3. 屏蔽主机结构

屏蔽主机结构将所有的外部主机强制与一个堡垒主机相连，从而不允许它们直接与内部网络的主机相连，因此屏蔽主机结构是由包过滤路由器和堡垒主机组成的。堡垒主机是 Internet 上的主机能连接到的唯一的内部网络上的系统。任何外部的系统要访问内部的系统或服务都必须先连接到这台主机。因此堡垒主机要保持更高等级的主机安全。屏蔽主机的优点是：实现了网络层和应用层的安全，安全性较高。缺点是：堡垒主机一旦被绕过，则堡垒主机和其他内部网络的主机之间没有任何保护网络安全的措施，内网将暴露。

4. 屏蔽子网结构

屏蔽子网结构使用了两个屏蔽路由器和两个堡垒主机。在该系统中，从外部包过滤路由器开始的部分是由网络系统所属的单位组建的，属于内部网络，也称为“DMZ 网络”。外部包过滤路由器与外部堡垒主机构成了防火墙的过滤子网；内部包过滤路由器和内部堡垒主机则用于对内部网络进行进一步的保护。屏蔽子网结构的优点是：支持网络层和应用层的安全功能。

7.6 试题分析

1. 下列行为不属于网络攻击的是_____。（2007 年上半年）

A. 连续不停 ping 某台主机　　B. 发送带病毒和木马的电子邮件

C. 向多个邮箱群发一封电子邮件　　D. 暴力破解服务器密码

【分析】：本题考查网络攻击的相关知识。

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。主动攻击包括窃取、篡改、假冒和破坏。IP 地址欺骗和服务拒绝攻击等都属于主动攻击。一个好的身份验证系统可以用于防范主动攻击，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 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 欺骗。

④ 电子邮件攻击。

⑤ 通过一个结点来攻击其他结点。

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。

ping 程序一般是用于确定本地主机是否能与另一台主机交换（发送与接收）数据报。但向某一 IP 发送大量的 ping，可能会严重堵塞网络，占用大量的系统资源，甚至造成系统崩溃，所以连续不停 ping 某台主机属于网络攻击。电子邮件攻击主要表现为两种方式：一是电子邮件轰炸

和电子邮件“滚雪球”，也就是通常所说的邮件炸弹，指的是用伪造的 IP 地址和电子邮件地址向同一信箱发送数以千万计甚至无穷多次的内容相同的垃圾邮件，致使受害人邮箱被“爆”，严重者可能会给电子邮件服务器操作系统带来危险，甚至导致系统瘫痪；二是电子邮件欺骗，攻击者佯称自己为系统管理员（邮件地址和系统管理员完全相同），给用户发送邮件要求用户修改口令或在貌似正常的附件中加载病毒或其他木马程序。但向多个邮箱群发一封电子邮件是正常的网络应用，不属于网络攻击。故选项 C 是正确的。

【参考答案】：C

2. 多形病毒指的是_____的计算机病毒。（2007 年上半年）

A. 可在反病毒检测时隐藏自己　　B. 每次感染都会改变自己

C. 可以通过不同的渠道进行传播　　D. 可以根据不同环境造成不同破坏

【分析】：本题考查多形病毒的相关知识。

多形病毒是指采用特殊加密技术编写的病毒，这种病毒在每感染一个对象时，采用随机方法对病毒主体进行加密。多形病毒主要是针对查毒软件而设计的，所以随着这类病毒的增多，使得查毒软件的编写变得更困难，还会带来许多的误报。多形病毒在每次感染时，放入宿主程序的代码互不相同，不断变化，即在每次感染后会改变自己。故选项 B 是正确的。

【参考答案】：B

3. 感染“熊猫烧香”病毒后的计算机不会出现_____的情况。（2007 年上半年）

A. 执行文件图标变成熊猫烧香　　B. 用户信息被泄露

C. 系统运行变慢　　D. 破坏计算机主板

【分析】：本题考查“熊猫烧香”病毒的相关知识。

“熊猫烧香”病毒是一种感染型的蠕虫病毒，它能感染系统中. exe、. com、. pdf、. 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 可执行文件图标全部被改成熊猫举着三根香的模样。“熊猫烧香”病毒一般情况下是不会破坏计算机主板的。故选项 D 是正确的。

【参考答案】：D

4. 某网站向 CA 申请了数字证书。用户登录该网站时，通过验证__（1）__，可确认该数字证书的有效性，从而__（2）__。（2007 年下半年）

（1）A. CA 的签名　B. 网站的签名　C. 会话密钥　D. DES 密码

（2）A. 向网站确认自己的身份　　B. 获取访问网站的权限

C. 和网站进行双向认证　　D. 验证该网站的真伪

【分析】：本题考查数字证书的相关知识。

数字证书是由认证中心（CA）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 Internet 交往中用它来证明自己的身份和识别对方的身份。数字证书能够验证一个实体身份，而这是在保证数字证书本身有效性这一前提下才能够实现的。验证数字证书的有效性是通过验证颁发证书的 CA 的签名实现的。作为一种数字证书，服务器证书被安装于服务器设备上，用来证明服务器的身份和进行通信加密。服务器证书可以用来防止假冒站点。故（1）中选项 A 是正确的，（2）中选项 D 是正确的。

【参考答案】:(1)A (2)D

5. 风险分析在软件项目开发中具有重要作用,包括风险识别、风险预测、风险评估和风险控制等。建立风险条目检查表是__(1)__时的活动,描述风险的结果是__(2)__时的活动。(2008年上半年)

(1) A. 风险识别 B. 风险预测 C. 风险评估 D. 风险控制

(2) A. 风险识别 B. 风险预测 C. 风险评估 D. 风险控制

【分析】:本题考查软件开发过程中的风险分析的基础知识。

风险分析包括风险识别、风险预测、风险评估和风险控制4个不同的活动。在风险识别过程中,要识别潜在的预算、进度、个体、资源、用户和需求等方面的问题及其对整个项目的影响,并建立风险条目检查表,列出所有可能的风险事项。在风险预测过程中,需建立一个风险可能性的参考标准,描述风险条目的结果,估计风险对项目的影响等。故(1)中选项A是正确的,(2)中选项B是正确的。

【参考答案】:(1)A (2)B

7.7 模拟训练

1. 下面不属于木马特征的是_____。

A. 自动更换文件名,难以被发现

B. 程序执行时不占太多系统资源

C. 不需要服务端用户的允许就能获得系统的使用权

D. 造成缓冲区的溢出,破坏程序的堆栈

2. 防火墙按自身的体系结构分为_____。

A. 软件防火墙和硬件防火墙 B. 包过滤型防火墙和双宿网关

C. 百兆防火墙和千兆防火墙 D. 主机防火墙和网络防火墙

3. 下面关于网络入侵检测的叙述不正确的是_____。

A. 占用资源少 B. 攻击者不易转移证据

C. 容易处理加密的会话过程 D. 检测速度快

4. 基于SET协议的电子商务系统中对商家和持卡人进行认证的是_____。

A. 收单银行 B. 支付网关

C. 认证中心 D. 发卡银行

5. 下面关于病毒的叙述正确的是_____。

A. 病毒可以是一个程序 B. 病毒可以是一段可执行代码

C. 病毒能够自我复制 D. ABC都正确

6. 图7.2所示的防火墙结构属于_____。

A. 简单的双宿主主机结构 B. 单DMZ防火墙结构

C. 带有屏蔽路由器的单网段防火墙结构 D. 双DMZ防火墙结构

7. 电子商务交易必须具备抗抵赖性,目的在于防止_____。

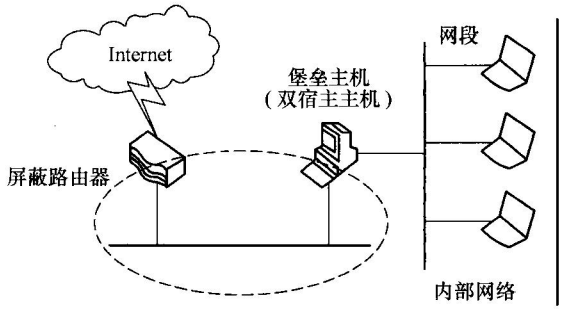

图 7.2 网络拓扑图

A. 一个实体假装成另一个实体

B. 参与交易的一方否认曾经发生过此次交易

C. 他人对数据进行非授权的修改、破坏

D. 信息从被监视的通信过程中泄露出去

8. 某公司使用包过滤制进出公司局域网的数据，在不考虑使用代理服务器的情况下，下面描述错误的是该防火墙能够_____。

A. 使公司员工只能访问 Internet 上与其有业务联系的公司的 IP 地址

B. 仅允许 HTTP 协议通过

C. 使员工不能直接访问 FTP 服务端口号为 21 的 FTP 服务

D. 仅允许公司中具有某些特定 IP 地址的计算机可以访问外部网络

9. 两个公司希望通过 Internet 进行安全通信，保证从信息源到目的地之间的数据传输以密文形式出现，而且公司不希望由于在中间结点使用特殊的安全单元增加开支，最合适的加密方式是__(1)__，使用的会话密钥算法应该是__(2)__。

(1) A. 链路加密　　B. 结点加密　　C. 端-端加密　　D. 混合加密

(2) A. RSA　　B. RC-5　　C. MD5　　D. ECC

10. 相对于 DES 算法而言，RSA 算法的__(1)__，因此，RSA __(2)__。

(1) A. 加密密钥和解密密钥是不相同的　　B. 加密密钥和解密密钥是相同的

C. 加密速度比 DES 要快　　D. 解密速度比 DES 要快

(2) A. 更适用于对文件加密　　B. 保密性不如 DES

C. 可用于对不同长度的报文生成报文摘要

D. 可以用于数字签名

11. 驻留在多个网络设备上的程序在短时间内同时产生大量的请求消息冲击某 Web 服务器，导致该服务器不堪重负，无法正常响应其他合法用户的请求，这属于_____。

A. 网上冲浪　　B. 中间人攻击　　C. DDoS 攻击　　D. MAC 攻击

参考答案：

1. D　2. B　3. C　4. B　5. D　6. B　7. B　8. B　9. (1)C　(2)B　10. (1)A　(2)D　11. C