第二章

2.23 假如A忽略自己的第一条消息和B的应答，直接发送自己的第二条消息（即直接发送ACK包），试问当B收到该ACK包后会怎样响应？  
答：当B收到该ACK包后，会检查该包所表示的连接四元组是否存在，因为没有开始建立过连接，因此查表查不到，B返回RST。

2.29 IP协议存在哪些安全威胁？这些安全威胁的根源是什么？

答：IP窃听：因为IP地址是明文传输的，因此可以获得IP地址和报文的内容

IP假冒攻击：路由器只根据IP分组的目的IP地址来确定该IP分组从哪个端口发送的，不关心源IP地址，因此任何节点都能构造假的源IP地址，并且成功发送到目的节点。

IP碎片攻击：IP协议允许发送者和转发者对IP报文进行分片，因此可以将IP报文分成很小的碎片发送给目标，目标在接收到之后重组分片会浪费大量资源。

2.32 域名解析协议主要面临的安全威胁有哪些？

答：DNS劫持攻击：

DNS缓存毒化：攻击者拥有自己的域和被攻破的DNS服务器，通过查询域迫使本地域名服务器询问被攻陷的DNS服务器。DNS服务器通过区域传送方式将篡改的其他DNS信息返回给本地域名服务器。

DNS ID欺骗：DNS基于UDP协议，客户端查询时会在包内包含一个16bit的随机数作为ID，收到的回复内有着个数则认为信息有效。攻击者如果在同一局域网内或可以窃听到DNS请求，就可以获得这个ID号，然后伪造合法的响应包。如果不能窃听到，可以发送大量包给DNS服务器，查询被攻击的域名(a.com)，然后构造大量的应答包(a.com=fakeip)，这样DNS服务器有概率收到fakeip。

DNS的DDoS攻击：

攻击者发送大量查询请求给DNS服务器，请求包的源地址设置为被攻击者的IP，这样DNS服务器就会发送大量的响应包给被攻击者，占用被攻击者的处理能力。

第三章

3.8 个人防火墙是对单一的个人主机提供保护的防火墙系统。试结合具体的操作系统，说明如何实现个人防火墙系统。  
答：在Windows系统下，首先要有一个驱动作为网卡和上层接口的中间件，拦截所有经过网卡的流量。然后使用包过滤技术、状态检测技术等控制哪些包可以进出系统。还有文件系统监控，进程监控等功能，还要有审计系统，用于日志分析等。

第四章

4.11 入侵检测如何分类？  
答：根据入侵检测的数据源：  
 基于主机：通过分析主机的数据，例如系统日志、系统调用等  
 基于网络：通过截获网络的数据包并与攻击签名比较  
 混合型：有机结合基于主机和基于网络的入侵检测  
 按照检测方法：  
 异常检测：对正常状态建模，判断用户行为和资源情况是否为正常  
 误用检测：根据已知的攻击方法，定义入侵特征，检测此特征是否出现  
 按时间：  
 实时入侵检测：实时收集分析相关信息  
 定时入侵检测：将收集到的信息存储起来，入侵发生之后集中分析  
 按照系统体系结构：  
 集中式IDS：一个入侵检测服务器和多个不同主机上的审计程序组成  
 分布式IDS：由多个组件构成，分布在不同的设备上

4.13 常用的未知攻击检测方法有哪些？  
答：使用神经网络，统计分析，数据挖掘方法，都属于异常检测

4.15 入侵防御与入侵检测的相同点和不同点有哪些？入侵防御未来的发展趋势是什么？  
答：相同点：检测入侵行为并响应，保护系统安全  
 不同点：入侵防御在入侵检测的基础上实现了防御功能，入侵防御必须实时分析，入侵检测可以是事后分析  
 未来的发展趋势：针对新的攻击措施进行防御，提高运行效率

第五章

5.2 列举5种安全协议攻击方法。  
答：攻击基本协议缺陷：协议没有考虑攻击者的防范  
 攻击陈旧消息缺陷：未考虑消息的时效性  
 攻击并行会话缺陷：协议没有考虑并行会话，可以交换消息获得重要消息  
 攻击内部协议缺陷：协议缺少足够信息区分消息真实性  
 攻击密码系统缺陷：密码算法安全强度低

5.3 有哪些抗重放攻击方法？各自的特点是什么？  
答：挑战应答机制：发送挑战值确保消息的新鲜性  
 时戳机制：对消息加上本地时戳判断消息新鲜性  
 序列号机制：通过消息中的序列号判断消息新鲜性，需要先协商初始序列号

5.7 简述Kerberos认证协议的设计思想和实现方法？  
答：设计思想：通过票据重用和票据许可服务器、认证服务器让用户输入口令次数减少  
 实现方法：用户C向认证服务器AS发送口令，通过AS则给C一份有时间限制的购票许可证。C向票据许可服务器TGS发送购票许可证，若验证通过则给C一份有时间限制的票据。C用票据向服务器V请求服务。

第六章

6.3 计算机系统的物理安全威胁包括哪些方面？  
答：非人为因素：来自自然环境和技术故障等  
 人为因素：来自人员失误和恶意攻击等

6.5 列举计算机系统物理安全应考虑的因素。  
答：设备物理安全：设备的标志和标记、防止电磁信息泄露、抗电磁干扰、电源保护以及设备振动、碰撞、冲击适应性等  
 环境安全：机房场地选择、机房屏蔽、防火、防水、防雷、防鼠、防盗、防毁、供配电系统、空调系统、综合布线、区域防护等  
 系统物理安全：保证信息系统的安全可靠运行，降低或阻止人为或自然因素从物理层面对信息系统保密性、完整性、可用性带来的安全威胁

第七章

7.2 列举计算机系统的容错技术，并分别简要说明每种技术。  
答：硬件冗余：增加设备形成备份，当有故障发生时立刻替换；对数据进行备份，对损失文件进行恢复；双机容错系统，当一个CPU板故障时其他继续运行；双机热备份，CPU故障时由闲置状态的备份系统代替；三机表决系统，三台主机同时运行，少数服从多数对结果表决；集群系统，负载均衡的双机或多机系统

软件冗余：用多个不同软件执行同一功能  
 数据冗余：用磁盘阵列进行数据备份  
 时间冗余：多次执行同一操作来达到容错

7.5 容错与容灾的区别是什么？  
答：容错是使计算机能容忍故障，有故障的情况下能继续完成任务。容灾是遇到灾难（引起计算机系统非正常停机）时持续运行，保障关键业务的继续运行。

第八章

如何有效确保操作系统的安全性？  
答：在硬件级提供安全保护，例如特权级。保护进程的安全，例如进程的权限，共享的数据。有安全的内核，使用安全的策略和配置。有安全的身份认证机制和访问控制，防止对资源的非法访问。

第九章

9.1 思考安全审计与计算机取证技术的区别与联系？  
答：区别：安全审计是通过分析事件记录来调查有没有非法行为，计算机取证是已经有了非法行为，将犯罪者留下的痕迹进行提取，当作证据使用  
 联系：都要能分析检测非法行为，都是为了系统的安全