CTF——常见题型

原创

Vista、 于 2020-07-11 10:07:00 发布 2885 收藏 32

分类专栏： 信息安全 文章标签： CTF

本文链接：https://blog.csdn.net/qq2539879928/article/details/107280065

最近面试的时候，有面试官考察了一些常见的CTF题型。

于是索性，我将一些常见的CTF知识点整理如下：

为方便您的阅读，可戳下方蓝字，快速跳转！！！

01 WEB

命令注入：web页面输入款中注入Shell命令

SQL注入：Web页面输入框中注入SQL命令

文件上传：绕过文件上传限制上传webshell至服务器

文件包含：网站开放了特定函数，可浏览网站本地文件，最好配合webshell使用

XSS:注入脚本命令，弹窗关键信息，获取cookie

代码审计：检索源代码，寻找源代码中的漏洞

Restful API：打开Web世界通信的栈道

Owsap 10：10项最严重的的Web应用程序安全风险

BurpSuite：抓包改包神器，拦截、查看、修改Http/Https请求包

02 Crypto（密码学）

凯撒密码：英文字母表，不停的移位操作

摩斯密码：一句话：滴答滴答（-...） 对照密码本翻译

栅栏密码：固定一个行数，从上到下排列，在从左到右读

培根密码：每个字母转换位一组5个英文字母

云影密码：密文由01248数字构成

键盘密码：与键盘一一对应

Base64编码：64 = 26个小写字母 + 26个大写字母 +10 个数字 + 2 个特殊字符 + 1个尾巴，区分大小写、尾部可能有=、==

ASCII编码：全部都为数字或二进制，如56,45,53,63,45,33 、 0001010010100101010

URL编码：带有特殊符号%，如%9%h%d%s

unicode编码：带有许多/uxxx，如/uxxfdsafasd/uxxjfskdjfk

JS混淆:有eval和function存在,如eval(fdsajkfj)

aaencode编码：有表情符号，如(づ￣3￣)づ ╭❤～

03 MISC（安全杂项）

图片隐写：信息隐藏在jpg文件中，可利用kali下exiftool工具，如exiftool flag.jpg

GIF图片隐写：信息藏在gif文件中，可使用stegsollve 工具提取

PDF文件：信息隐藏在PDF文件中，可使用kali工具pdftotext，如pdftotext flag.pdf flag.txt

流量隐写：从pcap文件中提取隐藏信息

1、通过binwrok查看pack包里隐藏的文件

2、通过formost分离出隐藏文件

3、通过wireshark分析流量中的信息 过滤字符串 图片二进制的起点是 FFD8 终点是FFD9

4、通过hex对二进制文件进行保存 成为图片

残破的二维码复原/图片复原：残缺混乱的图片重新排列组合，可能缺定位符，用图片修改软件补上就好

04 PWN（溢出类）

缓冲区溢出：控制函数返回地址，可利用上python的pantool库

返回到Libc：其实也是缓冲区溢出，只不过溢出的同时，伪造了另一个函数栈，他需要安排另一个函数的入参和返回地址，这里一般溢出的时候进入system函数，然后安排一个binshell字符串，控制函数返回地址。

栈值覆盖：栈值覆盖也是缓冲区溢出，只不过它控制的不是函数的返回地址，而是栈上的一个地址，一般是if的一个判断值，将这个false改为true，从而改变函数的执行流程

整数溢出：int8的范围是0-255，那么256就是0。如果发生在if的判断里，通过整数溢出就可以进入一个新的分支，如果新的分支再有一个缓冲区溢出漏洞，就可以改变函数的执行流。

格式化字符串：%n任意地址写值，一个int*指针

05 REVERSE（逆向工程）

PEtools查壳：逆向题，先查壳在说

Upx脱壳：脱了壳才算开始

IDA pro静态反汇编：静态分析神器

OllyDbg动态调试:动态分析神器，通过各种断点调试进入到调试，改变函数流程等。

逆向签到题：通过对二进制文件扫描一下，linux下通过 strings demo | grep flag windows通过hex

以上文章，作为自己的学习笔记，仅供参考