第一章

1. 网络安全的本质是什么？
    - 网络安全的**本质**就是**网络上的信息安全**，是指**网络系统**的**硬件**、**软件**及其系统中的**数据**受到**保护**，不受**偶然**的或**恶意**的**原因**而**遭到破坏、更改或泄漏**；
    - 保证信息的**安全性、完整性、保密性、可用性。**
    - 信息安全目前最**薄弱的环境是使用网络的个人**，如果能**加强个人的网络安全意识**可以从**根本上加强网络安全，改善网络环境。**
    - 计算机网络安全包括**两方面**，即**硬安全（物理安全）和软安全（逻辑安全）**
2. 简述网络本身存在哪些安全缺陷？
    - (1)**机房安全**
    - (2)**病毒的侵入和黑客攻击**
    - (3)**管理不健全而造成的安全漏洞**
    - 开放的网络环境
    - TCP/IP协议的脆弱性
    - 软件缺陷
    - 网管设备设置错误
    - 操作系统存在安全隐患
    - 网络硬件存在安全隐患
    - 人为因素
3. 从层次上，网络安全可以分成哪几层？每层有什么特点？
    - **4个**层次：**物理安全、逻辑安全、操作系统安全和联网安全。**
    - **物理安全**：包括**5个方面**：**防盗、防火、防静电、防雷击和防电磁泄漏。**
    - **逻辑安全**：需要**用口令、文件许可等方法来实现。**
    - **操作系统安全**：操作系统**必须能区分用户**，以便**防止相互干扰。**操作系统**不允许一个用户修改由另一个账户产生的数据。**
    - **联网安全**：通过**访问控制服务**和**通信安全服务**两方面的**安全服务来达到。**
      ①**访问控制服务**.用来**保护计算机和联网资源不被非授权使用。**
      ②**通信安全服务**.用来**认证数据机要性与完整性，以及各通信的可信赖性。**

第二章

1. 一般的黑客攻击有哪些步骤？各步骤主要完成什么工作？(P32)
    1. **确定攻击的目标。**
    2. **收集被攻击对象的有关信息。** 黑客在获取了目标机及其所在的网络类型后,还需要进一步获取有关信息,如目标机的 IP 地址、操作系统类型和版本、系统管理人员的邮件地址等,根据这些信息进行分析,可得到被攻击方系统中可能存在的漏洞。
    3. **利用适当的工具进行扫描。** 收集或编写适当的工具,并在对操作系统分析的基础上对工具进行评估,判断有哪些漏洞和区域没有被覆盖。然后,在尽可能短的时间内对目标进行扫描。
    4. **建立模拟环境,进行模拟攻击。** 根据之前所获得的信息,建立模拟环境,然后对模拟目标机进行一系列的攻击,测试对方可能的反应。
    5. **实施攻击。** 根据已知的漏洞,实施攻击。
    6. **清除痕迹。**
    7. **创建后门。**通过创建额外账号等手段,为下次人侵系统提供方便。
2. 木马攻击的一般过程是什么？(木马攻击步骤)
    1. **木马的配置**：有客户端配置服务端。
    2. **木马的传播**：将配置好的服务端传播出去。

3. **木马的自启动**：进入目标之后设法获得启动机会。
4. **建立连接**：和控制端建立连接，有主动式和被动式。
5. **远程控制**：操控者利用木马控制目标，窃取目标信息。

3. 分布式拒绝服务供给的原理和供给过程是什么?
   - **拒绝服务攻击是**：指利用**系统与程序本身设计缺陷占用系统资源**,从而**造成系统运行的迟缓和瘫痪。 拒绝服务攻击降低了资源的可用性**（这些资源可以是处理器、磁盘空间、 CPU 、打印机、调制解调器, 甚至是系统管理员的时间），**攻击的结果是使系统减少或者失去服务能力。**它的**目的是使被攻击的目标无法提供正常的服务** 。
   - 死亡之 ping；泪滴；UDP 泛洪(UDP flood)；SYN 泛洪；Land 攻击；IP欺骗DoS
4. 常见的黑客拒绝服务攻击有
   1. 口令入侵。所谓口令入侵就是使用某些合法用户的账号和口令登录到目标主机，然后再实施攻击活动。这种方法的前提是，必须先得到该主机上的某个合法用户的账号，然后再进行合法用户口令的破译。、
   2. 端口扫描。所谓端口扫描是向目标主机的TCP/IP服务端口发送探测数据包，并记录目标主机的响应，从而侦查到目标主机的扫描端口是否处于激活状态、主机提供了哪些服务、提供的服务中是否含有某些缺陷等等。端口扫描也可以通过捕获本地主机或服务器的流入流出IP数据包来监视本地主机的运行情况，它仅能对接收到的数据进行分析，帮助发现目标主机的某些内在的弱点，而不会提供进入一个系统的详细步骤。
   3. 网络监听。网络监听是主机将网卡设置为混杂模式，在这种模式下，主机可以接收到本网段在同一条物理通道上传输的所有信息，而不管这些信息的发送方和接收方是谁。
   4. 木马程序攻击。攻击过程和原理同特洛伊木马攻击。
   5. 电子邮件攻击。电子邮件攻击是给被攻击方发送带有木马程序或病毒的电子邮件，当被攻击方接收并运行后，即达到攻击的目的。
   6. 网络欺骗技术。网络欺骗包括IP欺骗、E-mail欺骗、Web欺骗、DNS欺骗等。其中IP欺骗是指伪造他人的源IP地址，其实质就是让一台机器来扮演另一台机器，借以达到蒙混过关的目的。E-mail欺骗是指冒充他人给另一方发送邮件。We b欺骗是一种电子信息欺骗，攻击者在其中创造了整个We b世界的一个令人信服但是完全错误的拷贝，错误的We b看起来十分逼真，它拥有相似的网页和链接。然而，攻击者控制着错误的We b站点，这样受攻击者浏览器和We b之间的所有网络信息完全被攻击者所截获。DNS欺骗是攻击者冒充域名服务器的一种欺骗行为。
   7. 拒绝服务攻击。原理见前述。

第三章

1. 什么是宏病毒？宏病毒的主要特征是什么？
   - 一种**寄存在文档**或**模板**的**宏中**的**计算机病毒**，**一旦打开这样的文档，其中的宏就会被执行**，于是**宏病毒就会被激活**，**转移到计算机上**，并**驻留在Normal模板上。**能通过，**DOC文档及DoT模板进行自我复制及传播。**
   - ①**传播极快**——Word宏病毒通过.DOC文档及.DOT模板进行自我复制及传播，而计算机文档是交流最广的文件类型。
   - ②**制作和变种方便**——编写和修改宏病毒比以往病毒更容易
   - ③**破坏可能性极大**——对系统直接构成威胁，而Word在指令安全性、完整性上检测能力很弱，破坏系统的指令很容易被执行
   - ④**多平台交叉感染**——当WORD、EXCEL这类著名应用软件在不同平台（如Windows、WindowsNT、和MACINTOSH等）上运行时，会被宏病毒交叉感染
   - ⑤**地域性问题**
2. 什么是蠕虫病毒 ?蠕虫病毒的主要特征是什?
   - 蠕虫是**一种能够利用系统漏洞通过网络进行自我传播的恶意程序。**
   - 它是**利用网络进行复制和传播，传染途径是通过网络和电子邮件。**
   - 主要特征：

- **较强的独立性**，不需要宿主程序，能独立运行；
- **利用漏洞主动攻击**；传播更快更广，
- **具有更大的传染性**，它不仅仅感染本地计算机，而且会以本地计算机为基础，感染网络中所有的服务器和客户端；
- **更好的伪装和隐藏方式；技术更加先进；使追踪变得更困难**

第四章

1. 数据在网络上传输为什么要加密？现在常用的数据加密算法主要有哪些？
    - **用户在计算机网络上进行通信**，主要的**危险是所传送的数据被非法窃听**
    - **现代密码学主要有两种基于密钥的加密算法**，分别是**对称加密算法**和**公开密钥算法。**
    - **数据加密技术**是**保证信息安全的重要手段之一**，**不仅具有对信息进行加密的功能，还具有数字签名身份验证、秘密分存、系统安全**等功能。所以，**使用数据加密技术不仅可以保证信息的机密性**，还可以**保证信息的完整性**、**不可否认性等**安全要素。

第五章

1. 简述防火墙的分类。
    - 按**物理实体**分类：**软件防火墙、硬件防火墙以及芯片级防火墙。**
    - 按**部署结构**分类：**单一主机防火墙；路由器集成式防火墙；分布式防火墙**
    - 按防火墙**的应用部署位置**分类：**边界防火墙、个人防火墙、和混合型防火墙**
    - 按**技术**分类：**包过滤防火墙、应用代理型防火墙、状态检测防火墙、复合型防火墙**
2. 防火墙应具有的基本功能是什么？
    - 防火墙的**功能**：该**网络流入流出的所有网络通信均要经过此防火墙。**在**逻辑上，防火墙是分离器，也是限制器，更是一个分析器。限定内部用户访问特殊站点。防止未授权用户访问内部网络。记录通过防火墙的信息内容和活动。****对网络攻击进行监测和报警****。
        - **①针对用户制定各种访问控制策略。**
        - **②对网络存取和访问进行监控审计。**
        - **③支持VPN功能。**
        - **④支持网络地址转换**
        - **⑤支持身份的认证等**

第六章

1. Windows Server注册表中有哪几个根键？各存储哪方面的信息？
    - Windows共有**5个根键**
    - **HKEY_CLASSES_ROOT实现对各种文件和文档信息的访问**
    - **HKEY_CURRENT_USER包含当前用户的登录信息。**
    - **HKEY_USERS包含计算机上所有用户的配置文件，用户可以在这里设置自己的关键字和子关键字。**
    - **HKEY_LOCAL_MACHINE包含了本地计算机（相对网络环境而言)的硬件和软件的全部信息**
    - **HKEY_CURRENT_CONFIG包含了当前系统配置情况**

第七章

1. 针对Web浏览器及其用户的安全威胁主要有哪些？
    - **网页挂马**，在**获取网站服务器的权限**后，在**网页**文件**中插入一段恶意代码。**如果**系统没有更新恶意代码中利用的漏洞补丁**，则**会执行恶意代码程序，进行盗号等危险操作。**

- **网站钓鱼指不法分子利用各种手段，仿冒真实网站的URL地址以及页面内容**，或者**利用真实网站服务器程序上的漏洞在站点的某些网页中插入危险的代码，骗取用户银行或信用卡账号、密码**等。
- **浏览器劫持是故意误导浏览器的行进路线的现象**，常见的**浏览器劫持有：访问正常网站时被转向到恶意网页、当输入错误的网址时被转到劫持软件指定的网站、IE浏览器主页/搜索页等被修改为劫持软件指定的网站地址、自动添加网站到"受信任站点"、不经意的插件提示安装、收藏夹里自动反复添加恶意网站链接等**

2. 如何防御跨站脚本攻击?

- **在服务器端**，如**Web应用程序将用户提交的数据复制到响应页面中，则必须对用户提交数据的长度、类型、是否包含转义等非法字符、是否包含HTML与JavaScript的关键标签符号等方面进行严格的检查和过滤，以净化可能的恶意字符。**
- **在客户端**，由于**跨站脚本最终是在客户端浏览器上执行的，因此必须提升浏览器的安全设置（如提升安全等级、关闭Cookie功能等)以降低安全风险。**

3. 如何防御SQL注入攻击?

- **最小权限原则**，如非必要，不**要使用sa、dbo等权限较高的账户**
- **对用户的输入进行严格的检查**，**过滤掉一些特殊字符**，强制约束数据类型、约束输入长度等
- **使用存储过程代替简单的SQL语句。**
- **当SQL运行出错时**，**不要把全部的出错信息全部显示给用户**，**以免泄露一些数据库的信息。**

4. Web服务器软件的安全漏洞有哪些？各自有哪些危害?

- **数据驱动的远程代码执行安全漏洞。针对这类漏洞的攻击包括缓冲区溢出、不安全指针、格式化字符等远程渗透攻击。**
- **服务器功能扩展模块漏洞**
- **源代码泄露安全漏洞。**可以**利用这些漏洞查看到系统级的文件。**
- **资源解析安全漏洞。Web服务器在处理资源请求时，需要将同一资源的不同表示方式解析为标准化名称这个过程称为资源解析。一些服务器软件可能在资源解析过程中遗漏了一些对输入资源合法性、合理性的验证处理，从而导致目录遍历、敏感信息泄露甚至代码注入攻击。**