# 信息安全

第 5 章：信息安全作者：[希赛软考学院](http://www.educity.cn/jiaocheng/a%cf%a3%c8%fc%c8%ed%bf%bc%d1%a7%d4%ba.html)    来源：希赛软考学院    2017年11月21日

# 试题1(2017年下半年试题7-8)

与HTTP相比，HTTPS协议对传输的内容进行加密，更加安全。HTTPS基于（  ）安全协议，其默认端口是（  ）。  
（7）A．RSA  
B.DES  
C.SSL  
D.SSH  
  
（8）A．1023  
B.443  
C.80  
D.8080

**试题分析**

1、HTTPS是基于SSL(Secure Sockets Layer 安全套接层)的。  
2、http的端口号为80。

**试题答案**

（7）C（8）B

# ！！试题2(2017年下半年试题9)

下列攻击行为中，属于典型被动攻击的是（  ）。  
（9）A．拒绝服务攻击  
B.会话拦截  
C.系统干涉  
D.修改数据命令

**试题分析**

ABD为主动攻击。

**试题答案**

（9）C

# ！！试题3(2017年下半年试题10)

（  ）不属于入侵检测技术。  
（10）A．专家系统  
B.模型检测  
C.简单匹配  
D.漏洞扫描

**试题分析**

漏洞扫描为另一种安全防护策略。

**试题答案**

（10）D

# 试题4(2017年下半年试题11)

以下关于防火墙功能特性的叙述中，不正确的是（  ）。  
（11）A．控制进出网络的数据包和数据流向  
B.提供流量信息的日志和审计  
C.隐藏内部IP以及网络结构细节  
D.提供漏洞扫描功能

**试题分析**

D选项不是防火墙的功能特性。

**试题答案**

1. D

-------------------------------------------------------------------------------------------------

# 试题5(2017年上半年试题7)

HTTPS 使用（  ）协议对报文进行封装  
  
（7）A．SSH  
B.SSL  
C.SHA-1  
D.SET

**试题分析**

HTTPS以保密为目标研发，简单讲是HTTP的安全版。其安全基础是SSL协议，全称Hypertext Transfer Protocol over Secure Socket Layer。 它是一个URI scheme，句法类同http:体系。它使用了HTTP，但HTTPS存在不同于HTTP的默认端口及一个加密/身份验证层（在HTTP与TCP之间）。这个协议的最初研发由网景公司进行，提供了身份验证与加密通讯方法，现在它被广泛用于互联网上安全敏感的通讯，例如交易支付方面。 SSL极难窃听，对中间人攻击提供一定的合理保护。严格学术表述HTTPS是两个协议的结合，即传输层SSL＋应用层HTTP。

**试题答案**

（7）B

# 试题6(2017年上半年试题8)

以下加密算法中适合对大量的明文消息进行加密传输的是（  ）。  
  
（8）A．RSA  
B.SHA-1  
C.MD5  
D.RC5

**试题分析**

本题考查的是信息安全中的加密算法。其中：  
       RSA是非对称加密算法；SHA-1与MD5属于信息摘要算法；RC-5属于非对称加密算法。这些算法中SHA-1与MD5是不能用来加密数据的，而RSA由于效率问题，一般不直接用于大量的明文加密，适合明文加密的，也就只有RC-5了。

**试题答案**

（8）D

# ！！试题7(2017年上半年试题9)

假定用户A、B 分别在I1和I2两个 CA 处取得了各自的证书，下面（  ）是 A、B 互信的必要条件。  
  
（9）A．A、B互换私钥  
B.A、B互换公钥  
C.I1、I2互换私钥  
D.I1、I2互换公钥

**试题分析**

本题考查的是信息安全中的CA认证。题目难度较高，但用排除法来分析不难得出结论。首先，在公钥体系中，交换私钥是无论什么情况下都绝对不允许发生的情况，所以A与C选项必然错误。余下的B与D，B选项的做法没意义，要AB互信，其信任基础是建立在CA之上的，如果仅交换AB的公钥并不能解决信任的问题。而I1与I2的公钥交换倒是可以做到互信，因为I1与I2的公钥正是验证CA签名的依据。所以本题应选D。  
试题答案

**试题答案**

（9）D

# 试题8(2016年下半年试题7)

可用于数字签名的算法是（  ）。  
（7）A．RSA  
B.IDEA  
C.RC4  
D.MD5

**试题分析**

IDEA算法和RC4算法都对称加密算法，只能用来进行数据加密。MD5算法是消息摘要算法，只能用来生成消息摘要无法进行数字签名。  
RSA算法是典型的非对称加密算法，主要具有数字签名和验签的功能。

**试题答案**

（7）A

# 试题9(2016年下半年试题8)

（  ）不是数字签名的作用。  
（8）A．接收者可验证消息来源的真实性  
B.发送者无法否认发送过该消息  
C.接收者无法伪造或篡改消息  
D.可验证接收者合法性

**试题分析**

数字签名是信息的发送者才能产生的别人无法伪造的一段数字串，这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明。不能验证接收者的合法性。

**试题答案**

（8）D

# 试题10(2016年下半年试题9)

在网络设计和实施过程中要采取多种安全措施，其中（  ）是针对系统安全需求的措施。  
  
（9）A．设备防雷击  
B.入侵检测  
C.漏洞发现与补丁管理  
D.流量控制

**试题分析**

其他三项不是系统级安全需求 。

**试题答案**

（9）C

# 试题11(2016年上半年试题8)

传输经过SSL加密的网页所采用的协议是（  ）。  
（8）A．HTTP   
B.HTTPS   
C.S-HTTP   
D.HTTP-S

**试题分析**

HTTPS（全称：Hyper Text Transfer Protocol over Secure Socket Layer），是以安全为目标的HTTP通道，简单讲是HTTP的安全版。即HTTP下加入SSL层，HTTPS的安全基础是SSL，因此加密的详细内容就需要SSL。

**试题答案**

（8）B

# 试题12(2016年上半年试题9)

为了攻击远程主机，通常利用（  ）技术检测远程主机状态。  
（9）A．病毒查杀   
B.端口扫描   
C.QQ聊天   
D.身份认证

**试题分析**

端口扫描器通过选用远程 TCP/IP不同的端口的服务，并记录目标给予的回答，通过这种方法，可以搜集到很多关于目标主机的各种有用的信息。

**试题答案**

（9）B

# 试题13(2015年下半年试题7)

（  ）不属于主动攻击。  
（7）A．流量分析  
B.重放  
C.IP地址欺骗  
D.拒绝服务

**试题分析**

主动攻击包括拒绝服务攻击、分布式拒绝服务（DDos）、信息篡改、资源使用、欺骗、伪装、重放等攻击方法。

**试题答案**

（7）A

# 试题14(2015年下半年试题8)

防火墙不具备（  ）动能。  
（8）A．记录访问过程  
B.查毒  
C.包过滤  
D.代理

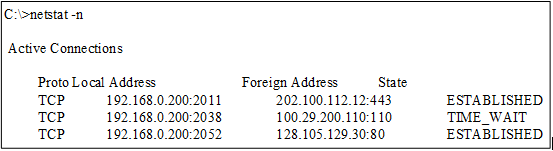
**试题分析**

网络防火墙就是一个位于计算机和它所连接的网络之间的软件。该计算机流入流出的所有网络通信均要经过此防火墙。防火墙对流经它的网络通信进行扫描，这样能够过滤掉一些攻击，以免其在目标计算机上被执行。防火墙还可以关闭不使用的端口。而且它还能禁止特定端口的流出通信，封锁特洛伊木马。最后，它可以禁止来自特殊站点的访问，从而防止来自不明入侵者的所有通信。  
防火墙的功能包括：访问控制；提供基于状态检测技术的ip地址、端口、用户和时间的管理控制；双向nat，提供ip地址转换和ip及tcp/udp端口映射，实现ip复用和隐藏网络结构：代理等。

**试题答案**

（8）B

# 试题15(2015年下半年试题9)

根据下图所示的输出信息，可以确定的是（  ）。  
  
（9）A．本地主机正在使用的端口号是公共端口号   
B.192.168.0.200正在与128.105.129. 30建立连接   
C.本地主机与202.100.112.12建立了安全连接   
D.本地主机正在与100.29.200.110建立连接

**试题分析**

Netstat命令的连接状态包括：  
LISTEN：侦听来自远方的TCP端口的连接请求。  
SYN-SENT：在发送连接请求后等待匹配的连接请求。  
SYN-RECEIVED：在收到和发送一个连接请求后等待对方对连接请求的确认。  
ESTABLISHED：代表一个打开的连接。  
FIN-WAIT-1：等待远程TCP连接中断请求，或先前的连接中断请求的确认。  
FIN-WAIT-2：从远程TCP等待连接中断请求。  
CLOSE-WAIT：等待从本地用户发来的连接中断请求。  
CLOSING：等待远程TCP对连接中断的确认。  
LAST-ACK：等待原来的发向远程TCP的连接中断请求的确认。  
TIME-WAIT：等待足够的时间以确保远程TCP接收到连接中断请求的确认。  
CLOSED：没有任何连接状态。

**试题答案**

（9）C

# 试题16(2015年上半年试题7)

（  ）协议在终端设备与远程站点之间建立安全连接。   
（7）A． ARP   
B.Telnet   
C.SSH   
D.WEP

**试题分析**

SSH 为 Secure Shell 的缩写，由 IETF 的网络工作小组（Network Working Group）所制定；SSH 为建立在应用层和传输层基础上的安全协议。SSH 是目前较可靠，专为远程登录会话和其他网络服务提供安全性的协议。利用 SSH 协议可以有效防止远程管理过程中的信息泄露问题。

**试题答案**

（7）C

# 试题17(2015年上半年试题8-9)

安全需求可划分为物理线路安全、网络安全、系统安全和应用安全。下面的安全需求中属于系统安全的是（  ），属于应用安全的是（  ）。  
（8）A．机房安全  
B.入侵检测  
C.漏洞补丁管理  
D.数据库安全  
  
（9）A．机房安全  
B.入侵检测  
C.漏洞补丁管理  
D.数据库安全

**试题分析**

机房安全属于物理安全，入侵检测属于网络安全，漏洞补丁管理属于系统安全，而数据库安全则是应用安全。

**试题答案**

（8）C（9）D

# 试题18(2014年下半年试题7)

网络系统中，通常把（  ）置于DMZ区。  
（7）A．网络管理服务器   
B.Web服务器   
C.入侵检测服务器   
D.财务管理服务器

**试题分析**

DMZ是英文“demilitarized zone”的缩写，中文名称为“隔离区”，也称“非军事化区”。它是为了解决安装防火墙后外部网络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全系统之间的缓冲区，这个缓冲区位于企业内部网络和外部网络之间的小网络区域内，在这个小网络区域内可以放置一些必须公开的服务器设施，如企业Web服务器、FTP服务器和论坛等。另一方面，通过这样一个DMZ区域，更加有效地保护了内部网络，因为这种网络部署，比起一般的防火墙方案，对攻击者来说又多了一道关卡。

**试题答案**

（7）B

# 试题19(2014年下半年试题8)

以下关于拒绝服务攻击的叙述中，不正确的是（  ）。  
（8）A．拒绝服务攻击的目的是使计算机或者网络无法提供正常的服务   
B.拒绝服务攻击是不断向计算机发起请求来实现的   
C.拒绝服务攻击会造成用户密码的泄漏   
D.DDoS是一种拒绝服务攻击形式

**试题分析**

拒绝服务攻击即攻击者想办法让目标机器停止提供服务或资源访问，是黑客常用的攻击手段之一。这些资源包括磁盘空间、内存、进程甚至网络带宽，从而阻止正常用户的访问。其实对网络带宽进行的消耗性攻击只是拒绝服务攻击的一小部分，只要能够对目标造成麻烦，使某些服务被暂停甚至主机死机，都属于拒绝服务攻击。拒绝服务攻击问题也一直得不到合理的解决，究其原因是因为这是由于网络协议本身的安全缺陷造成的，从而拒绝服务攻击也成为了攻击者的终极手法。攻击者进行拒绝服务攻击，实际上让服务器实现两种效果：一是迫使服务器的缓冲区满，不接收新的请求；二是使用IP欺骗，迫使服务器把合法用户的连接复位，影响合法用户的连接。DDos是分布式Dos的缩写，也是拒绝服务攻击的一种形式。从原理可以看出拒绝服务攻击Dos不会造成密码的泄露。

**试题答案**

（8）C

# 试题20(2014年下半年试题9)

（  ）不是蠕虫病毒。  
（9）A．熊猫烧香   
B.红色代码   
C.冰河   
D.爱虫病毒

**试题分析**

熊猫烧香是一种经过多次变种的“蠕虫病毒”变种，2006年10月16日由25岁的中国湖北武汉新洲区人李俊编写，这是名副其实的病毒，拥有感染传播功能，2007年1月初肆虐网络，它主要通过下载的档案传染，受到感染的机器文件因为被误携带间接对其它计算机程序、系统破坏严重。2013年6月病毒制造者张顺和李俊伙同他人开设网络赌场案，再次获刑。

“红色代码”病毒是2001年一种新型网络病毒，其传播所使用的技术可以充分体现网络时代网络安全与病毒的巧妙结合，将网络蠕虫、计算机病毒、木马程序合为一体，开创了网络病毒传播的新路，可称之为划时代的病毒。

冰河是一种木马软件。

2000年5月4日，一种名为“我爱你”的电脑病毒开始在全球各地迅速传播。这个病毒是通过Microsoft Outlook电子邮件系统传播的，邮件的主题为“I LOVE YOU”，并包含一个附件。一旦在Microsoft Outlook里打开这个邮件，系统就会自动复制并向地址簿中的所有邮件电址发送这个病毒。 “我爱你”病毒，又称“爱虫”病毒，是一种蠕虫病毒，它与1999年的梅丽莎病毒非常相似。据称，这个病毒可以改写本地及网络硬盘上面的某些文件。用户机器染毒以后，邮件系统将会变慢，并可能导致整个网络系统崩溃。

**试题答案**

（9）C

# ！！试题21(2014年下半年试题66)

PPP中的安全认证协议是（  ），它使用三次握手的会话过程传送密文。  
（66）A．MD5  
B.PAP  
C.CHAP  
D.HASH

**试题分析**

一、安全认证介绍

1、PPP的NCP可以承载多种协议的三层数据包。

2、PPP使用LCP控制多种链路的参数（建立、认证、压缩、回拨）

二、PPP的认证类型

1、PPP的pap认证是通过二次握手建立认证（明文不加密）

2、PPP的chap挑战握手认证协议，通过三次握手建立认证（密文采用MD5加密）

3、PPP的双向验证，采用的是chap的主验证风格

4、PPP的加固验证，采用的是两种（pap,chap）验证同时使用

**试题答案**

（66）C

# 试题22(2014年上半年试题7)

以下关于木马程序的叙述中， （  ）。

（7）A．木马程序主要通过移动磁盘传播  
B. 木马程序的客户端运行在攻击者的机器上  
C. 木马程序的目的是使计算机或网络无法提供正常的服务  
D. Sniffer是典型的木马程序

**试题分析**

传播方式：  
1、通过邮件附件、程序下载等形式传播  
2、通过伪装网页登录过程，骗取用户信息进而传播  
3、通过攻击系统安全漏洞传播木马，大量黑客使用专门的黑客工具来传播木马。木马程序危害在于多数有恶意企图，例如占用系统资源，降低电脑效能，危害本机信息安全（盗取QQ帐号、游戏帐号甚至银行帐号），将本机作为工具来攻击其他设备等。Sniffer 是用于拦截通过网络传输的TCP/IP/UDP/ICMP等数据包的一款工具，可用于分析网络应用协议，用于网络编程的调试、监控通过网络传输的数据、检测木马程序等。

**试题答案**

（7）B

# 试题23(2014年上半年试题8)

防火墙的工作层次是决定防火墙效率及安全的主要因素，以下叙述中，正确的是（  ）。   
（8）A． 防火墙工作层次越低，工作效率越高，安全性越高  
B. 防火墙工作层次越低，工作效率越低，安全性越低  
C. 防火墙工作层次越高，工作效率越高，安全性越低  
D. 防火墙工作层次越高，工作效率越低，安全性越高

**试题分析**

防火墙工作层次越低，工作效率越高，安全性越低。  
防火墙工作层次越高，工作效率越低，安全性越高。

**试题答案**

（8）D

# 试题24(2014年上半年试题9)

以下关于包过滤防火墙和代理服务防火墙的叙述中，正确的是（  ）。

（9）A．包过滤成本技术实现成本较高，所以安全性能高  
B.包过滤技术对应用和用户是透明的  
C.代理服务技术安全性较高，可以提高网络整体性能  
D.代理服务技术只能配置成用户认证后才建立连接

**试题分析**

包过滤防火墙工作在网络协议IP层，它只对IP包的源地址、目标地址及相应端口进行处理，因此速度比较快，能够处理的并发连接比较多，缺点是对应用层的攻击无能为力。 代理服务器防火墙将收到的IP包还原成高层协议的通讯数据，比如http连接信息，因此能够对基于高层协议的攻击进行拦截。缺点是处理速度比较慢，能够处理的并发数比较少。

**试题答案**

（9）B

# 试题25(2013年下半年试题7)

下列网络攻击行为中，属于DoS攻击的是（  ）。

（7）A．特洛伊木马攻击   
B.SYN Flooding攻击   
C.端口欺骗攻击   
D.IP欺骗攻击

**试题分析**

DoS是Denial of Service的简称，即拒绝服务，造成DoS的攻击行为被称为DoS攻击，其目的是使计算机或网络无法提供正常的服务。最常见的DoS攻击有计算机网络带宽攻击和连通性攻击。

作个形象的比喻来理解DoS。街头的餐馆是为大众提供餐饮服务，如果一群地痞流氓要DoS餐馆的话，手段会很多，比如霸占着餐桌不结账，堵住餐馆的大门不让路，骚扰餐馆的服务员或厨子不能干活，甚至更恶劣……

SYN Flooding攻击便是Dos攻击的典型代表，该攻击以多个随机的源主机地址向目的路由器发送SYN包，而在收到目的路由器的SYN ACK后并不回应，这样，目的路由器就为这些源主机建立了大量的连接队列，而且由于没有收到ACK一直维护着这些队列，造成了资源的大量消耗而不能向正常请求提供服务，甚至导致路由器崩溃。服务器要等待超时（Time Out）才能断开已分配的资源。

**试题答案**

（7）B

# 试题26(2013年下半年试题8)

PKI体制中，保证数字证书不被篡改的方法是（  ）。

（8）A．用CA的私钥对数字证书签名   
B.用CA的公钥对数字证书签名   
C.用证书主人的私钥对数字证书签名   
D.用证书主人的公钥对数字证书签名

**试题分析**

在PKI体制中，识别数字证书的颁发机构以及通过该机构核实证书的有效性，了解证书是否被篡改均通过一种机制——对数字证书做数字签名。数字签名将由CA机构使用自己的私钥进行。

**试题答案**

（8）A

# 试题27(2013年下半年试题9)

下列算法中，不属于公开密钥加密算法的是（  ）。

（9）A．ECC   
B.DSA   
C.RSA   
D.DES

**试题分析**

DES算法为密码体制中的对称密码体制。

**试题答案**

（9）D

# 试题28(2013年上半年试题7)

利用报文摘要算法生成报文接要的目的是（  ）。

（7）A．验证通信对方的身份防止假冒   
B.对传输数据进行加密防止数据被窃听   
C.防止发送言否认发送过数据   
D.防止发送的报文被篡改

**试题分析**

报文摘要是用来保证数据完整性的。传输的数据一旦被修改，摘要就不同了。只要对比两次摘要就可确定数据是否被修改过。

**试题答案**

（7）D

# 试题29(2013年上半年试题8)

防火墙通常分为内网、外网和DMZ三个区域，按照受保护程序，从高到低正确的排列次序为（  ）。

（8）A．内网、外网和DMZ   
B.外网、内网和DMZ   
C.DMZ、内网和外网   
D.内网、DMZ和外网

**试题分析**

DMZ是为了解决安装防火墙后外部网络不能访问内部网络服务器的问题，而设立的缓冲区，这个缓冲区位于内部网络和外部网络之间的小网络区域内。

**试题答案**

（8）D

# 试题30(2013年上半年试题9)

近年来，在我国出现各类病毒中（  ）病毒通过木马形式感染智能手机。

（9）A．欢乐时光   
B.熊猫烧香   
C.X卧底   
D.CIH

**试题分析**

 X卧底软件是一种安装在手机里的监控软件。

**试题答案**

（9）C

# 试题31(2012年下半年试题7)

下列安全协议中，与TLS最接近的协议是（  ）。

（7）A．PGP   
B.SSL   
C.HTTPS   
D.IPSec

**试题分析**

TLS是安全传输层协议的简称，用于在两个通信应用程序之间提供保密性和数据完整性。  
SSL是安全套接层协议的简称，它也是一种为网络通信提供安全和数据完整性的协议，它与TLS非常接近，它们都是在传输层对网络连接进行加密。  
PGP是一个基于RSA公匙加密体系的邮件加密软件。，用它可以对邮件保密以防止非授权者阅读。  
HTTPS即安全版的HTTP（超文本传输协议）的，它是在HTTP下加入SSL层，HTTPS的安全基础就是SSL。  
IPSec是网络层的安全协议，它通过使用加密的安全服务来确保在网络上进行保密而安全的通讯。

**试题答案**

（7）B

# ！！试题32(2012年下半年试题8-9)

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（  ）验证该证书的真伪，然后利用（  ）验证M的真实性。

（8）A．CA的公钥   
B.B的私钥   
C.A的公钥   
D.B的公钥   
  
（9）A．CA的公钥   
B.B的私钥   
C.A的公钥   
D.B的公钥

**试题分析**

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。  
因此要想验证用户A数字证书的真伪，需要用CA的公钥来完成，而因为消息M是A用其私钥加密后的结果，要验证其真实性，就需要用A的公钥来解密，如果能解密，说明消息M是A用其私钥进行了签名的。

**试题答案**

（8）A（9）C

# 试题33(2012年上半年试题7)

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（  ）验证该消息的真实性。

（7）A．甲的公钥   
B.甲的私钥   
C.乙的公钥   
D.乙的私钥

**试题分析**

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：先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。

**试题答案**

（7）A

# 试题34(2012年上半年试题9)

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（  ）。

（9）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。

**试题答案**

（9）B

# 试题35(2011年下半年试题8)

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（  ）。

（8）A．特洛伊木马   
B.蠕虫病毒   
C.宏病毒   
D.CIH病毒

**试题分析**

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。

**试题答案**

（8）A

# 试题36(2011年下半年试题9)

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

（9）A．CA的公钥   
B.CA的私钥   
C.B的公钥   
D.B的私钥

**试题分析**

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。

**试题答案**

（9）B

# 试题37(2011年上半年试题7)

用户A从CA获得用户B的数字证书，并利用（  ）验证数字证书的真实性。

（7）A．B的公钥   
B.B的私钥   
C.CA的公钥   
D.CA的私钥

**试题分析**

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。

**试题答案**

（7）C

# 试题38(2011年上半年试题8)

宏病毒一般感染以（  ）为扩展名的文件。

（8）A．EXE   
B.COM   
C.DOC   
D.DLL

**试题分析**

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。

**试题答案**

（8）C

# 试题39(2011年上半年试题9)

在IE浏览器中，安全级别最高的区域设置是（  ）。

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

**试题分析**

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。

**试题答案**

（9）D

# 试题40(2010年下半年试题7)

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（  ）攻击。

（7）A．拒绝服务   
B.口令入侵   
C.网络监听   
D.IP欺骗

**试题分析**

拒绝服务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。

**试题答案**

（7）A

# 试题41(2010年下半年试题8)

ARP攻击造成网络无法跨网段通信的原因是（  ）。

（8）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。

**试题答案**

（8）B

# 试题42(2010年下半年试题9)

下列选项中，防范网络监听最有效的方法是（  ）。

（9）A．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。

**试题答案**

（9）C

# ！！！RAS 试题43(2010年下半年试题66-67)

公钥体系中，私钥用于（  ），公钥用于（  ）。

（66）A．解密和签名   
B.加密和签名   
C.解密和认证   
D.加密和认证   
  
（67）A．解密和签名   
B.加密和签名   
C.解密和认证   
D.加密和认证

**试题分析**

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。

**试题答案**

（66）A（67）D