夺旗赛 CTF 六大方向基础工具简介集合（MISC，WEB，Crypto，Reverse，Pwn，Mobile）

原创

小哈里 于 2022-01-14 18:58:30 发布 11754 收藏 10

分类专栏： # 网络安全 文章标签： 前端 网络安全 CTF 工具

本文链接：https://blog.csdn.net/qq_33957603/article/details/122492189

一、MISC方向

杂项往往是不能被归到其他类别里的题目，所以什么样的题都有，工具也很杂。

主要的分类有：

1、视频音频图片类

- **Stegsolve.jar**
  一款图像隐写工具，支持使用不同方式解除图像隐写，是图像隐写的必备工具。可以破解色道隐写等，需要JAVA环境。
- **QR_Research.exe**
  用于扫描二维码，有些题目需要自己准备二维码定位角图用p图工具p上去
- **Audacity.exe**
  运行于windows的常用音频隐写工具
- **outguess（linux）**
  开源隐写算法，支持各种格式的文件，C语言编写
- MP3STEGO.exe
  一款用于音频的典型隐写工具。
- 隐形水印工具v1.2.exe
  用于添加和隐藏图片中的水印。
- tweakpng-1.4.6.exe
  png图片修改查看
- foremost（linux）
  开源隐写算法，支持各种格式的文件
- PotPlayer64
  视频逐帧播放，每一帧提取等。
- wbs43open隐写工具
  适用于pdf，bmp图片等格式的隐写。

2、压缩包、磁盘取证

- **010Editor**
  一款**专业的文本编辑器和十六进制编辑器**，其设计旨在轻松简便地快速编辑您计算机上任何文件的内容。
- **WinHEX**
  是一个德国软件公司X-Ways所开发**的十六进制数据编辑处理程序** 。
- **archpr（Advanced Archive Password Recovery）**
  压缩包密码解压工具，支持各种模式的破解。
- WinRARa64
  RAR格式解压工具。
- 7zip
  各种压缩格式解压工具。
- **Ziperello**
  ZIP密码破解工具(Ziperello)支持双重模式破解：暴力/字典，也具备断点续破、掩码破解等高级特性
- 密码字典生成器
  用于生成爆破压缩包密码的字典。
- **AccessData_FTK_Imager**
  磁盘镜像取证工具。可挂载镜像，创建镜像文件。
- **UltraISO**
  虚拟光驱、ISO烧录到U盘或光盘，小巧免费无广告
- **AlternateStreamView**
  NTFS数据流检查工具，可以一键扫描你的NTFS驱动器，查找所有的隐藏的备用流，之后可以将备用流提取到指定的文件夹中。
- **文件格式总结.txt**
  各种压缩包格式的整理
- **binwalk& foremost**
  检测 & 分离工具，扫描文件中是否有隐藏文件并将其分离。

3、wifi、蓝牙、流量包

- **Wireshark**
  多功能网络封包分析。是一个免费开源的网络数据包分析软件。网络数据包分析软件的功能是截取网络数据包，并尽可能显示出最为详细的网络数据包资料。
- **fiddler2**
  HTTP数据包抓取，用于HTTP调试的代理服务器应用程序。

4、环境（重要）

环境对于各个方向都是会用到的

- **Kali Linux（或WSL）**
  Kali Linux 是基于Debian的Linux发行版，设计用于数字鉴识和渗透测试。
  是著名的集成了众多工具的Linux。
- **Java环境**
  有许多的工具是基于java环境开发的（提供跨平台支持）。
- **python环境**
  Crypto，Reverse，Pwn，Mobile很多题目都需要写py代码实现。

二、WEB方向

1、渗透工具

- **Burp Suite**
  web应用程序渗透测试集成平台。 用于攻击web应用程序的集成平台。 它包含了许多工具，并为这些工具设计了许多接口，以促进加快攻击应用程序的过程。
  英文收费，有第三方早几代版本提供中文翻译以及注册服务。
- **HackBar-v2.3.1**
  一款用于安全测试的浏览器插件，可在Firefox和Chrome浏览器中使用，目前提供的功能有：常见编码和解码、POST/Cookies数据提交、SQL/XSS/LFI/XXE漏洞测试等。最新版本开始收费，可以用早先的版本注册。
- **sqlmap1.1.3官方版**
  Sqlmap是开源的自动化SQL注入工具。完全支持MySQL、Oracle、PostgreSQL、Microsoft SQL Server。在数据库证书、IP地址、端口和数据库名等条件允许的情况下支持不通过SQL注入点而直接连接数据库。
- Pangolin3.2.4
  SQL注入，扫描等
- DatabaseBrowser
  一款免费的数据库浏览器，开放源码的视觉工具，用于创建设计和修改数据库文件兼容的SQLite。
- **中国菜刀&Webshell**
  webshell、一句话后门
- **漏洞扫描：**
  御剑后台扫描珍藏版：目录扫描
  nmap-7.40官方版：强大的网站扫描，支持DOS和图形化
  DirBuster-0.12官方版：漏洞扫描、目录扫描，java语言编写
  AppScan 8.7 破解版：强大的WEB漏洞扫描工具

2、Web环境

- **phpStudy（小皮面板）**
  一个PHP调试环境的程序集成包。 该程序包集成最新的Apache+PHP+MySQL+phpMyAdmin+ZendOptimizer，
- **PuTTY**
  用于Linux系统远程连接，小巧免费无广告 。
  支持多种网络协议，包括**SCP，SSH，Telnet，rlogin**和原始的套接字连接。
  一次性安装，无须配置即可使用。
- **Termite-跳板机管理工具**
  一款内网穿透利器，分为管理端admin和代理端agent。它支持多平台、跳板机间正反向级联、内置shell管理等。
- **SecureCRTSecureFX_7.0.0.326**中文版
  一款的终端仿真程序，界面友好，可以在Windows下登陆Linux服务器主机，不仅支持**SSH1，SSH2，而且支持Telnet和rlogin协议** 。
- **WinSCP**
  一款免费开源的SCP客户端，运行于Windows系统下，遵照GPL发布。WinSCP除了SCP，还支持**SFTP、FTP** 、WebDAV、Amazon S3协议。
- phpMyAdmin
  phpMyAdmin密码爆破
- sunny-ngrok
  国内内网映射服务器，提供免费内网穿透。
- IP高精度定位
  查询IP地址的地理位置。
- IP代理池

三、Crypto工具

1、密码学综合

- **CTFCrackTools V4.0**
  米斯特安全官网开发， 内置目前主流密码（包括但不限于维吉利亚密码，凯撒密码，栅栏密码……）用户可自主编写插件。
  项目基于java和python，开源在github上。英文免费，有第三方早几代版本提供中文翻译。
- **CyberChef V9.20.3**
  英国情报机构政府通信总部（GCHQ）发布的一款新型的开源Web工具，为安全从业人员分析和解密数据提供了方便。号称“瑞士网络军刀”，以web页面的形式在浏览器中执行。
  项目开源在github上。英文免费，有第三方早几代版本提供中文翻译。
- **pyg密码学综合工具 v5.0**
  飘云大牛的综合了各种密码学的加密算法，研究密码学必备工具。
- **CAP4**
  CAP4 是一个很简单实用的验证加密算法的工具，是专门为教学而研制的密码制作与分析工具，已经在美国的很多高校得到了广泛使用。该工具囊括一些古典加密算法的破解，如凯撒密码、仿射密码等。
- 密码机器v1.0
  包括栅栏密码 凯撒密码 凯撒移位(中文版) 维吉尼亚密码 摩斯电码， MD5 置换密码 替代密码等等。

2、单项加解密

- **RSATool v17**
  可以用来计算 RSA 中的几个参数、生成密钥、加解密，一些不太复杂的破解工作也可以用它。
- **yafu**
  用于自动整数因式分解，在RSA中，当p、q的取值差异过大或过于相近的时候，使用yafu可以快速的把n值分解出p、q值，原理是使用Fermat方法与Pollard rho方法等。
- **TextForever V1.78**
  软件原名FineReader，包括HTML到文本文件的转换、文件合并、文件切分、段落合并、段落切分、内码转换（只能在Win 2k/XP下用）、文本替换、HTML整理、文本抽取、正则表达式（需要IE 5.5以上版本的支持）、批量OCR、tcr文件压缩/解压等功能。
- **小葵多功能转换工具**
  支持将普通编码转换URL/SQL_En/Hex/Asc/MD5_32/MD5_16/Base64等格式的编码，还支持解密base64编码。
- **md5crack3**
  MD5破解神奇，支持保存进度与自定义破解。
- **superdic超级字典生成器**
  一款密码字典生成工具。程序采用高度优化算法，制作字典速度极快。
- ASCII码随心换v3.0
  一款专门用来将字符转换成十进制和十六进制ASCII码的工具，还能将10进制和16进制ASCII码转换回字符。
- RegexTester
  使用工具regex tester来匹配正则表达式
- snow加密
  一种特定加密算法snow的解密工具
- 栅栏密码加解密1.10
  用于栅栏密码加解密
- UNICODE2ANSI转换器
  支持ascll码和unicode互相转换

3、在线工具（众多）

- **CTF 在线工具 by CTFcode**
  http://www.hiencode.com/
- CTF 工具资源库 by HBCTF team（含资源下载）
  https://www.ctftools.com/down/
- CTF-Wiki（可以github离线一下）
  https://ctf-wiki.org/introduction/resources/#ctf_1
- 萌研社 新约佛论禅
  http://hi.pcmoe.net/buddha.html
- 等等众多

四、Reverse方向工具

1、c家族的反编译

- **交互式反汇编器IDA Pro**
  目前最棒的一个**静态反编译软件**，交叉Windows或Linux WinCE MacOS平台主机来分析程序， 被公认为最好的花钱可以买到的逆向工程利器。**跨平台。 支持C家族的所有程序。**
- **Exeinfo PE**
  一款短小精悍且功能类似PEiD查壳程序的新一代万能查壳软件，内置海量PEiD的签名库并整合了近50种插件以及更加完整的中文语言包。
- **OllyDBG 第二代**
  一个新的**动态追踪工具**，将IDA与SoftICE结合起来的产物，Ring 3级调试器。
- C32Asm
  快速静态反编译PE格式文件(Exe、Dll等)。
  提供内存Dump、内存编辑、PE文件Dump、PE内存ImageSize修正等多种实用功能；提供内存反汇编功能，提供汇编语句直接修改功能，免去OPCode的直接操作的繁琐；

2、python反编译

- **pyinstxtractor**
  是一个用来反编译PyInstaller**打包成的exe的脚本**。基于python编写，开源于github。
- **Uncompyle6**
  可以把**pyc反编译**出py文件。基于python编写，开源于github。
- 在线pyc反编译工具
  https://tool.lu/pyc/

五、Pwn方向工具

1、基于python的库

- **pwn**
  一个 CTF (Capture The Flag) 框架, 并且是一个漏洞利用开发库 使用 Python 编写 它的主要被设计用于快速原型设计以及开发, 致力于让使用者编写尽可能简介的漏洞利用程序。
- **gmpy2**
  GNU高精度算术运算库，不但有普通的整数、实数、浮点数的高精度运算，还有随机数生成，尤其是提供了非常完备的数论中的运算接口，比如Miller-Rabin素数测试算法、大素数生成、欧几里德算法、求域中元素的逆、Jacobi符号、legendre符号等。
- **base64**
  py的内置库，支持base64的各种处理。base64一种任意二进制到文本字符串的编码方法，常用于在URL、Cookie、网页中传输少量二进制数据。
- requests
  是一个Python HTTP库，可以方便地发送http请求，以及方便地处理响应结果。
- Pillow
  是Python平台事实上的图像处理标准库了。

2、基于kali linux的工具

- **checksec**
  检查文件保护机制，检查可执行文件属性，例如PIE, RELRO, PaX, Canaries, ASLR, Fortify Source等等属性。
- **gdb**
  GNU symbolic debugger，一个强大的命令行调试工具。支持断点、单步执行、打印变量、观察变量、查看寄存器、查看堆栈等调试。
- **file**
  Linux file命令用于辨识文件类型。通过file指令，我们得以辨识该文件的类型。可以查看32 / 64位信息。
- **nc**
  netcat 的简写，有着网络界的瑞士军刀美誉。因为它短小精悍、功能实用，被设计为一个简单、可靠的网络工具。支持测试 linux 的 tcp 和 udp 端口，而且也经常被用于端口扫描。
- **objdump**
  用来显示二进制文件的信息，就是以一种可阅读的格式让你更多地了解二进制文件可能带有的附加信息。
- ROPgadget
  帮助你寻找合适的 gadgets，在编写你的 ROP exp 的时候有很大作用。

六、Mobile方向工具

1、java反编译

- **JEB Decompiler**
  一个功能强大的为安全专业人士设计的**Android应用程序的反编译工具** 。用于逆向工程或审计APK文件。
- **jd-gui-1.6.6**
  使用C++开发的一款**Java反编译工具**，它是一个独立图形界面的**Java源代码“.class”文件反编译**工具。只有3mb，开源于github，基于jd。
  JD是Java编程语言的反编译器，JD作为GUI工具以及Eclipse和IntelliJ IDEA集成开发环境的插件形式提供。
- **jadx**
  jadx 是一款功能强大的反编译工具，支持图形化的界面，拖拽式的操作。开源于github。可以跨平台使用。
- **ApkIDE_v3.3**
  一款可视化的、易用的、快捷的、一体化的**安卓APK修改工具**，集成了ApkTool、Dex2jar、JD-GUI等Apk修改工具，集Apk反编译、Apk查壳、加密解密、Apk调试分析、Apk打包、Apk签名，支持语法高亮的代码编辑器。
- **AndroidKiller_v1.3.1**
  可视化界面的一款反编译软件，省去了利用编译工具进行反编译的繁琐步骤。
- GDA3.97
  一款简洁、轻便、快速的交互式Android反编译分析工具

2、ARM汇编修改

- SO Helper 1.2
  简称SH，是一款可视化ARM汇编修改工具，它能快速的帮助你修改SO文件的汇编代码，并且SH也支持修改16进制。
- Arm汇编转换器
  一款不需要安装绿色小巧的汇编转换工具。使用这款Arm汇编转换助手可以轻松帮助用户将汇编转换成C语言。

3、Android解包工具

- **abe.jar**
  安卓备份文件提取 .bak文件解包成apk。
- **apktool.jar**
  apk格式文件与smali文件的转换
- **dex2jar.jar**
  dex格式文件与jar文件的转换
- **smali.jar**
  dex格式文件与smali文件的转换

4、Android运行工具

- **网易MUMU安卓模拟器**
  网易出品，界面简介，大概300M，不卡顿，功能也相对少，偶尔有广告。
- **蓝叠模拟器BlueStacks**
  印度公司研发。最有名，最古老的安卓模拟器之一。原理是把Android底层API接口翻译成Windows API，对PC硬件本身没有要求，在硬件兼容性方面有一定的优势。适合玩大游戏。
- **Virtualbox**
  Virtualbox是数据库巨头Oracle旗下的开源项目，通过在Windows内核底层直接插入驱动模块，创建一个完整虚拟的电脑环境运行安卓系统，加上CPU VT硬件加速，性能和兼容性都更好，但是对于电脑CPU有一定要求，超过五年以上的电脑使用起来比较吃力。
- **夜神模拟器**
  一款基于Virtualbox定制的安卓模拟器，直接集成NOVA桌面是它的一大特色。但多开效率需进行提升。卡顿、延迟、偶发性系统奔溃。