第一章 概述

1.软件缺陷 p5

软件缺陷，常常由被称作 BUG，是指计算机软件或程序中存在某种破坏正常运行能力的问题、错误，或者隐藏的功能缺陷，缺陷的存在会导致软件产品在某种程度上不能满足用户的需要。

2.软件安全主要包括哪几方面内容？ p5 3

软件安全主要包括：软件自身安全，恶意软件攻击与检测，软件逆向分析与防护。

3.软件漏洞 p5

软件漏洞是指软件在设计、实现、配置策略及使用过程中出现的的缺陷，其可能导致攻击者在未授权的情况下访问或破坏系统。

4.恶意软件包括哪些？ p6

最典型的有：计算机病毒、特洛伊木马、后门、僵尸、间谍软件等。

5.目前软件安全防护手段主要有哪些？p7

主要手段有：

（1）强化软件工程思想，将安全问题融入到软件的开发管理流程之中，在软件开发阶段尽量减少软件缺陷和漏洞的数量。

（2）保障软件自身的运行环境，加强系统自身的数据完整性校验。

（3）加强系统自身软件的行为认证——软件动态可信认证

（4）恶意软件检测与查杀。

（5）黑客攻击防护——主机防火墙、HIPS。

（6）系统还原。

（7）虚拟机、沙箱隔离技术等。

6.什么是沙箱？它在软件安全领域有哪些应用？ p12

沙箱（也叫沙盘或沙盒）之中的软件行为及其产生的系统修改是被隔离起来的。

通常用于运行一些疑似危险样本，可以隔离安全威胁，也可用于恶意软件分析。

第二章 软件安全基础

1.硬盘参数通常用原始的 CHS 参数表示，现代大容量硬盘一般用 LBA 线性地址方式来寻址。

C：柱面数（0~1023）。H：磁头数（0~255）。S：扇区数（1~63）。

2.CHS 到 LBA 转换计算公式 P14

LBA = (C - CS) * PH * PS + (H - HS) * PS + (S - SS)

一般情况下：CS=0; HS=0; SS=1, PS=63, PH=225;

3.主引导扇区由 MBR（主引导记录）,DPT（硬盘主分区表）和引导扇区标记三部分组成。 p15

4.Windows 操作系统支持的文件系统有哪些？Linux 操作系统支持的文件系统有哪些？ p16

Windows：FAT12、FAT16、FAT32、NTFS、WINFS

Linux：Ext2、Ext3、Minix、NTFS

5.FAT32 文件系统将磁盘空间划分为引导区、文件分配表和数据区。P16- 17

6.NTFS 文件系统示意图。P19

（1）一个引导扇区+15 个扇区的 NTLDR 区域

（2）MFT 元数据文件

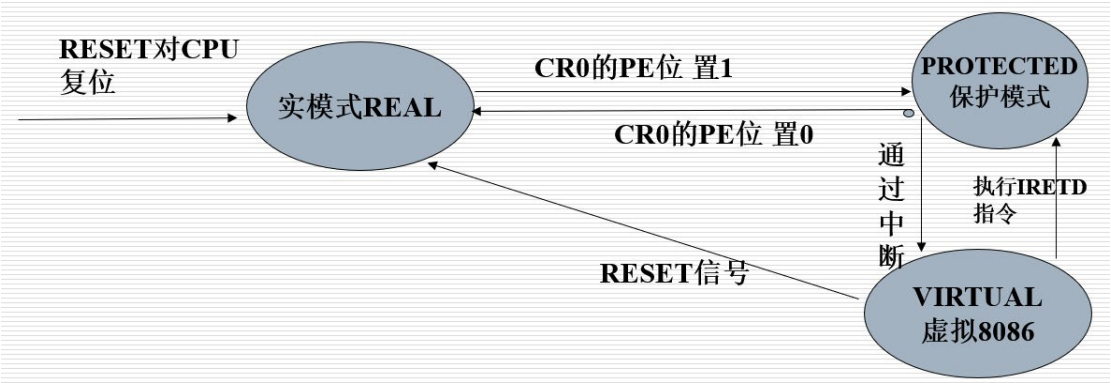
（3）MFT 分配的空间

（4）文件存储区

（5）MFT 前几个数据文件的备份

（6）文件存储区

7.理解 80X86 处理器支持的 3 种工作模式。P20
实模式，保护模式，虚拟 8086 模式
8.简述 80X86 处理器从实模式转入保护模式的基本过程。P21
通过在实模式下初始化控制寄存器,GDTR,LDTR 等管理寄存器以及页表,然后再通过加载 CR0,置其中的保护模式使能位，从而进入保护模式。
80X86 处理器三种工作模式关系：



9.保护模式的优点。P21
物理寻址空间高达 4GB；支持内存分页机制，提供了对虚拟内存的良好支持，支持优先级机制。
10.Windows 32 位系统用户模式区通常存放用户进程的哪些信息？ P23
主要包括：应用程序代码，全局变量，所有线程的线程栈以及加载的 DLL 代码等。
11.Windows NT 进程虚拟内存分布图 p23 4 部分 （用户模式区和内核模式区）
（1）操作系统使用不可读写 2GB
（1）用于防止跨用户/系统边界传输数据不可读写 64KB
（1）进程私有空间 128KB~2GB
（1）用户捕捉 NULL 指针不可读写 64KB
12.Win32 内存 API 分为虚拟内存管理、堆管理和内存映射文件管理。p26 用途和函数
13.PE 文件病毒如何在被感染程序运行时获得控制权。P35
（1）用户点击 HOST 程序
（2）装载 HOST 程序到内存中
（3）通过 PE 文件中的 AddressOfEntryPoint 和 ImageBase 之和来定位第一条语句的位置
（4）从第一条语句开始执行
（5）病毒主体代码执行完毕，将控制权交还给 HOST 程序
（6）HOST 程序继续执行
14.PE 文件结构图 P35 6 分
（1）MZ 文件头
（2）DOS 插桩程序
（3）NT 映像头
　　（1）字串“PE\0\0”（4H 字节）
　　（2）映像文件头（14H 字节）
　　（3）可选映像头（140H 字节）
（4）节表（Section table）
　　（1）Section 1
　　（2）Section 2

（3）Section 3
（4）……

第三章　软件缺陷与漏洞

1.漏洞分类(对系统威胁、漏洞成因、严重级别、利用方式) P53
（1）对系统威胁分类：获取访问权限漏洞、权限提升漏洞、拒绝服务攻击漏洞、恶意软件植入漏洞、数据丢失或泄露漏洞等。
（2）按漏洞成因分类：输入验证错误、访问验证错误、竞争条件错误、意外情况处理错误、设计错误、配置错误及环境错误。
（3）按漏洞严重性等级分类：高、中、低。（分别对应什么类型的漏洞）
（4）按漏洞被利用的方式分类：本地攻击、远程主动攻击、远程被动攻击。
2. 软件漏洞利用对系统的威胁 P55
非法获取访问权限、权限提升、拒绝服务、恶意软件植入。
3. CVE 及其优点。
CVE（common vulnerabilities and exposures）通用漏洞列表
CVE 的优点是将众所周知的安全漏洞的名称标准化，使不同的漏洞库和安全工具更容易共享数据，使得在其他数据库中搜索信息更容易。
4. 软件漏洞产生的技术因素 P56-58　7 点
（1）输入验证错误
（2）访问验证错误
（3）竞争条件
（4）意外情况处置错误
（5）逻辑设计错误
（6）配置错误
（7）环境错误
5. 软件漏洞产生的非技术因素 P59-60　5 点
（1）缺乏软件开发规范
（2）缺乏进度控制
（3）缺乏安全测试
（4）缺乏安全维护
（5）不稳定的开发团队
6. 软件漏洞利用方式有哪些？各举 1 例。p603
（1）本地攻击模式：本地权限提升漏洞
（2）远程主动攻击模式：MS08-067
（3）远程被动攻击模式：网页挂马
7. 缓冲区溢出漏洞会给系统带来哪些危害？P62　3
数据泄露、系统奔溃、甚至使攻击者获得控制权。
8. SQL 注入漏洞会给系统带来哪些危害？P62　2
读取并修改数据库中保存的所有数据，甚至完全控制运行数据库的服务器。
9.什么是远程代码执行漏洞?
攻击者通过浏览器提交执行命令，注入核心代码，恶意攻击。

第四章　软件漏洞的利用和发现

1.理解栈溢出的利用（修改邻接变量、修改函数返回地址和 S.E.H 结构覆盖）p69-72
三个图

2.简述堆溢出利用的基本原理。P77-78　4
利用精心构造的数据去溢出覆盖下一个堆块的块首，使其改写块首中的前向指针和后向指针，然后在分配、释放、合并等操作发生时伺机获得一次向内存任意地址写入任意数据的机会。
3.Heap Spray 技术基本思路。 P78 6
首先将 shell code 放入堆中，然后在栈溢出时，控制函数执行流程，跳转到堆中执行 shellcode。
4.格式化字符串漏洞，原因及后果 P80-p81 代码
5.SQL 注入漏洞的防范措施.P87　3 点
（1）参数化查询
（2）过滤与转换
（3）服务器与数据库安全设置
6.XSS 漏洞形成原因及防范措施.p87-p90　4 点
原因：攻击者嵌入恶意脚本代码到正常用户可能会访问的网页中，当正常用户访问时，恶意脚本代码被执行，从而达到恶意攻击用户的目的。
防范措施：（1）不信任用户提交的任何内容
（2）实现 session 标记（session token），CAPTCHA（验证码）系统或者 HTTP 引用头检查。
（3）cookie 防盗
（4）确认接收的内容被妥善的规范化。
7.CSRF 形成原因及防范措施.p90-91
原因：攻击者利用目标站点对用户的信任，诱使或强迫用户传输一些未授权的命令到该网站，从而达到攻击目的。
防范措施：验证码防范；更多的是在用户提交的每一个 HTTP 请求的主体或者 URL 中添加一个不可预测的 token，当用户请求时，验证 token 是否正确。
8. 软件漏洞利用中 exploit、Payload 和 Shellcode。 P95- P97
Exploit:用来触发漏洞并完成恶意操作的整个程序。
Payload:用于实现攻击的二进制串。
Shellcode:代表攻击者攻击意图的代码
9.0day 漏洞 P95
未被公布，未被修复的漏洞，一般具有极高的价值和极大的危害性。
10. Shellcode 典型功能有哪些？ P102-103 4
正向连接、反向连接、下载程序并执行、生成可执行文件并运行。
11.Metasploit Framework 包含哪些基本模块及其作用。p107 3
Exploit 模块：含有已公布漏洞的触发信息。
Payload 模块：含有可运行于多种操作系统下的各种用途的 shell code。
Encoder 模块：即编码算法。
Auxiliary 模块即额外的插件程序。
12.漏洞挖掘技术主要有哪些？P108 5 点
（1）基于源码的静态分析
（2）动态分析
（3）fuzzing 技术
（4）逆向分析
（5）基于补丁对比的逆向分析
13.文件 Fuzzing 工具的工作流程 。P111 4 点
（1）以一个正常的文件模板为基础，按照一定的规则产生一批畸形文件。

（2）将畸形文件逐个送入软件进行解析，并监视软件是否会抛出异常。
（3）记录软件产生的错误信息，如寄存器状态，栈状态等。
（4）用日志或其他形式向测试人员展示异常信息，以进一步鉴定这些错误是否为软件缺陷或漏洞。

第五章　构建安全软件

1.主动的安全开发过程分那几个阶段？P133
（1）安全教育阶段
（2）设计阶段
（3）开发阶段
（4）测试阶段
（5）发行和维护阶段

2.设计阶段的安全关键要素有哪些？P133-134　4 点
（1）定义安全体系结构和设计指导原则
（2）记录软件攻击面的要素
（3）对威胁进行建模
（4）定义补充性交付标准

3.确定安全目标，进行正确安全设计要考虑哪些方面内容。　p133-136 6 点
（1）设计阶段关键要素
（2）面试期间的安全问题
（3）定义产品的安全需求
（4）威胁建模
（5）设置 bug 门槛
（6）安全小组审查

4.Microsoft 公司的 SD3+C 策略指的是？ P137　6+3+3
SD3 就是设计安全（secure by design）、默认安全（secure by default）和部署安全（secure by deployment），C 代表通信。

5.安全设计法则 P138-140 12 点
（1）从错误中吸取教训
（2）尽可能缩小供给面
（3）纵深防御
（4）使用最小特权
（5）向下兼容总是不安全的
（6）假设外部系统使不安全的
（7）失败的应对计划
（8）失败时进入安全模式
（9）安全特性不等于安全的特性
（10）绝不要将安全仅维系与隐匿
（11）不要将代码和数据混在一起
（12）正确的解决安全问题

6.安全编码准则有哪些？ P140-141　6 点
（1）使用代码分析工具
（2）进行安全检查
（3）使用检查表进行代码安全检查
（4）验证所有用户的输入

（5）严格验证导出的和公共的 API 的所有参数
（6）使用 Windows 加密 API
7.安全编码应该避免哪些事项？5 点 P141
（1）避免缓冲区溢出
（2）不使用断言来检查外部输入
（3）不要硬编码的用户 ID 和密码
（4）不要认为使用加密功能可以解决所有安全问题
（5）避免使用规范化文件路径和 URL
8.安全开发和测试人员需要遵守和养成的习惯？ 3 点 p141
（1）检查应用程序中所有以前的安全缺陷
（2）检查所有错误路径
（3）不要为运行的应用程序设置管理员权限
9.安全性测试方法主要有哪些？P142 3 点
（1）静态的代码安全设置
（2）动态的渗透测试
（3）程序数据扫描
10.做好软件安全性测试的必要条件。 P143 3 点
（1）充分了解软件安全漏洞
（2）评估安全风险
（3）拥有高效的软件安全测试技术和工具。

第六章　恶意代码及机理分析

1.计算机病毒至少包括哪些基本模块？P164 3 点
（1）触发模块
（2）传播模块
（3）表现模块（破坏模块）
2.计算机病毒的传播方式有哪些？ 6 点 p166
（1）网页挂马
（2）电子邮件，FTP 等
（3）可移动存储设备
（4）局域网共享
（5）对等网络应用软件
（6）软件漏洞
（7）盗版软件下载
（8）即时通信软件
3.计算机病毒的感染方式。 4 点 P162
（1）感染可执行文件
（2）感染引导区
（3）感染文档文件
（4）感染系统
4. 网络蠕虫的行为特征。P199 3 点
（1）主动攻击
（2）行踪隐藏
（3）利用系统，网络应用服务漏洞
5.蠕虫危害。P199 5 点

（1）造成网络拥塞
（2）降低系统性能
（3）产生安全隐患
（4）反复性
（5）破坏性

6.网络蠕虫功能结构(基本 4)和扩展（5）

基础（1）信息收集模块
（2）扫描探测模块
（3）攻击渗透模块
（4）自我推进模块

扩展（1）实体隐藏模块
（2）宿主破坏模块
（3）信息通信模块
（4）远程控制模块
（5）自动升级模块

7.网络蠕虫防治方法 P203-204 3+3

检测（1）漏洞利用特征检测
（2）网络流量分析
（3）流量数据特征

防治（1）网关阻断
（2）补丁推送
（3）“良性”蠕虫对抗恶意蠕虫

8.远程控制型木马主要由那几部分构成，并简述各部分作用。P206

木马配置程序：配置木马程序的端口号，触发条件，木马名称等，使其在服务端更加隐蔽。

控制端程序：远程控制服务器

被控端程序：驻留在受害者系统中，非法获取操作权限，负责接收控制端指令，并根据指令或配置发送数据给控制端。

9.木马的通信方式有哪些？ P209 4

TCP,UDP,ICMP,HTTP 隧道。

10.木马的业务功能。P212-214 14 点

（1）进程管理
（2）文件管理
（3）注册表操作
（4）服务管理
（5）屏幕截取
（6）鼠标控制
（7）视频监视
（8）语音监听
（9）键盘记录
（10）远程 shell
（11）传播病毒
（12）破坏系统
（13）添加后门
（14）其他功能

11.Windows RootKit 主要涉及哪些技术？P221-　5 点
（1）rootkit 常用技术：用户态 HOOK,内核态 HOOK,直接内核对象操作
（2）进程隐藏技术
（3）文件隐藏技术
（4）通信隐藏技术
（5）注册表隐藏技术
12.目前针对手机的恶意软件主要有哪些类型？P240　5 点
木马，间谍软件，蠕虫，感染型病毒，破坏性程序
13.手机恶意软件的防御措施。P247 12 点
（1）慎用非正规渠道的 ROM
（2）避免越狱，保障系统自身的安全环境
（3）熟悉手机的常用功能和潜在功能，及时关闭不必要功能
（4）下载应用程序时，应到官方网站或者大型应用程序商店
（5）定期备份手机中的文件，并将备份文件保存于安全隔离位置
（6）安装手机反病毒软件
（7）认真阅读和理解系统弹出来的各类安全提示框

第七章　病毒检测及检测对抗技术

1.病毒检测技术 6 点 P249
（1）特征值检测技术
（2）校验和检测技术
（3）虚拟机检测技术
（4）启发式扫描技术
（5）主动防御技术
（6）云查杀技术
2.对抗特征值检测技术 3 p262
（1）事前对抗：代码加密混淆与加壳
（2）事后对抗：特征值针对性修改
（3）
3.对抗启发式扫描技术。 P264 16
（1）新的 PE 文件感染技术
（2）多节病毒
（3）加密宿主文件头的前置病毒
（4）感染第一节的闲散区域
（5）通过移动文件的节移位感染第一个节
（6）压缩感染首节
4.对抗云查杀技术 p267 3
（1）通过修改用户主机本地 hosts 域名解析文件，将云服务器域名重定向到其他地址，从而使得安全软件客户端无法正常上传样本
（2）病毒运行时，临时性断开用户网络连接，使得样本无法及时上传
（3）增加自身文件大小，使得样本文件大小超过云上传规则中规定的样本大小。
5.对抗虚拟机技术 p265 3
（1）虚拟机环境检测
（2）调试干扰与对抗
（3）动态启发式扫描对抗