# CTF学习指南

原创

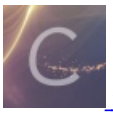
m78星□ 于 2020-06-24 17:41:28 发布 

分类专栏： 笔记



本文链接：https://blog.csdn.net/m0_48178474/article/details/106948678







CTF学习操作指南

Forensics（取证隐写）

1. 信息搜集
2. 编码分析（常见编码，转换技巧）
3. 数字取证&隐写分析
4. 赛题分析
   Crypto（密码学）
5. 古典密码学
   单表替换加密（通用特点、凯撒密码、基于秘钥的凯撒密码、移位密码、埃特巴什码、简单替换密码、仿射密码）
   多表替换加密（playfair密码、polybius密码、维吉尼亚密码、Nihilist密码、希尔密码、autokeycipher）
   其它加密（培根加密、栅栏密码、曲路密码、列移位加密、波利比奥斯方阵密码、01248密码、jsfuck密码、猪圈密码、舞动的小人密码、键盘密码）
6. 对称密码
   RC4、DES、AES、分组模式
7. 非对称密码
   RSA（模数相关、公钥指数、私钥d、选择密文、侧信道攻击）
8. 哈希函数
   MD5、SHA1、Hash攻击
9. 其它
   数字签名、证书格式、伪随机数
   Web
   Web安全（一）:1.Web CTF介绍；2.CTF中Web trick在实际中的运用；3.Web CTF中的常用工具
   Web安全（二）服务端漏洞:1.SQL注入攻击与防御；2.任意文件操作漏洞；3.认证与会话管理；4.命令注入；5.访问控制
   Web安全（三）前端漏洞：1. XSS漏洞挖掘与利用；2. CSRF利用；3. 域、同源；4. 挑战CSP及沙箱；5. XSS及CSRF防御
   Web安全（四）代码审计：1.PHP代码审计；2.Python代码审计
   Web安全（五）内网渗透：1.端口转发&&边界代理；2.获取shell ；3.信息收集(探测结构)；4.hash抓取；5.远程连接&&执行程序
   eg1:
   Wp：通过正常访问页面发现，ip不在允许的范围之内，排查应该是http协议的问题。于是进行代理抓包，构造访问ip 具体命令：burp内加入X-Forwarded-For:1.1.1.1 点击GO 直接查看返回信息，获得CTF字符串，直接解题。

RE（逆向工程）
逆向工程基础（X86/64，ARM，AARCH64各种架构：汇编10分钟入门、calling convention）
IDA Pro、HexRay、OllyDBG、GDB工具准备与快速入门
PE/ELF文件格式
Windows逆向：MFC分析、.Net逆向、X64逆向等
Linux逆向：LD_PRELOAD、混淆与反混淆、OLLVM
加壳与脱壳：壳简介、各类手工脱壳方法
反调试技术：去除花指令、反虚拟机、反调试各种trick
常见算法分析与识别
WinDBG和驱动调试：WinDBG、微软符号表、rootkit调试、加载驱动
其他技巧：符号执行、Pintools、恢复符号、识别虚表、编写IDA Processor
Mobile（移动安全）
1.安卓背景介绍（安卓生态圈简介、安卓安全架构、常用概念和技术）
2. 安卓分析环境与工具准备
3.逻辑代码保护与逆向技术的对抗（编译与反编译、加壳与脱壳、原生代码混淆与解混淆、隐藏与取证、Hook与注入）
4.应用层漏洞分析（组件、传输、存储、加密、凭证安全）
5. 安卓ROOT攻击：未加锁、锁定设备root
6.题目解析（直接逆向技术题目、原生层混淆题目、加脱壳技术题目）
Pwn
Pwn（一）栈溢出：

1. 各种基础(栈 调用约定等）
2. 各种工具的使用(GDB IDA pwntools等)
3. 格式化字符串(%p AAR %n AAW)
4. 栈溢出(各种类型：ret2shellcode/ret2syscall/ret2libc/ret2__scu_init/ret2reg/ret2dl resolve/SROP/ret2VDSO/overflow ebp/JOP/COP等)
   Pwn（二）堆溢出：
5. Linux堆管理基础
6. 各种堆利用技巧(unlink/UAF/Fastbin Attack/各种house of xxx)
   Pwn（三）其他漏洞：
7. IO_FILE利用
8. 整数溢出转堆栈溢出
9. 多线程Race Condition
10. Linux内核和驱动漏洞利用
    Pwn（四）Win平台漏洞：
    Windows平台漏洞利用

- windows下的防护机制
- windows平台漏洞调试工具的使用
- windows下的栈漏洞的利用技术
- windows下的堆漏洞的利用技术
  Pwn（五）漏洞挖掘：
  CTF常见漏洞快速挖掘与发现方法：
  污点追踪（Pin-tools）
  Fuzzing（AFL系列）
  符号执行（Angr/KLEE等）
  其他方法