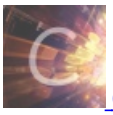
misc总结

原创

博闻善行 于 2022-01-27 22:31:13 发布 40 收藏

分类专栏： CTF 文章标签： git github https



1.uncompyle2是Python2.7的反编译工具，它可以把python生成的pyo、pyc字节码文件反编译为十分完美的源码，并可以将反编译后的源码再次生成字节码文件
安装方法：
git clone https://github.com/wibiti/uncompyle2
cd uncompyle2
python setup.py install
使用方法示例：
使用帮助：
uncompyle2 -h
查看了帮助会觉得里面操作有点麻烦，就是-o outfile必须先写，
例如有一个pcat.pyc，想反编译输出文件为pcat.py，你必须这样写：

uncompyle2 -o pcat.py pcat.pyc

2.工具winhex 和010Editor都需要安装

3.AES秘钥解密
#coding=utf-8
from Crypto.Cipher import AES
key=“copy__white__key”
obj=AES.new(key,AES.MODE_ECB)
path="/home/adworld/MISC/i_chunqiu/CryMisc_E1C844B98C4CAC14060994BD1933AF9F/gogogo/AES.encryt"
s=open(path,“rb”).read()
str=obj.decrypt(s)
with open(r’next.zip’,‘wb’) as f:
f.write(str)#解密后得到文件

3.zsteg可以检测PNG和BMP图片里的隐写数据。
git clone http://www.github.com/zed-0xff/zsteg
安装方法：
git clone https://github.com/zed-0xff/zsteg
cd zsteg/
gem install zsteg

4.在线PS网址https://www.uupoop.com/

5.git泄露：考虑 git 泄露 下载 Git_Extract 使用 python git_extract.py 加上.git 所在目录，还原出另一个 flag.txt,及 s.py, 删除原来的 flag.txt，将新抽取的 flag.txt.xxx 重命名为 flag.txt，运行 s.py 得到 flag
提取远程 git 泄露或本地 git 的工具
下载地址：https://github.com/gakki429/Git_Extract

6.压缩包解密工具除了一个archpr工具外还有一个azpr

7.winhex进行16进制搜索查找简单编辑，hdx可以大量文本编辑，下载地址

8.要复制winhex16进制对应的文本内容，可以先吧16进制复制出来进行字符串转换即可

10.xjki的培训文档带上

11.流量包分析时对请求方式筛选很有用：http.request.method==POST

13.除了使用binwalk提取文件以外，kali自带了foremost工具用来提取文件

14.存储该文件电脑的一个内存快照题目解法：https://www.ichunqiu.com/writeup/detail/1415

15.常用网址总结：
（1）16进制字符串文本转换https://www.bejson.com/convert/ox2str/
（2）unicode在线编解码：https://www.css-js.com/tools/unicode.html
（3）在线摩斯密码解密 https://www.bejson.com/enc/morse/
（4）MD5在线爆破 https://www.cmd5.com/
（5）维吉利亚在线解密 https://guballa.de/startseite
https://www.guballa.de/vigenere-solver