2022 知识点练习->上午->5.信息安全答案解析

1. A

解析1：

本题计算机网络相关交互协议。

用户在电子商务网站上使用网上银行支付时，必须通过支付网关才能在Internet与 银行专用网之间进行数据交换。

A、支付网关：是银行金融网络系统和Internet网络之间的接口，是由银行操作的将Internet上传输的数据转换为金融机构内部数据的一组服务器设备，或由指派的第三方处理商家支付信息和顾客的支付指令。

B、防病毒网关：防病毒网关是一种网络设备，用以保护网络内（一般是局域网）进出数据的安全。主要体现在病毒杀除、关键字过滤（如色情、反动）、垃圾邮件阻止的功能，同时部分设备也具有一定防火墙（划分Vlan）的功能。如果与互联网相连，就需要网关的防病毒软件。

C、出口路由器：一般指局域网出外网的路由器，或者指一个企业、小区、单位、城域网、省级网络、国家网络与外界网络直接相连的那台路由器。在网络间起网关的作用，是读取每一个数据包中的地址然后决定如何传送的专用智能性的网络设备。

D、堡垒主机：堡垒主机是一种被强化的可以防御进攻的计算机，作为进入内部网络的一个检查点，以达到把整个网络的安全问题集中在某个主机上解决，从而省时省力，不用考虑其它主机的安全的目的。

2. B

解析1：

考查应用级关于屏蔽子网的防火墙。

在一个用路由器连接的局域网中,我们可以将网络划分为三个区域：安全级别最高的LAN Area（内网）,安全级别中等的DMZ区域和安全级别最低的Internet区域（外网）。三个区域因担负不同的任务而拥有不同的访问策略。我们在配置一个拥有DMZ区的网络的时候通常定义以下的访问控制策略以实现DMZ区的屏障功能。

3. C

解析1：

考查包过滤防火墙的工作原理。

包过滤防火墙是最简单的一种防火墙，它在网络层截获网络数据包，根据防火墙的规则表，来检测攻击行为。包过滤防火墙一般作用在网络层（IP层），故也称网络层防火墙（Network Lev Firewall）或IP过滤器（IP filters）。数据包过滤（Packet Filtering）是指在网络层对数据包进行分析、选择。通过检查数据流中每一个数据包的源IP地址、目的IP地址、源端口号、目的端口号、协议类型等因素或它们的组合来确定是否允许该数据包通过。在网络层提供较低级别的安全防护和控制。

4. A

解析1：

IGMP：属于网络的组播协议，不能实现相关应用层的远程登录。

SSH：SSH 为建立在应用层基础上的安全协议。SSH 是较可靠，专为远程登录会话和其他网络服务提供安全性的协议。

Telnet：Telnet协议是TCP/IP协议族中的一员，是Internet远程登录服务的标准协议和主要方式。它为用户提供了在本地计算机上完成远程主机工作的能力。在终端使用者的电脑上使用telnet程序，用它连接到服务器。

RFB：RFB （ Remote Frame Buffer 远程帧缓冲） 协议是一个用于远程访问图形用户界面的简单协议。由于 RFB 协议工作在帧缓冲层，因此它适用于所有的窗口系统和应用程序。

5. C

解析1：

AES是一个迭代的、对称密钥分组的密码，它可以使用128、192和256位密钥。并且使用128位分组加密和解密数据。

6. C

解析1：

部署防火墙：防火墙技术是通过有机结合各类用于安全管理与筛选的软件和硬件设备，帮助计算机网络于其内、外网之间构建一道相对隔绝的保护屏障，以保护用户资料与信息安全性的一种技术，并不能有效的防范病毒。

部署入侵检测系统：入侵检测系统（intrusion detection system，简称"IDS"）是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备。是对一种网络传输的监视技术，并不能有效的防范病毒。

安装并及时升级防病毒软件：针对于防病毒软件本身就是防范病毒最有效最直接的方式。

定期备份数据文件：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。是为了防止系统数据流失，不能有效的防范病毒。

7. A

解析1：

A选项：IPSec工作于网络层，为IP数据报文进行加密。

B选项：PP2P工作于数据链路层，用于链路加密。

C选项：HTTPS是HTTP与SSL的结合体，为传输层以上层次数据加密。

D选项：TLS安全传输层协议用于在两个通信应用程序之间提供保密性和数据完整性。

8. D

解析1：

SQL注入攻击，就是通过把SQL命令插入到 Web表单提交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令。其首要目的是获取数据库访问权限。

9. B

解析1：

典型的对称加密算法：DES，3DES，AES等。

典型的非对称加密算法：RSA，ECC等。本题选B选项。

典型的摘要算法：SHA，MD5等。

10. B

解析1：

A选项：跨站脚本（cross-site scripting，XSS），一种安全攻击，其中，攻击者在看上去来源可靠的链接中恶意嵌入译码。它允许恶意用户将代码注入到网页上，其他用户在观看网页时就会受到影响。不影响服务的提供。

B选项：拒绝服务，对信息或其它资源的合法访问被无条件地阻止，会让服务器拒绝提供服务。本题选择B选项。

C选项：信息篡改，指主动攻击者将窃听到的信息进行修改(如删除和/或替代部分或者全部信息)之后再将信息传送给原本的接受者。与提供服务无关。

D选项：口令猜测，攻击者攻击目标时常常把破译用户的口令作为攻击的开始。只要攻击者能猜测或者确定用户的口令，他就能获得机器或者网络的访问权，并能访问到用户能访问到的任何资源。与提供服务无关。

11. C

解析1：

A选项：TLS安全传输层协议用于在两个通信应用程序之间提供保密性和数据完整性。

B选项：TCP是可靠的传输层协议，与安全无关。

C选项：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。本题选择C选项。

D选项：TFTP（Trivial File Transfer Protocol,简单文件传输协议）是TCP/IP协议族中的一个用来在客户机与服务器之间进行简单文件传输的协议，提供不复杂、开销不大的文件传输服务。

12. A

解析1：

本题考查信息安全知识。

数据的机密性（保密性）是指数据在传输过程中不能被非授权者偷看；

数据的完整性是指数据在传输过程中不能被非法篡改，本题涉及到修改的只有完整性；

数据的真实性（不可抵赖性）是指信息的发送者身份的确认或系统中有关主体的身份确认，这样可以保证信息的可信度；

可用性指的是发送者和接受者双方的通信方式正常。

故正确答案选择A选项。

13. A

解析1：

本题考查信息安全机制相关问题。

安全审计对主体访问和适用客体的情况进行记录和审查，以保证安全规则被正确执行，并帮助分析安全事故产生的原因。与访问控制无关。

授权、确定存取权限、实施存取权限都是安全访问控制的任务，故正确答案选择A选项。

14. C

解析1：

本题考查信息安全认证和加密的情况。

认证一般有账户名/口令认证、使用摘要算法认证和基于PKI的认证。

认证只能阻止主动攻击，不能阻止被动攻击。A、B、D都说法都是正确的，C选项说法错误。

故答案选择C选项。

15. AB

解析1：

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CA的公钥验证CA的签名，从而确认数字证书的有效性，然后验证网站的真伪。

16. B

解析1：

重放攻击（Replay Attacks）又称重播攻击、回放攻击或新鲜性攻击（Freshness Attacks），是指攻击者发送一个目的主机已接收过的包，来达到欺骗系统的目的，主要用于身份认证过程，破坏认证的正确性。

Kerberos系统采用的是时间戳方案来防止重放攻击，这种方案中，发送的数据包是带时间戳的，服务器可以根据时间戳来判断是否为重放包，以此防止重放攻击。

17. D

解析1：

公开密钥加密（public-key cryptography），也称为非对称加密（asymmetric cryptography），一种密码学算法类型，在这种密码学方法中，需要一对密钥，一个是私人密钥，另一个则是公开密钥。

常见的公钥加密算法有： RSA、ElGamal、背包算法、Rabin（RSA的特例）、迪菲 - 赫尔曼密钥交换协议中的公钥加密算法、椭圆曲线加密算法（Elliptic Curve Cryptography, ECC）；DSA数字签名（又称公钥数字签名），将摘要信息用发送者的私钥加密，接收者只有用发送者的公钥才能解密被加密的摘要信息，也是属于公开密钥加密算法。

DES是典型的私钥加密体制，属于对称加密，不属于公开秘钥加密，所以本题选择D选项。

18. C

解析1：
MIME它是一个多用途互联网邮件扩展类型的标准，扩展了电子邮件标准，使其能够支持多媒体信息传输，与安全无关。与安全电子邮件相关的是S/MIME安全多用途互联网邮件扩展协议。

A选项SSL和B选项HTTPS涉及邮件传输过程的安全，D选项PGP（全称：Pretty Good Privacy，优良保密协议），是一套用于信息加密、验证的应用程序，可用于加密电子邮件内容。

19. C

解析1：
启用无痕浏览模式，下载文件仍然会被保留。

20. D

解析1：
震网（Stuxnet），指一种蠕虫病毒。它的复杂程度远超一般电脑黑客的能力。这种震网（Stuxnet）病毒于2010年6月首次被检测出来，是第一个专门定向攻击真实世界中基础（能源）设施的"蠕虫"病毒，比如核电站，水坝，国家电网。
A选项引导区病毒破坏的是引导盘、文件目录等，B选项宏病毒破坏的是OFFICE文件相关，C选项木马的作用一般强调控制操作。

21. AD

解析1：
第一空考查的是关于用户身份进行认证也就是数字签名的认证，这里使用的应该是发送方的公钥，这4个选项中，能包含发送方公钥的只有A选项数字证书；
第二空确保消息不可否认，也就是考查确保发送者身份的不可抵赖，所以这里使用的应该是发送方的数字签名。

22. C

解析1：
MIME它是一个互联网标准，扩展了电子邮件标准，使其能够支持，与安全无关。与安全电子邮件相关的是S/MIME安全多用途互联网邮件扩展协议。
A选项SSL和B选项HTTPS涉及邮件传输过程的安全，D选项PGP（全称：Pretty Good Privacy，优良保密协议），是一套用于信息加密、验证的应用程序，可用于加密电子邮件内容。

23. B

解析1：
包过滤防火墙：包过滤防火墙一般有一个包检查块（通常称为包过滤器），数据包过滤可以根据数据包头中的各项信息来控制站点与站点、站点与网络、网络与网络之间的相互访问，但无法控制传输数据的内容，因为内容是应用层数据，而包过滤器处在网络层和数据链路层之间，不符合本题要求。
应用级网关防火墙：应用代理网关防火墙彻底隔断内网与外网的直接通信，内网用户对外网的访问变成防火墙对外网的访问，然后再由防火墙转发给内网用户。所有的通信都必须经应用层代理软件转发，它可对应用层的通信数据流进行监控和过滤。
数据库防火墙：数据库防火墙技术是针对关系型数据库保护需求应运而生的一种数据库安全主动防御技术，数据库防火墙部署于应用服务器和数据库之间，不符合本题要求。
Web防火墙：Web防火墙是入侵检测系统，入侵防御系统的一种。从广义上来说，Web应用防火墙就是应用级的网站安全综合解决方案，与我们所讲到的防火墙概念有一定区别，不符合本题要求。

24. B

解析1：《软件设计师教程（第5版）》P45页：MD5是一种摘要算法，经过一系列处理后，算法的输出由四个32位分组组成，将这四个32位分组级联后将生成一个128位散列值。

25. D

解析1：《软件设计师教程（第5版）》P566页：计算机病毒具有隐蔽性、传染性、潜伏性、触发性和破坏性等特定。因此本题选择D选项，自毁性不属于计算机病毒的特征。

26. B

解析1： 对于非对称加密又称为公开密钥加密，而共享密钥加密指对称加密。常见的对称加密算法有：DES，三重DES、RC-5、IDEA、AES，因此本题选择B选项。

27. A

解析1： 重放攻击（Replay Attacks）又称重播攻击、回放攻击，是指攻击者发送一个目的主机已接收过的包，来达到欺骗系统的目的，主要用于身份认证过程，破坏认证的正确性。重放攻击可以由发起者，也可以由拦截并重发该数据的敌方进行。

28. D

解析1： 加强内防内控主要通过访问授权、安全策略、安全检查与行为审计等多种安全手段的综合应用来实现。终端接入的数量影响的是网络的规模、数据交换的性能，不是内防内控关注的重点。

29. BA

解析1： 数字签名技术是将摘要信息用发送者的私钥加密，与原文一起传送给接收者。接收者只有用发送者的公钥才能解密被加密的摘要信息，然后用HASH函数对收到的原文产生一个摘要信息，与解密的摘要信息对比。如果相同，则说明收到的信息是完整的，在传输过程中没有被修改，否则说明信息被修改过，因此数字签名能够验证信息的完整性。
数字签名是个加密的过程，数字签名验证是个解密的过程。保证信息传输的完整性、发送者的身份认证、防止交易中的抵赖发生。

30. D

解析1： SSH 为 Secure Shell 的缩写，由 IETF 的网络小组（Network Working Group）所制定；SSH 为建立在应用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。

31. D

解析1： D选项不是防火墙的功能特性。

32. D

解析1： 漏洞扫描为另一种安全防护策略。

33. C

解析1：
A选项拒绝服务（DOS）： 对信息或其它资源的合法访问被无条件地阻止。

B选项会话拦截：未授权使用一个已经建立的会话。

D选项修改数据命令：截获并修改网络中传输的数据命令。

ABD为主动攻击。

C选项系统干涉：指的是攻击者获取系统访问权，从而干涉系统的正常运行，一般可以归于被动攻击。

34. CB

解析1： 1、HTTPS是基于SSL(Secure Sockets Layer 安全套接层)的。
2、http的端口号为80，而HTTPS的默认端口是443，注意区分。

35. D

解析1： 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$I_1$与$I_2$的公钥交换倒是可以做到互信，因为$I_1$与$I_2$的公钥正是验证CA签名的依据。所以本题应选D。

36. D

解析1： 本题考查的是信息安全中的加密算法。其中：

对大量明文进行加密，考虑效率问题，一般采用对称加密。

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。

37. B

解析1： 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。

38. C

解析1：

安全防范体系的层次划分：

（1）物理环境的安全性。包括通信线路、物理设备和机房的安全等。物理层的安全主要体现在通信线路的可靠性（线路备份、网管软件和传输介质）、软硬件设备的安全性（替换设备、拆卸设备、增加设备）、设备的备份、防灾害能力、防干扰能力、设备的运行环境（温度、湿度、烟尘）和不间断电源保障等。

（2）操作系统的安全性。主要表现在三个方面，一是操作系统本身的缺陷带来的不安全因素，主要包括身份认证、访问控制和系统漏洞等；二是对操作系统的安全配置问题；三是病毒对操作系统的威胁。

（3）网络的安全性。网络层的安全问题主要体现在计算机网络方面的安全性，包括网络层身份认证、网络资源的访问控制、数据传输的保密与完整性、远程接入的安全、域名系统的安全、路由系统的安全、入侵检测的手段和网络设施防病毒等。

（4）应用的安全性。由提供服务所采用的应用软件和数据的安全性产生，包括Web服务、电子邮件系统和DNS等。此外，还包括病毒对系统的威胁。

（5）管理的安全性。包括安全技术和设备的管理、安全管理制度、部门与人员的组织规则等。管理的制度化极大程度地影响着整个计算机网络的安全，严格的安全管理制度、明确的部门安全职责划分与合理的人员角色配置，都可以在很大程度上降低其他层次的安全漏洞。

本题选择C选项。A选项属于物理环境的安全性。B、D选项属于网络的安全性。

39. D

解析1： 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。

40. A

解析1： IDEA算法和RC4算法都是对称加密算法，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。

41. B

解析1： 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。

42. B

解析1： 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。

43. B

解析1： 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。

44. A

解析1： 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。

45. CD

解析1： 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。

安全防范体系的层次划分：
（1）物理环境的安全性。包括通信线路、物理设备和机房的安全等。物理层的安全主要体现在通信线路的可靠性（线路备份、网管软件和传输介质）、软硬件设备的安全性（替换设备、拆卸设备、增加设备）、设备的备份、防灾害能力、防干扰能力、设备的运行环境（温度、湿度、烟尘）和不间断电源保障等。
（2）操作系统的安全性。主要表现在三个方面，一是操作系统本身的缺陷带来的不安全因素，主要包括身份认证、访问控制和系统漏洞等；二是对操作系统的安全配置问题；三是病毒对操作系统的威胁。
（3）网络的安全性。网络层的安全问题主要体现在计算机网络方面的安全性，包括网络层身份认证、网络资源的访问控制、数据传输的保密与完整性、远程接入的安全、域名系统的安全、路由系统的安全、入侵检测的手段和网络设施防病毒等。
（4）应用的安全性。由提供服务所采用的应用软件和数据的安全性产生，包括Web服务、电子邮件系统和DNS等。此外，还包括病毒对系统的威胁。
（5）管理的安全性。包括安全技术和设备的管理、安全管理制度、部门与人员的组织规则等。管理的制度化极大程度地影响着整个计算机网络的安全，严格的安全管理制度、明确的部门安全职责划分与合理的人员角色配置，都可以在很大程度上降低其他层次的安全漏洞。

46. C

解析1： 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。

47. C

解析1：
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质询握手认证协议，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

48. C

解析1：

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他计算机程序、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。

49. C

解析1： 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。

50. B

解析1： 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。

51. B

解析1：

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，包过滤成本与它的安全性能没有因果关系，而应用程序和用户对于包过滤的过程并不需要了解，因此该技术对应用和用户是透明的，本题选择B选项。

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，所以不能提高网络整体性能，而代理对于用户认证可以设置。

52. D

解析1：

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。

53. B

解析1：

传播方式：

1、通过邮件附件、程序下载等形式传播，因此A选项错误。

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账号、游戏账号甚至银行账号），将本机作为工具来攻击其他设备等，因此，C选项错误；

4、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，因此D选项错误。

本题只有B选项是正确的。

54. D

解析1：
公开密钥加密（public-key cryptography），也称为非对称加密（asymmetric cryptography），一种密码学算法类型，在这种密码学方法中，需要一对密钥，一个是私人密钥，另一个则是公开密钥。

常见的公钥加密算法有： RSA、ElGamal、背包算法、Rabin（RSA的特例）、迪菲 - 赫尔曼密钥交换协议中的公钥加密算法、椭圆曲线加密算法（Elliptic Curve Cryptography, ECC）；

DES是典型的私钥加密体制，属于对称加密。

DSA数字签名（又称公钥数字签名），将摘要信息用发送者的私钥加密，接收者只有用发送者的公钥才能解密被加密的摘要信息。

55. A

解析1：
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。

56. B

解析1：
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。

57. C

解析1：
X卧底软件是一种安装在手机里的监控软件。

58. D

解析1：
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。

59. D

解析1：
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。

60. AC

解析1：
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。

61. B

解析1：

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。

62．B

解析1：

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。

63．A

解析1：

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（认证），若能认证，则表明该信息确实是由A发送的。这就是数字签名技术。

64．B

解析1：

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。

65．A

解析1：
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。

66. B

解析1：
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，利用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。

67. D

解析1：
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。

68. C

解析1：
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。

69. C

解析1：
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。

70. AD

解析1：
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。

71. C

解析1：
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。

72. B

解析1：
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。

73. A

解析1：
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。

74. DB

解析1：
本题考查计算机病毒方面的基础知识
计算机病毒的分类方法有许多种，按照最通用的区分方式，即根据其感染的途径以及采用的技术区分，计算机病毒可分为文件型计算机病毒、引导型计算机病毒、宏病毒和目录型计算机病毒。
文件型计算机病毒感染可执行文件（包括EXE和COM文件）。
引导型计算机病毒影响软盘或硬盘的引导扇区。
目录型计算机病毒能够修改硬盘上存储的所有文件的地址。
宏病毒感染的对象是使用某些程序创建的文本文档、数据库、电子表格等文件，从文件名可以看出Macro.Melissa是一种宏病毒，所以题中两空的答案是D和B。

75. C

解析1：
本题考查对网络安全中常用攻击方法的了解。
多个网络设备上的程序在短时间内同时向某个服务器产生大量的请求，导致该服务器不堪重负，这是典型的分布式拒绝服务攻击（DDoS）。

76. AD

解析1：
本题考查有关密码的基础知识。
DES是对称密钥密码算法，它的加密密钥和解密密钥是相同的。RSA是非对称密钥密码算法，它使用不同的密钥分别用于加密和解密数据，还可以用于数字签名。对称密钥密码算法的效率要比非对称密钥密码算法高很多，适用于对文件等大量的数据进行加密。

77. D

解析1：
熊猫烧香是一种感染型的蠕虫病毒，它能感染系统中exe，~、pif， src， html和asp等文件，还能中止大量的反病毒软件进程并且会删除扩展名为gho的文件，该文件是一系统备份工具GHOST的备份文件，使用户的系统备份文件丢失。
被感染的用户系统中所有.exe可执行文件全部被改成熊猫举着三柱香的模样。

78. B

解析1：
多形病毒是一种较为高级的病毒，这种病毒在每次感染后会改变自己。

79. C

解析1：

网络攻击是以网络为手段窃取网络上其他计算机的资源或特权，对其安全性或可用性进行破坏的行为。网络攻击又可分为主动攻击和被动攻击。被动攻击就是网络窃听，截取数据包并进行分析，从中窃取重要的敏感信息。被动攻击很难被发现，因此预防很重要，防止被动攻击的主要手段是数据加密传输。为了保护网络资源免受威胁和攻击，在密码学及安全协议的基础上发展了网络安全体系中的5类安全服务，它们是身份认证、访问控制、数据保密、数据完整性和不可否认。对这5类安全服务，国际标准化组织ISO已经有了明确的定义。主动攻击包括窃取、篡改、假冒和破坏。字典式口令猜测，IP地址欺骗和服务拒绝攻击等都属于主动攻击。一个好的身份认证系统（包括数据加密、数据完整性校验、数字签名和访问控制等安全机制）可以用于防范主动攻击，但要想杜绝主动攻击很困难，因此对付主动攻击的另一措施是及时发现并及时恢复所造成的破坏，现在有很多实用的攻击检测工具。

常用的有以下9种网络攻击方法。

1.获取口令。

2.放置特洛伊木马程序。

3.WWW的欺骗技术。

4.电子邮件攻击。

5.通过一个节点来攻击其他节点。

6.网络监听。

7.寻找系统漏洞。

8.利用账号进行攻击。

9.偷取特权。

80. A

解析1：

本题考查防火墙的概念。防火墙是指设置在不同网络或网络安全域之间的一系列部件组合，是不同网络或网络安全域之间信息的唯一出入口，能根据安全策略控制出入网络的信息流。

防火墙一般由软件以及支持该软件运行的硬件系统构成,能控制经过防火墙的双向信息，而不仅仅是某个方向的信息;防火墙可以过滤一些网络攻击，但一般无法定位攻击。防火墙的主要支撑技术是包过滤技术。

从上面的内容可以看出，B、C、D三个选项都是错误的，只有A是正确的。

81. CA

解析1：

试题（7）正确答案为C，因为删除服务器中的ping.exe和cmd.exe会影响服务器运行ping命令和一些基于命令行的程序。ping命令测试机器联通情况实际上是使用了ICMP协议，因此，关闭服务器中的ICMP端口可以使别的计算机不能通过ping命令测试服务器的连通情况。

试题（8）正确答案为A，因为Telnet使用的是TCP协议，缺省情况下使用23端口。

82. B

解析1：

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。

83. D

解析1：

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。

84. C

解析1：

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。

85. A

解析1：

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的签名来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。

86. C

解析1：

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。

87. D

解析1：

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。