《计算机信息安全技术(第二版)》

课后习题参考答案

目　录

习题 1

一、单项选择题

1.关于访问控制服务的描述中，正确的是____A____。

A.可控制用户访问网络资源　B.可识别发送方的真实身份

C.不限制用户使用网络服务　D.可约束接收方的抵赖行为

2.关于信息安全问题的描述中，不正确的是____A____。

A.仅依赖技术手段就可以解决　B.需要政府制定政策加以引导

C.需要通过立法约束网络行为　D.需要对网络用户进行安全教育

3.第三方假冒发送方的身份向接收方发送信息称为____D____。

A.窃取信息　B.重放信息　C.篡改信息　D.伪造信息

4.在以下几个国际组织中，制定 X.805 安全标准的是____B____。

A. ISO　B. ITU　C. IRTF　D. NIST

5.在信息安全的基本要素中，防止非授权用户获取网络信息的是____C____。

A.可用性　B.可靠性　C. 保密性　D.完整性

二、填空题

1.OSI 安全体系结构中，五大类安全服务是指__鉴别服务__、__访问控制服务__、__数据机密性服务_、__数据完整性服务_和__抗抵赖性服务_。

2.在我国信息安全等级保护标准中，满足访问验证保护功能的等级是__第五级：访问验证保护级__。

3. 在 PPDR 模型中，通常由四个主要部分组成：安全策略(Policy)、保护(Protection)、检测(Detection)和响应(Response)。

4.在 ITSEC 的安全等级中，C2 级的安全要求比 B3 级更___低___。

5.国际标准化组织的英文缩写是____ISO____。

三、简答题

1．计算机信息系统安全的威胁因素主要有哪些？

答：计算机信息系统安全的威胁因素主要有三种，即：

(1) 直接对计算机系统的硬件设备进行破坏。

(2) 对存放在系统存储介质上的信息进行非法获取、篡改和破坏等。

(3) 在信息传输过程中对信息非法获取、篡改和破坏等。

2．从技术角度分析引起计算机信息系统安全问题的根本原因是什么？

答：从技术的角度分析，根本原因主要有三个方面，即：

1）人为的无意失误；

2) 人为恶意攻击；

3) 软件设计不完善。

3．信息安全的 CIA 指的是什么？

答：C 代表机密性(Confidentiality)，即保证信息为授权者拥有而不泄露给未经授权者。I 代表完整性(Integrity)，它包含两方面的含义，一是数据完整性，即数据未被非授权者篡改或损坏；二是系统完整性，即系统未被非授权操纵，按既定的功能运行。A 代表可用性(Availability)，即保证信息和信息系统随时为授权者提供服务，而不要出现非授权者滥用却

对授权者拒绝服务的情况。

４．简述 PPDR 安全模型的构成要素及运作方式。
答：PPDR 模型由四个主要部分组成：安全策略(Policy)、保护(Protection)、检测(Detection)和响应(Response)。PPDR 模型是在整体的安全策略的控制和指导下，综合运用防护工具(如防火墙、身份认证、加密等)的同时，利用检测工具(如漏洞评估、入侵检测系统)了解和评估系统的安全状态，通过适当的安全响应将系统调整到一个比较安全的状态。保护、检测和响应组成了一个完整的、动态的安全循环。
５．计算机信息安全研究的主要内容有哪些？
答：计算机信息安全技术研究的内容应该包括如下三个方面的内容：一是计算机外部安全；二是计算机信息在存储介质上的安全，有时也称为计算机内部安全；三是计算机信息在传输过程中的安全，也称为计算机网络安全。

６．计算机信息安全的定义是什么？
答：信息安全是研究在特定应用环境下，依据特定的安全策略，对信息及其系统实施防护、检测和恢复的科学。

７．计算机安全系统中，人、制度和技术之间的关系如何？
答：人是第一位的，然后人必须按照制度办事，超越了或者不制度办事就有漏洞。技术当然是需要的，需要有懂技术的人才能在一定程度上堵住漏洞；但更重要的是制度必须执行。

习题 2

一．选择题

1.下列哪种算法属于公开密钥算法____C____。
A．AES 算法　　B．DES 算法　C．NTRU 算法　　D．天书密码

2.下列（ B ）算法属于置换密码
A. 移位密码　B. 天书密码　C. Vigenère 密码　D. 仿射密码

3. DES 加密过程中，需要进行__B__轮变换。
A. 8　B. 16　C.24　D.32

4. 关于 ECC 的描述中，正确的是___C___。
A. 它是一种典型的基于流的对称密码算法
B. 它的安全基础是大素数的因子分解非常困难
C. 在安全性相当时，其密钥长度小于 RSA 算法
D. 在密钥长度相当时，其安全性低于 RSA 算法

5. 在以下几种分组密码操作中，最简单的操作模式是____A____。
A. ECB 模式　B. CBC 模式　C. OFB 模式　D. CFB 模式

6. 在以下几种密钥长度中，不符合 AES 规范的是____B____。
A. 128 位　B. 168 位　C. 192 位　D. 256 位

二．填空题

(1)给定密钥 K=10010011，若明文为 P=11001100，则采用异或加密的方法得到的密文为

__01011111_____。

(2)在数据加密标准中 DES 中，需要进行____16____轮相同的变换才能够得到 64 位密文输出。

(3)RSA 算法的安全性完全取决于__p、q 的保密性__以及____大数分解的难度_____。

4. Diffie-Hellman 算法的最主要应用领域是__密钥交换_____。

5. DES 算法中，每次加密的明文分组大小为____64_____位。

三．简答题

1．请说明研究密码学的意义以及密码学研究内容是什么？

答：密码学技术是保障信息和信息系统安全的核心技术之一，它起源于保密通信技术。密码学的研究分为密码编码学(Cryptography)和密码分析学(Cryptanalysis)两大部分，其中密码编码学是研究如何对信息编码以实现信息和通信安全的科学，而密码分析学则是研究如何破解或攻击受保护的信息的科学；这两者既相互对立，又相互促进，推动了密码学不断向前发展。

2．请比较代替密码中移位密码、单表代换密码和多表代换密码的安全性优劣，说明理由。

答：移位密码中只用到了一个参数，因此，很容易受到统计分析的攻击；单表代换密码的安全性较移位密码有很多的改进，但仍然不能避免统计分析的攻击；多表代换密码采用多个表的组合方式实现对明文的加密，可以有效销平某些字母出现的频率特性，从而可以有效防止统计分析这种攻击方法，具有较好的安全性。

3．已知仿射密码的加密函数可以表示为：

$$f(a) = (aK_1 + K_0) \bmod 26$$

明文字母 e、h、对应的密文字母是 f、w，请计算密钥 K_1 和 K_0 来破译此密码。

答： 由题意有

$$\begin{cases} 4 * k_1 + k_0 = 5 \bmod 26 \\ 7 * k_1 + k_0 = 22 \bmod 26 \end{cases}$$

解该方程组可得 $k_1 = 23$， $k_0 = 17$。

4．用 Vigenère 密码加密明文“please keep this message in secret”，其中使用的密码为“computer”，是求其密文。

答： 加密结果为：rzqpmxovgdfwclqvugmvybrjgqdtn

5．设英文字母 a，b，c，…，分别编号为 0，1，2，…，25，仿射密码加密变换为 c = (3m + 5) mod 26，其中 m 表示明文编号，c 表示密文编号。

(1) 试对明文 security 进行加密。

(2) 写出该仿射密码的解密函数。

(3) 试对密文进行解密。

答：（1）加密结果 hrlnedkz

（2）解密函数 $m = 3^{-1} * (c - 5) \bmod 26 = 9 * (c - 5) \bmod 26$

（3）解密结果 security

6．简述序列密码算法与分组密码算法的不同。

答：
尽管分组和序列密码算法非常不同，但分组密码也可作为序列密码使用，反之亦然。分组密码算法是对一个大的明文数据块（分组）进行固定变换的操作；序列密码算法是对单个明文比特的随时间变换的操作。两者之间的区别主要体现在实现上。每次只能对一个数据比特进行加解密的序列密码算法并不适用于软件实现。分组密码算法就可以很容易地用软件来实现，因为它可以避免耗时的位操作，并且它易于处理由计算机界定大小的数据分组。当然另一方面，序列密码更适合用硬件实现，因为使用硅材料可以非常有效地实现它。

7. 简述 DES 算法中 S-盒的特点。
答：S 盒不是它所输入变量的线性函数；改变 S 盒的一个输入位至少要引起两位的输出改变；对任何一个 S 盒，如果固定一个输入比特，当其它输入变化时，输出数字中 0 和 1 的总数近于相等。
8. 简述 AES 和 DES 的相同之处。
答：1）DES 和 AES 都是对称密码算法，分组密码算法；2）算法中都有迭代过程；3）加解密过程都有轮函数；4）密钥也要经过一定变换才参与算法的加密过程；5）算法的解密过程都与加密过程类似，只是迭代是逆序。

9. 画出 RSA 算法的流程图。
答：略
10. 使用 RSA 算法时，选择有关参数应该注意哪些问题？
答：1）p 和 q 之差要大。2）p-1 和 q-1 的最大公因子应很小。3）p 和 q 必须为强素数。

11. 在一个使用 RSA 的公开密钥系统中，如果攻击者截获了公开密钥 pk=5，公开模数 r=35，密文 c=10，明文是什么？
答：分解 r=35=7×5，于是 p=7,q=5。ϕ（r）=6×4=24。因为 pk=5，根据 pk.sk=1 mod ϕ（r），求出 sk=5。

根据 $M = c^{sk} \bmod r = 10^5 \bmod 35 = 5$ 。

12. 简述 RSA 算法的优缺点。
答：优点：RSA 算法的加密密钥和加密算法分开，使得密钥分配更为方便。
缺点：RSA 的 密钥很长，加密速度慢。

13. 在一个使用 RSA 的公开密钥系统中，假设用户的私人密钥被泄露了，他仍使用原来的模数重新产生一对密钥，这样做安全吗？
答：安全。当私人密钥被泄漏以后，攻击者只是得到了{sk，n}，如果要得到新产生的密钥，仍然需要进行大数分解才能找到新的密钥，计算难度和破解之前是一样的。
9. 请说明对称密码与公钥密码的主要区别，以及它们的主要应用领域。
答：对称密码只有一个共用的密钥；非对称密码有两个不同的密钥, 用一个加密, 另外一个解密. 非对称密码计算量要大很多, 一般是使用双方确定了一对非对称密码密钥, 用来传输临时决定的一个对称密码密钥, 然后用对称密码进行大量数据的加密通信.
10. 请说明对称密钥与非对称密钥算法中密钥分发的主要区别，以及它们所采用的主要技术手段。
答：对称密钥算法中，加密密钥和解密密钥相同或者可以从一个推出另外一个，因此对密钥

的保密性要求较高，密钥分发必须在安全信道中进行传输；而非对称密钥体制中，加密密钥和解密密钥不同，而且不能相互推出，因此公钥可以在公共信道中公开传输。在对称密钥体制中，通常密钥传输需要借助公钥密码体制的加密技术来完成，而公钥密码体制中则无此限制。

习题 3

一、选择题

1.身份认证是安全服务中的重要一环，以下关于身份鉴别的叙述不正确的是(B)。

A. 身份认证是授权控制的基础

B. 身份认证一般不用提供双向的认证

C. 目前一般采用基于对称密钥加密或公开密钥加密的方法

D. 数字签名机制是实现身份认证的重要机制

2. 数据完整性可以防止以下哪些攻击(D)。

A. 假冒源地址或用户的地址欺骗攻击　　B. 抵赖做过信息的递交行为

C. 数据中途被攻击者窃听获取　　D. 数据中途被攻击者篡改或破坏

3.数字签名要预先使用单向 Hash 函数进行处理的原因是(C)。

A. 多一道加密工序使密文更难破译

B. 提高密文的计算速度

C. 缩小签名密文的长度，加快数字签名和验证签名的运算速度

D. 保证密文能正确地还原成明文。

4.下列（ A ）运算在 MD5 中没有使用到。

A. 幂运算　　B.逻辑与或非　　C.异或　　D.移位

5.关于安全散列算法的描述中，错误的是（ B ）

A.它是一系列散列函数的统称　　B.SHA-1 生成的特征值长度为 160 位

C.生成的特征值通常称为摘要　　D.SHA-512 处理的分组长度为 512 位

二、填空题

1.MD5 和 SHA1 产生的散列值分别是__128__位和___160____位。

2.基于哈希链的口令认证，用户登录后将口令表中的(ID，k-1，H_{k-1}(PW))替换为_(ID,k-2,H_{k-2}(PW)_。

3 Denning-Sacco 协议中使用时间戳 T 的目的是__防止重放攻击对密钥安全性的威胁__。

4. Woo-Lam 协议中第[6][7]步使用随机数 N_2 的作用是_使 B 确信 A 已经获得正确的会话密钥。

5. 消息认证技术中，MD 算法可以用于为消息计算_消息摘要___。

三、简答题

1.弱抗碰撞性和强抗碰撞性有什么区别？

答：给定的消息 M，要找到另一消息 M’，满足 H(M)=H(M’)在计算上是不可行的，称为弱抗碰撞性。该性质是保证无法找到一个替代报文，否则就可能破坏哈希函数进行封装或者签名的各种协议的安全性。哈希函数的重要之处就是赋予 M 唯一的指纹。对于任意两个不同的消息 M≠M’，它们的散列值不可能相同，这条性质叫强抗碰撞性。强抗碰撞性对消息的哈希函数的要求更高，这条性质保证了对生日攻击的防御能力。在弱抗碰撞中，只要求找到另

外一条消息的哈希值在计算上不可行就可以了，也就是说对哈希函数的要求是允许出现碰撞。在通常的哈希函数中，强抗碰撞性是十分难达到的。

2.什么是消息认证码？

答：

是指使合法的接收方能够检验消息是否真实的过程。消息认证码实际上是对消息产生的一个指纹信息——MAC（消息认证），消息认证码是利用密钥对待认证消息产生的新数据块，并对该数据块加密得到的。它对待保护的信息来说是唯一的，因此可以有效地保证消息的完整性，以及实现发送消息方的不可抵赖和不能伪造性。

3.比较 MD5 和 SHA1 的抗穷举攻击能力和运算速度。

答：

由于MD5 与SHA-1均是从MD4 发展而来,它们的结构和强度等特性有很多相似之处。SHA-1与 MD5 的最大区别在于其摘要比 MD5 摘要长 32 比特。对于强行攻击，产生任何一个报文使之摘要等于给定报文摘要的难度：MD5 是 2^128 数量级的操作，SHA-1 是 2^160 数量级的操作。产生具有相同摘要的两个报文的难度:MD5 是 2^64 是数量级的操作,SHA-1 是 2^80 数量级的操作。因此,SHA-1 对强行攻击的强度更大。但由于 SHA-1 的循环步骤比 MD5 多（80:64）且要处理的缓存大（160 比特:128 比特），SHA-1 的运行速度比 MD5 慢。

4.MD5 和 SHA1 的基本逻辑函数是什么？

答：

MD5 基本逻辑函数：

F(X,Y,Z)=(Z∧Y) ∨((¬ X) ∧Z)

G(X,Y,Z)=(X∧Z) ∨(Y∧(¬ Z))

H(X,Y,Z)=X⊙Y⊙Z

G(X,Y,Z)=Y⊙(∨(X∧(¬ Z))

SHA-1 基本逻辑函数：

$$f_t(X,Y,Z)=\begin{cases}(X\wedge Y)\vee((\neg X)\wedge Z) & 0\le t\le 19\\ X\oplus Y\oplus Z & 20\le t\le 39\\ (X\wedge Y)\vee(X\wedge Z)\vee(Y\wedge Z)) & 30\le t\le 59\\ X\oplus Y\oplus Z & 40\le t\le 79\end{cases}$$

5.Woo-Lam 协议一共 7 步，可以简化为 5 步：

[1]A→B：

[2]B→KDC：

[3]KDC→B

[4]B→A：

[5]A→B：

请给出每步中传输的信息。

答：

[1]A→B：$E_{KPb}(N_1||ID_A)$

[2]B→KDC：$ID_B||ID_A||E_{KPk}(N_1)$

[3]KDC→B：$E_{KSk}(ID_A||K_{Pa})||E_{KPb}(E_{KSk}(N_1||K_S||ID_B))$

[4]B→A：$E_{KPa}(E_{KSk}(N_1||K_S||ID_B)||N_2)$

[5]A→B：$E_{Ks}(N_2)$

6.Needham-Schroeder 协议存在的一个致命漏洞是旧的会话密钥仍有价值，假设黑客 H 通过某种途径获得旧的密钥 K_S，H 就可以假装成 A 发起一次攻击，请说明 H 是在协议的哪一步起发动攻击的，详细说明其过程。(假设 H 能获得协议中每次传输的内容)

答：

攻击者 X 可能从某些途径获得一个过期的会话密钥，然后，X 就可以冒充 A 重放第 3 步的报文，欺骗 B 使用过期的会话密钥，除非 B 明确记得以前与 A 通信所使用的所有会话密钥，否则 B 无法确定是否是重放的消息。

习题 4

一、选择题

1.关于计算病毒，下列说法不正确的是：___C_____

A.计算机病毒不感染可执行文件和.COM 文件

B.计算机病毒不感染文本文件

C.计算机病毒只能复制方式进行传播

D.计算机病毒可以通过读写磁盘和网络等方式传播

2.与文件型病毒对比，蠕虫病毒不具有的特征是___A_____。

A.寄生性　B.传染性　C.隐蔽性　D.破坏性

3.关于木马的描述中，正确的是_____C_____。

A.主要用于分发商业广告　B.主要通过自我复制来传播

C.可通过垃圾邮件来传播　D.通常不实现远程控制功能

4.关于特征码检测技术的描述中，正确的是_____B_____。

A.根据恶意代码行为实现识别　B.检测已知恶意代码的准确率高

C.具有自我学习与自我完善的能力　D.有效识别未知恶意代码或变体

5.关于宏病毒的描述中，正确的是_____B_____。

A.引导区病毒的典型代表　B.脚本型病毒的典型代表

C.僵尸型病毒的典型代表　D.蠕虫型病毒的典型代表

二、填空题

1. 与普通病毒不同，宏病毒不感染 EXE 文件和 COM 文件，也不需要通过引导区传播，它只感染__文档文件___。

2. 计算机病毒的一般由 3 个基本模块组成，即__安装模块__、_传染模块_和__破坏模块。

3.如果某封电子邮件中含有广告信息，并且是由发送方大批量的群发，则这封邮件称为垃圾邮件___。

4.根据病毒的寄生方式分类，计算机病毒可以分为_网络病毒_，文件型病毒，_引导型病毒_和混合型病毒四种。

三、简答题

１．简述计算机病毒的定义和基本特征。

答：计算机病毒定义为：编制或在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。

计算机病毒有如下三个基本特征，即传染性，破坏性和隐蔽性。病毒能通过自我复制来传染正常文件，达到破坏计算机正常运行的目的，即传染性。任何计算机病毒感染了系统后，都会对系统产生不同程度的影响。病毒都是可执行程序，当病毒代码运行时就会降低系统的工作效率，占用系统资源，即计算机病毒的破坏性。计算机病毒具有很强的隐蔽性，它一般都是具有很高编程技巧的、短小精悍的代码，通常附在正常的程序之中或藏在磁盘隐秘的地方，即计算机病毒得隐蔽性。

２．计算机病毒有哪几种类型？

答：常见的计算机病毒类型有引导型病毒、文件型病毒、蠕虫病毒和木马等。引导型病毒主要感染磁盘的引导扇区或硬盘主引导区；文件型病毒主要通过感染宿主文件的方式来进行传染和破坏；蠕虫病毒实际上是一种恶意代码；木马实际上是一种典型的黑客程序。

3．简述计算机病毒的一般构成。

答：计算机病毒一般由 3 个基本模块组成，即安装模块、传染模块和破坏模块。对每个病毒程序来说，安装模块、传染模块是必不可少的，而破坏模块则可以直接隐含在传染模块中，也可以单独构成一个模块。

4．计算机病毒的制作技术有哪些？

答：1）采用自加密技术。计算机病毒采用自加密技术就是为了防止被计算机病毒检测程序扫描出来，并被轻易地反汇编。计算机病毒使用加密技术后，给分析和破译计算机病毒的代码及清除病毒等工作增加了难度。

2）采用特殊的隐形技术。 当计算机病毒采用特殊的隐形技术后，可以在计算机病毒进入内存后，使计算机用户几乎感觉不到它的存在。

3）对抗计算机病毒防范系统。计算机病毒采用对抗计算机病毒防范系统技术时，当发现磁盘中某些著名的杀毒软件或在文件中查到出版这些软件的公司名，就会删除这些杀毒软件或文件，造成杀毒软件失效，甚至引起系统崩溃。

4）反跟踪技术。计算机病毒采用反跟踪技术的主要目的是要提高计算机病毒程序的防破译和防伪能力。

5．目前使用的查杀病毒的技术有哪些？

答：对病毒的检测方法主要有：特征代码法、校验和法、行为监测法和软件模拟法等。

6．什么是特洛伊木马？特洛伊木马一般有哪几部分组成的。

答：木马全称是“特洛伊木马”， 实际上是一种典型的黑客程序，它是一种基于远程控制的黑客工具。通过木马，攻击者可以远程窃取用户计算机上的所有文件、查看系统消息、窃取用户口令、篡改文件和数据、接收执行非授权者的指令、删除文件甚至格式化硬盘，还可以将其他病毒传染到计算机上，可以远程控制计算机鼠标、键盘、查看用户的一举一动，甚至可造成系统的崩溃、瘫痪。

木马系统程序一般有两个部分组成：一个是服务端程序，另一个是客户端程序。如果某台计算机中安装了黑客服务端程序，那么黑客就可以利用自己的客户端程序进入这台计算机中，通过客户端程序达到控制和监视这台计算机的目的。以冰河程序为例，被控制段可视为一台服务器，而控制端则是一台客户机，服务端安装了 G_Server.exe 服务程序，客户端安装了 G_Client.exe 控制程序，如果有客户端向服务端的端口提出连接请求，服务端的相应程序就会自动运行，响应客户端的请求。

7．编写一个病毒演示程序，实现自动执行、自动传染和删除指定文件的功能。

略。

8．分析下面的代码，程序运行将有什么结果？

```
<html>
<body>
<A href="" onmouseover="while(true){window.open()}">点击可进入你需要的网站</A>
</body>
</html>
```

答：该代码可以实现每当鼠标移动到该页面的时候就打开一个新的窗口，最终出现大量的窗口。

习题 5

一、 选择题。

1 B 是使计算机疲于响应这些经过伪装的不可到达客户的请求，从而使计算机不能响应正常的客户请求等，从而达到切断正常连接的目的。

A．包攻击　　B．拒绝服务攻击

C．缓冲区溢出攻击　　D．口令攻击

2 C 就是要确定你的 IP 地址是否可以到达，运行哪种操作系统，运行哪些服务器程序，是否有后门存在。

A．对各种软件漏洞的攻击　　B．缓冲区溢出攻击

C．IP 地址和端口扫描　　D．服务型攻击

3 分布式拒绝服务 DDoS 攻击分为 3 层： C 、主控端、代理端，三者在攻击中扮演着不同的角色。

A．其它　　B．防火墙　　C．攻击者　　D．受害主机

4 有一种称为嗅探器 D 的软件，它是通过捕获网络上传送的数据包来收集敏感数据，这些数据可能是用户的账号和密码，或者一些机密数据等等。

A．softice　　B．Unicode　　C．W32Dasm　　D．Sniffer

5 攻击者在攻击之前的首要任务就是要明确攻击目标，这个过程通常称 B 。

A．安全扫描　　B．目标探测

C．网络监听　　D．缓冲区溢出

6 从技术上说，网络容易受到攻击的原因主要是由于网络软件不完善和 A 本身存在安全缺陷造成的。

A．网络协议　　B．硬件设备

C．操作系统　　D．人为破坏

7 每当新的操作系统、服务器程序等软件发布之后，黑客就会利用 C 寻找软件漏洞，从而达到导致计算机泄密、被非法使用，甚至崩溃等目的。

A．IP 地址和端口扫描　　B．口令攻击

C．各种软件漏洞攻击程序　　D．服务型攻击

8 A 攻击是指借助于客户机/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DoS 攻击，从而成倍地提高拒绝服务攻击的威力。

A．分布式拒绝服务　　B．拒绝服务

C．缓冲区溢出攻击　　D．口令攻击

9 B 是一种破坏网络服务的技术，其根本目的是使受害主机或网络失去及时接收处理外界请求，或无法及时回应外界请求的能力。

A．包攻击　　B．拒绝服务

C．缓冲区溢出攻击　　D．口令攻击

二、填空题

1.分布式拒绝服务攻击的英文缩写是 DoS 。

2.窃听与分析网络中传输数据包的程序通常称为 嗅探器 。

3. 拒绝服务 攻击是一种既简单又有效的攻击方式，通过某些手段使得目标系统或者网络不能提供正常的服务。

4. ARP 欺骗攻击 就是针对 ARP 协议的一种攻击技术，可以造成内部网络的混乱，让某些被欺骗的计算机无法正常访问网络。

5. SQL 注入漏洞攻击 是一种比较常见、危害严重的网络攻击，它主要针对 Web 服务器端的特定数据库系统。

三、简答题

1. 什么是目标探测？目标探测的方法主要有哪些？

答：目标探测是通过自动或人工查询的方法，获得与目标网络相关的物理和逻辑参数。目标探测是防范不法黑客攻击行为的手段之一，同时也是黑客攻击的第一步。

目标探测的主要方法有：利用 Ping 命令方法，Whois 查询，VisualRoute 和 Traceroute 等工具的方法。

2. 从整个信息安全角度来看，目前扫描器主要由哪几种类型？

答：从信息安全角度来看，目前扫描器主要有 2 种类型，即端口扫描器和漏洞扫描器。

端口扫描器用于发现远程主机开放的端口，也就是发现那些服务在运行。漏洞扫描能够暴露网络上潜在的脆弱性，避免遭受不必要的攻击。

3. 如何有效防止端口扫描？

答：为了有效防止端口扫描，主要有如下两种方法：(1) 关闭闲置和有潜在危险的端口。（2）利用网络防火墙软件。

4. 网络监听的主要原理是什么？

答：目前流行的以太网协议工作方式为：将要发送的数据包发往连接在一起的所有主机，包中包含着应该接收数据包主机的正确地址，只有与数据包中目标地址一致的那台主机才能接收。但是，当主机工作在监听模式下，无论数据包中的目标地址是什么，主机都将接收(当然只能监听经过自己网络接口的那些包)。这样只要把计算机网卡的工作模式修改为混杂模式，就可以实现对局域网上的网络监听。

5. 如何检测网络监听？如何防范网络监听？

答：网络监听可以通过如下几种方法进行检测：

(1)反应时间。向怀疑有网络监听行为的网络发送大量垃圾数据包，根据各个主机回应的情况进行判断，正常的系统回应的时间应该没有太明显的变化，而处于混杂模式的系统由于对大量的垃圾信息照单全收，所以很有可能响应时间会发生较大的变化。

(2) 观测 DNS。许多的网络监听软件都会尝试进行地址反向解析，在怀疑有网络监听发生时，在 DNS 系统上观测有没有明显增多的解析请求。

(3) 利用 ping 模式进行监测。当一台主机进入混杂模式时，以太网的网卡会将所有不属于他的数据照单全收。按照这个思路，向网络中的一个伪造的硬件地址发送一个 Ping 数据包，任何正常的主机会检查这个数据包，比较数据包的硬件地址，和自己的不同，于是不理会这个数据包，而处于网络监听模式的主机，它不会去对比这个数据包的硬件地址，而是将这个数据包直接传到上层，上层检查数据包的 ip 地址，符合自己的 ip，于是会对这个 ping 包做出回应。

(4) 利用 arp 数据包进行监测。向局域网内的主机发送非广播方式的 arp 包，如果局域网内的某个主机响应了这个 arp 请求，那么我们就可以判断它很可能就是处于网络监听模式了，这是目前相对而言比较好的检测模式。

防范网络监听的方法主要有如下 2 种方法：

（1）采用加密手段进行信息传输，如果监听到的数据都是以密文形式传输的，那么对入侵者来说，即使抓取到了传输的数据信息，意义也是不大的。

(2) 使用交换机目前也是一个应用比较多的方式，不同于工作在第一层的 hub，交换机是工作在二层，也就是说数据链路层的。交换机转发的报文是一一对应的。对二层设备而言，仅有两种情况会发送广播报文，一是数据包的目的 MAC 地址不在交换机维护的数据库中，此时报文向所有端口转发，二是报文本身就是广播报文。由此，可以看到，这在很大程度上解决了网络监听的困扰。

6. 请举例说明缓冲区溢出攻击的原理是什么？

答：缓冲区(Buffer)是程序运行期间，在内存中分配的连续区域，用于保存各种数据类型。溢出是所填充的数据超出了原有缓冲区的边界，并非法占据了另一端内存区域。缓冲区溢出是指由于填充数据越界而导致程序原有流程的改变，黑客借此精心构造填充数据，让程序转而执行特殊的代码，最终获得系统的控制权。

通过往程序的缓冲区写超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其它指令，以达到攻击的目的。

缓冲区溢出原理举例如下：

```
void function(char*szParal)
{
    char buff[16];
    strcpy(buffer,szParal);
}
```

程序中利用 strcpy()函数将 szParal 中的内容拷贝到 buff 中，只要 szParal 的长度大于 16，就会造成缓冲区溢出。存在类似 strcpy()函数这样问题的 C 语言函数还有:strcat(),gets(),scanf()。

7. 如何防范缓冲区溢出攻击？

答：1) 编写正确的代码。在开发过程中，尽量使用带有边界检查的函数版本，或者自己进行越界检查。

2)及时安装漏洞补丁。缓冲区溢出是代码中固有的漏洞，除了在开发阶段注意编写正确的代码外，对于用户的一般防范措施就是关闭不必要的端口和服务，并及时安装厂商提供的补丁是解决缓冲区溢出问题最有效的方法。

3)借助于防火墙阻止缓冲区溢出。

8. 指出下述程序段存在的问题，请修改它。

```
char str[10];
char bigstr[20];
…
while(scanf("%20s", bigstr)!=NULL)
{
    bigstr[20]='\0';
    strcpy(str, bigstr);
    …
}
```

答：该程序中用到的函数 strcpy(str，bigstr)；是不安全的函数，当输入串的长度超过 20 的时候，会出现缓冲区溢出的错误。修改的方式就是用安全的函数 strncpy。即修改为：

```
char str[10];
char bigstr[20];
…
```

```
while(scanf("%20s", bigstr)!=NULL)
{
    bigstr[20]='\0';
    strncpy(str, bigstr, sizeof(str));
    …
}
```

9. 下面的程序是一个缓冲区溢出演示程序，请编译和执行一下，逐渐增加输入字符个数，分析程序执行结果。如何执行 hacker 函数？

```
#include <stdio.h>
#include <string.h>
void function(const char *input)
{
  char buffer[5];
  printf("my stack looks: \n%p \n%p \n%p \n%p \n%p \n%p \n%p \n%p \n%p \n\n");
  strcpy(buffer, input);
  printf("%s \n", buffer);
  printf("Now my stack looks like: \n%p \n%p \n%p \n%p \n%p \n%p \n%p \n%p \n%p
  \n\n");
}
void hacker(void)
{
  printf("Oh, I've been hacked! \n");
}
int main(int argc, char *argv[])
{
  printf("address of function=%p \n", function);
  printf("address of hacker=%p \n", hacker);
  function(argv[1]);
  return 0;
}
```

提示：

（1） 在 Visual C++环境中，由于 Debug 模式包含了对栈问题进行检测的操作，因此需要在 Release 模式下编译和运行。

（2） 根据屏幕显示结果找到 EBP 和 RET 的地址。

（3） 为了能使程序执行 hacker 函数，可编写一段名为 hacker.pl 的 pearl 脚本。

```
$arg="aaaaaaaaa…"."hacker 函数地址";
$cmd="该程序文件名", $arg;
system($cmd);
pearl hacker.pl
```

程序就可能会执行 hacker 函数(取决于所使用的编译器)。

答：略。

10． 什么是拒绝服务 DoS 攻击?什么是分布式拒绝服务攻击 DDoS?

答：拒绝服务攻击即攻击者想办法让目标机器停止提供服务，是黑客常用的攻击手段之一。分布式拒绝服务(DDoS:Distributed Denial of Service)攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DoS 攻击，从而成倍地提高拒绝服务攻击的威力。

11． 如何有效防范 DDoS 攻击？

答：1)及早发现系统存在的漏洞，及时安装系统补丁程序。对一些系统重要信息建立和完善备份机制。对一些特权账号的密码设置要谨慎。

2)经常检查系统的物理环境，禁止不必要的网络服务。建立边界安全界限，确保输出的包受到正确限制。经常检查系统配置信息，并注意查看每天的安全日志。

3)充分利用防火墙等网络安全设备，加固网络的安全性，配置好它们的安全规则，过滤掉所有可能伪造的数据包。

12． 什么是欺骗攻击？简述欺骗攻击的原理。

IP 欺骗主要是针对 Unix 操作系统的，在 Windows 操作系统中有没有 IP 欺骗的问题？

答：欺骗攻击是利用 TCP/IP 协议等本身的漏洞而进行的攻击行为。这些攻击包括 IP 欺骗、DNS 欺骗、ARP 欺骗等等。

IP 欺骗通过利用主机之间的正常信任关系来发动。既然 A 和 B 之间的信任关系是基于 IP 地址的，如果能够冒充 B 的 IP，那么就可以使用 rlogin 登录到 A，而不需要任何口令验证。

ARP 欺骗攻击就是通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗。

习题 6

一、选择题

1 关于防火墙，以下哪种说法是错误的？(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

2 防火墙是确保网络安全的重要设备之一，如下各项中可以由防火墙解决的一项网络安全问题是(A)

A. 从外部网伪装为内部网　　B. 从内部网络发起的攻击

C. 向内部网用户发送病毒携带文件　D. 内部网上某台计算机的病毒问题

3 包过滤防火墙工作在 OSI 的哪一层？(C)。

A. 物理层　　B. 传输层　　C. 网络层和传输层　　D. 应用层

4 防火墙对数据包进行状态检测时，不可以进行检测过滤的是(D)。

A. 源地址和目的地址　　B. 源端口和目的端口

C. IP 协议号　　D. 数据包中的内容

5.关于防火墙的描述中，正确的是__A__。

A. 常用的访问控制设备之一　　B. 仅在网络层实现访问控制

C. 只能通过硬件设备来实现　　D. 通过加密来实现访问控制

6. 关于网络地址转换的描述中，错误的是__C__。

A. 最初用于缓解 IP 地址短缺　　B. 分为静态 NAT 和动态 NAT

C. 防火墙的最基本实现方式　　D. 可隐藏内部网络中的主机

二、填空题

1 常见防火墙按采用的技术分类主要有 包过滤防火墙 、 状态检测防火墙 和 应用代理防火墙 。

2 双宿主主机结构 是防火墙体系的基本形态。

3 应用层网关型防火墙的核心技术是 代理服务器技术 。

4. 在 NAT 设备中，如果 IP 分组需要进入内部网络，其中的目的地址将从全局地址转换为 内部地址 。

5.在代理型防火墙技术的发展过程中，经历了两个不同版本：第一代应用层网关代理型防火墙和 电路层网关防火墙 。

三、简答题

1. 什么是防火墙？古代防火墙与网络安全中的防火墙有何联系和区别？

答：防火墙是一个位于内部网络与 Internet 之间的网络安全系统，是按照一定的安全策略建立起来的硬件和(或)软件的有机组成体，以防止黑客的攻击，保护内部网络的安全运行。

古代防火墙是人们在寓所之间砌起的砖墙，一旦火灾发生，它能够防止火势蔓延到别的寓所。网络防火墙是在该网络和 Internet 之间插入一个中介系统，竖起一道安全屏障。这道屏障的作用是阻断来自外部通过网络对本网络的威胁和入侵，提供扼守本网络的安全和审计的唯一关卡，它的作用与古时候的防火砖墙有类似之处。

2. 分析防火墙的局限性?

答：防火墙系统有如下的局限性：

1) 传统的防火墙在工作时，入侵者可以伪造数据绕过防火墙或者找到防火墙中可能开启的后门；

2) 防火墙不能防止来自网络内部的袭击。通过调查发现，有将近一半以上的攻击都来自网络内部，对于那些将要泄漏企业机密的员工来说，防火墙形同虚设；

3) 由于防火墙性能上的限制，通常它不具备实时监控入侵的能力；

4) 防火墙不能防御所有新的威胁。防火墙仅仅是一种被动的防护手段，只能用来防备已知的威胁，无法检测和防御最新的拒绝服务攻击(DoS)及蠕虫病毒的攻击。

3. 包过滤防火墙的工作机制和包过滤类型。

答：包过滤型防火墙工作在 OSI 网络参考模型的网络层和传输层，它根据数据包头源地址，目的地址、端口号和协议类型等标志确定是否允许通过。只有满足过滤条件的数据包才被转发到相应的目的地，其余数据包则被从数据流中丢弃。

包过滤类型主要包括 2 种，即第一代静态包过滤防火墙和第二代动态包过滤性防火墙。

4. 简述包过滤防火墙的工作过程及特点。

答：包过滤防火墙根据定义好的过滤规则审查每个数据包，以便确定其是否与某一条包过滤规则匹配。过滤规则基于数据包的报头信息进行制订。包头信息中包括 IP 源地址、IP 目标地址、传输协议(TCP、UDP、ICMP 等等)、TCP/UDP 目标端口、ICMP 消息类型等。

包过滤方式是一种通用、廉价和有效的安全手段。之所以通用，是因为它不是针对各个具体的网络服务采取特殊的处理方式，适用于所有网络服务；之所以廉价，是因为大多数路由器都提供数据包过滤功能，所以这类防火墙多数是由路由器集成的；之所以有效，是因为它能满足绝大多数安全要求。

5. 试述代理防火墙的工作原理及特点。

答：应用代理型防火墙是工作在 OSI 的最高层，即应用层。它完全“阻隔”了网络通信流，通过对每种应用服务编制专门的代理程序，实现监视和控制应用层通信流的作用。

代理型防火墙的特点主要体现在如下二点：1）安全性高，由于它工作于最高层，所以它可以对网络中任何一层数据通信进行筛选保护，而不是像包过滤那样，只是对网络层的数据进行过滤。另外代理型防火墙采取是一种代理机制，它可以为每一种应用服务建立一个专门的代理，所以内外部网络之间的通信不是直接的，而都需先经过代理服务器审核，通过后再由代理服务器代为连接，根本没有给内、外部网络计算机任何直接会话的机会，从而避免了入侵者使用数据驱动类型的攻击方式入侵内部网。

2）代理防火墙的最大缺点就是速度相对比较慢，当用户对内外部网络网关的吞吐量要求比较高时，代理防火墙就会成为内外部网络之间的瓶颈。

6. 常见的防火墙系统有哪几种？比较他们的优缺点。

答：常见的防火墙系统很多，比如天网防火墙，McAfee Internet security, ZoneAlarm Extreme Secutiry 等，具体优缺点略。

7. 屏蔽子网的防火墙系统是如何实现的?

答：屏蔽子网结构也称为屏蔽子网网关结构，就是在屏蔽主机结构中的内部网和外部网之间再增加一个被隔离的子网，这个子网由堡垒主机、应用级网关等公用服务器组成，习惯上将这个子网称为“非军事区”DMZ(DeMilitarised Zone)。用边界网络来隔离堡垒主机与内部网，就能减轻入侵者在攻破堡垒主机后带给内部网的压力。入侵者即使攻破堡垒主机也不可能对内部网进行任意操作，而只可能进行部分操作。

在最简单的屏蔽子网结构中，有二台都与边界网络相连的过滤路由器，一台位于边界网络与内部网络之间，而另一台位于边界网络与外部网之间，在这种结构下，入侵者要攻击到内部网必须通过二台路由器的安全控制，即使入侵者通过了堡垒主机，他还必须通过内部路由器才能抵达内部网，这样，整个网络安全机制就不会因一点攻破而全部瘫痪。

8. 双宿主堡垒主机与单宿主堡垒主机的区别是什么?

答：堡垒主机是网络中最容易受到侵害的主机,所以堡垒主机也必须是自身保护最完善的主机。一个堡垒主机使用两块网卡，每个网卡连接不同的网络。一块网卡连接公司的内部网络用来管理、控制和保护，而另一块连接另一个网络，通常是公网也就是 Internet。通过这种隔离措施，提高局域网的安全性。

但宿主堡垒主机通常只有一块网卡，由内外部网络共享，因此成为整个网络的一个弱点。

9. 状态检测防火墙的技术特点是什么？

答：状态检测防火墙的技术特点主要体现在如下几个方面：1） 安全性好。状态检测防火墙工作在数据链路层和网络层之间，它从这里截取数据包，因为数据链路层是网卡工作的真正位置,网络层是协议栈的第一层,这样防火墙确保了截取和检查所有通过网络的原始数据包。

2） 性能高效。状态检测防火墙工作在协议栈的较低层，通过防火墙的所有的数据包都在低层处理，而不需要协议栈的上层处理任何数据包，这样减少了高层协议头的开销，执行效率提高很多。

3）扩展性好。状态检测防火墙不区分每个具体的应用，只是根据从数据包中提取出的信息、对应的安全策略及过滤规则处理数据包，当有一个新的应用时，它能动态产生新的应用的新的规则，而不用另外写代码，所以具有很好的伸缩性和扩展性。

4）配置方便,应用范围广。状态检测防火墙不仅支持基于 TCP 的应用，而且支持基于无连接协议的应用，如 RPC、基于 UDP 的应用(DNS 、WAIS、 Archie 等)等。

习题 7

一、选择题

1 下列哪种功能是入侵检测实现的(　D　　)。

A. 过滤非法地址　　B. 流量统计

C. 屏蔽网络内部主机　　D. 检测和监视已成功的安全突破

2 有一种攻击是不断对网络服务系统进行干预，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(　　C　)。

A. 重放攻击　　B. 反射攻击　　C. 拒绝服务攻击　　D. 服务攻击

3 入侵检测系统的第一步是：(　B　)

A．信号分析　　B．信息收集　　C．数据包过滤　　D．数据包检查

4 以下哪一项不属于入侵检测系统的功能：(　D　)

A．监视网络上的通信数据流　　B．捕捉可疑的网络活动

C．提供安全审计报告　　D．过滤非法的数据包

5.基于网络的 IDS 中，检测数据通常来源于　B　。

A．操作系统日志　　B．网络监听数据　　C．系统调用信息　　D．安全审计数据

二、填空题

1 根据信息的来源将入侵检测系统分为基于 主机 的 IDS、基于 网络 的 IDS 和 分布式 的 IDS。

2. 由被入侵的众多主机构成、可被攻击者远程控制的逻辑网络称为_____。

3. 入侵检测技术根据检测方法可分为 基于异常的入侵检测 和 基于误用的入侵检测 两大类。

4. 入侵防护系统根据部署方式可以分为 3 类：基于网络的入侵防护系统、 基于主机的入侵检测系统 和 分布式入侵检测系统 。

三、简答题

1． 什么是入侵检测系统？

答： 入侵检测系统是是对入侵行为发现和响应的系统。它通过对计算机网络或计算机系统中的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象，进行入侵检测的软件与硬件的组合便是入侵检测系统。

2． 简述入侵检测系统目前面临的挑战。

答：入侵检测系统面临的挑战：1）漏报和误报的矛盾。一个有效的入侵检测系统应限制误报出现的次数，但同时又能有效截击。误报是入侵检测系统最头疼的问题，攻击者可以而且往往是利用包的结构伪造无威胁的正常假警报，而诱导没有警觉性的管理员把入侵检测系统关掉。没有一个入侵检测能无敌于误报，因为没有一个应用系统不会发生错误，原因主要有四个：缺乏共享数据机制、缺乏集中协调机制、缺乏揣摩数据在一段时间内变化的能力、缺乏有效的跟踪分析。

3. 为什么要进行入侵检测？

答：由于性能的限制，防火墙通常不能提供实时的入侵检测能力，对于企业内部人员所做的攻击，防火墙形同虚设。

入侵检测是对防火墙极其有益的补充，入侵检测系统能使在入侵攻击对系统发生危害前，检测到入侵攻击，并利用报警与防护系统驱逐入侵攻击。在入侵攻击过程中，能减少入侵攻击所造成的损失。在被入侵攻击后，收集入侵攻击的相关信息，作为防范系统的知识，添加入知识库内，增强系统的防范能力，避免系统再次受到入侵。入侵检测被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监听，从而提供对内部攻击、外部攻击和误操作的实时保护,大大提高了网络的安全性。

4. 简述主机入侵检测系统的工作原理。

答：主机入侵检测系统通常在被重点检测的主机上运行一个代理程序。该代理程序扮演着检测引擎的角色，它根据主机行为特征库对受检测主机上的可疑行为进行采集、分析和判断，并把警报信息发送给控制端程序，由管理员集中管理。此外，代理程序需要定期给控制端发出信号，以使管理员能确信代理程序工作正常。如果是个人主机入侵检测，代理程序和控制端管理程序可以合并在一起，管理程序也简单得多。

5. 简述网络入侵检测系统的工作原理

答： NIDS 在混杂模式下监视网段中传输的各种数据包，并对这些数据包的内容、源地址、目的地址等进行分析和检测。如果发现入侵行为或者可疑事件，入侵检测系统就会发出警报，甚至切断网络连接。它通常安装在网络上比较重要的网段，也可以说容易出问题的地方，利用网络侦听技术，通过对网络上的数据流进行捕捉、分析，以判断是否存在入侵。它以网络上传输的信息包为主要研究对象，保护网络的运行。

6. 简述误用检测的技术实现。

答：收集非正常操作的行为特征，建立相关的特征库，也就是所谓的专家知识库。通过监测用户的或系统行为，将收集到的数据与预先确定的特征知识库里的各种攻击模式进行比较，如果能够匹配，则判断有攻击，系统就认为该行为是入侵。误用入侵检测技术有时也称为规则入侵检测技术。顾名思义，是进行规则库的匹配。

误用检测能迅速发现已知的攻击，并指出攻击的类型，便于采取应对措施；同时用户可以根据自身情况选择所要监控的事件类型和数量；并且误用检测没有浮点运算，效率较高。但其缺点也是显而易见的：由于依赖误用模式库，它只能检测数据库中已有的攻击，对未知的攻击无能为力，这便要求不断地升级数据库，加入新攻击的特征码；随着数据库的不断扩大，检测所要耗费的存储和计算资源也会越来越大；由于没有通用的模式定义语言，数据库的扩展很困难，增加自己的模式往往很复杂；并且将对攻击的自然语言描述转换成模式是比较困难的，如果模式不能被正确定义，将无法检测到入侵。

误用检测中常用的方法有：简单的模式匹配、专家系统和状态转移法。

7. 简述异常检测的技术实现。

答：这种方法主要是建立计算机系统中正常行为的模式库，然后根据收集到的信息数据，通过某种方法，看是否存在重大偏差，如果偏差在规定范围之外，则认为发生了入侵行为，否则视为正常。

异常检测的一个很大的优点是不需要保存各种攻击特征的数据库，随着统计数据的增加，检测的准确性会越来越高，可能还会检测到一些未知的攻击。但由于用户的行为有很大的不确定性，很难对其行为确定出正常范围，因此门限值的确定也比较困难，出错的概率比较大。同时，它只能说明系统发生了异常的情况，并不能指出系统遭受了什么样的攻击，这给系统管理员采取应对措施带来了一定困难。

异常检测中常用的方法有：量化分析、统计分析和神经网络。

7. 请简要说明入侵检测系统和入侵防护系统的差别。

答：IPS 是位于防火墙和网络的设备之间的设备。这样，如果检测到攻击，IPS 会在这种攻击扩散到网络的其它地方之前阻止这个恶意的通信。而 IDS 只是存在于你的网络之外起到报警的作用，而不是在你的网络前面起到防御的作用。

IPS 检测攻击的方法也与 IDS 不同。一般来说，IPS 系统都依靠对数据包的检测。IPS 将检查入网的数据包，确定这种数据包的真正用途，然后决定是否允许这种数据包进入你的网络。

习题 8

一、选择题：

1.（ B ）是 Windows 2000(NT/2003)最基本的入侵检测方法，是一个维护系统安全性的工具。

A. 应用日志　　B. 事件查看器

C. 开启审核策略　　D. 入侵检测系统

2．Windows Server 2003 系统的安全日志通过（ A ）设置。

A. 事件查看器　　B. 服务管理器

C. 网络适配器　　D. 本地安全策略

3．用户匿名登录主机时，用户名为（ A ）。

A. guest　　B. anonymous

C. administrator　　D. admin

4．（ C ）不是 Windows 的系统进程。

A. System Idle Process　　B. winlogon.exe

C. explorer.exe　　D. svchost.exe

5．Windows 使用 Ctrl+Alt+Del 启动登录信息，是激活了下列哪个进程？（ D ）

A. System Idle Process　　B. winlogon.exe

C. explorer.exe　　D. taskmgr.exe

6．Windows Server 2003 中删除硬盘 D 的默认共享命令是：（ C ）

A. net share d$：　　B. del net share d$：

C. net share d$ /del　　D. net share /del d$

二、填空题

1. Unix/Linux 系统结构由 用户层 、 内核层 和 硬件层 三个层次组成。

2.在 windows 7 中， 内存保护模块使用的安全技术主要有： 地址空间随机化分布 、安全结构化异常处理 、数据执行防护（Data Execution Protection，DEP）、安全堆管理和 GS 栈保护等。

3. Windows 7 有三种类型的账户，即来宾账户、标准账户和 管理员账户 。

4. Linux 是一个类 Unix 操作系统。

三、简答题

1．什么是安全的操作系统？

答：安全操作系统是指计算机信息系统在自主访问控制、强制访问控制、标记、身份鉴别、客体重用、审计、数据完整性、隐蔽信道分析、可信路径、可信恢复等十个方面满足相应的安全技术要求。 安全操作系统主要特征：1）最小特权原则，即每个特权用户只拥有能进行他工作的权力；2）自主访问控制；强制访问控制，包括保密性访问控制和完整性访问控制；3）安全审计； 4）安全域隔离。

2. Unix 主要有哪些安全机制？

答：在 Unix/Linux 基本系统中，提供的安全机制包括用户账号标识、口令安全、文件系统安全、文件加密和日志审计机制等。

3．Windows 7 系统有哪些安全机制？

答：Windows7 主要采用内核完整性、内存保护、系统完整性及用户空间防护等安全机制对系统进行保护。内存保护机制使得攻击代码在目标计算机上很难得到执行，用户空间的

权限控制机制让攻击代码即使执行了，也只能处于比较低的权限级别，无法对目标计算机进行深入控制，加上内核的完整性验证机制，攻击代码更难以在目标计算机上长期存在。

4．什么是 Windows 安全设置模板？

答：安全模板是一种 ASCII 文本文件，它定义了本地权限、安全配置、本地组成员、服务、文件和目录授权、注册表授权等方面的信息。创建好安全模板之后，我们只要一个命令就可以将它定义的信息应用/部署到系统，所有它定义的安全配置都立即生效——原本需要数小时修补注册表、倒腾管理控制台“计算机管理”单元以及其他管理工具才能完成的工作，现在只需数秒就可以搞定。

5. Unix/Linux 安全设置时要注意哪些事项？

答：1）合理设置系统的安全级别；2）合理设置用户权限 3）指定主控台及终端登录的限制；4）合理配置/etc/inetd.conf 文件 ；5）合理设置/etc/ftpusers 文件；6）合理设置网段及路由；7）不设置 UUCP；8）删除不用的软件包及协议；9）正确配置.profile 文件；10）创建匿名 ftp；11）应用用户同维护用户分开

6．如何关闭 Windows 中不必要的端口和服务？

答：关闭 windows 端口通常有 2 种方法，一种就是利用防火墙软件来过滤某些端口的关闭与否；另外一种就是通过网络属性中进行端口关闭设置。

具体设置方法请参考网址 http://www.jb51.net/os/windows/94203.html。

7．Windows 中的安全账号管理器的主要作用是什么？

答：安全帐户管理器 (SAM) 是运行 Windows Server 2003 的服务器上的一个数据库，用于存储本地计算机上用户的用户帐户和安全描述符。

习题 9

一、选择题

1. 常用的数据备份方式包括完全备份、增量备份、差分备份。这三种方式在数据恢复速度方面由快到慢的顺序是（ B ）

A.完全备份、增量备份、差分备份　B. 完全备份、差分备份、增量备份

C. 增量备份、差分备份、完全备份 D. 差分备份、增量备份、完全备份

2.（ C ）使用多台服务器组成服务器集合，可以提供相当高性能的不停机服务。在这个结构中，每台服务器都分担着一部分计算任务，由于集合了多台服务器的性能，整体的计算实力被增加了。

A.双机容错　B. 系统备份 C. 集群技术　D. 克隆技术

3.磁带备份是当前一种常用的备份介质。在下述磁带轮换策略中，（ C ）不是常用的磁带轮换策略。

A. 三带轮换策略　B. 六带轮换策略 C. 九带轮换策略　D. 祖-父-子轮换策略

4.下述的软件中，（ C ）不是数据备份与恢复软件。

A. EasyRecovery　B. File Genie　C. OfficePasswordRemover　D. Second Copy

5.下列关于数据库备份，错误的是（ C ）。

A. 数据库备份介质一定要具有统一通用性

B. 制定完整的备份和恢复计划

C. 用人工操作进行简单的数据备份来代替专业备份工具的完整解决方案

D. 平时备份的时候一定要做好异地备份。

二、填空题

1. 热备份是计算机容错技术的一个概念，是实现计算机系统高可用性的主要方式，避免因单点故障（如磁盘损伤）导致整个计算机系统无法运行，从而实现计算机系统的高可用性。最典型的实现方式是 双机备份 。

2. 目前最常见的网络数据备份系统按其架构不同可以分为四种：基于网络附加存储结构，Lan-based ， Lan-free 和 Server-Free 结构。

3. 数据恢复 是数据备份的逆过程，就是利用保存的备份数据还原出原始数据的过程。

4.第一次对数据库进行的备份一定是 完全备份 。

5. 硬盘的分区类型有 主分区 、扩展分区，在扩展分区基础上，可以建立 逻辑 分区

三、简答题

１．什么是数据备份，数据备份的主要原因是什么？

答：数据备份是容灾的基础，是指为防止系统出现操作失误或系统故障导致数据丢失，而将全部或部分数据集合从应用主机的硬盘或阵列复制到其它的存储介质的过程。

数据备份的原因主要体现在如下两个方面：

1) 在数据遭到意外事件破坏时，通过数据恢复还原数据。可以说，做好数据备份是防止数据丢失，防止系统遭受破坏最有效、最简单的手段。

2)数据备份是历史数据存档的最佳方式。数据备份为用户进行历史数据查询、统计和分析，以及重要信息归档保存提供了可能。

２．什么是系统数据备份？

答：系统数据备份主要是针对计算机系统中的操作系统、设备驱动程序、系统应用软件及常用软件工具等的备份。

3．系统还原卡的基本原理是什么？请仔细观察一下你周围的环境，还有哪里用到了还原卡？

答：还原卡的基本原理是在系统启动时，首先由系统还原卡接管 BIOS 的 INT13 中断，将 FAT、引导区、CMOS 信息、中断向量表等信息都保存到卡内的临时存储单元中，用自带的中断向量表来代替原始的中断向量表；再将 FAT 等信息保存到临时存储单元中作为第二个备份，用来应付系统运行时对硬盘数据所作的修改；最后在硬盘上辟出一部分连续空间，将当前系统操作的数据保存在这部分空间中。

当用户向硬盘写入数据时，数据并没有真正修改到硬盘中的 FAT 表。由于保护卡接管了 INT13，当发现写操作时，便将原先的数据目的地址重新指向预先准备的连续磁盘空间，并将已备份的第二个 FAT 中被修改的相关数据指向这片空间。当要读取数据时，还原卡首先在第二个备份的 FAT 中查找相关文件。如果是在启动后修改过的，便在重新定向的空间中读取，否则就在第一个备份的 FAT 中查找，并读取相关文件。删除时就是将文件的 FAT 记录从第二个备份的 FAT 中删除。

在我们的周围环境中，网吧、学校的机房、公共的机房等环境中大多都采用了系统还原卡。

4．什么是用户数据备份？Second Copy 主要有哪些功能？

答：用户数据备份是针对具体应用程序和用户产生的数据，将用户的重要数据与操作系统数据分别进行存储备份。

Second Copy 主要有如下功能：定时备份、同时对多个文件对象执行备份、可自定义备份文件类型，支持复制、移动、压缩、同步等多种备份功能。

5．网络数据备份主要有哪些方法？

答：网络数据备份是一套比较成熟的备份方案，其基本设计思想是利用一台服务器连接合适的备份设备，实现对整个网络系统各主机上关键业务数据的自动备份管理。网络数据备份系统按其架构不同可以分为四种方式：基于网络附加存储(DAS-Based)结构，基于局域网(LAN-Based)结构，基于 SAN 结构的 LAN-Free 和 Server-Free 结构。

6．解释 DAS-based、LAN-based、LAN-free 和 Server-free 四种网络数据备份方法的异同点。

答：略

7．数据恢复之前应该注意哪些问题？

答：数据出现问题时，应该注意如下问题：1）立即中止设备原来的使用方法；2）如遇硬件异常，请不要随意加电；3)准备一台恢复用机，去掉其自动写盘的途径；4) 连至恢复用机，阵列盘请勿通过 RAID 控制器；5)如果可能，请对待恢复设备做镜像备份；6)尝试使用可靠的数据恢复软件进行恢复；7) 向专业数据恢复公司寻求帮助。

8．硬盘数据恢复的基本原理是什么？

答：当向硬盘里存放文件时，系统首先会在文件分配表内写上文件名称、大小，并根据数据区的空闲情况在文件分配表上继续写上文件内容在数据区的起始位置。然后开始向数据区写上文件的实际数据，一个文件存放操作才算完毕。

当删除一个文件时，系统只是在文件分配表内，在该文件前面作一个删除标志，表示该文件已被删除，它所占用的空间已被“释放”，其他文件可以使用它占用的空间。所以，当我们删除文件又想找回它(数据恢复)时，只需用工具将删除标志去掉，数据被恢复回来了。

格式化操作和删除相似，都只操作文件分配表，不过格式化是将所有文件都加上删除标志，或干脆将文件分配表清空，系统将认为硬盘分区上不存在任何内容。格式化操作并没有对数据区做任何操作，目录空了，内容还在，借助数据恢复知识和相应工具，数据仍然能够被恢复回来。

9．EasyRecovery 有哪些功能？

答：EasyRecovery 的主要功能如下。

(1)修复主引导扇区(MBR)。

(2)修复 BIOS 参数块(BPB)。

(3)修复分区表。

(4)修复文件分配表(FAT)或主文件表(MFT)。

(5)修复根目录。

(6)恢复丢失的 Microsoft Office 文档。

(7)恢复 WinZip 文件。

(8)修复可移动存储器中的数据。

(9)可以根据制定要求进行高级搜索，并支持超过 90 多种的文件类型。

(10)可以生成恢复报告，以查看恢复的具体情况。

(11)EasyRecovery 还可以在如下 4 种情况下恢复硬盘中的数据。分区或格式化后硬盘中的数据；误删除的数据；断电或非法关机造成的数据丢失；由程序误操作或系统故障造成的数据丢失。

习题 10

1、 为什么要对软件进行保护？在你的周围，最常见的软件保护方法是什么？

答：软件保护技术是软件开发者为了维护软件的知识产权和经济利益，不断寻找各种有效方法和技术来维护软件版权，增加其盗版的难度，或延长软件破解的时间，尽可能防止软件被非法使用，所采用的保护方法。

在我们的周围，软件保护的方法很多，例如采用加密狗的方法，在线软件保护的方法，序列号保护的方法，等等。

2、 常用的软件保护技术有哪些？在这些软件保护技术中，你认为哪种方式最有效？

答：常用的软件保护技术有：序列号保护机制，警告窗口方式；功能限制的方法；试用时间限制；注册文件等方式。

通常有效的保护方式应该是综合多种软件保护技术进行保护，对单一某一种保护技术来说，注册文件保护方式会适当提高破解的难度。

3、 为什么在对软件进行分析时有些软件壳是 overlay 的，但却不用处理这些数据？

答：略。

4、 一个加过壳的软件在经过脱壳之后，是否还会和原文件保持一样？请说明理由。

答：不一样，通常软件在脱壳以后，文件的大小会增加，因为壳的一个重要作用就是压缩，脱壳以后自然就会将数据恢复大原来大小。

5、 在使用注册机算出软件注册码并成功注册后，软件正常使用了一段时间，突然提示用户“该软件已经注册过期，需要重新注册”，为什么会出现这样的情况？

答：有可能该软件的保护方式综合采用了几种保护的方法。

6、 目前，网络上有很多软件都不可以长期免费使用，怎样才能够下载可以免费试用的软件，且能够无限期的免费使用它们？

答：略。

习题 11

一、选择题

1. IPSec 是（　　C　）VPN 协议标准。

A. 第 2.5 层　B.第二层　C. 第三层　D.第四层

2. (　A　)是 IPSec 规定的一种用来自动管理 SA 的协议，包括建立、协商、修改和删除 SA 等。

A. IKE　B. AH　C. ESP　D. SSL

3. 如下关于 VPN 的论述中错误的一项是（ D　）。

A. VPN 的实现需要借助 SSL

B. VPN 可以实现远程站点身份认证

C. VPN 只支持 TCP/IP

D. VPN 是指用户自己租用线路和公共网络物理上完全隔离的、安全的线路

4. VPN 不能提供如下（　A　）功能：

A. 数据有序到达目的主机　B.数据加密

C. 信息认证和身份认证　D.访问权限控制

5.以下关于虚拟专用网的叙述中，不正确的是（ A ）。

A. VPN 是指建立在私有网络上的、由某一组织或某一群用户专用的通信网络

B.VPN 的虚拟性表现在任意一对 VPN 用户之间没有专用的物理连接，而是通过 ISP 提供的公用网络来实现通信

C. VPN 的专用型表现在 VPN 之外的用户无法访问 VPN 内部资源

D.隧道技术是实现 VPN 的关键技术之一

二、填空题

1. IETF 对基于 IP 的 VPN 定义：使用　IP 机制　仿真出一个私有的广域网。

2. VPN 系统中的认证技术包括　用户身份认证　和　信息认证　两种类型。

3. IPSec 在　隧道　模式下把数据封装在一个 IP 包传输以隐藏路由信息。

4. 在第三层隧道协议中，有两种常用的实现方式，即 GRE 和　IPSec　。

5. VPN 业务按用户需求定义，根据 VPN 服务类型进行分类，可以分为如下三种： Intranet VPN、 Access VPN 和　Extranet VPN　。

三、简答题

1． 什么是 VPN？VPN 的系统特性有哪些？

2． IPSec 包括哪几种基本协议，它们之间有什么关系？

3． AH 包括哪几种工作模式，它们的数据包格式分别是什么样的？

4． ESP 包括哪几种工作模式，它们的数据包格式分别是什么样的？

5． IKE 的作用是什么？
6． SA 的作用是什么？
7． L2TP 协议的优点是什么？
8. SSL 工作在哪一层？简单比较 SSL VPN 和 IPSec VPN

习题 12

一、选择题

1．SSL 协议的 Sever_Hello 使用随机数的目的是_____B_____。
A. 做为加密密钥　　B. 用于密钥交换中的抗重放攻击
C. 做为客户端的 ID　D. 可以省略，没用

2. SET 协议中的数字信封对要传送的消息密钥是通过下面___A___产生的。
A. 接收方的公钥　　B. 接收方随机产生　　C. 发送方随机产生　　D. 事先通过协商

3.SSL 协议使用的加密算法是（ D ）
A.仅使用对称加密算法　　B. 仅使用公钥加密算法
C. 同时使用 DES 加密算法和散列密码　D.同时使用对称加密算法和公钥加密算法

4. 认证中心的核心职责是（ A ）
A.签发和管理数字证书　B. 验证信息　C. 公布黑名单　D.撤销用户的证书

5. 下面有关 SSL 的描述，不正确的是（D ）
A. 目前大部分 Web 浏览器都内置了 SSL 协议
B. SSL 协议分为 SSL 握手协议和 SSL 记录协议两部分
C. SSL 协议中的数据压缩功能是可选的
D. SET 协议在功能和结构上与 SSL 完全相同

二、　填空题

1．SSL 是一种综合利用___对称密钥___和___非对称密钥_技术进行安全通信的工业标准。
2．SET 协议的参与方主要由持卡人、商家、_支付网关__、_证书授权机构_ 、发卡行和收单行等六个部分组成。
3. SSL 协议由 SSL 记录协议、_握手协议_ 、_加密规范_和报警协议组成。
4.SET 协议主要通过使用_公钥密码算法_和_X.509 数字证书_的方式解决电子商务交易过程中的安全性问题。

三、　简答题

1. 电子商务有哪些优点？
2. 电子商务的安全需求有哪些？
3. SSL 记录协议的工作步骤有哪些？
4. 以图形化的方式画出 SSL 协议的握手过程。
5. SET 提供了哪些安全服务？
6. 列举 SET 协议中的各个参与方。
7. 数字信封的作用是什么？
8. 双重签名的定义和目的是什么？
9. 在 SSL 中为什么有单独的修改密码规范协议，而不是在握手协议中包含修改密码规范？
10. 分析 SSL 协议，并说明 SSL 如何抵抗下列 Web 安全性威胁：
(1)穷举密码分析攻击：穷举传统加密算法的密钥空间。

(2)重放攻击：重放先前的 SSL 握手消息。
(3)中间人攻击：在密钥交换时，攻击者向服务器假扮客户端，向客户端假扮服务器。

习题 13

一、　选择题

1. 在 TCSEC 中，美国国防部按处理信息的等级和应采用的响应措施，将计算机信息安全从低到高分为（ C ）。

A. A、C1、C2、B1、B2、B3、D　B. D、B1、B2、C1、C2、C3、A

C. D、C1、C2、B1、B2、B3、A　D. A、B1、B2、C1、C2、C3、D

2. Unix、Linux、Windows 在 TCSEC 中属于哪个安全级别的操作系统 C 。

A．A　B. D　C. C2　D. B1

3. 端口扫描主要检测端口开放性问题，SQL Server、IIS 和 FTP 的默认端口号分别是 D 。

A．1433 端口、80 端口和 23 端口　B.1414 端口、8080 端口、21 端口

C. 1434 端口、80 端口、21 端口　D.1433 端口、80 端口、21 端口

4. 我们通常所说的 CC 是指以下哪一个标准 D 。

A．TCSEC　B.SSE-CMM　C.ISO17799　D. ISO15408

5. 信息安全风险管理应该 C 。

A．将所有的信息安全风险都消除　B.在风险评估之前实施

C.基于可接受的成本采取相应的方法和措施　D. 以上说法都不对

二、填空题

1. TCSEC 可以从安全策略模型、可追究性、 保证 和 文档 4 个方面进行描述。

2. 通用评估方法 CC 中目前不包括 EAL4 级以上的评估方法。

3. CC 作为通用的评估准则，本身并不涉及具体的评估方法，信息技术的评估方法论主要由 通用评估方法（CEM） 给出。

三、简答题

1.简述网络安全检测与评估对保障计算机网络信息系统安全的作用。

略。

2.简述 CC 评估标准的 7 个评估保证级的评估要求。

略。

3.简述 CEM 评估模型的评估流程。

略。