1、信息系统安全威胁有哪四种？用实例说明这几种威胁的含义与特点。

2、信息系统安全目标体现在哪三个方面？与上述的四种安全威胁有何关系？

3、计算机入侵的最易渗透原则（最薄弱环节原则）指的是什么？对安全管理工作有何指导意义？

4、本课程所涉及的几个古典加密算法的加密过程。(包括替换算法和置换算法)

5、DES 加密算法的基本思路以及加密过程；DES 加密与解密算法的关系以及证明。

6、何为对称(秘钥)加密算法和非对称(公钥)加密算法？试说明各自的特点以及主要应用场合。

7、Hash 函数的特点与作用

8、基于 Hash 函数实现消息认证的几种典型方案

9、密钥交换的目的与实现

10、数字签名的作用，数字签名与验证的过程。

11、证书的作用是什么？如何实现？（PKI & CA）

12、数字信封技术的作用是什么？如何实现？

13、何为缓冲区溢出漏洞？它可能会产生哪些危害？

14、举例说明何为“检查时刻到使用时刻（TOCTTOU）”漏洞？请简述其解决方案。

15、计算机病毒的特点以及运行机制。（包括传统计算机病毒、

宏病毒以及蠕虫病毒）

16、木马程序的特点、功能以及运行机制。（从程序结构、植入方式、控制等几方面阐述）

17、何为跳板入侵？分析其原理以及实现方法。

18、何为间谍程序？试分析其特点以及危害。避免间谍程序侵入有哪些对策？

19、何为陷门？何为 salami 攻击？

20、何为隐蔽通道？试说明它通常有哪些实现方法？

21、试简述操作系统对一般对象常用的访问控制方法，分析这些方法的特点并比较之。

22、试简述 unix 系统中 Suid 访问许可的特点以及应用。

23、口令攻击一般有哪些方法？在选择口令时要注意什么？如何构造一个安全的鉴别系统？

24、何为 salt 口令？其作用是什么？采用 salt 口令时的用户鉴别过程。

25、试简述数据库的两阶段更新的实现方案。

26、举例说明数据库统计推理攻击的原理以及常用的对策。

27、TCP/IP 协议中各层的作用是什么？各层提供的服务有哪些？

28、DNS 域名解析的作用以及实现的过程

29、钓鱼网站(Phishing，网络钓鱼)攻击原理以及预防方法

30、典型中间人（MITM）攻击手段有哪些？试分析它们各自的

实现机制。(包括 ARP 攻击、DNS 欺骗、代理中间人攻击等)

31、常见的拒绝服务(DoS)攻击有哪些？试分析各自的特点以及实现机制。

32、何为分布式拒绝服务(DDoS)攻击？试分析其特点以及实施过程。

33、分析 ARP 攻击、DNS 欺骗的原理以及实现机制。它们是如何实现中间人攻击和拒绝服务攻击的？

34、在网络结构设计中如何考虑信息系统安全的需求？

35、何为链路加密和端对端加密？试分析它们各自的特点以及利弊。

36、何为 VPN？有何作用？如何实现？

37、SSL 建立安全通信通道的过程(包括服务器端和客户端的认证)。HTTPS 协议和 FTPS 协议的特点以及安全机制。

38、签名代码的机制以及实现过程。

39、一次性口令（口令令牌)、质询响应系统（挑战响应系统）的实施方案（原理、用户鉴别过程）以及特点比较。

40、以请求访问文件服务器中的一个文件 F 为例，试从用户身份鉴别、访问请求授权、访问请求的实现三方面来阐述 Kerberos 系统的运行机制以及特点。(看课程视频)

41、何为通信流推理威胁？简述对付通信流推理威胁的常用方法。

42、何为 Tor 路由(洋葱式路由)？试分析其作用以及实现过程。

43、试从邮件（电子支票）的机密性、完整性、真实性、不可否认性（抗抵赖性）和加密密钥的交换等方面阐述安全邮件系统（电子支票系统）的实现方案。(即为数字信封技术)

44、了解基于 Tor 路由技术的暗网实现（看课程视频）

45、了解信息安全保障体系（看课程视频）

期末试卷组成：

1、选择题（15 题）	**30%**
2、判断题（15 题）	**15%**
3、简答题（5 题）	**35%**
4、综合题（2 题）	**20%**