(1) 教材上的术语和讲义上讲的一些术语

(2) 掌握 TCP/IP 协议的分层结构及各层的功能；理解地址和寻址，路由；掌握数据包嗅探和伪造方式

(3) 理解并掌握与协议头有关的漏洞，针对协议交互逻辑的漏洞，与认证有关的漏洞，与流量有关的漏洞(嗅探，拒绝服务等)的定义及相关的实例

(4) 掌握物理网络层常见的攻击方法:硬件地址欺骗，物理攻击等；了解物理网络层数据传输的机理及典型的协议(无线和有线状态下的 CSMA/CD 协议)，掌握物理网络层面临的与协议头、协议交互逻辑、认证和流量这四个方面的一些风险和一些典型的消除机制(WEP，WPA，VLAN…)；重点掌握 ARP 攻击的原理与缓解机制、Wardriving 攻击与消除机制、恶意访问接入点攻击与假冒访问接入点攻击的区别及消除机制等

(5) 围绕网络层上的地址、路由等相关概念、工作原理和相关的协议(IPv4,ICMP)等，掌握路由追踪攻击、报文分片攻击，Smurf 攻击、ICMP redirect 攻击，IP 地址欺骗攻击等；掌握 BOOTP、DHCP 协议的工作机理及面临的安全风险(DHCP starvation 攻击,DHCP 中毒攻击)；掌握在 IP 层上的一些攻击缓解机制：NAT，IP 地址过滤、IPSec 与 VPN 等。

(6) 了解 TCP 协议、UDP 协议的工作机制；掌握并理解基于 TCP 或 UDP 的多种端口扫描技术(TCP SYN Scanning 等)的原理;掌握指纹技术的原理；掌握 SYN Flooding Attack、TCP Reset Attack 和会话劫持攻击等的机理;理解 DNS 的体系架构，工作原理和协议，掌握本地和远程的 DNS Cache Poisoning 攻击、DNS 上的 DOS 攻击等;掌握 TCP 层上的一些攻击缓解机制：TLS 等

(7) 对于邮件安全,了解 SMTP,POP&IMAP\MIME;掌握钓鱼、隐私泄露、垃圾邮件和恶意邮件等几种攻击;掌握 PGP、取证等防御机制

(8) 对于防火墙和入侵检测系统：理解 P2DR 模型，掌握包过滤防火墙、会话过滤防火墙和应用层防火墙的工作机理、优缺点，掌握堡垒主机的概念和防火墙的部署方式；掌握入侵检测系统的概念，掌握基于主机的入侵检测系统、基于网络的入侵检测系统的工作原理和优缺点，掌握误用检测技术、异常入侵检测技术的工作机理、优缺点。

要求能理论联系实际