马士兵教育
www.mashibing.com

网络安全大师课 2.0版

2022年最新课程简章

V2022.1

复合全能人才培养 / 一站式知识服务提供商 / 品牌保障

第一部分：基础与准备

1.1. 中华人民共和国网络安全法

- 网络安全行业介绍
- 什么是黑客和白帽子
- 网络安全课程整体介绍
- 网络安全的分类
- 常见的网站攻击方式
- 安全常见术语介绍
- 《网络安全法》制定背景和核心内容
- 《全国人大常委会关于维护互联网安全的决定》
- 《中华人民共和国计算机信息系统安全保护条例（2011年修正）
- 《中华人民共和国计算机信息网络国际联网管理暂行规定》
- 《计算机信息网络国际联网安全保护管理办法》
- 《互联网信息服务管理办法》
- 《计算机信息系统安全专用产品检测和销售许可证管理办法》
- 《通信网络安全防护管理办法》
- 《国家安全法》
- 《数据安全法》
- 《个人信息保护法》
- 《互联网安全产品漏洞管理规定》

1.2. Linux操作系统

- 操作系统发展历史与Linux
- 安装VMWare软件
- VMWare常用操作
- VMWare克隆和快照功能
- 安装和配置CentOS7
- 为虚拟机配置静态IP
- CentOS安装软件的方式
- Linux操作系统目录结构
- Linux命令格式
- Linux文件和目录操作命令
- Linux用户和用户组操作命令
- Linux查看和操作文件内容命令

- Linux文件压缩和解压缩命令
- Linux网络管理命令
- Linux磁盘管理和系统状态命令
- Linux安全加固

1.3. Linux网络管理

- 网络必备基础
- 物理层
- 数据链路层与交换机
- 网络模型OSI TCP对等传输
- 虚拟局域网VLAN
- 静态路由与配置
- 网络地址转换NAT
- 访问控制列表ACL
- IP协议与IP地址分类
- 子网掩码
- 网关
- 子网划分

1.4. HTML和CSS

- HTML简介和发展史
- 开发工具的使用
- HTML5骨架
- HTML基本语法
- HTML常用标签
- HTML标签的基本使用（有序和无序列表）
- HTML标签的基本使用-表格
- HTML标签的基本使用-form表单
- HTML布局常用标签-div和span
- CSS的基本介绍
- CSS常用属性-盒子
- CSS样式表的基本使用
- CSS选择器-基础选择器
- CSS选择器-高级选择器
- CSS继承性和层叠性
- CSS属性学习-color
- CSS属性学习-font-family

- CSS属性学习-line-height
- CSS属性学习-font-weight
- CSS属性学习-font-style和综合属性
- CSS盒模型
- CSS盒模型-width和height
- CSS盒模型-padding
- CSS盒模型-border
- CSS盒模型-margin
- CSS属性扩展-margin塌陷
- 浮动的基本使用
- 浮动的性质
- 浮动贴边特性练习
- 清除浮动方法
- a标签的伪类
- background属性学习
- 综合应用
- 相对定位（relative）
- 绝对定位（absoutle）
- 固定定位（fixed）

1.5. JavaScript

- JavaScript简介
- JavaScript用途
- JavaScript组成
- 数字类型字面量
- 变量基本使用
- 变量提升
- 类型检测
- 数学运算
- 比较运算
- 逻辑运算
- if语句
- switch基础应用
- 嵌套循环
- break，continue while do while
- 函数认知
- 函数基本使用
- 局部变量

- 作用域
- return关键字
- 函数实战应用
- 回调
- 递归
- 函数自执行
- 数组
- 堆栈空间
- 正则表达式概述
- 正则使用技巧
- 正则字符集
- 正则边界符
- arguments
- 闭包
- DOM认识
- DOM方法
- 操作节点属性
- 操作节点样式
- 节点事件

1.6. PHP入门

- PHP简介与开发环境搭建
- PHP基本语法
- PHP变量与变量作用域
- 常量与数据类型
- 数据类型之复合类型
- 数据类型之特殊类型
- PHP运算符
- PHP流程控制
- superglobals 超全局变量
- PHP+Bootstrap 实现表单校验功能
- PHP+MySQL实现用户登录和注册功能

1.7. MySQL

- 数据库介绍：分类、安装、配置、登录、连接等
- 数据库基本操作：创建、查看、选中、查库表、删除数据库等相关命令行操作
- 数据字段操作：创建调整字段顺序排序删除等字段命令行操作

- 数据库表操作：创建选中删除数据库表等相关个命令行操作
- 数据类型：整型、浮点、字符、时间、符合型等
- 字符集合
- 索引
- 增删改查之更新记录、数据库权限操作

1.8. Python编程

- Python 介绍以及应用场景
- Python的安装
- 第一个 Python程序
- PyCharm的安装
- Python入门
- 变量练习题
- 字符串
- 分支语句
- 字符串分支语句练习题
- 列表
- 循环
- 元组
- 数组循环练习题
- 字典
- 函数
- 包和模块
- 类和对象

第二部分：渗透与攻防

2.1. SQL注入的渗透与防御

- 数据库基础
- 什么是SQL注入
- 产生SQL注入的原理
- SQL注入带来的危害有哪些
- GET型SQL注入漏洞是什么
- GET型SQL注入演示
- 工具以及靶场介绍
- POST注入是什么
- POST注入演示
- 判断SQL注入点
- 回归测试
- 注入类型
- Time-based基于时间的盲注
- Time-based基于时间的盲注注入手工演示
- Time-based基于时间的盲注注入脚本演示
- Time-based基于时间的盲注注入练习
- 基于User-Agent注入
- 基于User-Agent注入演示
- 基于User-Agent注入练习
- Error-based基于报错注入
- Error-based floor()基于报错注入演示
- Error-based extractvalue()基于报错注入演示
- 配合Burp Suite注入演示
- stacked queries基于堆叠注入
- stacked queries基于堆叠注入演示
- Bypass混淆绕过
- Bypass WAF绕过
- sqlmap的使用
- sqlmap原理以及源码阅读
- sqlmap实战1-COOKIE注入
- sqlmap实战2-USER-AGENT注入
- sqlmap实战3-手动注入与sqlmap对比
- sqlmap实战4-脱库

- sqlmap高级应用
- 如何防御SQL注入

2.2. XSS相关渗透与防御

- HTTP协议回顾
- Cookie和Session的作用
- XSS基本概念和原理介绍
- 反射型XSS和储存型XSS
- XSS获取Cookie
- XSS钓鱼获取用户密码
- XSS获取键盘记录
- XSS平台搭建xssplatform
- Kali beef-xss
- XSS漏洞检测和利用
- XSS防御与绕过
- XSS小游戏解题思路

2.3. 文件上传漏洞渗透与防御

- 文件上传代码实现
- 文件上传常见场景
- 文件上传漏洞原理
- Webshell介绍
- 网站控制工具：蚁剑、冰蝎、哥斯拉
- 漏洞带来的危害有哪些
- 工具以及靶场安装介绍
- 上传文件代码函数原理&上传图片拦截
- 后缀客户端验证-JS禁用&BURP改包&本地提交
- 后缀黑名单验证-大小写&加空格&符号点&::$DATA
- 后缀白名单验证-MIME修改&%00截断&0X00截断
- 文件头变异验证-验证MIME
- 二次渲染
- 代码逻辑&&条件竞争
- 如何挖掘和利用文件上传漏洞
- 如何防御文件上传漏洞

2.4. 文件包含渗透与防御

- 为什么要包含文件
- 文件包含漏洞概述及分类演示
- CVE实际漏洞案例
- PHP相关函数和伪协议
- DVWA靶场案例演示
- CTF题目案例
- 中间日志包含绕过
- PHP包含读写文件
- STRREPLACE函数绕过
- 包含截断绕过FNM_TBH函数绕过
- 文件包含漏洞挖掘与利用
- 文件包含漏洞修复方案

2.5. CSRF渗透与防御

- CSRF漏洞概述及原理
- CSRF案例分析：Gmail、Weibo
- CSRF漏洞危害
- CSRF和XSS的区别
- CSRF常见payload写法
- CSRF漏洞挖掘与自动化工具
- CSRF漏洞防御之Referer、Token、二次验证

2.6. SSRF渗透与防御

- SSRF漏洞概述和演示
- PHP SSRF相关函数和协议
- SSRF常见场景
- SSRF CTF题目分析
- 如何发现SSRF漏洞
- 如何防御SSRF漏洞

2.7. XXE渗透与防御

- XML基础知识之外部实体
- XXE 危害：读取任意文件、探测内网端口、执行命令、DoS
- 微信支付XXE漏洞分析

- XXE 漏洞发现和利用
- XXE 漏洞修复：禁用外部实体、过滤XML内容、WAF

2.8. 远程代码执行渗透与防御

- 远程代码执行原理介绍
- CVE实际漏洞分析
- Log4j RCE复现与原理详解
- PHP远程代码执行涉及函数
- pikachu和DVWA靶场案例分析
- CTF题目分析：eval执行、命令注入、过滤CAT、过滤空格、过滤目录符号
- 远程代码执行漏洞防御方法

2.9. 反序列化渗透与防御

- PHP类与对象回顾
- PHP Magic函数介绍
- 什么是PHP对象反序列化操作
- 为什么会出现安全漏洞
- CTF题目分析：攻防世界 unserialize3
- CVE-2016-7124漏洞利用
- Typecho CMS反序列化漏洞复现
- PHP反序列化漏洞如何修复
- Java反序列化演示
- Java反序列化漏洞演示
- Java反序列化漏洞发现利用点
- 如何避免反序列化漏洞

2.10. 逻辑相关渗透与防御

- 网络黑产事件与法律
- 逻辑漏洞挖掘必备技能
- 用户名遍历漏洞
- 恶意注册
- 未授权访问漏洞
- Session和Cookie伪造
- 验证码突破
- 密码找回漏洞
- 越权漏洞

- 短信轰炸漏洞
- 业务一致性相关漏洞
- 重定向漏洞

2.11. 暴力猜解与防御

- 密码安全概述
- 什么样的密码是不安全的
- 密码猜解思路
- Python代码实现暴力破解
- Burp Suite Intruder实现暴力破解
- Hydra爆破SSH密码
- Medusa暴力破解SSH密码
- msf破解SSH密码
- wfuzz爆破web密码
- 密码暴力破解防御手段
- 用户如何提升密码安全性

2.12. Redis未授权访问漏洞

- Redis服务器被挖矿案例
- Redis常见用途
- Redis环境安装
- Redis持久化机制
- Redis动态修改配置
- Webshell提权案例
- 定时任务+Bash反弹连接提权案例
- SSH Key提权案例
- Redis安全加固分析

2.13. AWVS漏洞扫描

- AWVS多平台安装方式与激活
- AWVS功能模块介绍
- AWVS扫描web站点
- AWVS生成报告
- AWVS扫描结果分析
- AWVS+Burp联动
- AWVS+Goby联动

2.14. Appscan漏洞扫描

- AppSacn介绍
- AppSacn扫流程和扫描方式介绍
- AppSacn安装与激活
- web应用程序扫描
- 环境搭建
- 扫描web应用程序
- AppScan被动手动探索扫描
- AppScan绕过登录验证码深入漏洞扫描
- AppScan自定义扫描策略，扫描针对性漏洞
- AppScan扫描报告解读

2.15. Nessus漏洞扫描

- Nessus安装与激活、配置
- Nessus功能模块介绍
- Nessus扫描Web站点
- Nessus生成扫描报告
- Nessus扫描报告解读

2.16. MSF-Metasploit Framework

- msf发展历史
- 缓冲区溢出漏洞
- Linux安装msf
- Kali更新msf
- Windows安装msf
- msf图形化界面
- msf目录结构
- msf核心功能
- msf核心模块与功能
- msfvenom常用命令参数
- msfconsole漏洞利用流程
- meterpereter功能介绍
- PHP反弹连接演示
- MS17_010永恒之蓝漏洞演示
- Linux脏牛漏洞提权演示
- msf后渗透

- 后渗透之访问文件系统
- 后渗透之上传下载文件
- 后渗透之屏幕截图
- 后渗透之键盘记录
- 后渗透之调用摄像头
- 后渗透之创建账号
- msf进阶
- msf Auxiliary辅助模块
- msf编码免杀
- msf清除事件日志

2.17. 社会工程学

- 社工学之交流模型概述
- 社工学之通过交流方式收集渗透信息
- 社工学之“香农”-“韦弗”模型概述
- 社工学 香农-韦弗模型基础
- 社工学 香农-韦弗模型分层
- SMCR通信模型
- SMCR通信模型规则
- 制定交流模型
- 真实钓鱼邮件案例解说
- 工具-诱导篇
- 工具-诱导含义
- 工具-诱导交谈的步骤
- 工具-成功诱导的条件和技巧
- 工具-提问的艺术

2.18. ARP渗透与防御

- 章节1:ARP原理
- 章节2:ARP断网攻击
- 章节3:ARP流量分析
- kali数据包转发
- dsniff工具介绍
- url流量分析过程讲解
- 章节4:ARP-wireshark获取用户数据
- wireshark工具介绍
- ARP攻击截获用户信息步骤

- wireshark过滤命令讲解
- 章节5:ARP-Ettercap-截获流量信息
- Ettercap工具介绍
- Ettercap界面操作攻击
- Ettercap功能讲解
- Ettercap命令行攻击
- 章节6:ARP网速限制
- TC工具介绍
- TC命令介绍
- ARP攻击限制网速的具体步骤
- 限速原理讲解
- 章节7:ARP-DNS欺骗
- ARP-DNS原理和劫持概念讲解
- ARP-DNS常用命令讲解
- ARP-DNS攻击步骤01
- ARP-DNS攻击步骤02
- ARP-DNS攻击课堂小结
- 章节8:ARP防御
- ARP防御方法介绍
- ARP防火墙防护ARP攻击
- ARP设置临时绑定网关MAC地址为静态
- ARP设置永久绑定网关mac地址
- linux防御ARP攻击
- 网关或者路由器防御ARP攻击
- web服务器防御ARP攻击

2.19. 系统权限提升渗透与防御

- WINDOWS 提权常用命令
- WINDOWS 提权实战、提权防范
- WINDOWS 提权后期密码安全性测试
- LINUX 权限提升以及提权必备的命令学习
- LINUX 脏牛提权以及 SUID 提权

2.20. DOS与DDOS渗透与防御

- SYN+FLOOD攻防还原
- IP地址欺骗攻防
- DNS放大攻击攻防还原

- SNMP放大攻击攻防还原
- NTP放大攻击攻防还原
- 应用层CC攻防攻防还原
- 其它类型压力测试
- DDOS安全防范

2.21. 内网相关渗透与防御

- 外到内渗透渗透
- 内到内渗透渗透
- 内网渗透测试
- BURP + PROXIFER抓包(解决有些APP无法获取数据包)

2.22. 无线相关渗透与防御

- 章节1:环境准备
- 协议补充
- wifi协议
- AP和客户端介绍
- Ap专业术语介绍
- 网卡工作模式
- wifi渗透环境搭建
- 章节2:专属字典打造
- 概念介绍
- 亦思社会工程学密码生成器
- 真空密码生成器
- safe6密码生成器
- Crunch密码生成器
- 千万常用密码
- 章节3:Windows下对附近无线网络进行扫描
- windows扫描附近的wifi
- windows-ntesh探索WiFi密码
- 章节4:熟悉kismet
- kismet软件介绍
- kismet嗅探wifi
- 章节5:aircrack-ng探索防护WEP加密
- WEP介绍
- 认证类型讲解
- 加密算法介绍

- WEP加密和解密
- Aircrack-ng 常用工具包
- Aireplay-ng 的 6 种攻击模式
- WEP wifi探索步骤-1
- WEP wifi探索步骤-2
- 遇到错误的处理方式
- 章节6:Gerix-wifi-cracker自动化探索防护WEP加密
- gerix-wifi-cracker环境准备
- gerix-wifi-cracker探索步骤讲解
- gerix-wifi-cracker探索实操讲解
- 章节7:WEP-wifite自动化渗透WEP加密
- wifite工具介绍
- wifite扫描讲解
- wifite渗透步骤讲解
- 章节8:WEP渗透新思路
- Hirte介绍
- Hirte渗透姿势1
- Hirte渗透姿势2
- 章节9:aircrack-ng渗透WPA加密
- WPA概念介绍
- WPA工作原理
- wifi设置讲解
- WPA专属字典打造
- WPA渗透步骤讲解
- WAP渗透家用路由器
- 章节10:WPA-hashcat跑包渗透
- hashcat介绍
- 渗透姿势讲解
- 章节11:WPA-创建Hash-table加速并用Cowpatty渗透
- Cowpatty介绍
- cowpatty渗透
- hast-table加速渗透
- 章节12:WPA-自动化渗透WPA加密
- 章节13:WPA渗透-windows下GPU跑包加速
- 章节14:WPA渗透-pyrit：batch-table加速_“attack_db”模块加速
- 章节15:WPA渗透-pyrit：GPU加速_Hash-table加速_batch-table加速
- 章节16:WPA渗透-使用airolib-ng创建彩虹表加速
- 章节17:WPS渗透-reaver工具穷举pin码

- 章节18:WPS渗透-Pixiewps秒破WPS_wifite穷举

2.23. 木马免杀问题与防御

- Metasploit 木马免杀介绍
- MSF木马攻击以及防御
- Exploits漏洞利用模块对目标进行漏洞利用
- Payloads在目标机器执行的代码
- Encoders编码模块绕过入侵检测和过滤系统
- Evasion躲避模块生成免杀payload

第三部分：工程与实战

3.1. 渗透报告编写

- 大中型企业渗透测试报告编写注意事项
- 遵从规范
- 行业标准
- 专业服务
- 文档
- 报告格式
- 封面页
- 保密声明
- 文档控制
- 时间表
- 执行总结、方法论
- 渗透测试流程
- 调查结果总结
- 漏洞
- 网络考虑的因素及建议
- 附录
- 术语表
- 工作说明书
- 外部渗透测试
- 工作说明书附加材料
- 渗透测试报表工具说明
- 小结

3.2. 等级保护

1）为什么要学习等保

- 什么是等级保护
- 什么是信息系统
- 什么是信息系统安全
- 等保的发展历程
- 等保的关注对象
- 等保的实施流程

- 等保的参与角色
- 课程学习目标

2）等保常见问题解答

- 哪些行业需要等级保护？
- 不做等级保护可以吗？
- 等保是按单位实施还是按系统实施？
- 系统部署在阿里云，需要做等保吗？
- 内网系统需要做等保吗？
- 做等级保护测评需要多久？
- 等保测评是一次测评，终身有效吗？
- 做等级保护要多少钱？
- 是不是定级越低越好？
- 等级保护测评的难点有哪些？

3）等级保护相关概念介绍

- 第三方测评机构
- 等保测评师岗位
- 安全产品服务和厂商
- 关保：关键信息基础设施保护
- 分保：涉及国家秘密的信息系统分级保护管理办法
- 重保：重要时期安全保障服务
- ISO27000体系
- 风险评估

4）等保2.0解读

- 等级保护发展历程
- 等级保护与网络安全法
- 等保2.0修订背景
- 等保2.0变化内容
- 等保2.0标准体系

5）等保2.0通用要求解读

- 安全框架
- 安全通用要求
- 控制类和控制项

- 2.0网络拓扑结构设计
- 安全设备配置建议
- 2.0扩展要求解读

6) 等保实施流程

- 定级备案
- 风险评估、差距分析
- 安全规划设计
- 建设整改
- 等级测评
- 监督检查

7) 等保案例分析

3.3. 应急响应

- 企业安全应急响应流程
- 木马实战演练
- 服务器入侵实战演练
- Windows系统入侵实战演练
- ARP欺骗攻击实战演练

3.4. 代码审计

- 代码安全测试介绍
- 代码安全测试方法
- 代码审计的通用思路
- 漏洞产生的原因
- 漏洞挖掘流程分析
- 手工代码审计实例分析
- SEAY源代码审计系统使用
- 工具局限性

3.5. 风险评估

- 项目准备
- 实施申请
- 培训事项

- 物理环境
- 网络结构
- 硬软件资产
- 信息系统
- 数据资产
- 服务器资产
- 安全管理
- 安全措施

1）脆弱性评估

- 网络设备脆弱性评估、交换机、路由器、安全设备
- 数据库脆弱性评估MySQL、MSSQL、Oracle
- 中间件脆弱性评估
- 主机璀错性评估
- 安全渗透测试

2）信息系统风险控制规划

- 安全技术控制规划
- 安全管理控制规划

3）报告输出

- 信息系统脆弱性评估报告
- 信息系统威胁评估报告
- 信息系统资产评估报告
- 信息系统风险评估综合报告

3.6. 安全巡检

- 漏洞扫描(绿盟、安恒、启明及开源漏洞扫描器在企业中应用,同时完成漏洞扫描之后如何编写漏洞扫描报告
- 实战案例:策略检查(交换机、路由器、安全设备、操作系统、数据库、应用安全配置等进行策略检查)
- 实战案例:日志审计(分别通过安全日志分析工具及手工方式对攻击日志进行分析)
- 实战案例:监控分析(系统监控、态势感知、WAF设备等监控分析)
- 行业巡检(金融、教育、医疗行业等安全巡检)
- 巡检总体汇总报告

第四部分：开发与提升

4.1. 密码学

- 剖析基本概念
- 什么是加密与解密
- 寻找银弹
- 入门加密与解密
- 数据完整性
- 对称密码
- 公钥密码
- 公钥密码
- 非对称密钥生成器
- 密钥规范管理
- 数字签名
- 数字证书相关管理
- 安全套接字
- 简单并常用的BASE64
- 文件校验
- 打破出口限制
- 编码转化辅助工具

4.2. Java入门

- Java入门
- 数据类型
- 运算符
- 流程控制
- 方法的定义、调用、重载
- 数组

4.3. C语言

- C语言开篇
- 数据类型
- C语言输入和输出
- 运算符和表达式

- 流程控制
- 数组
- 函数
- C语言预处理
- 指针
- 复合数据类型
- C程序的组成

4.4. C++

- C++概述
- C++对C的拓展
- 类和对象
- 继承
- 多态
- 异常
- 强制类型转换
- 泛型编程

4.5. Shell编程

- 编程入门技能
- 变量概念介绍
- 特殊变量进阶
- 数值计算实践
- 条件测试比较
- 条件判断语句
- 流程控制语句
- 循环语句应用
- 循环控制语句
- 函数知识精讲
- 数组知识精讲
- 开发环境规范
- 调试优化实践
- 自动化实战项目

4.6. CTF夺旗赛

1) CTF-WEB题型

- CTF-WEB 题型[GKCTF2021]HACKME
- CTF-WEB 题型[GKCTF2021]EASYNODE
- CTF-WEB 题型[GKCTF2021]EASYCMS
- CTF-WEB 题型[GKCTF2021]CHECKBOT
- CTF-WEB 题型[GKCTF2021]BABYCAT

2) CTF-REVERSE题型

- CTF-REVERSE 题型[GKCTF2021\]SOMUCHCODE]
- CTF-REVERSE 题型[GKCTF2021]QQQQT
- CTF-REVERSE 题型[GKCTF2021]KILLERAID
- CTF-REVERSE 题型[GKCTF2021]CRASH
- CTF-REVERSE 题型[GKCTF2021]APP-DEBUG

3) CTF-PWN题型

- CTF-PWN 题型[GKCTF2021]ESAPESH
- CTF-PWN 题型[GKCTF2021]DEMO_CATROOM
- CTF-PWN 题型[GKCTF2021]CHECKIN
- CTF-PWN 题型 YCB_2020_MIPSPWN
- CTF-PWN 题型 YCB_2020_REPWN

4) CTF-CRYPTO题型

- CTF-CRYPTO 题型[GKCTF2021]XOR
- CTF-CRYPTO 题型[GKCTF2021]RRRRSA
- CTF-CRYPTO 题型[GKCTF2021]RANDOM
- CTF-CRYPTO 题型[羊城杯 2020]GMC
- CTF-CRYPTO 题型[羊城杯 2020]RRRRRRRSA

5) CTF-MOBILE

- CTF-MOBILE 题型[ISCC2021]1A2B
- CTF-MOBILE 题型[ISCC2021]LOCKK
- CTF-MOBILE 题型[ISCC2021]MOBILEEASY
- CTF-MOBILE 题型[ISCC2021]MOBILENORMAL

- CTF-MOBILE 题型[ISCC2021]OHHH

6) CTF-MISC

- CTF-MISC 题型[GKCTF2021]FIREFOXFORENSICS
- CTF-MISC 题型[GKCTF2021]EXCEL 骚操作
- CTF-MISC 题型[GKCTF2021]银杏岛の奇妙冒险
- CTF-MISC 题型[GKCTF2021]签到
- CTF-MISC 题型[GKCTF2021]你知道 APNG 吗

4.7. Windows逆向

- 章节1:壳的概念
- 1 壳的概念
- 2 什么是PE文件
- 3 什么是OEP
- 章节2:壳的分类-压缩壳
- 1 压缩壳-无壳PE映射到内存过程 原理
- 2 压缩壳-加壳过程原理
- 3 压缩壳-压缩壳的执行过程
- 4 压缩壳-压缩壳的应用场景+实战添加UPx壳
- 5 压缩壳实战-添加ASPack壳
- 章节3:壳的分类-加密壳
- 1 什么是加密壳
- 2 ASProtect加壳原理
- 3 ASProtect执行原理原理
- 4 加密壳使用场景
- 5 常见加密壳&实战添加ASProtect壳
- 6 ASProtect安装激活教程
- 7 加密壳实战-添加vmp壳
- 章节4:查壳
- 1 PEiD 查壳
- 2 Detect-It-Easy查壳
- 3 ExeinfoPe查壳
- 章节5:学习OD
- 1 认识OD 上
- 2 认识OD 中
- 3 认识OD 下
- 5 跟踪40270C 函数

- 6 跟踪40104F跳转
- 7 查找main()函数
- 8 跟踪main（）函数
- 9 调试器指令
- 10快速返回到EP
- 章节6 脱壳（更新中……）

4.8. 安卓逆向

- 安卓逆向有何意义
- 安卓逆向的学习路径
- 安卓逆向的发展和就业前景
- 安卓搭建环境
- 安卓开发功能
- 安卓编译、打包到开发机
- 安卓普通发布与加固发布
- 安卓逆向反编译路径
- 基本的反编译方法
- burp suite抓包工具基本使用
- 抓包https协议的内容
- 为什么要Root
- Root的原理
- 对于设备的选择
- Root的基本过程（以小米为例）
- 什么是钩子(hook)?
- Frida的使用
- 安卓高级逆向
- 修改smali并重新打包
- 安卓逆向基本思路
- 需要掌握的技能点
- 最佳实践