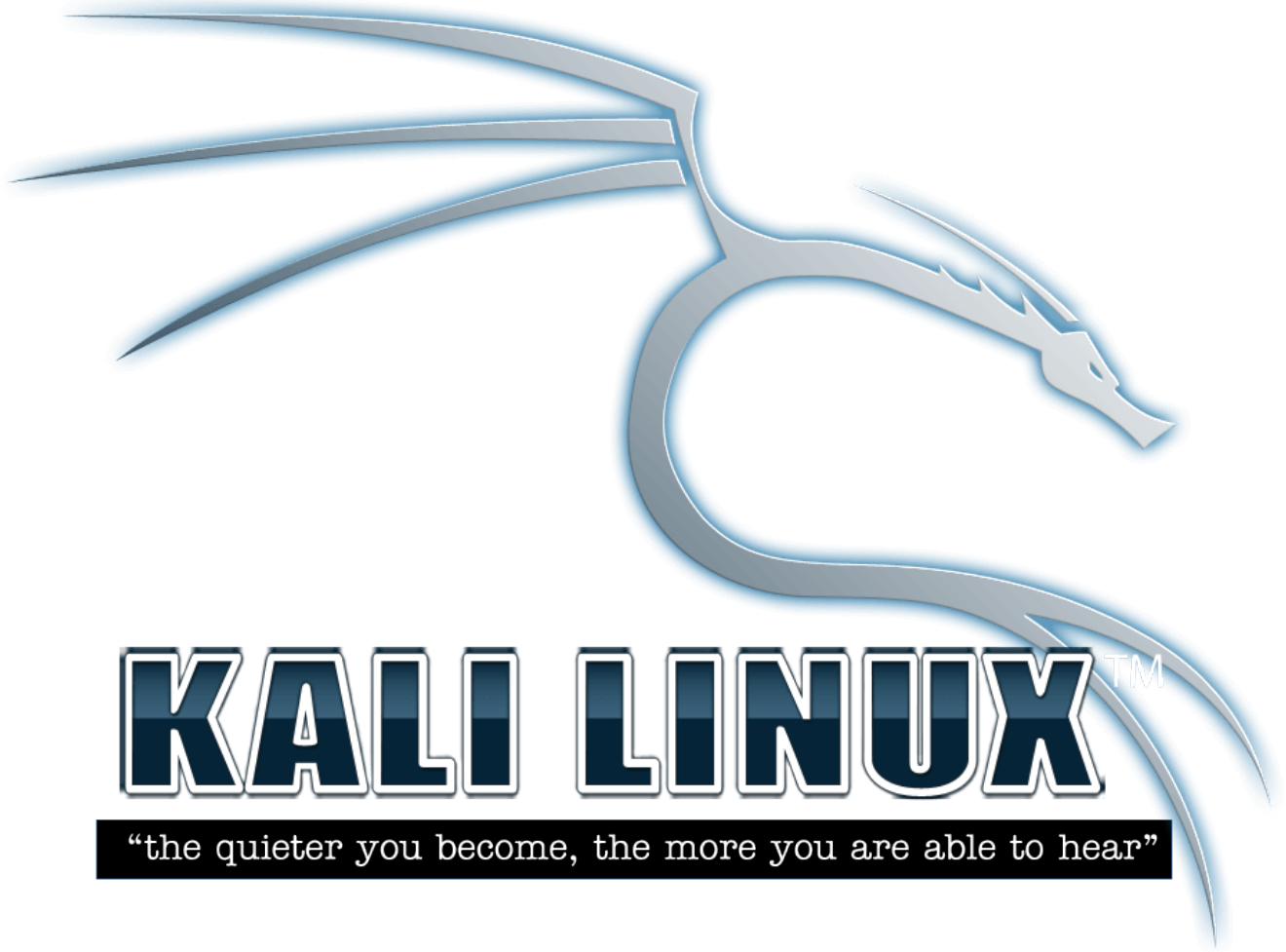
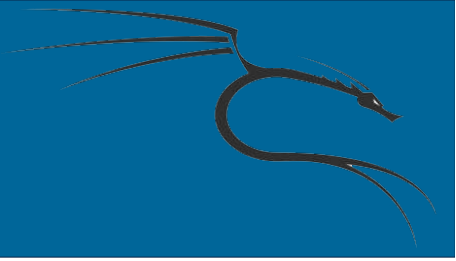
Pentest com Kali Linux





Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Encontrar redes ocultas

Nessa aula, vamos encontrar redes ocultas ao nosso de redor. Essa tática é usada para que as pessoas não vejam quais pontos de acessos temos em nossa volta por questões de segurança. Porém, vamos usar o `airodump-ng` para descobrir.

```
# airmon-ng start wlan1
```

```
# airodump-ng wlan1mon
```

Encontrar redes ocultas

Para que seja efetivo a nossa descoberta, é preciso anter um cliente conectado ao nosso alvo.

Encontrar redes ocultas

```
CH  9 ][ Elapsed: 0 s ][ 2016-10-24 17:24

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

C0:A0:BB:7E:1F:C1  -84        4        0    0   9  54e  WPA2 CCMP   PSK  Familia Alcantara__Gaslar
68:15:90:F4:4D:81  -47        5        3    0   9  54e  WPA2 CCMP   PSK  MZ2(2.4 GHz)
C4:E9:84:99:70:99  -70        5        2    0   9  54e. WPA2 CCMP   PSK  MZ2(2.4 GHz)
6A:15:90:F4:4D:82  -47        5        2    0   9  54e  WPA2 CCMP   PSK  <length:  4>
A8:9D:D2:D2:72:06  -83        3        0    0   7  54e  WPA2 CCMP   PSK  Vivo_EFE0C
A8:9D:D2:D2:72:07  -85        3        1    0   7  54e  WPA2 CCMP   PSK  HouseHansen
C4:E9:84:8E:B5:45  -70        5        0    0   1  54e. WPA2 CCMP   PSK  Jennifer
C8:3A:35:29:B7:48  -88        2        0    0   1  54e  WPA  TKIP   PSK  Multilaser_WS01

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

Encontrar redes ocultas

Agora que sabemos o MAC do nosso alvo, vamos usar o airodump-ng para descobrir o seu SSID.

```
# airodump-ng -c 9 --bssid 6A:15:90:F4:4D:82 wlan1mon
```

Se caso for preciso, use o ataque de DoS de desautenticação para forçar o cliente a se re-conectar ao ponto de acesso até então oculto por nós.

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