XMAN misc writeup

原创

RobinZZX 于 2019-08-03 20:17:49 发布 1247 收藏

分类专栏： 日志 资料 文章标签： 网络安全 misc ctf

本文链接：https://blog.csdn.net/RobinZZX/article/details/98373017

日志 同时被 2 个专栏收录

25 篇文章 0 订阅

订阅专栏

资料

18 篇文章 0 订阅

订阅专栏

misc：

cephalopod
pcap是常见的数据报存储格式，在这个题目中我们首先用binwalk检查出pcap中含有一个png文件，
然后使用tcpxtract从pcap找那个提取出png文件，文件内容即flag

easycap
直接追踪流然后将FLAG后面部分base64解密

Erik-Baleog-and-Olaf
文件名字叫stego100，提示我们使用stegsolve工具，说明文件可能隐藏着图片，用010editor打开，
文件头和文件尾正是png的格式，直接改文件后缀名.png，打开之后看到一张三个矮人的图片，
使用stegsolve打开，在某一色域时看到中心的二维码，保存之后用ps修改清晰，扫描可得flag

Miscellaneous-300
是一个加密的压缩包，暴力破解之后发现还有很多层压缩包，使用py脚本进行爆破，最后出一个12345.zip的压缩包继续爆破，

modbus
是一个pcap包，由题目提示可以先查找modbus包 ，追踪包并设置流为2即可看到flag

mysql

肥宅快乐题
视频文件，跳到57帧即可查看到数据，使用base64解密得flag

很普通的数独
很多张数独，将1 5 21张调换之后，将有数字的转成黑色方块，无数字的转成白色方块，即得到二维码

神奇的压缩包
利用了ntfs文件流，题目文件解压后的txt文件，在cmd模式下可以用winrar解压，得到flag包

小小的pdf
使用010editor查看，搜索后，发现有实际包含三张图片，其中一张是flag，提取出来即可

问题：
追踪流的概念
脚本
modbus
二维码