红亚2015-3月杯季赛 CTF题部分writeup

转载

hello_sec 于 2015-10-08 17:56:51 发布 3065 收藏 2
分类专栏： 信息安全 CTF 文章标签： 源代码 经验 技术 博客


信息安全 同时被 2 个专栏收录
5 篇文章 0 订阅
订阅专栏


CTF
1 篇文章 0 订阅
订阅专栏

红亚2015-3月杯季赛 CTF题部分writeup

最近一直特别特别忙，没有时间写Blog，连续两周每天都忙到凌晨，连续两个周六都是快十一点才回宿舍。中途，间接地做了些红亚上，原来的一些CTF老题，积累了不少经验。不过这学习的效率太低了。。。。

废话不多说，进入正题，做了一部分，就写下来记录一下吧。本身也是菜比。

==========我是分割线~(～￣▽￣)～==========

技能题第一关：
根据提示，查看源代码，没技术含量。

1

得到KEY：WeLc0m3_2012

技能题第二关：

根据提示base64 解码：

PD9waHAgQGV2YWwoJF9QT1NUWyd0aGlzX2lzX3lpanVodWEnXSk7Pz4=

得到KEY。
KEY:this_is_yijuhua

技能题第三关：

根据提示UTF-7 。纠结了好久UTF-7的解码。找解释器什么什么的。。。

原来只需要处理一下，base64解密即可。看来得重点学习一下编码这方面的知识。
+AGsAZQB5ADoAaQBhAG0AdQB0AGYANwBlAG4AYwBvAGQAZQBk-

取加号减号中间的字符串，在最后加=
base64解密即可得到KEY
KEY：iamutf7encoded

技能题第四关：

JS challenge ，无非就是JavaScript，假期学了一些，差不多能看懂。

firebug查看源码，解密 加密后的JS代码得到：


同时 form 表单的内容为：

JavaScript 的代码中parseInt() 函数的作用是解析字符串并返回数字 （可以理解为将string 转化为 int 类型）
接下来看判断语句即可得知 本关KEY就是 复活咒语。
KEY:201211

技能题第五关：

本关考察Linux的复制命令
cp /Cardinal/YUI /home/kirito/local-memory/
MD5加密后的 小写32位即为本关KEY
KEY:cc92711eef5fe0de1750eef92f848f9d

技能题第六关：

下载发现优盘镜像 .img文件，用 winImage 打开，到处发现有三个文件，一个文件夹，文件夹里是VBS脚本文件。两张学习资料的图片，没看出什么东西。

接着看autorun.inf，这个镜像自启动的配置文件，查看autrun参数下的文件

打开这个脚本文件 

得到KEY:b4D0V1ruS

技能题第七关 

下载发现是eml文件，安装 Windows Live Mail，打开之后发现附件 meizi.jpg


查看源代码，并未发现KEY的字样，根据经验，把jpg后缀改成rar，打开图像的KEY。
KEY:HideFileInImages

技能题第八关

提示是Inject。但是。。。。

没解出来。。。暂且放一下，回过头来再做。

技能题第九关

简单明了。

执行命令：
net user zealadmin admin /add && net localgroup administrators zealadmin /add

验证即可得到

KEY:Windows_CMD_is_useful!

第十关到第十三关的逆向，Flash，什么的都不会做。。。

技能题十四关：

根据题意，从图像当中查找账号密码，然后登陆就能得到KEY了。

保存图片到本地，查看代码，在代码最后发现username：XiDI@nUser

由于图像是gif文件，拆开发现第二帧的图像就是password。

发现password：luby’sphoto
不过提交，并不对。思路应该不错，不过不对就不知道什么情况了。

就此告一段落吧。