每章课后习题
第二章 网络攻击行径分析
1. 利用向目标主机发送非正常消息而导致目标主机崩溃的攻击方法有哪些？
2. 破坏性攻击的原理及其常用手段
3. 扫描的作用和常见的扫描方法
4. 网络欺骗的原理以及常用的欺骗方法
5.IP 欺骗的原理与过程
6. 攻击的一般目的
7. 攻击的一般过程和注意事项
8. 口令猜测的方法和步骤
ppt
1. 安全威胁分类
第三章 网络侦查技术
1. 什么是网络扫描？什么是扫描器？
2. 扫描的类型和功能
3. 什么是网络监听
4. 简述以太网的网络监听
5. 简述 sniffer 的工作原理
6. 如何防范网络监听？
7. 什么是字典文件？在攻击中的作用？
PPT 问题
1. ping 的优缺点
第四章 拒绝服务攻击
课后习题
1. 什么是拒绝服务攻击？如何分类？
2. 外部用户针对网络连接发动拒绝服务攻击有哪几种模式？并举例
3. 同步包风暴(SYN Flooding)拒绝服务攻击的原理、特点、如何防止
4. 简述 smurf 攻击的原理、特点、怎样防止
5. 简述 Ping Of Death 原理、怎样防止
6. 简述 TearDrop 原理、怎样防止
7. 简述 Winnuke 原理、怎样防止
8. 简述 Land 原理、怎样防止
9. 简述电子邮件轰炸拒绝服务攻击的原理、造成的危害、如何防止
10. 什么是 DDOS 攻击？特点？为什么危害性更强？
11. 如何应对 ddos 攻击，并举例
PPT 问题
1.反弹技术(曹越 PPT 48)
2.如何发现自己正在受到消耗网络资源的 dos 攻击
第五章 缓冲区溢出攻击
课后习题
1. 什么是缓冲区
2. 描述一个具体程序的执行过程了解栈帧的结构
3. 缓冲区溢出的基本原理
4. 缓冲区溢出攻击的一般目标

5. 要让程序跳转到安排好的地址空间执行，有哪些方法
6. 为什么缓冲区溢出会成为操作系统、数据库等应用最普遍的漏洞之一

PPT 问题

1. 什么程序会发生缓冲区溢出

第七章 欺骗攻击

课后习题

1. 常见的欺骗攻击方式、共同特点、其他欺骗攻击
2. DNS 的工作原理、DNS 解析的过程中可能被欺骗的地方
3. 3. DNS 欺骗攻击的原理和过程
4. 假如你的主机在面临 DNS 欺骗攻击，应该采取什么样的策略和解决方案
5. E-mail 欺骗攻击的原理和过程
6. 加入你是一名网络管理员，对于邮件欺骗攻击你的忠告
7. Web 欺骗攻击有哪些具体形式、原理
8. 如果你是开发者，采用何种手段避免你的网站受到潜在的 Web 欺骗攻击
9. 简述 tcp 建立连接的过程
10. 10. IP 欺骗的原理和过程(同第二章第 5 点
11. 11. TCP、Ipv4 协议在安全性欠缺考虑的地方，如何改进

PPT 问题

1. 不在一个子网中的 tcp 劫持(欺骗手法)

第九章 访问控制技术

课后习题

1. 访问控制包含哪些内容？举例
2. 身份认证包含哪些信息？这些认证信息主要用于什么方面？
3. 简述口令认证技术的认证方法。用哪些方法可以提高口令认证技术的安全性？
4. 网络的物理隔离技术包含哪几方面？他们各自采用了什么技术？
5. 什么叫自主访问控制？方法有哪些？有哪几种类型？
6. 为什么自主访问控制无法抵御特洛伊木马攻击？请举例说明？
7. 什么是强制访问控制方式？如何防止特洛伊木马的非法访问？
8. 简述 BLP 模型的安全策略，并举例说明
9. 9. 简述 Biba 模型的安全策略，并距离说明
10. 什么是基于角色的访问控制技术？它与传统的访问控制技术有什么不同？
11. 简述 4 中 RBAC 模型技术。他们各自有什么特点？

PPT 问题

1. 如何确保身份认证数据的真实性？
2. 如何结合 MAC 和 DAC？
3. BLA(BLP)不足
4. 网络安全隔离卡如何交换数据？
5. 网卡、隔离卡的区别

第十章 防火墙技术

课后习题

1. 经典安全模型中的参考监视器的基本功能是？
2. 防火墙规则的处理过程中，“REJECT”和“DROP“的区别是什么？
3. 防火墙产品的两条基本原则是？
4. "IP 源地址 = 192.168.1.1 and IP 目的地址 = 192.168.2.1 and 协议 = TCP and

源端口 > 1024 and 目的端口 = 80 and" 表示什么样的数据包？

5. 数据包过滤规则向内向外之分？
6. 访问某些经典网站的响应速度加快，而其它站点响应速度较慢？
7. 如果防火墙允许周边网络上的主机访问内部网络上的任何基于 TCP 协议的服务，而禁止外部网络访问周边网络上的任何基于 TCP 协议的服务，给出实现的具体思路

PPT 问题

1. 防火墙的体系结构
2. 构建防火墙步骤

第十一章 入侵检测技术

课后习题

1. 入侵检测系统的入侵内容主要是什么？

书 P288

外部攻击检测

内部特权滥用检测

2. 入侵检测系统按引擎类别分，可以划分为几种类型？这些引擎的实现方式是什么？

书 P290

异常检测

模式匹配(误用检测)

3.商业 IDS 系统主要采用的技术有哪些？这些技术的特点是什么？

第十二章 VPN 技术

1. VPN 的定义
2. VPN 的组成
3. 3. VPN 的类型
4. 4. VPN 使用了哪些安全协议，处于 OSI 的哪些层？
5. 5. 什么是隧道？
6. 6. 隧道协议有哪些？
7. 7. 隧道协议的功能
8. 8. 比较 PPTP 和 L2TP
9. 9. 简述 IPSec 中 AH 协议功能
10. 10. 简述 IPSec 中 ESP 协议的功能