# 第一章 利其器，善其事：基础知识（殷悦）

## 1.1 Linux常用命令

### 1.1.1 目录操作

### 1.1.2 文件搜索

### 1.1.3 字符串搜索处理

### 1.1.4 网络操作基本命令

### 1.1.5 Vim教程

### 1.1.6 实例1：配置Linux网络

## 1.2 CTF常用工具集

### 1.2.1 文本查看

### 1.2.2 文件分析

### 1.2.3 密码破解

### 1.2.4 Web

### 1.2.5 音视频图片处理

### 1.2.6 Android

### 1.2.7 实例2：常见文件破解实例

## 1.3 Wireshark数据包分析

### 1.3.1 数据包查看

### 1.3.2 协议简介

### 1.3.3 搜索过滤机制

### 1.3.4 Linux下的WireShark:TCPDump

### 1.3.5 实例3：网页抓包分析

## 1.4 计算机网络

### 1.4.1 IP和端口

### 1.4.2 TCP/IP协议

### 1.4.3 Arp协议

### 1.4.4 ICMP协议

### 1.4.5 NAT

### 1.4.6 Linux工具 iptables route

### 1.4.7 实例4：netcat通信演示 反弹Shell 配置iptables防火墙

## 1.5 汇编语言

### 1.5.1 寄存器介绍

### 1.5.2 基本指令

### 1.5.3 堆栈介绍

### 1.5.4 实例5：制作植物大战僵尸外挂

## 1.6 C语言

### 1.6.1推荐书籍

### 1.6.2 GCC的使用

### 1.6.3 Makefile编写规则

### 1.6.4 GDB调试

### 1.6.5 实例6：编译iodine

## 1.7 Java

### 1.7.1基本语法

### 1.7.2 函数,接口,类

### 1.7.3 继承,派生

### 1.7.4 实例7：编写一个安卓聊天软件

## 1.8 Python

### 1.8.1 基本语法

### 1.8.2 实例小程序

### 1.8.3 实例8：手写Python密码破解工具，Python Telnet SSH密码暴力破解

## 1.9 SQL语句

### 1.9.1 基本语法

### 1.9.2 常见注入类型

### 1.9.3 实例9：注入拿下网站数据库

## 1.10 JavaScript

### 1.10.1 基本语法

## 1.11 Windows程序设计

### 1.11.1 实例：同实例5

# 第二章 不破不逆：逆向分析（魏子豪）

## 2.1 x86反汇编（Windows环境）

### 2.1.1 知识提要

#### 2.1.1.1 8086汇编基础（堆、栈及栈帧、调用约定）

#### 2.1.1.2 PE文件结构

#### 2.1.1.3 Windows程序设计（消息机制、常用API等）

#### 2.1.1.4 壳

#### 2.1.1.5 常用调试工具和反编译工具简介

### 2.1.2 C++逆向分析技术

### 2.1.3 MFC消息机制分析及拦截

### 2.1.4 脱壳

## 2.2 Android逆向

### 2.2.1 环境配置

### 2.2.2 初识APK、Dalvik字节码以及Smali

### 2.2.3 深入Smali文件

### 2.2.4 Smali函数分析

### 2.2.5 Smali实战分析

### 2.2.6 了解JAVA反编译工具

### 2.2.7 了解JEB和IDA使用

## 2.3 pyc逆向

### 2.3.1 解释器，pyc文件格式及Python代码对象

### 2.3.2 CTF题目一览

# 第三章 由Web而内：Web安全（杨智）

## 3.1基础准备

### 3.1.1基础语言

HTML／CSS、JavaScript、PHP、SQL.了解一个index.php是如何解析的

### 3.1.2其它基础

#### 3.1.2.1基本的C/S物理结构

#### 3.1.2.2基本的HTTP协议相关知识

#### 3.1.2.3基本的浏览器解析的流程与原理

#### 3.1.2.4了解常见编码

#### 3.1.2.5了解同源策略

## 3.2常见攻击方式

### 3.2.1 SQL注入

### 3.2.2 XSS攻击

### 3.2.3文件上传

### 3.2.4 CSRF

### 3.2.5文件包含

### 3.2.6命令执行

### 3.2.7 PHP审计

## 3.3 常用工具使用

### 3.3.1 Burpsuite

### 3.3.2 Fierfox(重要插件：Firebug,Hackbar,Fiddler)

### 3.3.3 Sqlmap的使用

### 3.3.4 其他利器

## 3.4 其它

### 3.4.1 源码泄露

### 3.4.2 旁注

### 3.4.3 其它注入方式

# 第四章 It`s mine!: Pwn（柴冕汉郎，李云鑫）

## 4.1 ELF

### 4.1.1 基本概念

### 4.1.2 文件相关代码

### 4.1.3 操作方法

## 4.2 PLT与GOT的分析

### 4.2.1 PLT与GOT是什么及其联系

### 4.2.2 结合实例分析PLT与GOT表

## 4.3 堆栈

### 4.3.1 堆栈基本概念

### 4.3.2 内存与寄存器

### 4.3.3 堆栈工作原理

### 4.3.4 反编译相关

### 4.3.5 溢出

### 4.3.6 攻击应用

## 4.4 ROP攻击技术的学习及应用

### 4.4.1 ROP技术的产生背景及原理

### 4.4.2 ROP技术的实例教程

## 4.5 Ret2libc攻击方法学习级应用

### 4.5.1Ret2libc攻击原理

### 4.5.2 Ret2libc 技术的实例教程分析

## 4.6 UAF漏洞分析

### 4.6.1 Uaf 漏洞的产生原理

### 4.6.2 Uaf 漏洞的利用方法

## 4.7 Doublefree漏洞分析

### 4.7.1 Doublefree 漏洞的产生原理

### 4.7.2 Doublefree 漏洞的利用方法

## 4.8 Pwntools的安装及其应用

### 4.8.1 Pwntools 的安装教程

### 4.8.2 Python借助Pwn库对于实例操作分析

## 4.9 gdb的插件安装及使用方法

### 4.9.1 Linux下gdb的使用命令详解

### 4.9.2 gdb插件peda的安装及其使用命令详解

# 第五章 达芬奇密码：密码学（吴华瑞）

## 5.1 对称密钥加密

### 5.1.1传统对称密钥密码

#### 5.1.1.1代换密码

#### 5.1.1.2换位密码

#### 5.1.1.3流密码和分组密码

### 5.1.2现代对称密钥密码

#### 5.1.2.1现代分组密码

#### 5.1.2.2现代流密码

## 5.2 公钥（非对称）密钥加密

### 5.2.1.素数及其相关的同余方程

### 5.2.2大数分解和离散对数算法

### 5.2.3公钥加密

## 5.3 附录

# 第六章 火眼金睛：常见文件格式（周帅）

## 6.1 各类文件格式的头文件标志

# 第七章 秘而不宣：隐写术（黄晓雪）

# 第八章 又见一帘数论：RSA算法专题（罗晓倩）

## 8.1 RSA简述

## 8.2 主要攻击及破解方法

### 8.2.1 参数的提取

#### 8.2.1.1 pem文件

#### 8.2.1.2 pcap文件

#### 8.2.1.3 ppc模式

### 8.2.2 模数n的分解

### 8.2.3 选择密文攻击

### 8.2.4 低加密指数攻击

### 8.2.5 低解密指数攻击

### 8.2.6 明文攻击

### 8.2.7 共模攻击

### 8.2.8执行攻击

## 8.3 工具

8.3.1 模数n分解工具：

8.3.1.1在线：tactordb

8.3.1.2 Python源码

8.3.2 明文计算工具：大数计算器，Python的pow（）函数

## 8.4 例题

## 8.5 参考资料