第 8 章：信息安全知识　　作者：希赛教育软考学院　来源：希赛网　2014年05月05日

考点脉络

根据考试大纲，本章要求考生掌握以下几个方面的知识点。

（1）信息系统安全基础知识

（2）信息系统安全管理

（3）保障完整性与可用性的措施

（4）加密与解密机制基础知识

（5）风险管理（风险分析、风险类型、抗风险措施和内部控制）

（6）计算机安全相关的法律、法规基础知识

从历年的考试情况来看，本章的考点主要集中于加密解密技术、网络安全、计算机病毒等方面。

上一节　本书简介　下一节

第 8 章：信息安全知识　　作者：希赛教育软考学院　来源：希赛网　2014年05月05日

安全基础技术

在软件设计师的考试中，经常会考到与安全相关的一些基础概念及技术原理，如：区分对称与非对称算法，什么情况下用哪种密钥加密解密、信息摘要的用途等。下面将详细介绍这些相关技术。

上一节　本书简介　下一节

第 8 章：信息安全知识　　作者：希赛教育软考学院　来源：希赛网　2014年05月05日

考点精讲

1. 对称加密

对称加密是指加密系统的加密密钥和解密密钥相同，或者虽然不同，但从其中的任意一个可以很容易地推导出另一个。

对称加密算法的优点是：使用简单、加密解密快捷高效，其致命弱点是：加密强度不高、密钥分发困难。

常见对称密钥加密算法包括：DES、3DES、RC-5、IDEA。

2. 非对称加密

前面提到了对称加密技术中的“对称”意思是加密与解密使用了同样的密钥。顾名思义，非对称加密技术中所使用的加密与解密密钥是不同的。并且不可能从任何一个推导出另一个。它的优点在于可以适应开放性的使用环境，可以实现数字签名与验证。最常见的非对称密钥技术就是RSA。它的理论基础是数论中大素数分解，但如果使用RSA来加密大量的数据则速度太慢了，因此RSA广泛用于密钥的分发。

在非对称加密体系中，密钥是成对出现的，一对密钥包括一个公钥和一个私钥。如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。

非对称加密算法的优点在于：解决了对称密钥加密强度不高及密钥分发困难的问题，其缺点是：加密速度极慢。所以非对称加密算法通常只对极小的数据量进行加密，如对信息摘要进行加密，或用于加密对称密钥。

常见非对称密钥加密算法：RSA、ECC。

3. Hash函数和信息摘要

Hash函数又称为杂凑函数、散列函数，它提供了这样的一种计算过程：输入一个长度不固定的字符串，返回一串定长的字符串（又称为Hash值），单向Hash函数用于产生信息摘要。

信息摘要简要地描述了一份较长的信息或文件，它可以被看做是一份长文件的“数字指纹”，信息摘要可以用于创建数字签名。对于特定的文件而言，信息摘要是唯一的，而且不同的文件必将产生不同的信息摘要。常见的信息摘要算法包括MD5（产生一个128位的输出，输入是以512位的分组进行处理的）和SHA（安全散列算法，也是按512位的分组进行处理，产生一个160位的输出）。它们可以用来保护数据的完整性。

4. 数字签名

数字签名是通过一个单向函数对要传送的报文进行处理，得到用以认证报文来源并核实报文是否发生变化的一个字母数字串。它与数据加密技术一起构建起了安全的商业加密体系：传统的数据加密是保护数据的最基本方法，它只能够防止第三者获得真实的数据（数据的机密性），而数字签名则可以解决否认、伪造、篡改和冒充的问题（数据的完整性和不可抵赖性）。

数字签名可以使用对称加密技术实现，也可以使用非对称加密技术（公钥算法）实现。但如果使用对称加密技术实现，需要第三方认证，比较麻烦。因此现在通常使用的是公钥算法。

整个数字签名应用过程很简单：

（1）信息发送者使用一单向散列函数对信息生成信息摘要。

（2）信息发送者使用自己的私钥签名信息摘要。

（3）信息发送者把信息本身和已签名的信息摘要一起发送出去。

（4）信息接收者通过使用与信息发送者使用的同一个单向散列函数对接收的信息本身生成新的信息摘要，再使用信息发送者的公钥对信息摘要进行验证，以确认信息发送者的身份是否被修改过。

如果接收者收到的信息是P（用E代表公钥、D代表私钥），那么要保留的证据就应该是：E发送者(P)，这也就证明了信息的确是“发送者”发出的。

5. 数字证书

非对称加密技术的提出，解决了密钥传输的问题，但在实际应用过程中，我们遇到了一个新的问题：密钥只是一串数字或字符，并不能通过密钥得知它的主人是谁。这样就产生了安全隐患，所

以提出了数字证书的概念。数字证书简单一点理解，就是密钥与身份信息的结合体。

数字证书的格式一般使用X.509国际标准。X.509是广泛使用的证书格式之一，X.509用户公钥证书是由可信赖的证书权威机构（CA——证书授权中心）创建的，并且由CA或用户存放在X.500的目录中。任何一个用户只要得到CA中心的公钥，就可以得到该CA中心为该用户签署的公钥。每个用户的证书上都有CA中心用其私钥进行的数字签名，所以只需使用CA中心的公钥便可验证数字证书的真伪。

较通行的数字证书格式还有PGP。

上一节　本书简介　下一节

一点一练

试题1

甲和乙要进行通信，甲对发送的消息附加了数字签名，乙收到该消息后利用__(1)__验证该消息的真实性。

（1）A．甲的公钥 B．甲的私钥

C．乙的公钥 D．乙的私钥

试题2

从认证中心CA获取用户B的数字证书，该证书用__(2)__作数字签名；从用户B的数字证书中可以获得B的公钥。

（2）A．CA的公钥　B．CA的私钥　C．B的公钥　D．B的私钥

试题3

用户A从CA获得用户B的数字证书，并利用__(3)__验证数字证书的真实性。

（3）A．B的公钥　B．B的私钥　C．CA的公钥　D．CA的私钥

第 8 章：信息安全知识　作者：希赛教育软考

一点一练

（4）A．解密和签名　B．加密和签名　C．解密和认证　D．加密和认证

（5）A．解密和签名　B．加密和签名　C．解密和认证　D．加密和认证

版权方授权希赛网发布，侵权必究

上一节　本书简介　下一节

解析与答案

试题1分析

数字签名技术是对非对称加密技术与信息摘要的综合应用。通常的做法是对正文产生信息摘要，之后使用发送者A的私钥对该信息摘要进行加密，这就完成了签名。当接收者B收到签了名的摘要以后，会对摘要使用发送者A的公钥进行解密，若能解密，则表明该信息确实是由A发送的。这就是数字签名技术。

试题1答案

（1）A

试题2分析

数字证书就是互联网通讯中标志通讯各方身份信息的一系列数据，就好比日常生活中个人身份证一样。数字证书是由一个权威机构证书授权中心（CA）发行的。最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。其中证书授权中心的数字签名是用它自己的私钥完成的，而它的公钥也是公开的，大家可以通过它的公钥来验证该证书是否是某证书授权中心发行的，以达到验证数字证书的真实性。因此本题答案选B。

试题2答案

（2）B

试题3分析

本题主要考查数字证书的相关知识。

数字证书就是互联网通讯中标志通讯各方身份信息的一系列数据，就好比日常生活中个人身份证一样。数字证书是由一个权威机构证书授权中心（CA）发行的。最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。其中证书授权中心的数字签名是用它自己的私钥完成的，而它的公钥也是公开的，大家可以通过它的公钥来验证该证书是否是某证书授权中心发行的，以达到验证数字证书的真实性。因此本题答案选C。

试题3答案

（3）C

试题4分析

公钥体系即非对称加密体系，其密钥分为公钥与私钥。一般公钥用于加密，而私钥用于解密。公钥一般是公开的，大家都可以知道，适合用于认证；而私钥只有密钥拥有者自己知道，可用于签名。

试题4答案

（4）A（5）D

第 8 章：信息安全知识　作者：希赛教育软考学院　来源：希赛网　2014年05月05日

网络安全

网络安全知识是指与网络相关的一些安全性知识，包括：网络安全协议、常见的网络攻击、入侵检测技术、防火墙技术、VPN技术、漏洞扫描等。

考点精讲

1. 网络安全协议

互联网自上个世纪提出，至今不过区区几十年，但其发展速度之迅猛，让人始料不及。原本只作为资源共享而提出的互联网络，目前已是各类应用的基础平台。在此环境下，网络安全提到了一个前所未有的高度来看待。在软件设计师考试中，要求考生熟悉常见安全协议的工作层次，以及基本特性，他们的工作层次关系如图8-1所示。

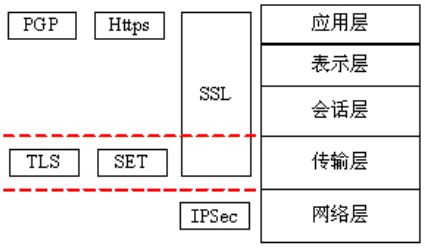

图8-1 安全协议层次图

（1）PGP协议

PGP（Pretty Good Privacy）是一个基于RSA公钥加密体系的邮件加密协议。可以用它对邮件保密以防止非授权者阅读，它还能对邮件加上数字签名从而使收信人可以确信邮件发送者。除此之外PGP还可用于文件存储的加密。

PGP承认两种不同的证书格式：PGP证书和X.509证书。

（2）SSL协议

SSL工作于传输层以上（跨越了多个网络层次），用于在Internet上传送机密文件。SSL协议由SSL记录协议、SSL握手协议和SSL警报协议组成。

SSL握手协议被用来在客户与服务器真正传输应用层数据之前建立安全机制，当客户与服务器第一次通信时，双方通过握手协议在版本号、密钥交换算法、数据加密算法和Hash算法上达成一致，然后互相验证对方身份，最后使用协商好的密钥交换算法产生一个只有双方知道的秘密信息，客户和服务器各自根据该秘密信息产生数据加密算法和Hash算法参数。

SSL记录协议根据SSL握手协议协商的参数，对应用层送来的数据进行加密、压缩、计算消息鉴别码，然后经网络传输层发送给对方。

SSL警报协议用来在客户和服务器之间传递SSL出错信息。

SSL协议是一个保证计算机通信安全的协议，对通信对话过程进行安全保护，其实现过程主要经过如下几个阶段：

1>接通阶段：客户机通过网络向服务器打招呼，服务器回应；

2>密码交换阶段：客户机与服务器之间交换双方认可的密码，一般选用RSA密码算法，也有的选用Diffie-Hellmanf和Fortezza-KEA密码算法；

3>会谈密码阶段：客户机器与服务器间产生彼此交谈的会谈密码；

4>检验阶段：客户机检验服务器取得的密码；

5>客户认证阶段：服务器验证客户机的可信度；

6>结束阶段：客户机与服务器之间相互交换结束的信息。

发送时信息用对称密钥加密，对称密钥用不对称算法加密，再把两个包绑在一起传送过去。接收的过程与发送正好相反，先打开有对称密钥的加密包，再用对称密钥解密。因此，SSL协议也可用于安全电子邮件。

（3）SET协议

SET（Secure Electronic Transaction，安全电子交易）协议向基于信用卡进行电子化交易的应用提供了实现安全措施的规则。它是由Visa国际组织和MasterCard组织共同制定的一个能保证通过开放网络（包括Internet）进行安全资金支付的技术标准。SET在保留对客户信用卡认证的前提下，又增加了对商家身份的认证。由于设计较为合理，得到了诸如微软公司、IBM公司、Netscape公司等大公司的支持，已成为实际上的工业技术标准。

（4）IPSec协议

IPSec工作于网络层。它有两种加密方式：第一种，是将原IP数据包进行整体加密（包括IP包头），然后产生新的IP包进行传送；第二种，是将原IP数据包中的数据取出来，加密，然后通过原IP包头信息产生新的IP头。区别在于一个是整体加密，另一个是数据加密。

（5）TLS协议

安全传输层协议（TLS）用于在两个通信应用程序之间提供保密性和数据完整性。

该协议由两层组成： TLS 记录协议（TLS Record）和 TLS 握手协议（TLS Handshake）。较低的层为 TLS 记录协议，位于某个可靠的传输协议（例如 TCP）上面。 TLS 记录协议提供的连接安全性具有两个基本特性：

私有─对称加密用以数据加密（DES 、RC4 等）。对称加密所产生的密钥对每个连接都是唯一的，且此密钥基于另一个协议（如握手协议）协商。记录协议也可以不加密使用。

可靠─信息传输包括使用密钥的 MAC 进行信息完整性检查。安全哈希功能（ SHA、MD5 等）用于 MAC 计算。记录协议在没有 MAC 的情况下也能操作，但一般只能用于这种模式，即有另一个协议正在使用记录协议传输协商安全参数。

2. 网络攻击

网络攻击有许多种类型，在此介绍两种常见攻击方式：DDoS攻击与ARP欺骗攻击。

（1）DDoS攻击

DDoS是英文Distributed Denial of Service的缩写，意思是“分布式拒绝服务”。DDoS攻击通过很多“肉鸡”（被攻击者入侵过或可间接利用的主机）向受害主机发送大量看似合法的网络包，从而造成网络阻塞或服务器资源耗尽而导致拒绝服务，分布式拒绝服务攻击一旦被实施，攻击网络包就会犹如洪水般涌向受害主机，从而把合法用户的网络包淹没，导致合法用户无法正常访问服务器的网络资源。这就好比有1000个人同时给你家里打电话，这时候你的朋友还打得进来吗？因此，拒绝服务攻击又被称之为“洪水式攻击”。拒绝服务攻击不能通过安装防火墙、更新杀毒软件等方式进行防治。但可通过：限制源IP、关闭不必要的服务、限制同时打开的Syn半连接数目、缩短Syn半连接的time out 时间等手段缓解。

（2）ARP欺骗攻击

ARP欺骗攻击：修改IP地址和MAC地址的映射关系，使发送给正确主机的数据包发送给另外一

台由攻击者控制的主机。

ARP欺骗攻击得以实现，是因为ARP协议本身存在漏洞。ARP协议用于维护计算机中的IP至MAC映射表，在局域网中，一台计算机与另一台计算机通信时，需要借助这个映射表，将目标IP转化为目标MAC。而ARP欺骗攻击就是通过向局域网中各台主机发送伪造的网关报文，将网关IP与黑客主机的MAC对应起来，这样，局域网中主机要与网关通信时，实际数据包被发送至黑客主机，从而达到攻击的目的。

3. 入侵检测

入侵检测技术是为保证计算机系统的安全而设计与配置的一种能够及时发现并报告系统中未授权或异常现象的技术，是一种用于检测计算机网络中违反安全策略行为的技术。违反安全策略的行为有：入侵—非法用户的违规行为；滥用—用户的违规行为。

入侵检测系统所采用的技术可分为特征检测与异常检测两种。

（1）特征检测。特征检测也称为误用检测，假设入侵者活动可以用一种模式来表示，系统的目标是检测主体活动是否符合这些模式。它可以将已有的入侵方法检查出来，但对新的入侵方法无能为力。其难点在于如何设计模式既能够表达“入侵”现象又不会将正常的活动包含进来。

（2）异常检测。假设是入侵者活动异常于正常主体的活动。根据这一理念建立主体正常活动的“活动简档”，将当前主体的活动状况与“活动简档”相比较，当违反其统计规律时，认为该活动可能是“入侵”行为。异常检测的难题在于如何建立“活动简档”以及如何设计统计算法，从而不把正常的操作作为“入侵”或忽略真正的“入侵”行为。

4. 防火墙

防火墙是网络安全的第一道门户，可以实现内部网（信任网络）和外部不可信任网络之间，或者是内部网不同网络安全区域之间的隔离与访问控制，保证网络系统及网络服务的可用性。狭义的防火墙是指安装了防火墙的软件或路由器系统，而广义的防火墙还包括整个网络的安全策略和安全行为。

根据防火墙组建结构的不同，可以分为屏蔽路由器、双穴主机、屏蔽主机防火墙、屏蔽子网防火墙四种基本结构，以及一些变体，下面则详细地说明了它们的优缺点与应用场合。

（1）包过滤型防火墙

包过滤型防火墙工作于网络层，它对进出内部网络的所有信息进行分析，并按照一定的安全策略对进出内部网络的信息进行限制。这种防火墙的优点是处理速度快、费用低、对用户透明。缺点是维护比较困难，只能阻止少部分IP欺骗，不支持有效的用户认证，日志功能有限，过滤规则增加会大大降低吞吐量，无法对信息提供全面控制。

（2）双宿网关防火墙

双宿网关防火墙由一台至少装有两块网卡的堡垒主机作为防火墙，位于内外网络之间，分别与内外网络相离，实现物理上的隔开。它有两种服务方式：一种是用户直接登录到双宿主机上；另一种是在双宿主机上运行代理服务器。其安全性比屏蔽路由器高。但入侵者一旦得到双穴主机的访问权，内部网络就会被入侵，因此需具有强大的身份认证系统，才可以阻挡来自外部的不可信网络的非法入侵。

（3）屏蔽主机防火墙

屏蔽主机防火墙是由包过滤型防火墙和双宿网关防火墙组合形成的一种防火墙，它强迫所有的外部主机与一个堡垒主机相连接，而不让它们直接与内部主机相连接。这种防火墙的优点是实现了

网络层安全（包过滤）和应用层安全（代理），因此安全等级比屏蔽路由器要高。其缺点是堡垒主机可能被绕过，堡垒主机与其他内部主机间没有任何保护网络安全的东西存在，一旦被攻破，内网就将暴露。

（4）屏蔽子网防火墙

屏蔽子网防火墙用了两个屏蔽路由器和一个堡垒主机，也称为“单DMZ防火墙结构”。这种防火墙的结构的优点在于定义了“非军事区（DMZ）”网络后，支持网络层和应用层安全功能，在黑客攻破第一道防火墙，进入DMZ区后，只能对DMZ区进行破坏，无法影响到内部网络，所以这也是目前最安全的防火墙系统。

5. VPN

虚拟专用网（VPN）是企业网在因特网等公共网络上的延伸，它通过一个私有的通道在公共网络上创建一个安全的私有连接。因此，从本质上说VPN是一个虚信道，它可用来连接两个专用网，通过可靠的加密技术方法保证其安全性，并且是作为一个公共网络的一部分存在的。实现VPN的关键技术主要有隧道技术、加解密技术、密钥管理技术和身份认证技术。图8-2是一个VPN构成的原理示意图。

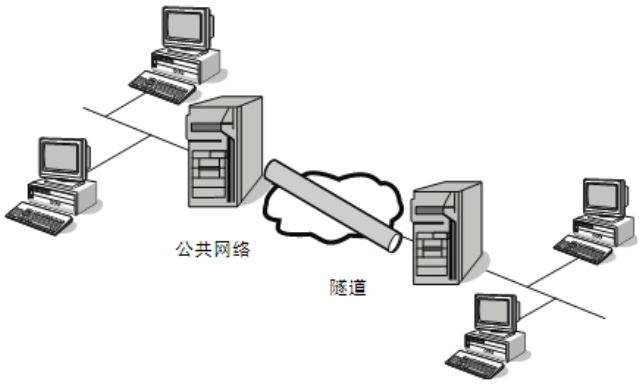

图8-2 VPN构成原理示意图

隧道技术是VPN关键技术之一（此外还包括加解密技术、密钥管理技术和身份认证技术），它是一种数据封装协议，也就是将一种协议封装在另一种协议中传输，从而实现被封装协议对封装协议的透明性。根据其工作的层次可以分为以下两类。

二层隧道技术：包括PPP基础上的PPTP（点到点隧道协议）和L2F（二层转发协议）、L2TP（二层隧道协议）；

三层隧道技术：主要代表是IPSec（IP层安全协议，它是IPv4和IPv6的安全标准）、移动IP协议和虚拟隧道协议（VTP）。

6. 漏洞扫描

漏洞扫描是指基于漏洞数据库，通过扫描等手段，对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用的漏洞的一种安全检测（渗透攻击）行为。

漏洞扫描是对电脑进行全方位的扫描，检查你当前的系统是否有漏洞，如果有漏洞则需要马上进行修复，否则电脑很容易受到网络的伤害甚至被黑客借助于电脑的漏洞进行远程控制那么后果将不堪设想，所以漏洞扫描对于保护电脑和上网安全是必不可少的，而且需要每星期就进行一次扫描，一但发现有漏洞就要马上修复，有的漏洞系统自身就可以修复，而有些则需要手动修复。

人们往往使用漏洞扫描技术达到以下目的：

检查目标主机的存活状态（开/关机）；

检查目标主机的端口开放状态；

识别目标主机操作系统及其运行的服务程序的类型和版本；

根据已知漏洞信息，分析系统的脆弱点；

上一节　本书简介　下一节

一点一练

试题1

如果使用大量的连接请求攻击计算机，使得所有可用的系统资源都被消耗殆尽，最终计算机无法再处理合法用户的请求，这种手段属于__(1)__攻击。

（1）A．拒绝服务　B．口令入侵　C．网络监听　D．IP欺骗

试题2

ARP攻击造成网络无法跨网段通信的原因是__(2)__。

（2）A．发送大量ARP报文造成网络拥塞

B．伪造网关ARP报文使得数据包无法发送到网关

C．ARP攻击破坏了网络的物理连通性

D．ARP攻击破坏了网关设备

试题3

下列选项中，防范网络监听最有效的方法是__(3)__。

（3）安装防火墙　B．采用无线网络传输　C．数据加密　D．漏洞扫描

试题4

利用__(4)__可以获取某FTP服务器中是否存在可写目录的信息。

（4）A．防火墙系统 B．漏洞扫描系统

C．入侵检测系统 D．病毒防御系统

试题5

IIS6.0支持的身份验证安全机制有4种验证方法，其中安全级别最高的验证方法是__(5)__。

（5）A．匿名身份验证 B．集成Windows身份验证

C．基本身份验证 D．摘要式身份验证

试题6

在IE浏览器中，安全级别最高的区域设置是__(6)__。

（6）A．Internet　B．本地Intranet　C．可信任站点　D．受限站点

版权方授权希赛网发布，侵权必究

上一节　本书简介　下一节

解析与答案

试题1分析

拒绝服务即Dos攻击，他是指通过向服务器发送大量连接请求，导致服务器系统资源都被消耗，从而无法向正常用户提供服务的现象。

试题1答案

（1）A

试题2分析

ARP攻击就是通过伪造IP地址和MAC地址实现ARP欺骗，它通过伪造网关ARP报文与你通信，而使得你的数据包无法发送到真正的网关，从而造成网络无法跨网段通信。

试题2答案

（2）B

试题3分析

网络监听是一种监视网络状态、数据流程以及网络上信息传输的管理工具，使用网络监听便可以有效地截获网络上传送的数据。对网络监听最有效的防范方法是对传送的数据进行加密，这样即便传送的数据被截获，对方没有密钥，也很难获取到有用的信息。

试题3答案

（3）

试题4分析

防火墙是位于两个（或多个）网络间，实施网络间访问控制的一组组件的集合，它是一套建立在内外网络边界上的过滤封锁机制。防火墙的主要功能有：过滤掉不安全服务和非法用户；控制对特殊站点的访问；提供了监视Internet安全和预警的方便端点。

漏洞扫描系统通常是指基于漏洞数据库，通过扫描等手段，对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用的漏洞的，利益漏洞扫描系统可以获取某FTP服务器中是否存在可写目录的信息。

入侵检测是防火墙的合理补充，帮助系统对付网络攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高了信息安全基础结构的完整性。它从计算机网络系统中的若干关键点收集信息，并分析这些信息，看网络中是否有违反安全策略的行为和遭到袭击的迹象。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测，从而提供对内部攻击、外部攻击和误操作的实时保护。

病毒防御系统是一个用来防止黑客、病毒、木马的防御系统。

试题4答案

（4）B

试题5分析

为了阻止对Web站点未经授权的访问，可以对用户进行身份验证，拒绝不能提供有效Windows用户名和密码的用户的访问。其中IIS6.0支持的身份验证安全机制有以下4种验证方法：

（1）匿名访问

匿名验证使用户无需输入用户名或密码便可以访问Web或FTP站点的公共区域，是默认的认证方式。当用户使用匿名验证访问公共Web和FTP站点时，IIS服务器向用户分配特定的Windows用户

帐号IUSR_computername，computername是指运行IIS的服务器名称。默认情况下，IUSR_computername帐户包含在Windows用户组Guests中。

（2）基本身份验证

基本验证在允许用户访问某个站点之前，提示用户在“登录”对话框中输入用户名和密码，然后Web浏览器尝试使用这些信息建立连接。如果输入的用户名和密码有效，则建立连接，否则Web浏览器将反复显示“登录”对话框，直到用户输入有效的用户名和密码或关闭此对话框。

（3）摘要式身份验证

摘要式验证的验证过程与基本验证类似，但在传送验证信息时使用了不同方法。基本验证使用明码传输，因而是不安全的；而摘要式验证的验证凭据则采用单向传送的“散列算法”。

摘要式验证是HTTP 1.1的一项新功能，并非所有的浏览器都支持它。如果不兼容的浏览器对服务器请求摘要式验证，服务器将拒绝请求并向客户端发送错误消息。

（4）集成式Windows身份验证

集成Windows验证(以前称 NTLM 或 Windows NT 质询/响应验证)是一种安全的验证形式，这是因为用户名和密码不通过网络发送，使用的是在客户端当前的Windows登录信息。当启用集成Windows验证时，用户的浏览器通过与Web服务器进行密码交换，包括散列，来证明其知晓密码，它是安全级别最高的验证方法。

试题5答案

（5）B

试题6分析

在IE浏览器中，安全级别最高的区域设置是受限站点。

其中Internet区域设置适用于Internet网站，但不适用于列在受信任和受限制区域的网站；本地Intranet区域设置适用于在Intranet中找到的所有网站；可信任站点区域设置适用于你信任的网站；而受限站点区域设置适用于可能会损坏你计算机或文件的网站，它的安全级别最高。

试题6答案

（6）D

计算机病毒与木马

计算机病毒与木马是信息系统安全的一个重要方面，因为如果计算机中了病毒或木马，这些恶意代码将对系统造成破坏。下面将详细介绍相关情况。

考点精讲

1. 病毒与木马的概念

在计算机中，恶意代码主要分两类，即病毒与木马。

病毒：一段可执行的程序代码，通过对其他程序进行修改，可以感染这些程序，使其含有该病毒程序的一个复制。

计算机病毒的生命周期包括4个阶段：潜伏期（不做任何事，等待激活事件，并非所有病毒都有该阶段），繁殖阶段（也就是传染阶段，开始复制复本），触发阶段（也就是开始执行破坏性工作的阶段），执行阶段（功能完成）。

木马：实质上是一个网络客户端/服务器程序，是一种基于远程控制的黑客工具。其主要特征包括：

不需要服务端用户的允许就能够获得系统的使用权；

程序体积十分小，执行时不会占太多的资源；

执行时很难停止它的活动，并且不会在系统中显示出来；

一次启动后就会自动加载在系统的启动区，在每次启动时能够自动运行；

一次执行后会通过更换文件名之类的方法来隐藏自己；

实现服务端用户无法显示执行的动作。

木马通常由服务器端和客户端组成，服务器端将运行在被控制的主机中，而客户端则是攻击者用来远程控制的主要工具。

2. 病毒的分类

病毒的分类，有多种方式，从应考的角度，需要掌握以下类型：

系统引导型病毒：又称开机型病毒，是藏匿和感染硬盘的第一个扇区，即平常我们所说的引导扇区。引导型病毒籍由引导动作而侵入内存。

文件型病毒：文件型病毒通常寄生在可执行档（如 *.COM，*.EXE等）中。当这些文件被执行时，病毒的程序就跟着被执行。

目录型病毒：这一类型病毒通过装入与病毒相关的文件进入系统，而不改变相关文件，它所改变的只是相关文件的目录项。

蠕虫病毒：蠕虫病毒是一种常见的计算机病毒。它是利用网络进行复制和传播，传染途径是通过网络和电子邮件。最初的蠕虫病毒定义是因为在DOS环境下，病毒发作时会在屏幕上出现一条类似虫子的东西，胡乱吞吃屏幕上的字母并将其改形。蠕虫病毒是自包含的程序（或是一套程序），它能传播自身功能的拷贝或自身（蠕虫病毒）的某些部分到其他的计算机系统中（通常是经过网络连接）。

宏病毒：一种寄存在Office系统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。从此以后，所有自动保存的文档都会“感染”上这种宏病毒，而且如果其他用户打开了感染病毒的文档，宏病毒又会转移到他的计算机上。

3. 病毒种类命名

一种病毒都有自己的名称，从名称我们通常可以判断出该病毒的类型。

（1）系统病毒

系统病毒的前缀为：Win32、PE、Win95、W32、W95等。这些病毒的一般共有的特性是可以感染windows操作系统的 *.exe 和 *.dll 文件，并通过这些文件进行传播。

（2）蠕虫病毒

蠕虫病毒的前缀是：Worm。这种病毒的共有特性是通过网络或者系统漏洞进行传播，很大部分的蠕虫病毒都有向外发送带毒邮件，阻塞网络的特性。比如冲击波（阻塞网络），小邮差（发带毒邮件）等。

（3）木马病毒、黑客病毒

木马病毒其前缀是：Trojan，黑客病毒前缀名一般为 Hack。QQ消息尾巴木马：Trojan.QQ3344，还有大家可能遇见比较多的针对网络游戏的木马病毒如 Trojan.LMir.PSW.60。

（4）脚本病毒

脚本病毒的前缀是：Script。脚本病毒的共有特性是使用脚本语言编写，通过网页进行的传播的病毒，如红色代码（Script.Redlof）。脚本病毒还会有如下前缀：VBS、JS（表明是何种脚本编写的），如欢乐时光（VBS.Happytime）、十四日（Js.Fortnight.c.s）等。

（5）宏病毒

宏病毒也是脚本病毒的一种，由于它的特殊性，因此在这里单独算成一类。宏病毒的前缀是：Macro，第二前缀是：Word、Excel其中之一。如：Macro.Word.WhiteScreen、美丽莎（Macro.Melissa）。

（6）后门病毒

后门病毒的前缀是：Backdoor。该类病毒的共有特性是通过网络传播，给系统开后门，给用户电脑带来安全隐患。

（7）病毒种植程序病毒

这类病毒的共有特性是运行时会从体内释放出一个或几个新的病毒到系统目录下，由释放出来的新病毒产生破坏。如：冰河播种者（Dropper.BingHe2.2C）、MSN射手（Dropper.Worm.Smibag）等。

（8）破坏性程序病毒

破坏性程序病毒的前缀是：Harm。这类病毒的共有特性是本身具有好看的图标来诱惑用户点击，当用户点击这类病毒时，病毒便会直接对用户计算机产生破坏。如：格式化C盘（Harm.formatC.f）、杀手命令（Harm.Command.Killer）等。

（9）玩笑病毒

玩笑病毒的前缀是：Joke。也称恶作剧病毒。这类病毒的共有特性是本身具有好看的图标来诱惑用户点击，当用户点击这类病毒时，病毒会做出各种破坏操作来吓唬用户，其实病毒并没有对用户电脑进行任何破坏。如：女鬼（Joke.Girl ghost）病毒。

（10）捆绑机病毒

捆绑机病毒的前缀是：Binder。这类病毒的共有特性是病毒作者会使用特定的捆绑程序将病毒与一些应用程序如QQ、IE捆绑起来，表面上看是一个正常的文件，当用户运行这些捆绑病毒时，会表面上运行这些应用程序，然后隐藏运行捆绑在一起的病毒，从而给用户造成危害。如：捆绑QQ（Binder.QQPass.QQBin）、系统杀手（Binder.killsys）等。

关于病毒与木马，考生除了解以上基本内容外，还应该关注最近最为著名的病毒或木马的主要特征，以前考试曾多次以当时最流行病毒为题。如2007年“熊猫烧香”病毒盛行，所以在2007年5

月的软件设计师考试中考到了“机器中熊猫烧香病毒的症状”。

第 8 章：信息安全知识 作者：希赛教育软考学院 来源：希赛网 2014年05月05日

一点一练

试题1

通过内部发起连接与外部主机建立联系，由外部主机控制并盗取用户信息的恶意代码为__(1)__。

（1）A．特洛伊木马 B．蠕虫病毒 C．宏病毒 D．CIH病毒

试题2

宏病毒一般感染以__(2)__为扩展名的文件。

（2）A．EXE B．COM C．DOC D．DLL

试题3

杀毒软件报告发现病毒Macro.Melissa，由该病毒名称可以推断病毒类型是__(3)__，这类病毒主要感染目标是__(4)__。

（3）A．文件型 B．引导型 C．目录型 D．宏病毒

（4）A．EXE或COM可执行文件 B．Word或Excel文件

C．DLL系统文件 D．磁盘引导区

第 8 章：信息安全知识 作者：希赛教育软考学院 来源：希赛网 2014年05月05日

解析与答案

试题1分析

特洛伊木马一种秘密潜伏的能够通过远程网络进行控制的恶意程序，它使控制者可以控制被秘密植入木马的计算机的一切资源和行为。

蠕虫病毒是一种常见的利用网络进行复制和传播的病毒。病毒发作时会在屏幕上出现一条类似虫子的东西，胡乱吞吃屏幕上的字母并将其改形。

宏病毒是一种寄存在文档或模板的宏中的病毒。一旦打开这样的文档，其中的宏就会被执行，宏病毒就会被激活，转移到计算机上，并驻留在Normal模板上。

CIH病毒是一种能够破坏计算机系统硬件的恶性病毒，有时还会破坏计算机的BIOS。

试题1答案

（1）A

试题2分析

宏病毒是一种脚本病毒，它的最主要特征是它是一种寄存在文档或模板的宏中的计算机病毒。宏病毒主要感染文件有 Word、Excel 的文档。并且会驻留在Normal面板上。宏病毒的前缀是：Macro，第二前缀是：Word、Excel其中之一。如：Macro.Word.WhiteScreen、美丽莎（Macro.Melissa）等。

在本题中，题目给出的4个选项中，扩展名为DOC的一般为Word文档，因此容易感染宏病毒。

试题2答案

（2）C

试题3分析

题目给出的病毒名是“Macro.Melissa”，它的前缀为“Macro”，从这个前缀可以看出病毒属于宏病毒，宏病毒是针对Office系列的。

试题3答案

（3）D（4）B

上一节　本书简介　下一节

作者：希赛教育软考学院　来源：希赛网　2014年05月05日

考前冲刺

试题1

下面关于漏洞扫描系统的叙述，错误的是__(1)__。

（1）A．漏洞扫描系统是一种自动检测目标主机安全弱点的程序

B．黑客利用漏洞扫描系统可以发现目标主机的安全漏洞

C．漏洞扫描系统可以用于发现网络入侵者

D．漏洞扫描系统的实现依赖于系统漏洞库的完善

试题2

网络安全包含了网络信息的可用性、保密性、完整性和网络通信对象的真实性。数字签名是对__(2)__的保护。

（2）A．可用性　B．保密性　C．连通性　D．真实性

试题3

计算机感染特洛伊木马后的典型现象是__(3)__。

（3）A．程序异常退出 B．有未知程序试图建立网络连接

C．邮箱被垃圾邮件填满 D．Windows系统黑屏

试题4

网络安全体系设计可从物理线路安全、网络安全、系统安全、应用安全等方面来进行。其中，数据库容灾属于__(4)__。

（4）A．物理线路安全和网络安全 B．物理线路安全和应用安全

C．系统安全和网络安全 D．系统安全和应用安全

试题5

包过滤防火墙对数据包的过滤依据不包括__(5)__。

（5）A．源IP地址 B．源端口号

C．MAC地址 D．目的IP地址

试题6

某网站向CA申请了数字证书，用户通过__(6)__来验证网站的真伪。

（6）A．CA的签名 B．证书中的公钥

C．网站的私钥 D．用户的公钥

试题7

网络安全体系设计可从物理线路安全、网络安全、系统安全、应用安全等方面来进行。其中，数据库容灾属于__(7)__。

（7）A．物理线路安全和网络安全 B．物理线路安全和应用安全

C．系统安全和网络安全 D．系统安全和应用安全

试题8

包过滤防火墙对数据包的过滤依据不包括__(8)__。

（8）A．源IP地址 B．源端口号

C．MAC地址 D．目的IP地址

试题9

某网站向CA申请了数字证书，用户通过__(9)__来验证网站的真伪。

（9）A．CA的签名 B．证书中的公钥

C．网站的私钥 D．用户的公钥

试题10

下列安全协议中，与TLS最接近的协议是__(10)__。

（10）A．PGP B． SSL C． HTTPS D．IPSec

试题11

用户B收到用户A带数字签名的消息M，为了验证M的真实性，首先需要从CA获取用户A的数字证书，并利用__(11)__验证该证书的真伪，然后利用__(12)__验证M的真实性。

（11）A．CA的公钥 B．B的私钥 C．A的公钥 D．B的公钥

（12）A．CA的公钥 B．B的私钥 C．A的公钥 D．B的公钥

上一节 本书简介 下一节

作者：希赛教育软考学院 来源：希赛网 2014年05月05日

习题解析

试题1分析

本题考查漏洞扫描系统的基本概念。

漏洞扫描系统是一种自动检测目标主机安全弱点的程序，漏洞扫描系统的原理是根据系统漏洞

库对系统可能存在的漏洞进行一一验证。黑客利用漏洞扫描系统可以发现目标主机的安全漏洞从而有针对性的对系统发起攻击；系统管理员利用漏洞扫描系统可以查找系统中存在的漏洞并进行修补从而提高系统的可靠性。漏洞扫描系统不能用于发现网络入侵者，用于检测网络入侵者的系统称为入侵检测系统。

试题1答案

（1）C

试题2分析

本题考查网络安全方面的基础知识。

数字签名（Digital Signature）技术是不对称加密算法的典型应用。数字签名的应用过程是：数据源发送方使用自己的私钥对数据校验和或其他与数据内容有关的变量进行加密处理，完成对数据的合法“签名”；数据接收方则利用对方的公钥来解读收到的“数字签名”，并将解读结果用于对数据完整性的检验，以确认签名的合法性。数字签名技术是在网络系统虚拟环境中确认身份的重要技术，完全可以代替现实过程中的“亲笔签字”，在技术和法律上有保证，可见数字签名是对签名真实性的保护。

试题2答案

（2）D

试题3分析

本题考查计算机病毒相关知识。

特洛伊木马是一种通过网络传播的病毒，分为客户端和服务器端两部分，服务器端位于被感染的计算机，特洛伊木马服务器端运行后会试图建立网络连接，所以计算机感染特洛伊木马后的典型现象是有未知程序试图建立网络连接。

试题3答案

（3）B

试题4分析

网络安全体系设计是逻辑设计工作的重要内容之一，数据库容灾属于系统安全和应用安全考虑范畴。

试题4答案

（4）D

试题5分析

本题考查防火墙相关知识。

包过滤防火墙对数据包的过滤依据包括源IP地址、源端口号、目标IP地址和目标端口号。

试题5答案

（5）C

试题6分析

本题考查数字证书相关知识点。

数字证书是由权威机构——CA证书授权（Certificate Authority）中心发行的，能提供在Internet上进行身份验证的一种权威性电子文档，人们可以在因特网交往中用它来证明自己的身份和识别对方的身份。

数字证书包含版本、序列号、签名算法标识符、签发人姓名、有效期、主体名和主体公钥信息

等并附有CA的签名，用户获取网站的数字证书后通过验证CA的签名和确认数字证书的有效性，从而验证网站的真伪。

在用户与网站进行安全通信时，用户发送数据时使用网站的公钥（从数字证书中获得）加密，收到数据时使用网站的公钥验证网站的数字签名，网站利用自身的私钥对发送的消息签名和对收到的消息解密。

试题6答案

（6）A

试题7分析

网络安全体系设计是逻辑设计工作的重要内容之一，数据库容灾属于系统安全和应用安全考虑范畴。

试题7答案

（7）D

试题8分析

本题考查防火墙相关知识。

包过滤防火墙对数据包的过滤依据包括源IP地址、源端口号、目标IP地址和目标端口号。

试题8答案

（8）C

试题9分析

本题考查数字证书相关知识点。

数字证书是由权威机构——CA证书授权（Certificate Authority）中心发行的，能提供在Internet上进行身份验证的一种权威性电子文档，人们可以在因特网交往中用它来证明自己的身份和识别对方的身份。

数字证书包含版本、序列号、签名算法标识符、签发人姓名、有效期、主体名和主体公钥信息等并附有CA的签名，用户获取网站的数字证书后通过验证CA的签名和确认数字证书的有效性，从而验证网站的真伪。

在用户与网站进行安全通信时，用户发送数据时使用网站的公钥（从数字证书中获得）加密，收到数据时使用网站的公钥验证网站的数字签名，网站利用自身的私钥对发送的消息签名和对收到的消息解密。

试题9答案

（9）A

试题10分析

本题考查网络安全协议。

网络安全协议这个知识点，主要要求掌握安全协议的功能以及工作层次。备选答案中，只有SSL与TLS一样，工作于传输层，所以他们的关联最大，最接近。

试题10答案

（10）B

试题11分析

本题考查数字证书的相关知识。

数字证书这个知识点，考查频度最高的是与之相关的公钥与私钥及其用途。首先需要了解到的

是：在数字证书中，会封装证书持有人A的公钥，这个公钥的用途是当别人要向A发送秘密消息时，要使用A的公钥进行加密；而要验证某个消息是否为A发出时，要用A的公钥对数字签名进行验证。这是一个非常重要的密钥。而另一个重要密钥是CA的公钥。CA的公钥又是在什么时候需要用到呢？我们知道每个数字证书在诞生时，CA中心就会对证书做一个数字签名，这个数字签名正是我们验证一个证书是否为合法证书的唯一标识。所以CA的公钥正是用于验证证书上数字签名的。

试题11答案

（11）A（12）C

上一节　本书简介　下一节

考点脉络

多媒体主要是指文字、声音和图像等多种表达信息的形式和媒体，它的出现大大丰富了计算机应用的表现力。本知识点考查分值较少，本章将对常考的两个知识点进行分析。

根据考试大纲，本章要求考生掌握以下几个方面的知识点。

（1）多媒体系统基础知识。

（2）简单图形的绘制，图像文件的处理方法。

（3）音频和视频信息的应用。

（4）多媒体应用开发过程。

从历年的考试情况来看，本章的考点主要集中于：多媒体基础概念、多媒体相关计算及常见多媒体标准。

上一节　本书简介　下一节

多媒体基础概念

多媒体基础概念部分涉及：声音和图像的相关概念以及在此基础之上的一些参数计算问题。

上一节　本书简介　下一节

考点精讲