## Wifi捕获与攻击

### 实验目的和主要内容

本实验通过编程实现Wifi捕获与攻击。

本实验在Window 10利用Native Wifi Api实现了Wifi捕获与攻击，实现了捕获Wifi、显示Wifi详细信息、Wifi密码攻击等功能。

### Wifi安全简介

Wi-Fi是一种允许电子设备连接到一个无线局域网（WLAN）的技术，通常使用2.4G UHF或5G SHF ISM 射频频段。连接到无线局域网通常是有密码保护的；但也可是开放的，这样就允许任何在WLAN范围内的设备可以连接上。

在享受WiFi带来便利的同时，由于人们普遍缺乏WiFi上网的安全防范意识，WiFi安全已经成为各种网络陷阱、钓鱼诈骗的重灾区。

无线网络存在巨大的安全隐患，公共场所的免费WiFi热点有可能就是钓鱼陷阱，而家里的路由器也可能被恶意攻击者轻松攻破。在毫不知情的情况下，就可能面临个人敏感信息遭盗取，访问钓鱼网站，甚至造成直接的经济损失。

钓鱼陷阱。黑客就提供一个名字与商家类似的免费WiFi接入点，吸引网民接入。一旦连接到黑客设定的WiFi热点，上网的所有数据包，都会经过黑客设备转发，这些信息都可以被截留下来分析，一些没有加密的通信就可以直接被查看。除了伪装一个和正常WiFi接入点雷同的WiFi陷阱，攻击者还可以创建一个和正常WiFi名称完全一样的接入点。由于无线路由器信号覆盖不够稳定，你的手机会自动连接到攻击者创建的WiFi热点。在你完全没有察觉的情况下，又一次掉落陷阱。

主动攻击。黑客可以使用黑客工具，攻击正在提供服务的无线路由器，干扰连接，家用型路由器抗攻击的能力较弱的网络连接就这样断线，继而连接到黑客设置的无线接入点。攻击者首先会使用各种黑客工具破解家用无线路由器的连接密码，如果破解成功，黑客就成功连接你的家用路由器，共享一个局域网。攻击者除了免费享用网络带宽，还会尝试登录你的无线路由器管理后台。由于市面上存在安全隐患的无线路由器相当常见，黑客很可能破解家用路由器登录密码。

本实验将在Window10 平台下，通过Native Wifi Api捕获wifi，并利用密码库攻击无密码或弱密码Wifi。

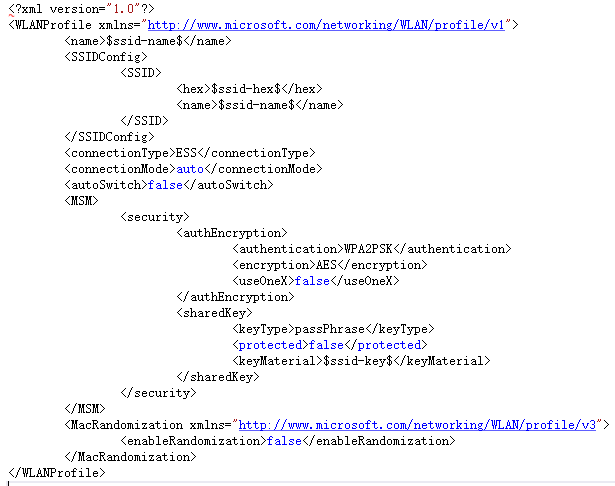
### Native Wifi API

Native Wifi API是微软开放的Window平台下管理无线网络的程序接口，通过Native Wifi API可实现获取Wifi、连接Wifi、监听Wifi、断开Wifi信号等功能。

Native Wifi API包含四部分内容Native Wifi Enumerations、Native Wifi Structures、Native Wifi Functions和Profile XML Schema。其主要API如下：

|  |  |
| --- | --- |
| Native Wifi API | |
| api | 功能 |
| WlanOpenHandle | 获取操作句柄 |
| WlanEnumInterfaces | 获取网络接口 |
| WlanGetAvailableNetworkList | 获取可用无线网络列表 |
| WlanGetProfile | 获取连接信息 |
| WlanSetProfile | 设置连接信息 |
| WlanConnect | 连接无线网络 |
| WlanDisconnect | 断开无线网络 |

含密码的ProfileXml模板如下：



无密码的ProfileXml模板如下：



通过替换$ssid-name$、$ssid-hex$、$ssid-key$来构造连接Wifi的ProfileXml文件。

### Wifi捕获与攻击

可执行文件说明：

文件WinWifiAttack.exe是可执行文件。

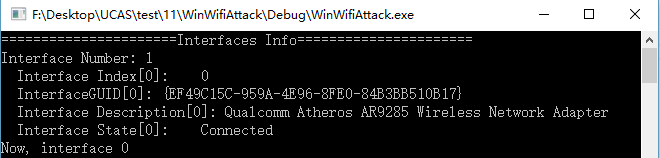
文件xml-key.txt中是含密码的wifi连接信息模板。

文件xml-open.txt中是不含密码（开发）wifi连接信息模板。

文件key-list.txt是密码库，每一行一个密码。

执行WinWifiAttack.exe，执行过程如下：

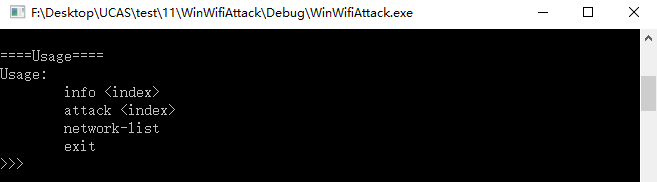
1. 通过WlanEnumInterfaces获取网络接口及网络接口信息：



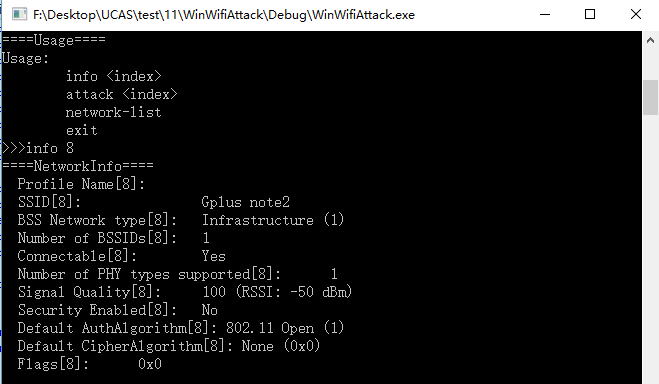
1. 通过WlanGetAvailableNetworkList获取可用网络，并显示简要信息：



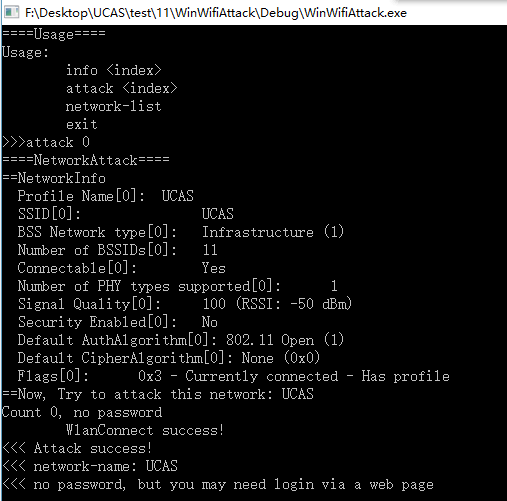
1. 支持查看指定网络详细信息或攻击指定网络：



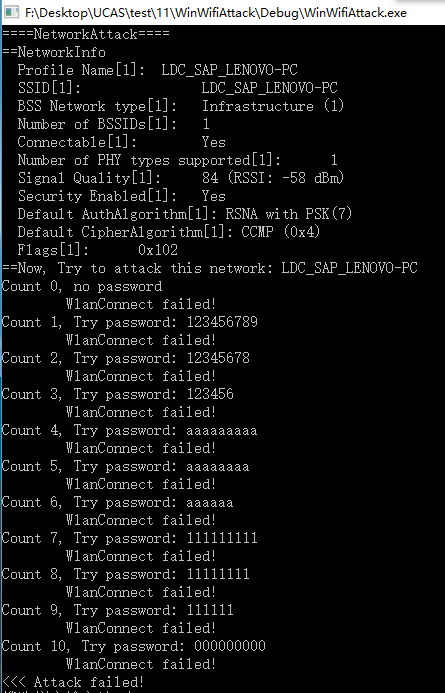
1. 显示指定网络详细信息：



1. 攻击指定网络，成功：



1. 攻击指定网络，失败：



### 存在问题

目前程序能够捕获Wifi信息，并攻击登录无密码Wifi，但在攻击有密码Wifi时还存在问题。问题是：在使用一个密码去攻击指定Wifi，使用WlanConnect尝试连接该Wifi，密码正确和失败的返回值相同，所以不能作为密码正确或错误的判断标准，所以还需要尝试其它的判断方法。

### 实验总结

通过本实验，了解、学习和掌握了以下内容：了解了Wifi安全相关内容，包括Wifi安全隐患、Wifi攻击方法、Wifi攻击防御方法等；学习了Native Wifi API，并编程实现Wifi捕获和攻击。此外，除了本实验的Wifi弱密码攻击，还可以尝试中间人攻击、路由器密码攻击等攻击方法。