

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：用来认证数据机密性与完整性，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。Web欺骗是一种电子信息欺骗，攻击者在其中创造了整个Web世界的一个令人信服但是完全错误的拷贝，错误的Web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Web站点，这样受攻击者浏览器和Web

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马传播出去。

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)，然后写入注册表启动组，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过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？

第三章

1. 什么是宏病毒？宏病毒的主要特征是什么？

- 病毒制作者利用office中提供的宏命令编程，专门制作的一个或多个具有病毒特点的宏的集合，这种病毒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office文档及模板文件进行自我复制及传播。

2. 什么是蠕虫病毒？蠕虫病毒的主要特征是什么？

- 蠕虫病毒是一种常见的计算机病毒。它是通过网络和电子邮件进行复制和传播。蠕虫病毒是包含的程序（或是一套程序），它能将自身功能或它的某些部分拷贝到其他的计算机系统中（通常是经过网络连接）。与一般病毒不同，蠕虫不需要附着到宿主程序，蠕虫病毒一般是通过1434端口漏洞传播。

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为边界防火墙、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
 - ①HKEY_CLASSES_ROOT实现对各种文件和文档信息的访问
 - ②HKEY_CURRENT_USER包含当前用户的登录信息。
 - ③HKEY_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。
 - ④HKEY_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
 - ⑤HKEY_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？
 - ①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。
 - ②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。

- ③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。