某局点wips反制不生效经验案例

WIPS 范书珩 2023-07-13 发表

问题描述

某局点使用wips反制，但是发现wips针对安卓终端开启的热点反制效果比较好，针对苹果终端开启的热点反制效果差，苹果终端已经关闭了随机mac，ios系统为16.5

过程分析

首先检查wips的基本配置，现场针对Test测试信号进行反制，检查基本配置没有发现问题

```
wips
#
ap-classification rule 1
 ssid equal Test
#
classification policy 1
 apply ap-classification rule 1 rogue-ap severity-level 100
#
countermeasure policy 1
 countermeasure rogue-ap
 countermeasure enhance
#
detect policy 1
 ap-spoofing quiet 360
 client-spoofing
 client-association fast-learn enable
#
virtual-security-domain vsd1
 apply classification policy 1
 apply countermeasure policy 1
#
client-proximity-sensor random-mac-report enable
```

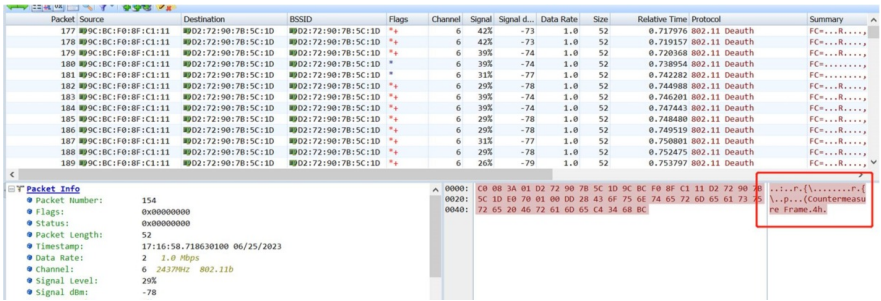
随后在AC上查看反制记录，发现AC上存在对苹果热点的反制记录，但是终端可以正常连接苹果手机释放的热点。

```
[DX-NH-WX3520X-AC1-wips-dtc-1]display wips virtual-security-domain vsd1 device | include 5c1d
d272-907b-5c1d AP    Rogue   00h 00m 28s 6     6     Inactive
[DX-NH-WX3520X-AC1-wips-dtc-1]dis wips virtual-security-domain vsd1 countermeasure record | in
5c1d
d272-907b-5c1d AP    Class   AP2       2     2023-06-25/16:57:12
d272-907b-5c1d AP    Class   AP3       2     2023-06-25/17:11:42
d272-907b-5c1d AP    Class   AP2       2     2023-06-25/17:11:42
d272-907b-5c1d AP    Class   AP3       2     2023-06-25/17:11:42
d272-907b-5c1d AP    Class   AP2       2     2023-06-25/17:14:24
d272-907b-5c1d AP    Class   AP2       2     2023-06-25/17:14:24
d272-907b-5c1d AP    Class   AP2       2     2023-06-25/17:14:24
```

虽然AC上存在反制记录，但是究竟是否真正执行了反制，还需要空口抓包进行确认，如下为苹果热点空口抓包

苹果热点mac：d272-907b-5c1d 测试手机mac:9cbc-f08f-c111

空口抓包看AP仿冒手机终端的mac不断的在给苹果热点发deauth报文，但是实际上终端依然可以稳定连接



理论上在wips反制过程中，AP不仅会仿冒终端mac发deauth给热点，也会仿冒热点发deauth给终端，而现场的AP只仿冒终端发deauth给热点,怀疑是AP没有仿冒热点 给终端发deauth报文导致的反制不成功，在经过确认后发现配置了countermeasure enhance后反制报文只有单方向的，随后删除counter measure enhance进行测试，空口抓包看到AP不仅仿冒终端mac发deauth给热点，也仿冒热点发deauth给终端，但是反制依然没有生效，终端依然可以稳定连接。

由于现场用的苹果手机系统版本是最新版本，经验来看wips针对之前版本的苹果手机热点是可以正常反制的，于是让现场找了一台老版本ios 15.6.1的手机测试，发现反制效果比较明显，那么问题可以基本确认为ios的新版本对wips反制做了一些保护措施，经过研究后发现ios16以上的版本默认使用了WPA3加密方式，如果连接热点的客户端也支持WPA3，那么客户端和苹果热点的管理帧在协议上被增加了保护措施，所以wips发的deauth报文就无法被终端和热点识别，因为反制报文终端和热点都是无效报文。另外安卓手机也是有支持wpa3和wpa2的选项，如果选择wpa3，也是和iphone一样，无法反制，所以现场对安卓的反制效果好，是因为安卓终端释放热点使用的是WPA2加密方式，ios 15的版本默认也是wpa2，所以wips反制没有问题。

解决方法

WPA3加密方式中的管理帧被加了保护，原理上WPA3的出现就是为了防止无线网络被攻击，反制实际上相当于一种攻击。如果释放热点的终端和连接热点的终端都使用了WPA3的加密方式，则无法针对使用WPA3的热点进行反制，目前发现ios16以上的版本默认使用了WPA3加密方式，部分安卓终端也可以释放WPA3的热点。