第二章

一、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

3. 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)

4. 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。

第三章 计算机病毒

选择题

1.计算机病毒的最基本特征是（　）。

A. 隐蔽性

B. 潜伏性

C. 破坏性

D. 传染性

2.以下（　）不是杀毒软件。

A. KV3000

B. 瑞星

C. PCTools

D. Norton AntiVirus

3.下列叙述中正确的是（　）。

A. 计算机病毒只感染可执行文件

B. 计算机病毒只感染文本文件

C. 计算机病毒只能通过软件复制的方式进行传播

D. 计算机病毒可以通过读写磁盘或网络等方式进行传播

4.以下关于计算机病毒的特征说法正确的是：（　）

A. 计算机病毒只具有破坏性，没有其他特征

B. 计算机病毒具有破坏性，不具有传染性

C. 破坏性和传染性是计算机病毒的两大主要特征

D. 计算机病毒只具有传染性，不具有破坏性

5.以下关于宏病毒说法正确的是：（　）

A. 宏病毒主要感染可执行文件

B. 宏病毒仅向办公自动化程序编制的文档进行传染

C. 宏病毒主要感染软盘、硬盘的引导扇区或主引导扇区

D. CIH病毒属于宏病毒

6.不属于计算机病毒防治的策略的是（　）

A. 确认您手头常备一张真正“干净”的引导盘

B. 及时、可靠升级反病毒产品

C. 新购置的计算机软件也要进行病毒检测

D. 整理磁盘

7.计算机病毒能够 (　)

A 破坏计算机功能或者毁坏数据

B 影响计算机使用

C 能够自我复制

D 保护版权

8.关于计算机病毒知识，叙述不正确的是（ ）
A 计算机病毒是人为制造的一种破坏性程序
B 大多数病毒程序具有自身复制功能
C 安装防病毒软件, 并不能完全杜绝病毒的侵入
D 不使用来历不明的软件是防止病毒侵入的最有效措施
9.计算机病毒的危害性有以下几种表现 ( )
A 删除数据
B 阻塞网络
C 信息泄漏
D 烧毁主板
10.计算机病毒的主要传播途径有 ( )
A 电子邮件
B 网络
C 存储介质
D 文件交换

11. 清除硬盘中的引导型计算机病毒必须洁净的系统启动，然后再清除病毒？( )
12. （ ）是计算机病毒的一种，利用计算机网络和安全漏洞来复制自身的一段代码。
13. 部署安全高效的防病毒系统，主要考虑以下几个方面（ ）
    A 、系统防毒
    B 、终端用户防毒
    C 、服务器防毒
    D 、客户机防毒。
14. 下列不属于计算机病毒特性的是（ ）
    A 、传染性
    B 、突发性
    C 、可预见性
    D 、隐藏性。
15. 计算机病毒（ ）
    A 、都具有破坏性
    B 、有些无破坏性
    C 、都破坏.exe文件
    D 、不破坏数据，只破坏文件
16. 计算机病毒（ ）
    A 、是生产计算机硬件时不注意产生的
    B 、都是人为制造的
    C 、都必须清除计算机才能使用
    D 、有可能是人们无意中制造的
17. 防范手机病毒的方法有（ ）
    A. 经常为手机查杀病毒
    B. 注意短信息中可能存在的病毒
    C. 尽量不用手机从网上下载信息
    D. 关闭乱码电话
18. 什么是宏病毒？宏病毒的主要特征是什么？

19.什么是蠕虫病毒 ?蠕虫病毒的主要特征是什?

答案

1.D 2.C 3.D 4.C 5.B 6.D 7.ABC 8.D 9.ABCD 10.ABCD 11.对 12.蠕虫病毒 13.ABCD 14.C 15.B 16.B 17.ABCD

18.宏病毒隐蔽性强，传播迅速，危害严重，难以防治与感染普通.EXE或.COM文件的病毒相比Wod宏病毒具有隐蔽性强，传播迅速，危害严重，难以防治等特点

19.特征：较强的独立性，利用漏洞主动攻击，传播更快更广，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. 下列()不是密码技术发展的一个阶段。C
   A.古典密码
   B.近代密码
   C.恺撒密码
   D.现代密码
2. DES算法的入口参数有3个：Key、Data和Mode。其中Key的实际长度为()位，是DES算法的工作密钥。D
   A、64
   B、7
   C、8
   D、56
3. ()是网络通信中标志通信各方身份信息的一系列数据，提供一种在Intenet上验证身份的方式。B
   A.数字认证
   B.数字证书
   C.电子证书
   D.电子认证
4. 以下关于数字签名说法正确的是：() D
   A.数字签名是在所传输的数据后附加上一段和传输数据毫无关系的数字信息
   B.数字签名能够解决数据的加密传输，即安全传输问题
   C.数字签名一般采用对称加密机制
   D.数字签名能够解决篡改、伪造等安全性问题
5. SET协议又称为() B
   A.安全套接层协议
   B.安全电子交易协议
   C.信息传输安全协议
   D.网上购物协议
6. DES算法将输入的明文分成(64位)的数据组块进行加密，密钥长(64位)，有效密钥长度为(54位)，其他(8位)用于奇偶校验。
7. RSA算法的安全是基于(分解两个大质数的积)的困难。
8. 以下关于对称加密的说法不正确的是？()B
   A、在对称加密中，只有一个密钥用来加密和解密信息
   B、在对称加密中，用到了二个密钥来加密和解密信息，分别是公共密钥和私用密钥
   C、对称加密是一个简单的过程，双方都必需完全相信对方，并持有这个密钥的备份
   D、对称加密的速度非常快，允许你加密大量的信息而只需要几秒钟
9. 采用字符串“work”为密钥，把明文“CAN YOU UNDERSTAND”,按照密钥由大到小的顺序进行矩阵排列加密。
10. 按照RSA算法，若选两奇数p=5,q=3,公钥e=7,则私钥d为()。

    A.6
    B.7
    C.8
    D.9
11. 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. 下列()不是硬件防火墙的端口。D
   A.WAN
   B.LAN
   C.DMZ(非军事化区)
   D.PCI
2. 下列()不是CPU构架下的防火墙分类。B
   A.X86架构防火墙
   B.Windows7防火墙
   C.P架构防火墙
   D.ASIC架构防火墙
3. 关于防火墙，以下说法错误的是()D
   A.防火墙能隐藏内部IP地址
   B.防火墙能控制进出内网的信息流向和信息包
   C.防火墙能提供VPN功能
   D.防火墙能阻止来自内部的威胁
4. ()技术不是实现防火墙的主流技术。B
   A.包过滤技术
   B.NAT技术(网络地址转换)
   C.应用级网关技术
   D.代理服务器技术
5. 防火墙采用的最简单的技术是()A
   A.包过滤
   B.隔离
   C.设置进入密码
   D.安装保护卡
6. 代理防火墙作用于网络层(X) 应用层
7. 双宿主主机网关中的双宿主主机是一台安装有一块网卡的计算机(X）两个网卡
8. 防火墙是指()。B
   A、防止一切用户进入的硬件
   B、阻止侵权进入和离开主机的通信硬件或软件
   C、记录所有访问信息的服务器
   D、处理出入主机的邮件的服务器
9. 防火墙能够()。B
   A、防范恶意的知情者
   B、防范通过它的恶意连接
   C、防备新的网络安全问题
   D、完全防止传送己被病毒感染的软件和文件
10. 防火墙的基本构件包过滤路由器工作在0SI的哪一层()C
    A、物理层
    B、传输层
    C、网络层

D、应用层

11. 防火墙对数据包进行状态检测过滤时，不可以进行检测过滤的是()D
    A、源和目的IP地址
    B、源和目的端口
    C、IP协议号
    D、数据包中的内容
12. 防火墙采用的最简单的技术是()C
    A.安装保护卡
    B.隔离
    C.包过滤
    D.设置进入密码
13. 采用防火墙的网络一定是安全的。 ()X
14. 防火墙能够完全防止传送已被病毒感染的软件和文件。 ()X
15. 非军事化区DMZ是为了解决安全防火墙后外部网路不能访问内部网络服务器的问题，而设立的一个非安全系统与安金系统之间的缓冲区。()√
16. 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
17. 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的注册表是不可编辑的 () X
2. 下面()项不是Windows Server的安全策略？D
   A.威胁和漏洞减少技术
   B.安全配置评估与管理技术
   C.身份认证和访问控制技术
   D.入侵规则管理技术
3. 下面()是存储当前计算机硬件和软件信息 B
   A.HKEY_CLASSER_ROOT
   B.HKEY_LOCAL_MACHINE
   C.HKEY_USER
   D.HKEY_CURRENT_CONFIG

4. 不是Windows Server的系统进程。B
   A.csrss.exe
   B.IEXPLORE.EXE
   C.lsass.exe
   D.services.exe
5. ()不是Windows的共享访问权限。D
   A.只读
   B.完全控制
   C.更改
   D.读取及执行
6. Windows操作系统设置账户锁定策略，这可以防止()B
   A.木马
   B.暴力攻击
   C.IP欺骗
   D.缓存溢出攻击
7. 为了设置基于用户的本地文件权限，必须采用()文件系统。C
   A.UID
   B.GID
   C.NTFS
   D.FAT
8. 打开本地组策略编辑器的命令是() D
   A.regedit
   B.cmd
   C.exit
   D.gpedit.msc
9. 打开注册表的命令是() A
   A.regedit
   B.cmd
   C.exit
   D.gpedit.msc
10. 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. 下列()不属于Web服务器存在的主要漏洞。D
   A.物理路径泄露
   B.CGI源代码泄露
   C.目录遍历
   D.网页下载

2. 下列()不是ActiveX控件组成的要素。C
   A.属性
   B.方法
   C.目标
   D.事件
3. 目前不是常用的Web服务器的是() D
   A.Apache
   B.IIS
   C.Tomcat
   D.Oracle
4. Web浏览器的不安全因素主要来自于()B
   A.黑客的攻击
   B.Web浏览器的漏洞
   C.用户自身错误
   D.服务器的风险
5. 不是Internet Explorer的安全威胁()A
   A.TCP/IP协议漏洞
   B.远程执行代码漏洞
   C.拒绝服务漏洞
   D.地址栏URI欺骗漏洞
6. HTTP协议是分布式的Web应用的核心技术协议，在TCP/IP协议栈中属于()层协议D
   A.会话层
   B.表示层
   C.网络层
   D.应用层
7. 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、E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
8. 如何防御跨站脚本攻击?
   - (1)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。
   - (2)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。
9. 如何防御SQL注入攻击?
   - ①最小权限原则，如非必要，不要使用sa、dbo等权限较高的账户
   - ②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
   - ③使用存储过程代替简单的SQL语句。
   - ④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。
10. Web服务器软件的安全漏洞有哪些？各自有哪些危害?
    - ①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。

- ②服务器功能扩展模块漏洞
- ③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。
- ④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。