实验吧——安全杂项之“A记录”详解

原创

Geekingdom 于 2018-11-11 11:02:53 发布 2548 收藏 2
分类专栏： CTF 文章标签： 实验吧 A记录详解 CTF题目 A记录

A记录

链接：

题目链接：http://www.shiyanbar.com/ctf/1853

附件链接：http://ctf5.shiyanbar.com/misc/shipin.cap

工具：Wireshark，aircrack-ng

思路及解法：

打开连接显示有题目的说明

通过说明可以了解到附件下载的应该是一个数据包，而且是在别人看视频的时候截取的，所以猜想什么情况下可以在别人看视频的时候可以截取数据包。

下载附件网址里的文件，的确是一个数据包文件，文件名是“shipin.cap”,首先想到是用Wireshark打开这个文件，不过在打开文件后发现里面并没有什么数据，应该是被加密过的，但是有一点值得关注，里面有Tp-Link的字样，应该是路由器相关的

再联想到题目说明，可以猜到这个数据包应该是通过无线网截取的，所以我开始搜寻如何破解无线网获取的数据包，发现一个工具“aircrack-ng”，根据这个工具的使用教程，一步步的操作。

首先用命令窗口进入这个工具所在的文件夹，打开相应的exe软件，输入规定的命令格式:

“aircrack-ng.exe 数据包文件完整路径”

执行之后可以后的该路由器的ESSID为0719；

然后进行下一步操作，输入命令格式：

“aircrack-ng.exe 数据包文件完整路径 -w 字典文件完整路径”并执行，结果为

可以获得该路由器的密码为“88888888”；

最后，再利用该工具的另一个子程序进行对数据包的解密，命令格式为：

“airdecap-ng.exe 数据包完整路径 -e ESSID -p 密码”并执行

然后会在该数据包所在文件夹里生成一个新的经过解密的数据包

然后再用Wireshark打开这个新的数据包文件，并且经过题目提示可以知道，这题的FLAG为该数据包的A记录第一条的网站名称，所以在Wireshark中搜寻“dns”就会出来数据包中的A记录，然后找到第一条A记录所对应的网址即为该题FLAG

结束！