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；系统连续、可靠、正常地运行，网络服务不中断**
2. 简述网络本身存在哪些安全缺陷？
    - 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？
    - 可将网络安全分成**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**主要包括：**防盗，防火，防静电，防雷击和防电磁泄漏。**
    - **逻辑安全**包括**访问控制、加密、安全管理及用户身份认证**
    - **操作系统**安全，**系统必须能区分用户，防止相互干扰。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. 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。

2. 一般的黑客攻击有哪些步骤？各步骤主要完成什么工作？
    - **隐藏IP**隐藏IP,就是隐藏黑客的位置，以免被发现
    - **踩点扫描**对所要攻击的目标进行多方了解，确保信息准确，确定攻击时间和地点
    - **获得特权**，实施攻击获得特权，即获得管理权限。侵袭网络
    - **种植后门**，黑客利用程序漏洞进入系统后安装后门程序，以便日后可不被察觉地再次进入系统
    - **隐身退出为了避免被发现**，在入侵完毕后会及时清除登录日志以及其他相关日志，隐身退出
3. 木马攻击的一般过程是什么
    1. **配置木马**：一般来说，一个设计成熟的木马都有木马配置程序，从具体的配置内容看，主要是为了实现以下两个功能。
        - **木马伪装**：木马配置程序为了在服务器端尽可能隐藏好，会采用多种伪装手段，如修改图标、捆绑文件、定制端口、自我销毁等。
        - **信息反馈**：木马配置程序会根据信息反馈的方式或地址进行设置，如设置信息反馈的邮件地址、IRC号、ICQ号等。
    2. **传播木马**
        - 配置好木马后，就要传播出去。木马的传播方式主要有：控制端通过E-mail将木马程序以附件的形式夹在邮件中发送出去，收信人只要打开附件就会感染木马；软件下载，一些非正规的网站以提供软件下载为名义，将木马捆绑在软件安装程序上，下载后，只要运行这些程序，木马就会自动安装；通过QQ等通信软件进行传播；通过病毒的夹带把木传播出去。
    3. **启动木马**
        - 木马程序传播给对方后，接下来是启动木马。一种方式是被动地等待木马或捆绑木马的程序被主动运行，这是最简单的木马。大多数首先将自身复制到Windows的系统文件夹中(C:Windows或C:\Windows\system32目录下)，然后写人注册表启动组，非启动组中设置好木马的触发条件，这样木马的安装就完成了。一般系统重新启动时木马就可以启动，然后木马打开端口，等待连接。
    4. **建立连接**
        - 一个木马连接的建立必须满足两个条件：一是服务器端已安装了木马程序；二是控制端、服务器端都要在线。在此基础上控制端可以通讨木马端口与服务器端建立连接。控制端可以根据提前配置的服务器地址、定制端口来建立连接；或者是用扫描器，根据扫描结果中检测哪些计算机的某个端口开放，从而知道该计算机里某类木马的服务器端在运行，然后建立连接；或者根据服务器端主动发回来的信息知道服务器端的地址、端口，然后建立连接。
    5. **远程控制**
        - 前面的步骤完成之后，就是最后的目的阶段，对服务器端进行远程控制，实现窃取密码、文件操作、修改注册表、锁住服务器端及系统操作等。
4. 木马攻击步骤
5. 分布式拒绝服务攻击的原理和攻击过程是什么？