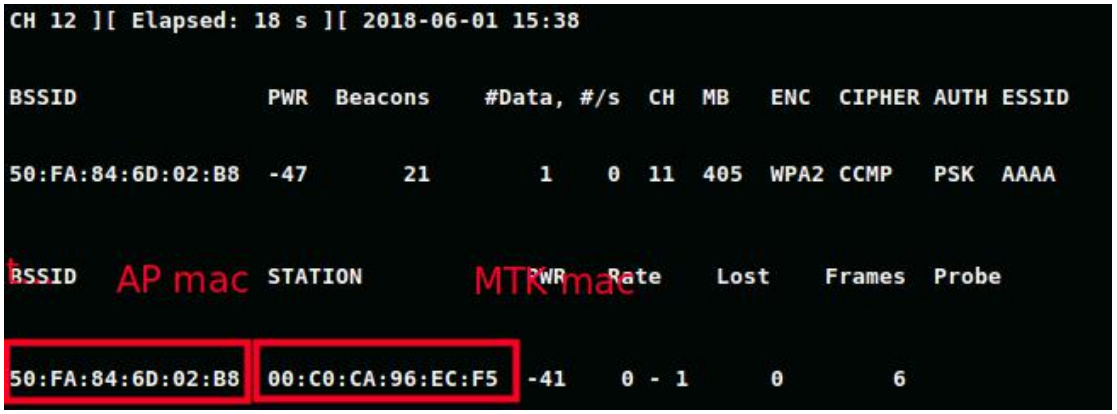
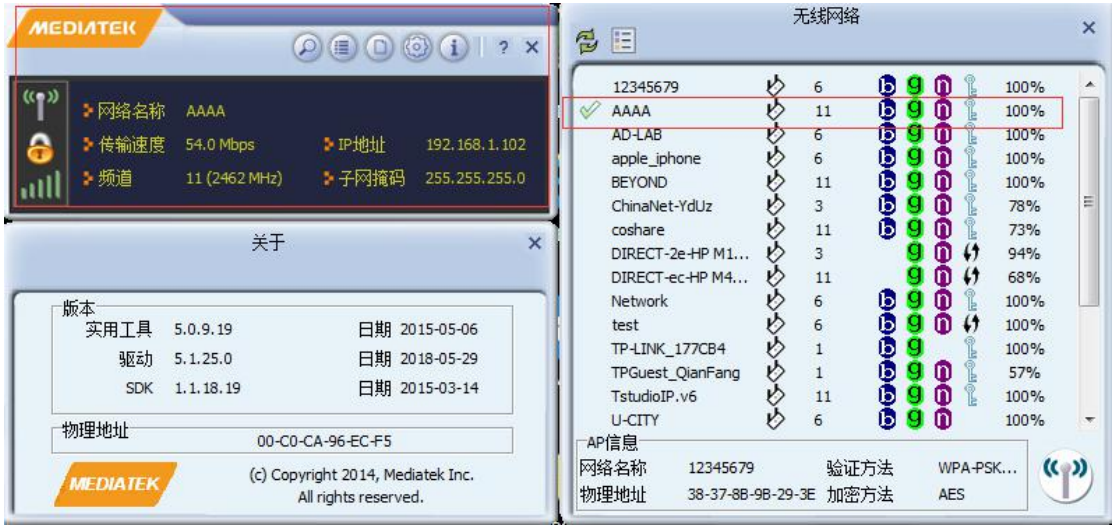
Test process

1. Attacker: In the first step, the attacker scans the MAC address of the target AP client. (MTK network card address)

system:Linux

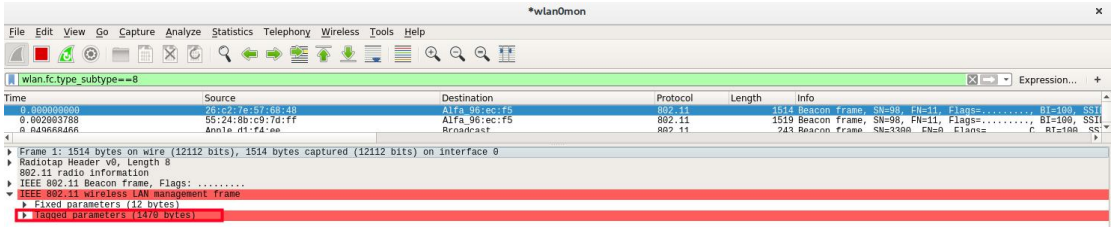


victim :The network card status at this time is normal.system:（win7）

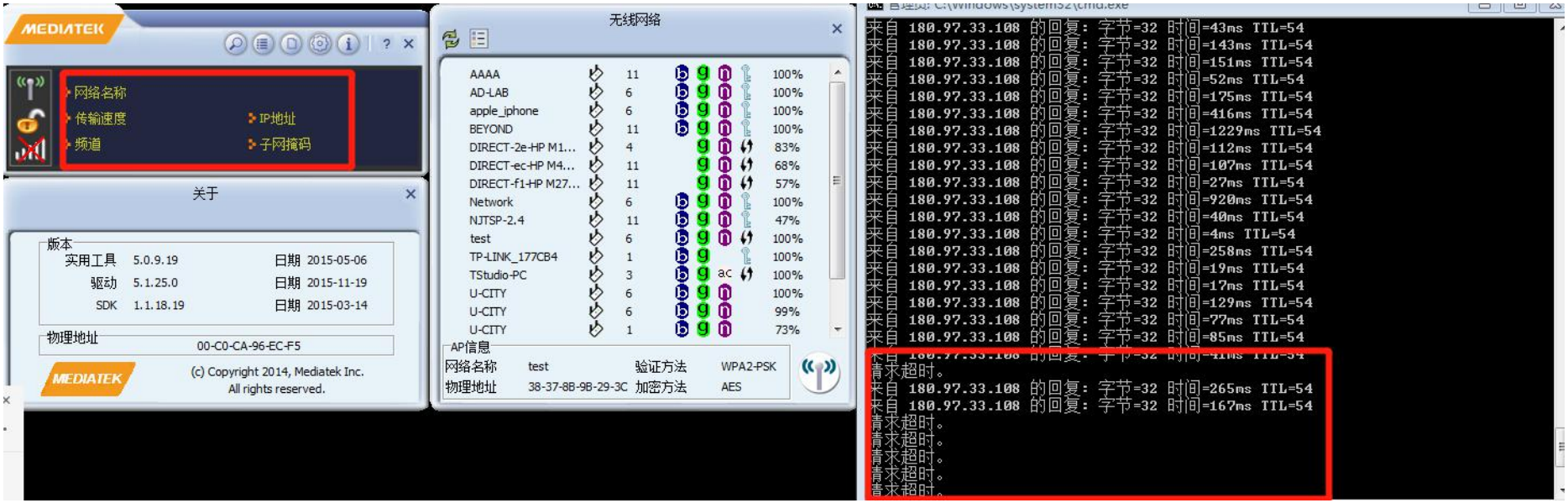


Attacker:Attacker sends malformed beacon frame system:(Linux)

Python xxx.py (payload)



Victim:Victims connected to the network are remotely attacked. System:(win7)


MEDIATEK
网络名称
传输速度
IP地址
频道
子网掩码
关于
版本
实用工具 5.0.9.19 日期 2015-05-06
驱动 5.1.25.0 日期 2015-11-19
SDK 1.1.18.19 日期 2015-03-14
物理地址
00-C0-CA-96-EC-F5
MEDIATEK
(c) Copyright 2014, Mediatek Inc.
All rights reserved.
无线网络
AAAA 11 100%
AD-LAB 6 100%
apple_iphone 6 100%
BEYOND 11 100%
DIRECT-2e-HP M1... 4 83%
DIRECT-ec-HP M4... 11 68%
DIRECT-f1-HP M27... 11 57%
Network 6 100%
NJTSP-2.4 11 47%
test 6 100%
TP-LINK_177CB4 1 100%
TStudio-PC 3 100%
U-CITY 6 100%
U-CITY 6 99%
U-CITY 1 73%
AP信息
网络名称 test 验证方法 WPA2-PSK
物理地址 38-37-8B-9B-29-3C 加密方法 AES
来自 180.97.33.108 的回复: 字节=32 时间=43ms TTL=54
来自 180.97.33.108 的回复: 字节=32 时间=143ms TTL=54
来自 180.97.33.108 的回复: 字节=32 时间=151ms TTL=54
来自 180.97.33.108 的回复: 字节=32 时间=52ms TTL=54
来自 180.97.33.108 的回复: 字节=32 时间=175ms TTL=54
来自 180.97.33.108 的回复: 字节=32 时间=416ms TTL=54
来自 180.97.33.108 的回复: 字节=32 时间=1229ms TTL=54
来自 180.97.33.108 的回复: 字节=32 时间=112ms TTL=54
来自 180.97.33.108 的回复: 字节=32 时间=107ms TTL=54
来自 180.97.33.108 的回复: 字节=32 时间=27ms TTL=54
来自 180.97.33.108 的回复: 字节=32 时间=920ms TTL=54
来自 180.97.33.108 的回复: 字节=32 时间=40ms TTL=54
来自 180.97.33.108 的回复: 字节=32 时间=4ms TTL=54
来自 180.97.33.108 的回复: 字节=32 时间=258ms TTL=54
来自 180.97.33.108 的回复: 字节=32 时间=19ms TTL=54
来自 180.97.33.108 的回复: 字节=32 时间=17ms TTL=54
来自 180.97.33.108 的回复: 字节=32 时间=129ms TTL=54
来自 180.97.33.108 的回复: 字节=32 时间=77ms TTL=54
来自 180.97.33.108 的回复: 字节=32 时间=85ms TTL=54
请求超时。
来自 180.97.33.108 的回复: 字节=32 时间=265ms TTL=54
来自 180.97.33.108 的回复: 字节=32 时间=167ms TTL=54
请求超时。
请求超时。
请求超时。
请求超时。
请求超时。

The victim will be attacked as long as he can receive the malformed beacon frame!