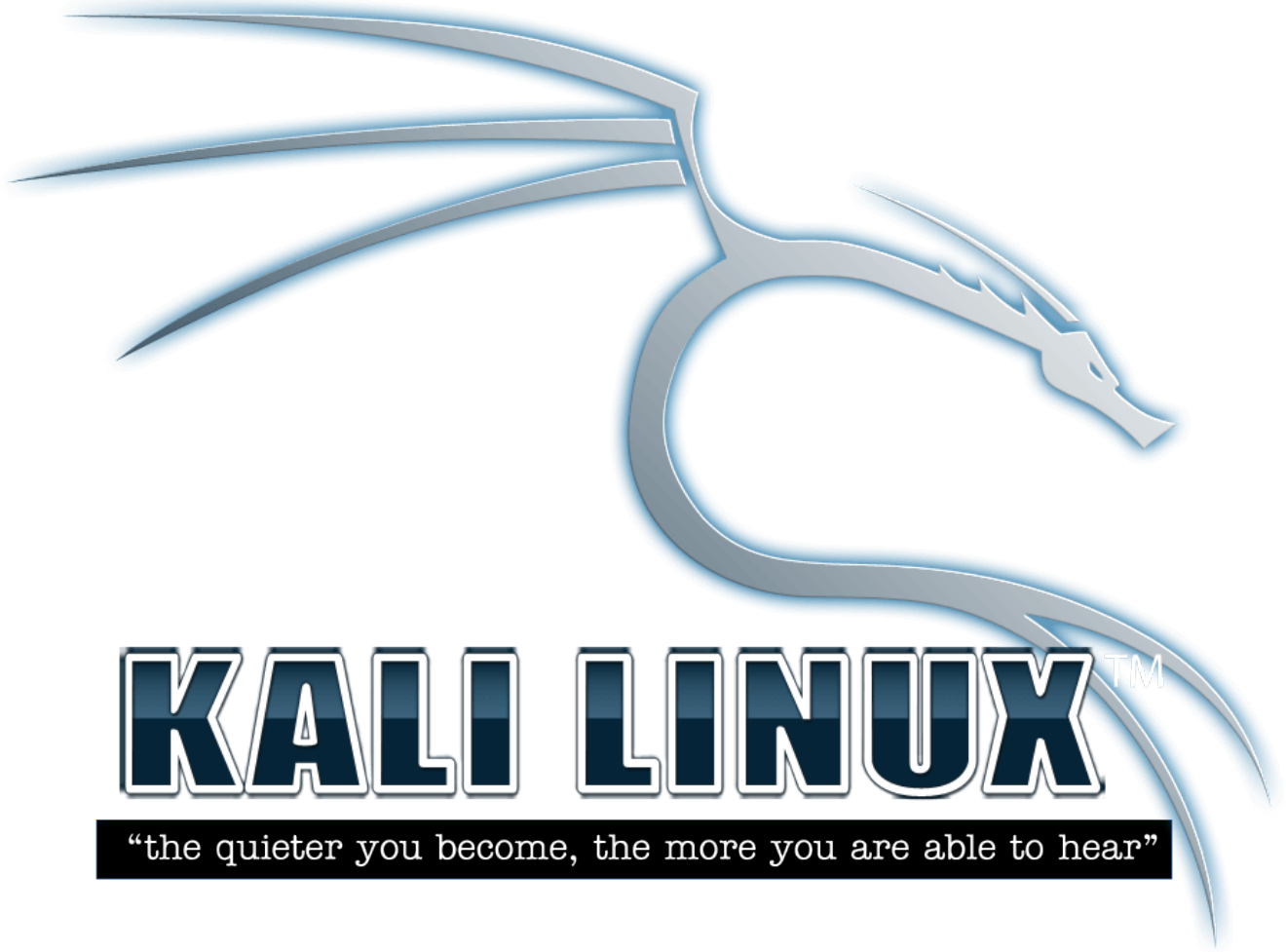
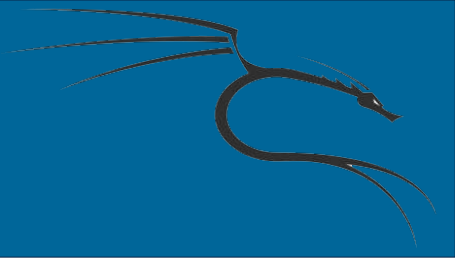
Pentest com Kali Linux





Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Fazendo ataques de SSLStrip

O SSLStrip é uma ferramenta de ataque Man in the Middle para sites com criptografia SSL/TLS (HTTPS, Certificado Digital), nesta aula vamos visualizar como o ataque pode ser realizado.

Fazendo ataques de SSLStrip

Primeiro, precisamos fazer uma configuração no iptables em seu Kali Linux para fazer um redirecionamento de portas com o PREROUTING e depois visualizar se realmente o iptables está funcionando.

```
# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 10000

# iptables -t nat -L
```

Fazendo ataques de SSLStrip

Agora, execute o sslstrip para fazer a captura de pacotes e conexões em SSL de nossos alvos!

```
# sslstrip -w captura.txt
```

Fazendo ataques de SSLStrip

Precisamos ainda alterar o nosso IP_FOWARD de nosso Kali Linux, para ele pegar esse pacote e levar para frente a conexão ao invés de fazer o descarte.

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Fazendo ataques de SSLStrip

Agora abra o Ettercap e faça o escaneamento de hosts e depois escolha a sua máquina alvo como TARGET 1 e o seu roteador como TARGET 2 e depois abra a opção MITM ARP Posing e dá um Sniff remote conections. E depois disto, inicie o ataque. Abra o navegador da máquina ifectada(no windows dê um arp -a para ver se está com o MAC alterado) e entre em um site que precise de login e senha e que use uma conexão SSL. Depois disto, abra o arquivo gerado pelo **sslstrip** e veja as senhas!