## 试题 1(2017 年上半年试题 6)

三重 DES 加密使用 2 个密钥对明文进行 3 次加密，其密钥长度为（ ）位。

A.56

B.112

C.128

D.168

**试题分析**

本题考查信息安全中的对称加密算法。

三重 DES 加密是使用 2 个 DES 密钥，进行多次操作来完成的，所以其密钥长度是：56*2=112 位。

**试题答案**

（6）B

## 试题 2(2017 年上半年试题 7)

要对消息明文进行加密传送，当前通常使用的加密算法是（ ）。

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，一般不直接用于明文加密，适合明文加密的，也就只有 RC-5 了。

**试题答案**

（7）D

## 试题 3(2017 年上半年试题 8)

假定用户 A、B 分别在 I1 和 I2 两个 CA 处取得了各自的证书，（ ）是 A、B 互信的必要条件。

A.A、B 互换私钥

B.A、B 互换公钥

C.$I_1$、$I_2$ 互换私钥

D.$I_1$、$I_2$ 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 $I_1$ 与 $I_2$ 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**

（8）D

## 试题 4(2017 年上半年试题 9)

SHA-1 是一种针对不同输入生成（ ）固定长度摘要的算法。

A.128 位

B.160 位

C.256 位

D.512 位

**试题分析**

本题考查信息安全中的摘要算法，常用的消息摘要算法有 MD5，SHA 等，市场上广泛使用的 MD5，SHA 算法的散列值分别为 128 和 160 位，由于 SHA 通常采用的密钥长度较长，因此安全性高于 MD5。

**试题答案**

（9）B

## 试题 5(2016 年上半年试题 6-8)

用户乙收到甲数字签名后的消息 M，为验证消息的真实性，首先需要从 CA 获取用户甲的数字证书，该数字证书中包含（ ），并利用（ ）验证该证书的真伪，然后利用（ ）验证 M 的真实性。A.甲的公钥

B.甲的私钥

C.乙的公钥

D.乙的私钥

A.CA 的公钥

B.乙的私钥

C.甲的公钥

D.乙的公钥

A.CA 的公钥

B.乙的私钥

C.甲的公钥

D.乙的公钥

**试题分析**

本题考查数字签名和 CA 方面的基础知识。

CA 是认证中心的简称，为了能够在互联网上认证通信双方的身份，可以在相应的认证中心申请自己的数字生疏。CA 为用户颁发的数字证书中包含用户的公钥信息、权威机构的认证信息和有效期等。用户收到经数字签名的消息后，须首先验证证书的真伪，即使用证书的公钥来验证，然后利用对方的公钥来验证消息的真实性。

**试题答案**

（6）A（7）A（8）C

## 试题 6(2016 年上半年试题 9)

下列不属于报文认证算法的是（ ）。A.MD5

B.SHA-1

C.RC4

D.HMAC

**试题分析**

RC4 是一种加密算法，并非摘要算法。

**试题答案**

（9）C

## 试题 7(2015 年上半年试题 7)

为了弥补 WEP 的安全缺陷，WPA 安全认证方案中新增的机制是（ ）。A.共享密钥认证

B.临时密钥完整性协议

C.较短的初始化向量

D.采用更强的加密算法

**试题分析**

WPA 是一种基于标准的可互操作的 WLAN 安全性增强解决方案，可大大增强现有以及未来无线局域网系统的数据保护和访问控制水平。WPA 源于正在制定中的 IEEE802.11i 标准并将与之保持前向兼容。部署适当的话，WPA 可保证 WLAN 用户的数据受到保护，并且只有授权的网络用户才可以访问 WLAN 网络。由于 WEP 业已证明的不安全性，在 802.11i 协议完善前，采用 WPA 为用户提供一个临时性的解决方案。该标准的数据加密采用了采用了可以动态改变密钥的临时密钥完整性协议 TKIP。

**试题答案**

（7）B

## 试题 8(2015 年上半年试题 8-9)

信息系统安全可划分为物理安全、网络安全、系统安全和应用安全，（ ）属于系统安全，（ ）属于应用安全。A.机房安全

B.入侵检测

C.漏洞补丁管理

D.数据库安全

A.机房安生

B.入侵检测

C.漏洞补丁管理

D.数据库安全

**试题分析**

作为全方位的、整体的系统安全防范体系也是分层次的，不同层次反映了不同的安全问题，根据网络的应用现状情况和结构，可以将安全防范体系的层次划分为物理层安全、系统层安全、网络层安全、应用层安全和安全管理。

（1）物理环境的安全性。物理层的安全包括通信线路、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。系统层的安全问题来自计算机网络内使用的操作系统的安全，例如，Windows Server 和 UNIX 等。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。应用层的安全问题主要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。安全管理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。

**试题答案**

（8）C（9）D

## 试题 9(2014 年上半年试题 6)

以下关于 IPsec 协议的描述中，正确的是（ ）。

A.IPsec 认证头（AH）不提供数据加密服务

B.IPsec 封装安全负荷（ESP）用于数据完整性认证和数据源认证

C.IPsec 的传输模式对原来的 IP 数据报进行了封装和加密，再加上了新 IP 头

D.IPsec 通过应用层的 Web 服务建立安全连接

**试题分析**

“Internet 协议安全性（IPSec）”是一种开放标准的框架结构，通过使用加密的安全服务以确保在 Internet 协议（IP）网络上进行保密而安全的通讯。

IPSec（InternetProtocolSecurity）是安全联网的长期方向。它通过端对端的安全性来提供主动的保护以防止专用网络与 Internet 的攻击。在通信中，只有发送方和接收方才是唯一必须了解 IPSec 保护的计算机。

IPsec 协议工作在 OSI 模型的第三层，使其在单独使用时适于保护基于 TCP 或 UDP 的协议（如 安全套接子层（SSL）就不能保护 UDP 层的通信流）。

与 IPsec 安全相关的协议是 AH 和 ESP。

AH 协议用来向 IP 通信提供数据完整性和身份验证,同时可以提供抗重放服务。

ESP 提供 IP 层加密保证和验证数据源以对付网络上的监听。因为 AH 虽然可以保护通信免受篡改，但并不对数据进行变形转换，数据对于黑客而言仍然是清晰的。为了有效地保证数据传输安全，在 IPv6 中有另外一个报头 ESP，进一步提供数据保密性并防止篡改。

IPsec 支持隧道模式和传输模式两种封装模式。

隧道（tunnel）模式：用户的整个 IP 数据包被用来计算 AH 或 ESP 头，AH 或 ESP 头以及 ESP 加密的用户数据被封装在一个新的 IP 数据包中。通常，隧道模式应用在两个安全网关之间的通讯。

传输（transport）模式 只是传输层数据被用来计算 AH 或 ESP 头，AH 或 ESP 头以及 ESP 加密的用户数据被放置在原 IP 包头后面。通常，传输模式应用在两台主机之间的通讯，或一台主机和一个安全网关之间的通讯。定义了一个通用格式。

**试题答案**

（6）A

## 试题 10(2014 年上半年试题 7)

防火墙的工作层次是决定防火墙效率及安全的主要因素，下面的叙述中正确的是（ ）。

A.防火墙工作层次越低，则工作效率越高，同时安全性越高

B.防火墙工作层次越低，则工作效率越低，同时安全性越低

C.防火墙工作层次越高，则工作效率越高，同时安全性越低

D.防火墙工作层次越高，则工作效率越低，同时安全性越高

**试题分析**

防火墙的工作层次是决定防火墙效率以及安全的主要因素。一般来说防火墙工作层次越低，则工作效率越高，但安全性就低了；反之，工作层次越高，工作效率就越低，则安全性越高。

**试题答案**

（7）D

## 试题 11(2014 年上半年试题 8)

在入侵检测系统中，事件分析器接收事件信息并对其进行分析，判断是否为入侵行为或异常现象，其常用的三种分析方法中不包括（ ）。

A.模式匹配

B.密文分析

C.数据完整性分析

D.统计分析

**试题分析**

入侵检测（Intrusion Detection），顾名思义，就是对入侵行为的发觉。他通过对计算机网络或计算机系统中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。

对于收集到的有关系统、网络、数据及用户活动的状态和行为等信息，一般通过三种技术手段进行分析: 模式匹配，统计分析和完整性分析。其中前两种方法用于实时的入侵检测，而完整性分析则用于事后分析。

**试题答案**

（8）B

## 试题 12(2014 年上半年试题 70)

2014 年 1 月，由于 DNS 根服务器被攻击，国内许多互联网用户无法访问.com 域名网站，这种恶意攻击可能造成的危害是（ ）。

A.创造条件，攻击相应的服务器

B.快速入侵互联网用户的计算机

C.将正常网站的域名解析到错误的地址

D.以上都是

**试题分析**

在 DNS 体系中，根服务器主要用来管理互联网的主目录，全世界只有 13 台。1 个为主根服务器，放置在美国。其余 12 个均为辅根服务器，其中 9 个放置在美国，欧洲 2 个，位于英国和瑞典，亚洲 1 个，位于日本。所有根服务器均由美国政府授权的互联网域名与号码分配机构 ICANN 统一管理，负责全球互联网域名根服务器、域名体系和 IP 地址等的管理。

当根域名服务器被攻击不能正常使用之后，带来的问题是访问网站时域名无法解析到正确的服务器上，无法解析，自然无法访问相应网站，此时有可能将正常网站的域名解析到错误的地址。

**试题答案**

（70）C

## 试题 13(2013 年上半年试题 6)

以下关于利用三重 DES 进行加密的说法，（ ）是正确的。

A.三重 DES 的密钥长度是 56 位

B.三重 DES 使用三个不同的密钥进行三次加密

C.三重 DES 的安全性高于 DES

D.三重 DES 的加密速度比 DES 加密速度快

**试题分析**

DES 是一种迭代的分组密码，明文和密文都是 64 位，使用一个 56 位的密钥以及附加的 8 位奇偶校验位。攻击 DES 的主要技术是穷举法，由于 DES 的密钥长度较短，为了提高安全性，就出现了使用 112 位密钥对数据进行三次加密的算法（3DES），即用两个 56 位的密钥 K1 和 K2，发送方用 K1 加密，K2 解密，再使用 K1 加密；接收方则使用 K1 解密，K2 加密，再使用 K1 解密，其效果相当于将密钥长度加倍。

从上述描述可知三重 DES 的密钥是 112 位，而非 56 位；在加密过程中是使用 2 个不同的密钥进行三次加密，而非 3 个；三重 DES 由于加密次数多，所以安全性比 DES 高，而加密速度比 DES 慢。

**试题答案**

（6）C

## 试题 14(2013 年上半年试题 7)

利用报文摘要算法生成报文摘要的目的是（ ）。

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.防止发送方否认发送过的数据

D.防止发送的报文被篡改

**试题分析**

报文摘要是使用单向哈希函数算法，将任意长度的报文经计算得出的固定位输出。所谓单向是指该算法是不可逆的找出具有同一报文摘要的两个不同报文是很困难的。正是因为报文摘要具备此特性，所以我们在传报文的过程中，会产生报文摘要，把摘要通过不同方式传送给对方，对方接收到报文与报文摘要后可以通过摘要对报文进行验证，以确定报文是否被篡改。所以报文摘要是一种保护数据完整性的手段，他可以防止发送的报文被篡改。

**试题答案**

（7）D

## 试题 15(2013 年上半年试题 8)

支持电子邮件加密服务的标准或技术是（ ）。

A.PGP

B.PKI

C.SET

D.Kerberos

**试题分析**

PGP 是一个基于 RSA 的邮件加密软件，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。PGP 的基本原理是，先用对称密钥加密传送的信息，再将该对称加密密钥以接收方的公钥加密，组成数字信封，并将此密钥交给公正的第三方保管; 然后，将此数字信封传送给接收方。接收方必须先以自己的私钥将数字信封拆封，以获得对称解密密钥，再以该对称解密密钥解出真正的信息，兼顾方便与效率。

PKI 是一种遵循既定标准的密钥管理平台，它能够为所有网络应用提供加密和数字签名等服务，以及所必需的密钥和证书管理体系。PKI 机制解决了分发密钥时依赖秘密信道的问题。

SET 安全电子交易协议主要应用于 B2C 模式中保障支付信息的安全性。SET 协议本身比较复杂，设计比较严格，安全性高，它能保证信息传输的机密性、真实性、完整性和不可否认性。SET 协议是 PKI 框架下的一个典型实现，同时也在不断升级和完善，如 SET 2.0 将支持借记卡电子交易。

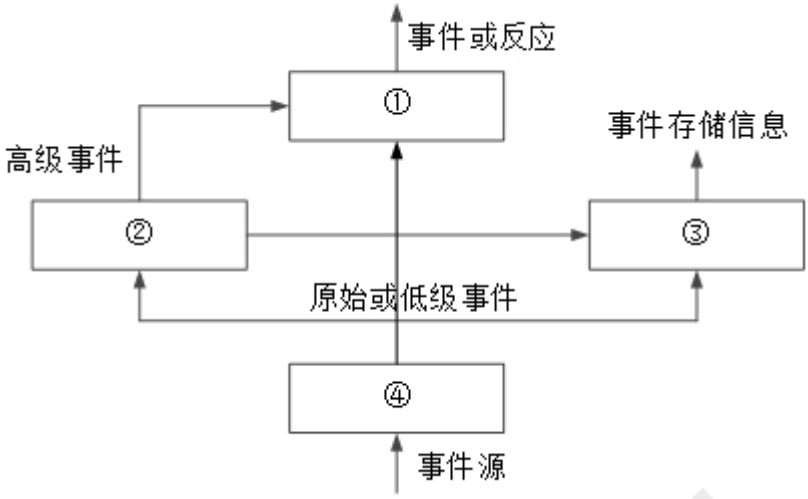
Kerberos 是一种网络身份认证协议，该协议的基础是基于信任第三方，它提供了在开放型网络中进行身份认证的方法,认证实体可以是用户也可以是用户服务。这种认证不依赖宿主机的操作系统或计算机的 IP 地址，不需要保证网络上所有计算机的物理安全性，并且假定数据包在传输中可被随机窃取和篡改。

**试题答案**

（8）A

## 试题 16(2013 年上半年试题 9)

下图为 DARPA 提出的公共入侵检测框架示意图，该系统由 4 个模块组成。其中模块①~④分别是（ ）。




A.事件产生器、事件数据库、事件分析器、响应单元

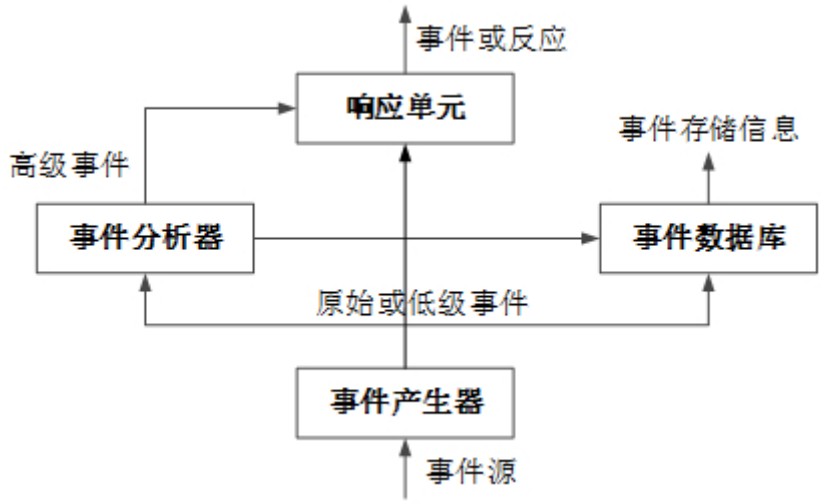
B.事件分析器、事件产生器、响应单元、事件数据库

C.事件数据库、响应单元、事件产生器、事件分析器

D.响应单元、事件分析器、事件数据库、事件产生器

**试题分析**

公共入侵检测框架示意图如下所示：




所以题目中①~④分别应为: 响应单元、事件分析器、事件数据库、事件产生器。

**试题答案**

（9）D

## 试题 17(2012 年上半年试题 6)

下面关于钓鱼网站的说法中错误的是（ ）。

A.钓鱼网站仿冒真实网站的 URL 地址

B.钓鱼网站通过向真实网站植入木马程序以达到网络攻击的目的

C.钓鱼网站用于窃取访问者的机密信息

D.钓鱼网站可以通过 E-mail 传播网址

**试题分析**

本题考查网络安全方面的知识。 钓鱼网站是指一类仿冒真实网站的 URL 地址、通过 Email 传播网址，目的是窃取用户账号密码等机密信息的网站。

**试题答案**

（6）B

## 试题 18(2012 年上半年试题 7)

支持安全 Web 应用的协议是（ ）。

A.HTTPS

B.HTTPD

C.SOAP

D.HTTP

**试题分析**

本题考查网络安全方面的知识。 Web 服务的标准协议是 HTTP 协议，HTTPS 对 HTTP 协议增加了一些安全特性; WINS 是 Windows 系统的一种协议，SOAP 是基于 HTTP 和 XML，用于 WebService 的简单对象访问协议。

**试题答案**

（7）A

## 试题 19(2012 年上半年试题 8)

甲和乙要进行通信，甲对发送的消息附加了数字签名，乙收到该消息可用（ ）验证该消息数字签名的真伪。

A.甲的公钥

B.甲的私钥

C.乙的公钥

D.乙的私钥

**试题分析**

本题考查数字签名的概念。 数字签名（Digital Signature）技术是不对称加密算法的典型应用: 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。数字签名主要的功能是: 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。

**试题答案**

（8）A

## 试题 20(2012 年上半年试题 9)

下列算法中，用于密钥交换的是（ ）。

A.DES

B.SHA-1

C.Diffie-Hellman

D.AES

**试题分析**

本题考查安全算法方面的知识。 题中的四个选项中，DES 是一种经典的数据加密算法，AES 是高级加密算法，Diffie-Hellman 是一种密钥交换算法，SHA 属于报文摘要算法。

**试题答案**

（9）C

## 试题 21(2011 年上半年试题 6)

下面病毒中，属于蠕虫病毒的是（ ）。

A.CIH 病毒

B.特洛伊木马病毒

C.罗密欧与朱丽叶病毒

D.Melissa 病毒

**试题分析**

本题考查计算机病毒的基础知识。

CIH 病毒是一种能够破坏计算机系统硬件的恶性病毒。

特洛伊木马病毒是一种秘密潜伏的能够通过远程网络进行控制的恶意程序。控制

者可以控制被秘密植入木马的计算机的一切动作和资源，是恶意攻击者进行窃取信息等的工具。

2000 年出现的“罗密欧与朱丽叶”病毒是一个非常典型的蠕虫病毒，它改写了病毒的历史，该病毒与邮件病毒基本特性相同，它不再隐藏于电子邮件的附件中，而是直接存在于电子邮件的正文中，一旦用户打开 Outlook 收发信件进行阅读，该病毒马上就发作，并将复制的新病毒通过邮件发送给别人，计算机用户无法躲避。

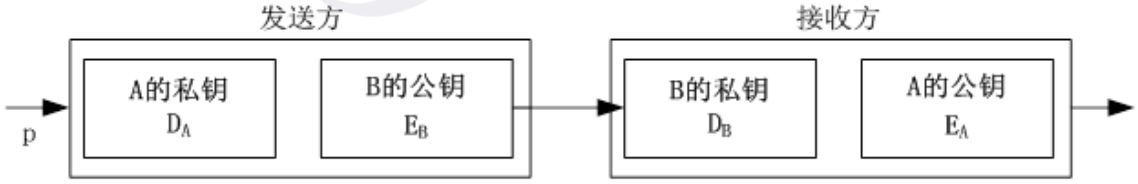
梅丽莎病毒是一种宏病毒，发作时将关闭 Word 的宏病毒防护、打开转换确认、模板保存提示；使“宏”、“安全性”命令不可用，并设置安全性级别为最低。

**试题答案**

（6）C

## 试题 22(2011 年上半年试题 7-8)

某数字签名系统如下图所示。网上传送的报文是（ ），如果 A 否认发送，作为证据的是（ ）。




A. P

B. $D_A(P)$

C. $E_B(D_A(P))$

D. $D_A$

A. P

B. $D_A(P)$

C. $E_B(D_A(P))$

D. $D_A$

**试题分析**

本题考查数字签名的实现细节。

图中所示为一种利用公钥加密算法实现的数字签名方案，发送方 A 要发送给接收方 B 的报文 P 经过 A 的私钥签名和 B 的公钥加密后形成报文 $E_B(D_A(P))$发送给 B，B 利用自己的私钥 $D_B$ 和 A 的公钥 $E_A$ 对消息 $E_B(D_A(P))$进行解密和认证后得到报文 P，并且保存经过 A 签名的消息 $D_A(P)$作为防止 A 抵赖的证据。

**试题答案**

（7）C（8）B

## 试题 23(2011 年上半年试题 9)

以下关于域本地组的叙述中，正确的是（ ）。

A.成员可来自森林中的任何域，仅可访问本地域内的资源

B.成员可来自森林中的任何域，可访问任何域中的资源

C.成员仅可来自本地域，仅可访问本地域内的资源

D.成员仅可来自本地域，可访问任何域中的资源

**试题分析**

本题考查 Windows Server 2003 活动目录中用户组的概念。

在 Windows Server 2003 的活动目录中，用户分为全局组（Global Groups）、域本地组（Domain Local Groups）和通用组（Universal

Groups）。其中全局组成员来自于同一域的用户账户和全局组，可以访问域中的任何资源；域本地组成员来自森林中任何域中的用户账户、全局组和通用组以及本域中的域本地组，只能访问本地域中的资源；通用组成员来自森林中任何域中的用户账户、全局组和其他的通用组，可以授予多个域中的访问权限。

**试题答案**

（9）A

## 试题 24(2011 年上半年试题 39)

信息安全的威胁有多种，其中（ ）是指通过对系统进行长期监听，利用统计分析方法对诸如通信频度、通信的信息流向、通信总量的变化等参数进行研究，从中发现有价值的信息和规律。

A.窃听

B.信息泄露

C.旁路控制

D.业务流分析

**试题分析**

本题考查信息化（信息安全）方面的基础知识。

业务流分析属于信息安全威胁的一种。它通过对系统进行长期监听，利用统计分析方法诸如通信频度、通信的信息流向、通信总量的变化等参数进行研究，从中发现有价值的信息规律。

**试题答案**

（39）D

## 试题 25(2011 年上半年试题 67)

下列选项中，同属于报文摘要算法的是（ ）。

A.DES 和 MD5

B.MD5 和 SHA-1

C.RSA 和 SHA-1

D.DES 和 RSA

**试题分析**

本题考查安全算法相关常识。

数据加密的基本过程就是对原来为明文的文件或数据按某种算法进行处理，使其成为不可读的一段代码，通常称为“密文”，使其只能在输入相应的密钥之后才能显示出本来内容，通过这样的途径来达到保护数据不被非法人窃取、阅读的目的。

常见加密算法有：DES（Data Encryption Standard）、3DES（Triple DES）、RC2 和 RC4、 IDEA（International Data Encryption Algorithm）、RSA。

报文摘要算法主要应用在“数字签名”领域，作为对明文的摘要算法。著名的摘要算法有 RSA 公司的 MD5 算法和 SHA1 算法及其大量的变体。

**试题答案**

（67）B

## 试题 26(2010 年上半年试题 6)

用户 A 从 CA 处获取了用户 B 的数字证书，用户 A 通过（ ）可以确认该数字证书的有效性。

A.用户 B 的公钥

B.用户 B 的私钥

C.CA 的公钥

D.用户 A 的私钥

**试题分析**

用户 B 的数字证书中包含了 CA 的签名，因此用 CA 的公钥可验证数字证书的有效性。

**试题答案**

（6）C

## 试题 27(2010 年上半年试题 7)

入侵检测系统的构成不包括（ ）。

A.预警单元

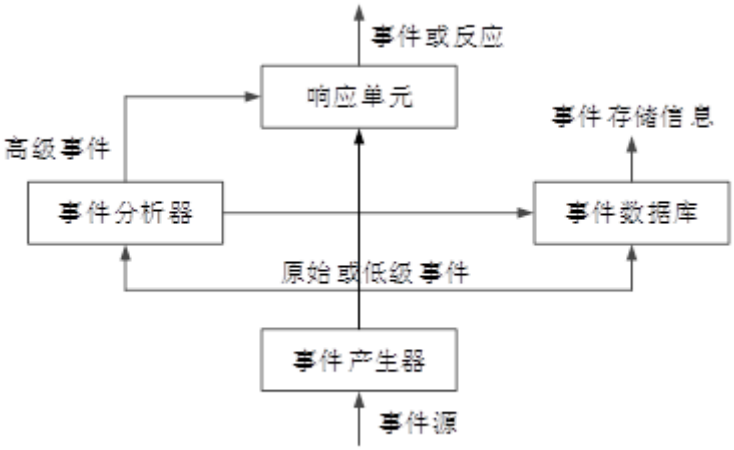
B.事件产生器

C.事件分析器

D.响应单元

**试题分析**

美国国防部高级研究计划局（DARPA）提出的公共入侵检测框架（Common Intrusion Detection Framework，CIDF ）由 4 个模块组成，见下图：




（l）事件产生器（Event generators，E-boxes ）：负责数据的采集，并将收集到的原始数据转换为事件，向系统的其他模块提供与事件有关的信息。入侵检测所利用的信息一般来自 4 个方面: 系统和网络的日志文件、目录和文件中不期望的改变、程序执行中不期望的行为、物理形式的入侵信息等。入侵检测要在网络中的若干关键点（不同网段和不同主机）收集信息，并通过多个采集点信息的比较来判断是否存在可疑迹象或发生入侵行为。

（2）事件分析器（Event Analyzers，A-boxes）：接收事件信息并对其进行分析，判断是否为入侵行为或异常现象，分析方法有下面三种：

① 模式匹配：将收集到的信息与已知的网络入侵数据库进行比较，从而发现违背安全策略的行为。

② 统计分析：首先给系统对象（例如用户、文件、目录和设备等）建立正常使用时的特征文件（Profile），这些特征值将被用来与网络中发生的行为进行比较。当观察值超出正常值范围时，就认为有可能发生入侵行为。

③ 数据完整性分析：主要关注文件或系统对象的属性是否被修改，这种方法往往用于事后的审计分析。

（3）事件数据库（Event Databases，D-boxes ）：存放有关事件的各种中间结果和最终数据的地方，可以是面向对象的数据库，也可以是一个文本文件。

（4）响应单元（Response units，R-boxes）：根据报警信息做出各种反应，强烈的反冲就是断开连按、改变文件属性等，简单的反应就是发出系统提示，引起操作人员注意。

因此，入侵检测系统的构成中不包括预警单元，故选 A。

**试题答案**

（7）A

## 试题 28(2010 年上半年试题 8-9)

如果杀毒软件报告一系列的 Word 文档被病毒感染，则可以推断病毒类型是（ ）；如果用磁盘检测工具（CHKDSK、SCANDISK 等）检测磁盘发现大量文件链接地址错误，表明磁盘可能被（ ）病毒感染。

A.文件型

B.引导型

C.目录型

D.宏病毒

A.文件型

B.引导型

C.目录型

D.宏病毒.

**试题分析**

本题考查计算机病毒方面的上基础知识。

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核技术区分，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。

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、电了表格等文件。

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，如果用户使用某些工具（如 SCANDISK 或 CHKDSK）检测受感染的磁盘，会发现大量的文件链接地址的错误，这些错误都是由此类计算机病毒造成的。

**试题答案**

（8）D（9）C