2021-09-10 网安实验-XCTF真题实战之流量分析

原创

愚公搬代码 于 2021-09-10 10:34:42 发布 24731 收藏

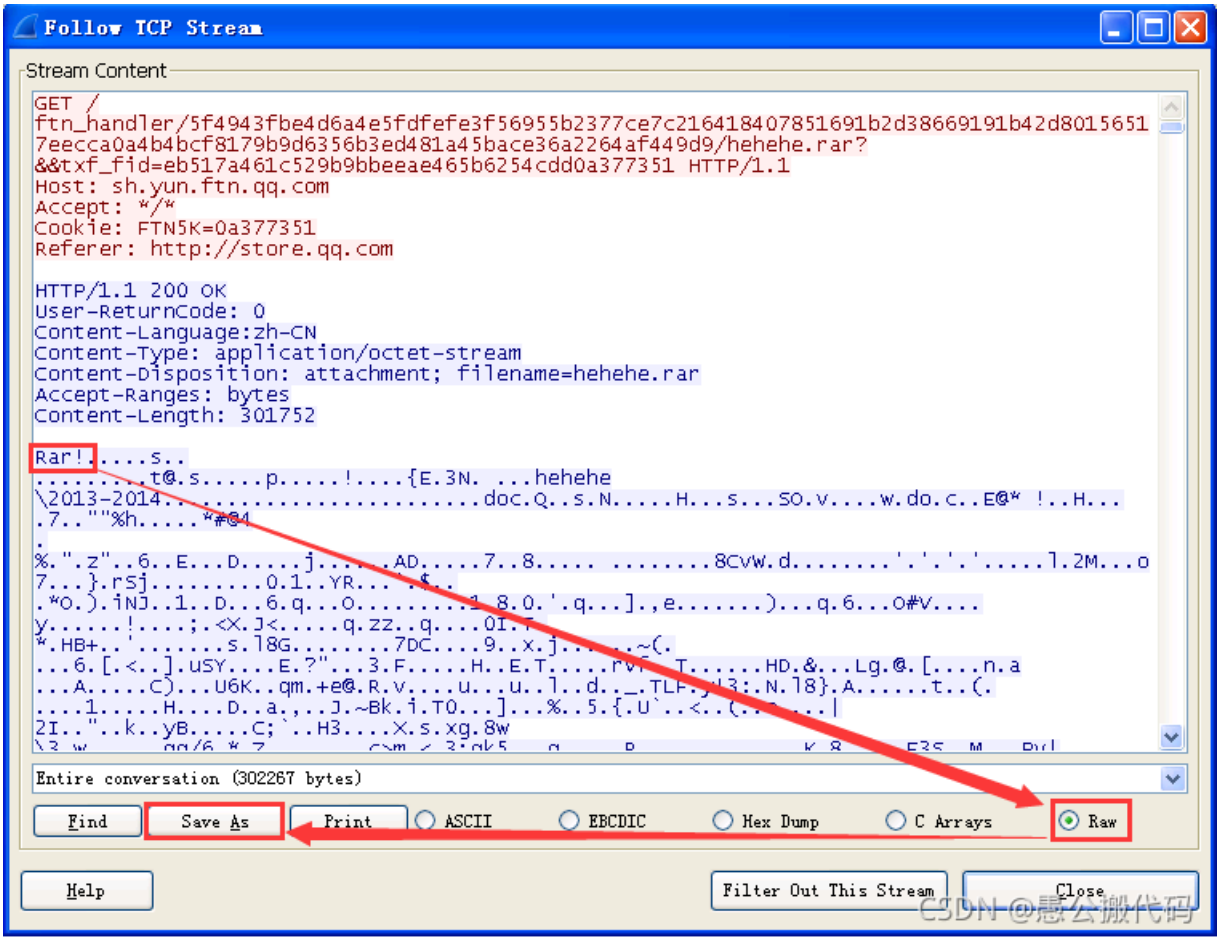
分类专栏： CTF-网络安全实验 文章标签： r语言 python

本文链接：https://blog.csdn.net/aa2528877987/article/details/120216683

通信流量分析

使用Wireshark打开HEHEHE.pcap文件。对于通信流量分析类题目，常用的一个解法就是使用过滤器tcp contains ".rar"来查看数据包中是否包含有rar文件，实际操作时rar可以换成zip等其他扩展名。

现在在Wireshark的Filter编辑框中输入过滤器tcp contains ".rar"，果然发了这样的通信记录，选中第一条结果，单击右键选择"Follow TCP Stream"，可以看到数据包里存在一个rar文件，这里将其Dump出来（在窗口中选择Raw，然后点击SaveAs按钮即可），如下图所示：



对保存的Rar文件进行解压，得到两个文件，分别为：2013-2014关于评选先进班集体的通知.doc、福利.jpg。从doc文件中似乎看不到什么有用的信息，从jpg文件中可以看到一个Key，为XPA087T24433PASS。

DES解密

通过对《2013-2014关于评选先进班集体的通知.doc》文件的分析，发现doc文件末尾附加了一段数据，那这一段数据是如何发现的呢？我们可以新建一个doc文件，然后将原始doc文件中的数据复制粘贴到新建的doc文件中，保存后对比两个文件的