Misc 总结 ----流量分析 无线wifi相关

M1n3 / 2018-01-20 22:57:47 / 浏览数 4555 安全技术 CTF 顶(0) 踩(0)

网络协议-无线

实验目的

掌握无线认证的方式
掌握deauth攻击的原理与结果
掌握使用wireshark分析无线数据包

实验环境

- 操作机：Windows 7
  - 实验工具：
    - Wireshark2.2
    - binwak for windows

实验内容

客户端与路由完成密钥交换的时间？(flag格式：flag{2015-09-01-12:05})

实验一

WEP已基本弃用，不安全。目前常用WPA2-presonal。WPA2包含一下几个点：预共享密钥；AES加密；CCMP完整性校验。

方法一 了解无线协议

- 操作步骤详解

要了解的无线网络协议的关键：

- 周期性的发送Beacon：宣告无线网络的存在，数据速率，信道，安全密码，密钥管理等。
- 节点获知AP的信息，发送proble request；
- AP返回proble response；
- 然后开始Authenticaion request。

WPA2的握手：

基于802.1X 协议，使用eapol key进行封装传输。

1. Authenticator -> Supplicant：
   key 描述：AES加密，HMAC-SHA1 MIC验证，Anonce，等等。
2. Supplicant -> Authenticator：
   Snonce，key 描述，key MIC(除了第一次握手都有MIC字段
)
3. Authenticator -> Supplicant：
   Install(安装 生成共享密钥),Key ACK,Key MIC,加密Key Data,SMK.
4. Supplicant -> Authenticator
   表明可以进行加密通信。

我们按协议排序这个流量包，可以很直观的看到握手过程：

wireshark已经根据key-information的顺序解析了这个握手1-4的过程。所以我们展开分组详情的信息可以获取到，第四次交换握手包的时间是：flag{2016-12-05-22:45}

方法二 Deauthentication Attack

Deauthentication是IEEE 802.11 协议所规定的，用来解除认证的帧。具有如下特点：

- 没有加密 任何人都可以发送
- 容易伪造来源MAC地址
- 强制客户端掉线

这个数据包中充斥着大量的Deauthentication的数据包，是强制客户端掉线重新连接的一个过程。

方法二 无线数据包的解密

在我们获得了数据包之后，这些客户端和AP之间的通信是被加密了的，但是我们如果知道SSID和无线密码可以解密这些流量。

wireshark官网提供了这样一个现在工具WPA-PSK生成：

这个数据包包连接的SSID是sudalover，密码：2.64*2.64，生成的PSK是：27d0ceba9040bbc863b804048160041f3360d0507d96968ae67e915f4aba440e

我们可以在wireshark的 编辑 - 首选项 - Protocol(协议) - IEEE802.11 - Decryption Keys导入它：

重新打开或载入这个数据包，我们在四次握手链接之后，传输的数据中就能看到更上层的通信数据了：

wlan.pcap.zip (0.025 MB) 下载附件

上一篇：Misc 总结 ----流量分析 ... 下一篇：安全事件关联规则讨论

1. 3 条回复

老锥 2018-01-25 20:02:35

支持

0 回复Ta

1815837370479554 2018-05-29 15:01:06

支持 支持

0 回复Ta

liuli_****@126.c 2018-12-11 23:04:41

请问这种认证是属于企业版，不是PSK吧

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板