## 第二章

1. 选择题  
   1.网络监听是（ ）。  
   A. 远程观察一个用户的计算机   
   B. 监视网络的状态、传输的数据流  
   C. 监视PC系统运行情况  
   D. 监视一个网站的发展方向  
   2. 2.关于DoS（拒绝服务）下面表述不正确的是（ ）。  
   A.用超过被攻击目标处理能力的海量数据包来消耗可用系统、宽带资源等方法的攻击。   
   B. 全称是Distributed Denial Service  
   C. 拒绝来自一个服务器所发送回应请求的指令  
   D. 入侵控制系统一个服务器远程关机  
   3.木马分为（ ）类。  
   A.5   
   B.6  
   C.7  
   D.8  
   4.木马的启动方式有（ ）类。  
   A.5   
   B.6  
   C.7  
   D.8  
   5.下列（ ）方式不是网络游戏木马采用的盗用用户信息的方式。  
   A.记录用户键盘输入  
   B.Hook游戏进程API函数等方式获取  
   C.直接提问、回答的方式  
   D.抽奖活动  
   6.通常黑客攻击的4个阶段是（ ）、（ ）、 （ ）和（ ）。(P32)  
   7.常见的黑客攻击有（ ）、 （ ）、 （ ）、 （ ）、 （ ）、 （ ）、 （ ）  
   8.传播木马的方式主要有两种：一种是通过（ ）；另一种是（ ）。  
   10.如果每次打开Word程序编辑文档时，计算机都会把文档传送到一台FTP服务器，那么可以怀疑Word程序已经被黑客植入（ ）。  
   A.蠕虫   
   B.FTP程序  
   C.特洛伊木马  
   D.陷门  
   11.以下网络攻击中，（ ）不属于主动攻击。  
   A.重放攻击  
   B.拒绝服务攻击  
   C.通信量分析攻击  
   D.假冒攻击  
   12.有一种攻击是不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪，这种攻击叫做（ ）。  
   A.重放攻击  
   B.拒绝服务攻击  
   C.反射攻击  
   D.服务攻击  
   13.（ ）为不属于防止口令猜测的措施。  
   A.严格限制从一个给定的终端进行非法认证的次数  
   B.确保口令不在终端上再现  
   C.防止用户使用太短的口令  
   D.使用机器产生的口令  
   14.网络攻击发展趋势是（ ）   
   A.黑客技术与网络病毒日益融合   
   B.攻击工具日益先进   
   C.病毒攻击   
   D.黑客攻击   
   15. 黑客造成的主要安全隐患包括 ( )   
   A.进入系统、损毁信息及谣传信息  
   B.攻击系统、获取信息及假冒信息   
   C.破坏系统、窃取信息及伪造信息  
   16.一般的黑客攻击有哪些步骤？各步骤主要完成什么工作？(P32)  
   17. 木马攻击的一般过程是什么？？  
   18.木马攻击步骤  
   19，分布式拒绝服务供给的原理和供给过程是什么？

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。

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。

\*\*（1）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。

\*\*（2）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。