## 2013年5月

## 试题11-命-技-N.GJ.21.p000-5.00-信息安全

攻击者通过搭线或在电磁波辐射范围内安装截收装置等方式获得机密信息，或通过对信息流量和流向、通信频率和长度等参数的分析推导出有用信息的威胁称为（11 ）。

A. 破坏

B. 抵赖

C. 截取

D. 窃取

**分析：**

计算机信息安全：http://www.baike.com/wiki/计算机信息安全

* 窃取：通过数据窃听的手段获得敏感信息。攻击者通过搭线窃听或电子辐射探测等手段截获机密信息，或通过信息流量的变化、流向的变化以及通信总量等参数分析出有用信息。
* 截取：非法用户通过特殊手段首先获得信息，再将此信息发送给真实接收者。

**参考答案：D**

## 试题13-喜-技-G.ZJ.30.p628-5.00-安全审计

下面有关安全审计的说法错误的是（13）。

A. 安全审计需要用到数据挖掘和数据仓库技术

B. 安全审计产品只包括主机类、网络类及数据库类

C. 安全审计的作用包括帮助分析安全事故发生的原因

D. 安全审计是主体对客体进行访问和使用情况进行记录和审查

**分析：**

高级教程p628：

概括地讲，安全审计是采用数据挖掘和数据仓库技术，实现在不同网络环境中终端对终端的监控和管理，在必要时通过多种途径向管理员发出警告或自动采取排错措施，能对历史数据进行分析、处理和追踪。

安全审计属于安全管理类产品。在管理类产品中，各类安全审计系统可在日常运行、维护中提供对网络安全的主动分析及综合审计。安全审计产品主要包括主机类、网络类及数据库类和应用系统级的审计产品。

答案B中的“只包括”太绝对！所以，此题是送分题。

**参考答案：B**

## 试题14-命-技-Y.GJ.24.p538-5.00-信息安全系统

信息安全保障系统可以用一个宏观的三维空间来表示，第一维是OSI网络参考模型，第二维是安全机制，第三维是安全服务。该安全空间的五个要素分别是（14）。

A. 应用层、传输层、网络层、数据链路层和物理层

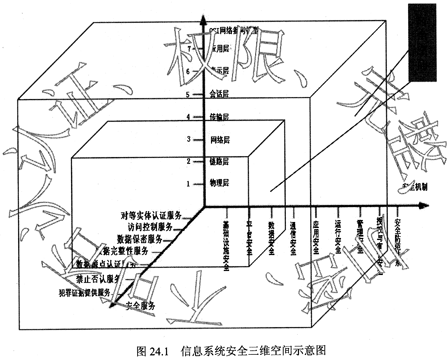
B. 基础设施安全、平台安全、数据安全、通信安全和应用安全

C. 对等实体服务、访问控制服务、数据保密服务、数据完整性服务和物理安全服务

D. 认证、权限、完整、加密和不可否认

**分析：**

高级教程p538：



由X、Y、Z三个轴形成的空间就是信息系统的“安全空间”，随着网络逐层扩展，这个空间不仅范围逐步加大，安全的内涵也就更丰富，达到具有认证、权限、完整、加密和不可否认五大要素。也叫做“安全空间”的五大“属性”。

**参考答案：D**

## 试题16-喜-技-N.GJ.00.p000-5.00-信息安全

网络入侵检测系统和防火墙是两种典型信息系统安全防御技术，下面关于入侵检测系统和防火墙的说法正确的是（16）。

A. 防火墙是入侵检测系统之后的又一道防线，防火墙可以及时发现入侵检测系统没有发现的入侵行为

B. 入侵检测系统通常是一个旁路监听设备，没有也不需要跨接在任何链路上，无须网络流量流经它便可以工作

C. 入侵检测系统可以允许内部的一些主机被外部访问，而防火墙没有这些功能，只是监视和分析系统的活动

D. 防火墙必须和安全审计系统联合使用才能达到应用目的，而入侵检测系统是一个独立的系统，不需要依赖防火墙和安全审计系统

**分析：**

入侵检测（IDS）：http://baike.baidu.com/view/20936.htm

我们做一个形象的比喻：假如防火墙是一幢大楼的门卫，那么IDS就是这幢大楼里的监视系统。一旦小偷爬窗进入大楼，或内部人员有越界行为，只有实时监视系统才能发现情况并发出警告。IDS入侵检测系统以信息来源的不同和检测方法的差异分为几类。根据信息来源可分为基于主机IDS和基于网络的IDS，根据检测方法又可分为异常入侵检测和滥用入侵检测。不同于防火墙，IDS入侵检测系统是一个监听设备，没有跨接在任何链路上，无须网络流量流经它便可以工作。因此，对IDS的部署，唯一的要求是：IDS应当挂接在所有所关注流量都必须流经的链路上。在这里，“所关注流量”指的是来自高危网络区域的访问流量和需要进行统计、监视的网络报文。在如今的网络拓扑中，已经很难找到以前的HUB式的共享介质冲突域的网络，绝大部分的网络区域都已经全面升级到交换式的网络结构。因此，IDS在交换式网络中的位置一般选择在：

（1）尽可能靠近攻击源

（2）尽可能靠近受保护资源

这些位置通常是：

* 服务器区域的交换机上
* Internet接入路由器之后的第一台交换机上
* 重点保护网段的局域网交换机上

防火墙：http://baike.baidu.com/view/3067.htm

所谓防火墙指的是一个由软件和硬件设备组合而成、在内部网和外部网之间、专用网与公共网之间的界面上构造的保护屏障。是一种获取安全性方法的形象说法，它是一种计算机硬件和软件的结合，使Internet与Intranet之间建立起一个安全网关（Security Gateway），从而保护内部网免受非法用户的侵入，防火墙主要由服务访问规则、验证工具、包过滤和应用网关4个部分组成，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或硬件。该计算机流入流出的所有网络通信和数据包均要经过此防火墙。

在网络中，所谓“防火墙”，是指一种将内部网和公众访问网（如Internet）分开的方法，它实际上是一种隔离技术。防火墙是在两个网络通讯时执行的一种访问控制尺度，它能允许你“同意”的人和数据进入你的网络，同时将你“不同意”的人和数据拒之门外，最大限度地阻止网络中的黑客来访问你的网络。换句话说，如果不通过防火墙，公司内部的人就无法访问Internet，Internet上的人也无法和公司内部的人进行通信。

**参考答案：B**

## 试题18-命-技-N.GJ.27.p588-5.00-信息安全

下面的无线网络加密方法中，（18）的安全性高。

A. MAC地址过滤

B. WEP

C. WPA

D. WPA2

**分析：**

WEP、WPA、WPA2：http://wenku.baidu.com/view/b33b2dcca1c7aa00b52acb4d.html

WEP：

有线等效加密（Wired Equivalent Privacy），又称无线加密协议（Wireless Encryption Protocol），简称WEP，是个保护无线网络（Wi-Fi）信息安全的体制。因为无线网络是用无线电把讯息传播出去，它特别容易被窃听。WEP 的设计是要提供和传统有线的局域网路相当的机密性，而依此命名的。不过密码分析学家已经找出 WEP 好几个弱点，因此在2003年被 Wi-Fi Protected Access (WPA) 淘汰，又在2004年由完整的 IEEE 802.11i 标准（又称为 WPA2）所取代。WEP 虽然有些弱点，但也足以吓阻非专业人士的窥探了。

WPA和WPA2：

WPA 全名为 Wi-Fi Protected Access，有WPA 和 WPA2两个标准，是一种保护无线电脑网路（Wi-Fi）安全的系统，它是应研究者在前一代的系统有线等效加密（WEP）中找到的几个严重的弱点而产生的。WPA 实作了 IEEE 802.11i 标准的大部分，是在 802.11i 完备之前替代 WEP 的过渡方案。WPA 的设计可以用在所有的无线网卡上，但未必能用在第一代的无线取用点上。WPA2 实作了完整的标准，但不能用在某些古老的网卡上。这两个都提供优良的保全能力，但也都有两个明显的问题：

* WPA或WPA2 一定要启动并且被选来代替 WEP 才有用，但是大部分的安装指引都把 WEP 列为第一选择。
* 在使用家中和小型办公室最可能选用的“个人”模式时，为了保全的完整性，所需的密语一定要比已经叫用户设定的六到八个字元的密码还长。

**参考答案：D**

## 试题19-悲-技-N.ZJ.17.p000-6.02-机房标准

根据《电子信息系统机房设计规范GB50174-2008》，下面的电子信息机房的设计方案不妥当的是（19）。

A. 主机房净高根据机柜高度及通风要求确定，设置为3.0M

B. 主机房采用了耐火等级为二级的建筑材料

C. 主机房用于搬运设备的通道净宽设为2.0M

D. B级电子信息系统机房的主机方中设置了两个外窗

**分析：**

标准原文：

6.1.3 主机房净高应根据机柜高度及通风要求确定，且不宜小于2.6m。

6.3.2 电子信息系统机房的耐火等级不应低于二级。

6.2.3 电子信息系统机房内通道的宽度及门的尺寸应满足设备和材料运输要求，建筑的入口至主机房应设通道，通道净宽不应小于1.5m。

6.4.6 A 级B 级电子信息系统机房的主机房不宜设置外窗。当主机房设有外窗时，应采用双层固定窗，并应有良好的气密性，不间断电源系统的电池室设有外窗时，应避免阳光直射。

**参考答案：D**

## 13下

## 试题15-悲-技-Y.ZJ.17.p431-5.00-信息安全

以下针对信息系统安全的说法中，（15）是错误的。

A、信息系统安全的侧重点随着信息系统使用者的需求不同而发生变化

B、信息系统安全属性包含：保密性、完整性、可用性与不可抵赖性

C、应用系统常用的保密技术有：最小授权原则、防暴露、信息加密、数字签名与公证

D、完整性是一种面向信息的安全性能，可用性是面向用户的安全性能

**分析：**

应用系统常用的保密技术如下。

①最小授权原则：对信息的访问权限仅授权给需要从事业务的用户使用。

②防暴露：防止有用信息以各种途径暴露或传播出去。

③信息加密：用加密算法对信息进行加密处理，非法用户无法对信息进行解密从而无法读懂有效信息。

④物理保密：利用各种物理方法，如限制、隔离、掩蔽和控制等措施，保护信息不被泄露。

**参考答案：C**

## 试题16-喜-技-Y.GJ.27.p578-5.00-信息安全

（16）不是对称加密算法的优点。

A. 加/解密速度快

B. 密钥管理简单

C. 加密算法复杂、加密强度高

D. 适宜一对一的信息加密传输过程

**分析：**

对称密钥算法优点：加/解密速度快、密钥管理简单、适宜一对一的信息加密传输

对称密钥算法缺点：加密算法简单，密钥长度有限（56比特/128比特），加密强度不高、密钥分发困难，不适宜一对多的加密信息传输。

根据常识，排除法即可！

**参考答案：C**

## 试题17-命-技-N.ZJ.00.p000-5.00-信息安全

入侵是指没有经过授权就非法获得系统的访问权限或相关授权的行为，其中攻击者利用默认密码进入系统内部属于（17）入侵方式。

A. 旁路控制 B. 假冒 C. 口令破译 D. 合法用户的非授权访问

**分析：**

默认密码也是密码！使用默认密码也是猜出来的，猜也是密码破译的过程！

参考高级教程p533。

冒充：

* 冒充领导发布命令、调阅密件。
* 冒充主机欺骗合法主机和合法用户。
* 冒充网络控制程序套取或修改使用权限、密码和密钥等信息，越权使用网络设备和资源。
* 接管合法用户，欺骗系统，占用合法用户的资源。

**参考答案：C**

## 试题18-喜-技-Y.GJ.27.p583-5.00-信息安全

我国实行密码等级管理制度，各密码等级为：商用密码，普用密码，绝密密码和军用密码。其中商用密码等级的使用范围为（18）

A. 政府、党政部门 B. 国内企业、事业单位

C. 中央和机要部门 D. 军队

**分析：**

我国实行密码分级管理制度，密码等级及适用范围如下：

（1）商用密码——国内企业、事业单位

（2）普用密码——政府、党政部门

（3）绝密密码——中央和机要部门

（4）军用密码——军队

送分题！

**参考答案：B**

## 14上

## 试题15-悲-技-Y.GJ.30.p627-5.00-信息安全

《计算机信息系统安全保护等级划分准则》规定了计算机系统安全保护能力的5个等级。其中，按照（15）的顺序从左到右安全能力逐渐增强。

A.系统审计保护级、结构化保护级、安全标记保护级

B.用户自主保护级、访问验证保护级、安全标记保护级

C.访问验证保护级、系统审计保护级、安全标记保护级

D.用户自主保护级、系统审计保护级、安全标记保护级

**分析：**

本标准规定了计算机系统安全保护能力的五个等级，即：

第一级：用户自主保护级；

第二级：系统审计保护级；

第三级：安全标记保护级；

第四级：结构化保护级；

第五级：访问验证保护级。

**参考答案：D**

## 试题16-喜-技-Y.GJ.24.p542-5.00-信息安全

## 试题17-喜-技-Y.GJ.24.p542-5.00-信息安全

OSI安全体系结构定义了五种安全服务，其中（16）用于识别对象的身份并对身份证实。（17）用于防止对资源的非授权访问，确保只有经过授权的实体才能访问受保护的资源

（16） A.安全认证服务 B.访问控制安全服务

C.数据保密性安全服务 D.数据完整性安全服务

（17） A.安全认证服务 B.访问控制安全服务

C.数据保密性安全服务 D.数据完整性安全服务

**分析：**

OSI安全体系结构的五类安全服务以及八类安全机制：http://www.cnitpm.com/pm/10693.html阅读理解，排除法即可！

五类安全服务包括认证（鉴别）服务、访问控制服务、数据保密性服务、数据完整性服务和抗否认性服务。 认证（鉴别）服务：在网络交互过程中，对收发双方的身份及数据来源进行验证。 访问控制服务：防止未授权用户非法访问资源，包括用户身份认证和用户权限确认。 数据保密性服务：防止数据在传输过程中被破解、泄露。 数据完整性服务：防止数据在传输过程中被篡改。 抗否认性服务：也称为抗抵赖服务或确认服务。防止发送方与接收方双方在执行各自操作后，否认各自所做的操作。

**参考答案：（16）A、（17）B**

## 试题23-喜-技-Y.GJ.27.p587-5.00-信息安全

（23）是WLAN常用的上网认证方式

A.WEP认证 B.SIM认证 C.宽带拨号认证 D. PPoE认证

**分析：**

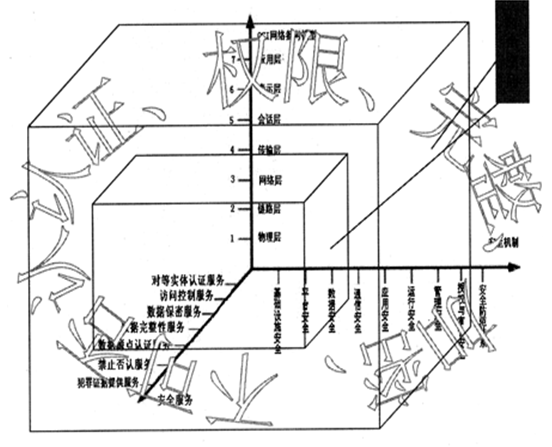
WEP是Wired Equivalent Privacy的简称，有线等效保密（WEP）协议是对在两台设备间无线传输的数据进行加密的方式，用以防止非法用户窃听或侵入无线网络。

**参考答案：A**

**14下**

## 试题16-命-技-Y.GJ.24.p538-5.00-信息安全

构建信息安全系统需要一个宏观的三维空间，如下图所示，请根据改图指出X轴是指（）



A、安全防范体系 B、管理安全

C、安全机制 D、安全策略

**分析：**

信息安全保障系统可以用一个宏观的三维空间来表示，Y轴是OSI网络参考模型，信息安全系统的许多技术、技巧都是在网络的各个层面上实施的。X轴是“安全机制”，Z轴是“安全服务”。

**参考答案：C**

## 试题17-命-技-Y.GJ.29.p616-5.00-信息安全

某信息系统采用了基于角色的访问机制，其角色的权限是由（）决定的。

A、用户自己 B、系统管理员

C、主体 D、业务要求

**分析：**

基于角色的访问机制，其角色的权限是由系统管理员分配的

**参考答案：B**

## 试题18-命-技-N.GJ.24.p000-5.00-信息安全

以下关于入侵检测系统功能的叙述中，（）是不正确的。

A、保护内部网络免受非法用户的侵入

B、评估系统关键资源和数据文件的完整性

C、识别已知的攻击行为

D、统计分析异常行为

**分析：**

入侵检测（Intrusion Detection）是对入侵行为的检测。它通过收集和分析网络行为、安全日志、审计入侵检测数据、其它网络上可以获得的信息以及计算机系统中若干关键点的信息，检查网络或系统中是否存在违反安全策略的行为和被攻击的迹象。入侵检测作为一种积极主动地安全防护技术，提供了对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前拦截和响应入侵。因此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。**入侵检测通过执行以下任务来实现：监视、分析用户及系统活动；系统构造和弱点的审计；识别反映已知进攻的活动模式并向相关人士报警；异常行为模式的统计分析；评估重要系统和数据文件的完整性；操作系统的审计跟踪管理，并识别用户违反安全策略的行为。**

**参考答案：A**

## 15年上

## 试题15-命-技-Y.GJ.25.p565-5.00-信息安全

15、信息系统安全风险评估是通过数字化的资产评估准则完成的，它通常会覆盖人员安全、人员信息、公共秩序等方面的各个要素，以下不会被覆盖的要素是（）。

A、立法及规章未确定的义务

B、金融损失或对业务活动的干扰

C、信誉的损害

D、商业及经济的利益

**分析：**

风险评估

评估是通过数字的资产评估准则完成的，它覆盖了以下几点：

①人员安全；

②人员信息；

③立法及规章所确定的义务；

④法律的强制性；

⑤商业及经济的利益；

⑥金融损失或对业务活动的干扰；

⑦公共秩序；

⑧业务政策及操作；

⑨信誉的损害。

**参考答案：A**

## 试题17-命-技-Y.GJ.29.p615-5.00-信息安全

17、访问控制是为了限制访问主体对访问客体的访问权限，从而使计算机系统在合法范围内使用的安全措施，以下关于访问控制的叙述中，（）是不正确的。

A、访问控制包括2个重要的过程：鉴别和授权

B、访问控制机制分为2种：强制访问控制（MAC）和自主访问控制（DAC）

C、RBAC基于角色的访问控制对比DAC的先进之处在于用户可以自主的将访问的权限授给其它用户

D、RBAC不是基于多级安全需求的，因为基于RBAC的系统中主要关心的是保护信息的完整性，即“谁可以对什么信息执行何种动作”

**分析：**

基于角色的访问控制

用户不能自主地将访问权限授给别的用户，这是RBAC与DAC的根本区别所在。

**参考答案：C**

## 15年下

## 试题12-命-技-Y.ZJ.17.p432-5.00-信息安全

12、信息的（ ）要求采用的安全技术保证信息接收者能够验证在传送过程中信息没有被修改，并能防范入侵者用假信息代替合法信息

A、隐蔽性 B、机密性

C、完整性 D、可靠性

**分析：**

2．完整性

完整性是信息未经授权不能进行改变的特性。即应用系统的信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放和插入等破坏和丢失的特性。

阅读理解即可。

**参考答案：C**

## 试题16-悲-技-Y.GJ.26.p571-5.00-信息安全

16、根据《信息安全等级保护管理办法》中的规定，信息系统的安全保护等级应当根据信息系统的国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后，对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危险程度等因素确定。其中安全标记保护级处于（ ）

A、第二级 B、第三级

C、第四级 D、第五级

**分析：**

需要处理好的关系

5．全等级保护的概念

第一级为用户自主保护级，适用于普通内联网用户；

第二级为系统审计保护级，适用于通过内联网或国际网进行商务活动、要保密的非重要单位；

第三级为安全标记保护级，适用于地方各级国家机关、金融单位机构、邮电通信、能源与水源供给部门、交通运输、大型工商与信息技术企业、重点工程建设等单位；

第四级为结构化保护级，适用于中央级国家机关、广播电视部门、重要物资储备单位、社会应急服务部门、尖端科技企业集团、国家重点科研单位机构和国防建设等部门；

第五级为访问验证保护级，适用于国防关键部门和依法需要对计算机信息系统实施特殊隔离的单位。

**参考答案：B**

## 试题17-悲-技-Y.GJ.27.p588-5.00-信息安全

17、以下关于WLAN安全机制的叙述中，（ ）是正确的

A、WPA是为建立无线网络安全环境提供的第一个安全机制

B、WEP和IPSec协议一样，其目标都是通过加密无线电波来提供安全保护

C、WEP2的初始化向量（IV）空间64位

D、WPA提供了比WEP更为安全的无线局域网接入方案

**分析：**

WLAN安全机制

至于WPA的身份认证系统，则为WLAN提供了更加安全的接入保护。

**参考答案：D**

## 试题18-命-技-N.GJ.26.p000-5.00-信息安全

18、在信息系统安全建设中，（ ）确立全方位的防御体系，一般会告诉用户应有的责任，组织规定的网络访问、服务访问、本地和远地的用户认证拨入和拨出、磁盘数据加密、病毒防护措施，以及雇员培训等，并保证所有可能受到攻击的地方必须以同样安全级别加以保护

A、安全策略 B、防火墙

C、安全体系 D、系统安全

**分析：**

安全策略的概念与内容

什么叫“安全策略”？计算机信息应用系统的“安全策略”就是指：人们为保护因为使用计算机信息应用系统可能招致的对单位资产造成损失而进行保护的各种措施、手段，以及建立的各种管理制度、法规等。

**参考答案：A**

## 试题28-悲-技-N.GJ.30.p000-5.00-信息安全

28、一般而言，网络安全审计从审计级别上可分为（ ）、应用级审计和用户级审计三种级别

A、组织级审计 B、物理审计

C、系统级审计 D、单元级审计

**分析：**

百度百科“网络安全审计”：

网络安全审计的类型

网络安全审计从审计级别上可分为3种类型：系统级审计、应用级审计和用户级审计。

1）系统级审计

系统级审计主要针对系统的登入情况、用户识别号、登入尝试的日期和具体时间、退出的日期和时间、所使用的设备、登入后运行程序等事件信息进行审查。典型的系统级审计日志还包括部分与安全无关的信息，如系统操作、费用记账和网络性能。这类审计却无法跟踪和记录应用事件，也无法提供足够的细节信息。

2）应用级审计

应用级审计主要针对的是应用程序的活动信息，如打开和关闭数据文件，读取、编辑、删除记录或字段的等特定操作，以及打印报告等。

3）用户级审计

用户级审计主要是审计用户的操作活动信息，如用户直接启动的所有命令，用户所有的鉴别和认证操作，用户所访问的文件和资源等信息。

**参考答案：C**

## 2016年上

## 试题16-命-技-Y.GJ.24.p543-5.00-信息安全

16、在信息系统安全保护中，信息安全策略控制用户对文件、数据库表等客体的访问属于（）安全管理

A、安全审计 B、入侵检测

C、访问控制 D、人员行为

**分析：**

3. 访问控制技术

访问控制按照事先确定的规则决定主体对客体的访问是否合法。当一主体试图非法使用一个未经授权的资源时，访问控制将拒绝这一企图，并将这一事件报告给审计跟踪系统，审计跟踪系统将给出报警并记录日志档案。

**参考答案：C**

## 试题17-悲-技-N.GJ.00.p000-5.00-信息安全

17、IDS发现网络接口收到来自特定IP地址的大量无效的非正常生成的数据包，使服务器过于繁忙以至于不能应答请求，IDS会将本次攻击方式定义为（）

A、拒绝服务攻击 B、地址欺骗攻击

C、会话劫持 D、信号包探测程序攻击

**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，是黑客常用的攻击手段之一。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，迫使服务器把非法用户的连接复位，影响合法用户的连接。

**参考答案：A**

## 试题18-命-技-N.GJ.26.p000-5.00-信息安全

18、通过收集和分析计算机系统或网络的关键节点信息，以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的技术被称为（）

A. 系统检测 B. 系统分析

C. 系统审计 D. 入侵检测

**分析：**

百度百科：

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。

**参考答案：D**

## 2016年下

## 试题16-命-技-N.ZJ.17.p000-5.00-信息安全

16、为了保护网络系统的硬件、软件及其系统中的数据，需要相应的网络安全工具，以下安全工具中，（）被比喻为网络安全的大门，用来鉴别什么样的数据包可以进入企业内部网。

A. 杀毒软件 B. 入侵检测系统

C. 安全审计系统 D. 防火墙

**分析：**

防火墙（Firewall），也称防护墙，是由Check Point创立者Gil Shwed于1993年发明并引入国际互连网（US5606668（A）1993-12-15）。它是一项信息安全的防护系统，依照特定的规则，允许或是限制传输的数据通过。在网络中，所谓“防火墙”，是指一种将内部网和公众访问网（如Internet）分开的方法，它实际上是一种隔离技术。防火墙是在两个网络通讯时执行的一种访问控制尺度，它能允许你“同意”的人和数据进入你的网络，同时将你“不同意”的人和数据拒之门外，最大限度地阻止网络中的黑客来访问你的网络。换句话说，如果不通过防火墙，公司内部的人就无法访问Internet，Internet上的人也无法和公司内部的人进行通信。

**参考答案：D**

## 试题17-悲-技-Y.GJ.29.p613-5.00-信息安全

17、信息系统访问控制机制中，（）是指对所有主体和客体部分分配安全标签用来标识所属的安全级别，然后在访问控制执行时对主体和客体的安全级别进行比较，确定本次访问是否合法性的技术或方法

A. 自主访问控制

B. 强制访问控制

C. 基于角色的访问控制

D. 基于组的访问控制

**分析：**

访问控制机制分类

系统独立于用户行为强制执行访问控制，用户不能改变他们的安全级别或对象的安全属性。这样的访问控制规则通常对数据和用户按照安全等级划分标签，访问控制机制通过比较安全标签来确定的授予还是拒绝用户对资源的访问。

**参考答案：B**

## 试题18-命-技-Y.ZJ.02.p127-5.00-信息系统审计

18、以下关于信息系统审计的叙述中。不正确的是（）

A. 信息系统审计是安全审计过程的核心部分

B. 信息系统审计的目的是评估并提供反馈、保证及建议

C. 信息系统审计是了解规划、执行及完成审计工作的步骤与技术，并尽量遵守国际信息系统审计与控制协会的一般公认信息系统审计准侧、控制目标和其他法律与规定

D. 信息系统审计的目的可以是收集并评估证据以决定一个计算机系统（信息系统）是否有效做到保护资产、维护数据完整、完成组织目标

**分析：**

新版中级教程p127-2.3.3 信息系统审计

信息系统审计是全部审计过程的一个部分。

**参考答案：A**