隐写术基础

原创

饼饼~ 于 2021-04-27 19:32:25 发布 175 收藏 2
文章标签： unctf 安全

1.图片隐写基础

常见类型:利用binwark工具分离图片　stegsovle工具利用　txt简写隐写　关键字搜索　16进制文件头补全修改png格式IHDR的问题　属性隐写+文件类型

常用工具：kali虚拟机（binwalk、foremost）　16进制编辑器（winhex、hexedit）　记事本或其他文本编辑器　stegsovle（基于java运行，需要配置java环境）

2.内存取证

类型：离线取证、在线取证、内存取证

内存取证：pc硬件架构、内存管理、ARM架构

内存取证技术：基于软件的内存获取技术和工具（硬件）禁止DMA获取内存技术，

基于物理内存分析的在线取证模型及其可信性，

影响内存获取可信性的因素：

内存获取的精密度，精准度和系统误差分析

分析获取工具的加载活动覆盖关键痕迹的概率

windowns内存分析原理：

windows操作系统关键组件

基于系统组件名称查找的windows内存分析方法

基于特征扫描和内存分析法

基于KPC结构方法

windows内存分析

进程信息分析：事件日志内存分析、注册表内存分析、内存的网络分析、服务的内存分析、内存中的文件。

linux操作系统内存分析原理

linux操作系统关键组件、ELF二进制格式、volatiltty物理内存分析方法

linux内存分析

进程信息、文件系统信息、网络连接信息、模块信息、系统信息、减缓文件分析

MAC os内存分析技术

系统配置信息的分析、进程信息分析、系统调用分析、SLAB分配器的分析、Bash命令获取、内核格式缓冲区信息的获取、挂载的文件系统信息分析、内核扩展分析、网络信息分析

安卓智能手机内存取证

智能手机的硬件组成

从数字取证到智能手机取证

智能手机的数据取证

安卓系统概述

安卓智能手机内存取证

内存分析

3.内存取证在云安全中的应用

云计算机服务模型

虚拟环境下面临的安全风险及研究现状

基于内存分析的虚拟机安全监控方法

基于内存分析的与云安全威胁监控技术

4.木马监测分析

恶意代码

APT攻击

windows恶意代码检测

linux恶意代码j检测

macos恶意代码检测

5.系统密码破解

密码认证机制

windows系统密码破解

linux密码破解

Macos x登录屏保密码破解

以修改内存方向macos植入应用程序