西普实验吧密码学题目--一个img文件

原创

Neil-Yale 于 2017-03-18 21:45:10 发布 4455 收藏 2

文章标签： 密码学 数据 CTF 软件 硬盘

本文链接：https://blog.csdn.net/yalecaltech/article/details/63291031

本来是准备把同种类型的题目只发一篇博客的，但是有些题目确实有些复杂，所以单独拿出来写Write Up.

题目连接：http://www.shiyanbar.com/ctf/60

下载来是一个.img格式的文件，img格式是镜像的一种。可以通过制作数据光盘或者使用虚拟光驱(如 WinMount)安装IMG数据文件。

题目的hint为恢复数据，故想到使用diskgenius。

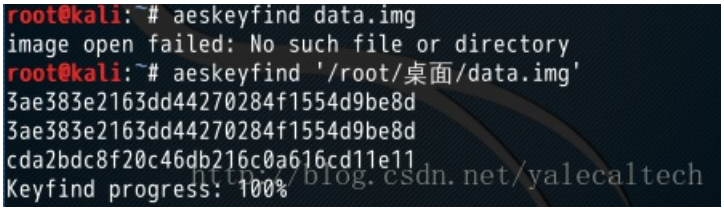
打开软件后-》硬盘-》打开虚拟硬盘文件-》选择data.img

选择data.img(383M)这个虚拟硬盘文件-》恢复文件

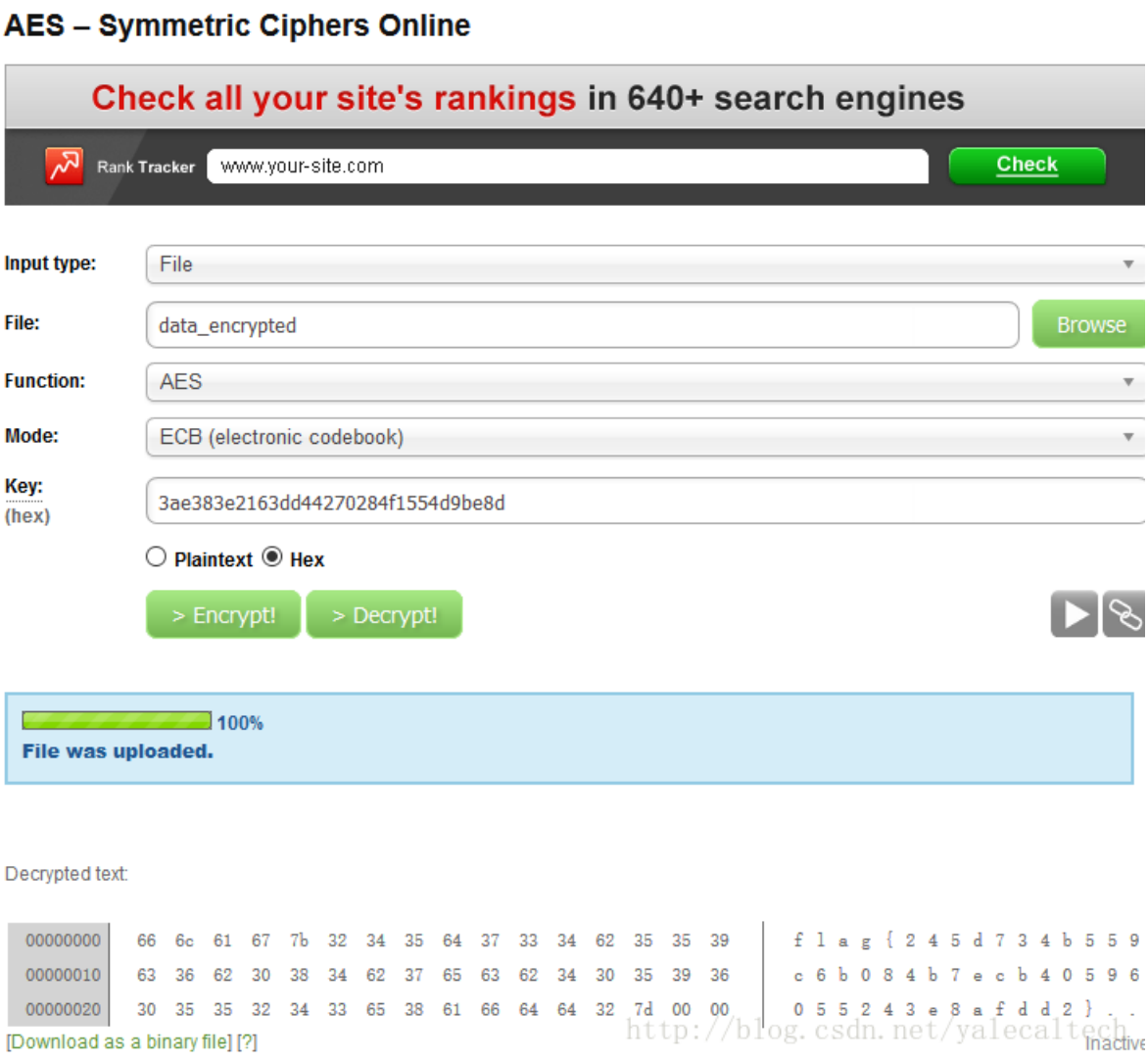
效果如图

通过winhex等十六进制软件查看或者直接在.zip文件上或者其他任何方式都可以发现两个文件内容完全一样。随机右击保存一个到桌面上待会儿会用到。

使用linux（我这里使用kali）apt-get install aeskeyfind 命令安装aeskeyfind.
将下载的data.img拖入kali中，输入aeskeyfind '/root/桌面/data.img'（路径按照自己的实际情况写）
即可得出结果（还没完呢）
如图所示



有三个结果，分别尝试，此处需要用到在线AES解密网站，我推荐http://aes.online-domain-tools.com/
各选项注意按照下图所示进行选择，即可得到flag



忘记说了，最后一张图File:选择的是之前我们保存在桌面的.zip文件解压后的文件即data_encrypted.而input type默认是Text,注意需要选择File