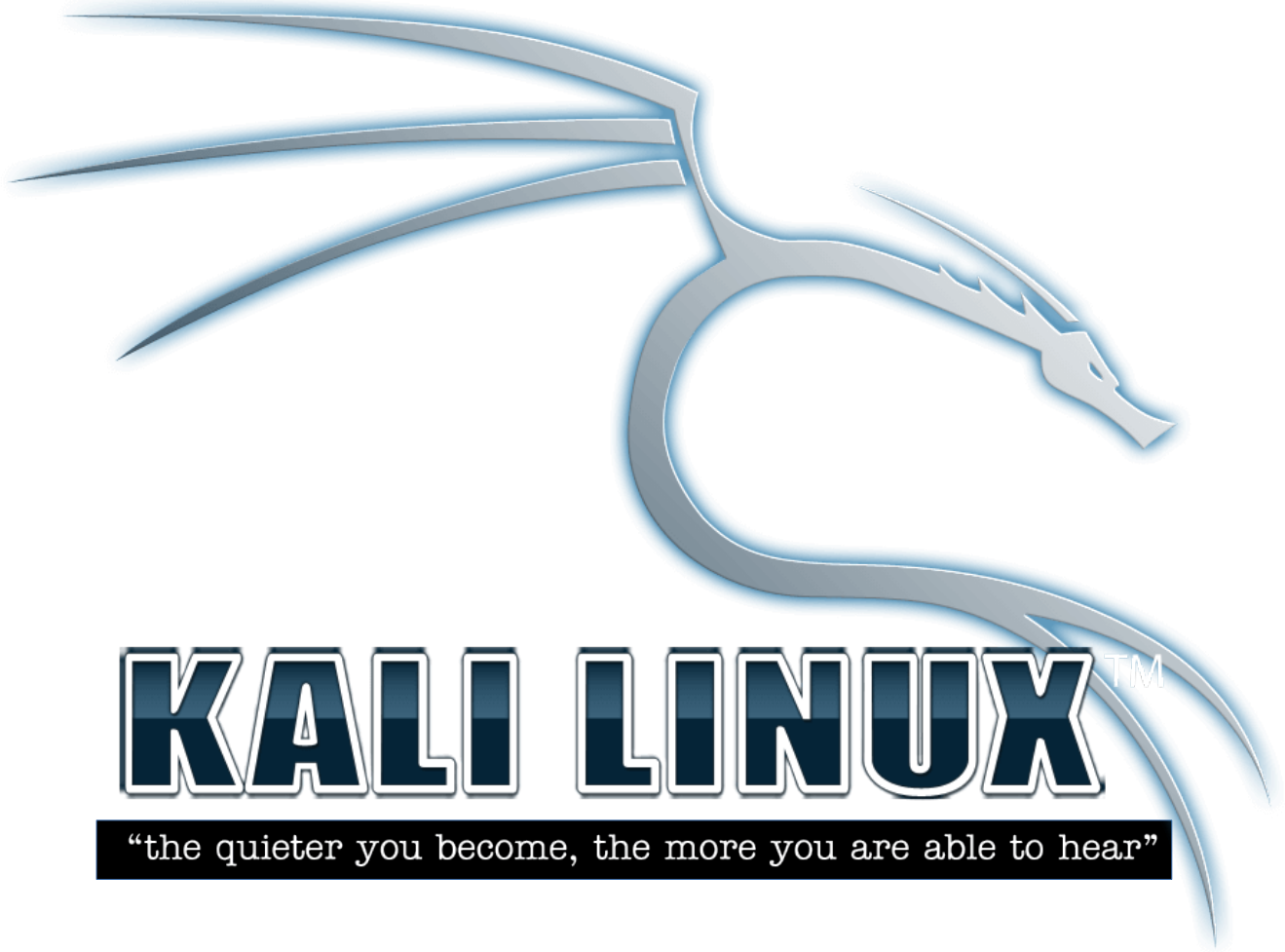
Pentest com Kali Linux



Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:
http://vmzsolutions.com.br

Procure por backdoors em seu sistema

Nesa aula, vamos usar o BackdoorMan é ajudar os desenvolvedores e webmasters a localizar por scripts maliciosos nos arquivos de um website em sistemas LINUX, pois hoje em dia é muito comum para os crackers colocarem algum tipo de *backdoor* nos sites invadidos. Um backdoor possibilita que o invasor tenha acesso contínuo aos arquivos, mesmo que os donos do site alterem todas as senhas.

Procure por backdoors em seu sistema

Primeira coisa é baixar o arquivo e depois executar nos diretórios que deseja fazer a verificação.

```
$ git clone https://github.com/cys3c/BackdoorMan

$ ./BackdoorMan --no-apis /home/vitor
```

Procure por backdoors em seu sistema

Podemos visualizar as seguintes informações no decorrer da varredura:

- Diretório onde está sendo realizada a varredura;
- Status da atividade e indicação do nome do arquivo possivelmente malicioso;
- Destalhe sobre a atividade realizada pelo arquivo malicioso;
- Número da linha para referenciar a atividade suspeita;
- Caminho completo do possível arquivo malicioso;
- Dono do arquivo;
- Tamanho do arquivo.