**信息安全工程师每日一练（2016/9/3）**

第**1**题： 以下关于入侵检测系统的描述中，说法错误的是（ ）。
A. 入侵检测系统能够对网络活动进行监视
B. 入侵检测能简化管理员的工作，保证网络安全运行
C. 入侵检测是一种主动保护网络免受攻击的安全技术
D. 入侵检测是一种被动保护网络免受攻击的安全技术

第**2**题： 网络安全体系设计可从物理线路安全、网络安全、系统安全、应用安全等方面来进行。其中，数据库容灾属于（ ）
A、物理线路安全和网络安全  B、物理线路安全和应用安全
C、系统安全和网络安全  D、系统安全和应用安全

第**3**题： 衡量一个漏洞扫描产品功能强弱的重要因素()。
A、能扫描的操作系统数目B、能扫描的应用服务的数目C、能扫描漏洞特征的数目D、能扫描的协议数目

第**4**题： 不影响异常检测的误警率的因素有()。
A、特征量的选择B、攻击签名的正确表示C、参考阈值的选择D、特征轮廓的更新

第**5**题： 下面哪个功能属于操作系统中的安全功能()
A、控制用户的作业排序和运行
B、实现主机和外设的并行处理以及异常情况的处理
C、保护系统程序和作业，禁止不合要求的对程序和数据的访问
D、对计算机用户访问系统和资源的情况进行记录

第**6**题： 私网地址用于配置本地网络、下列地址中属于私网地址的是？（）
A、100.0.0.0    B、172.15.0.0   C、192.168.0.0     D、244.0.0.0

第**7**题： 在入侵检测的基础上，锁定涉嫌非法使用的用户，并限制和禁止该用户的使用。这种访问安全控制是？（）
A、入网访问控制     B、权限控制    C、网络检测控制    D、防火墙控制

第**8**题： 在计算机房出入口处或值班室，应设置（）和应急断电装置。
A、电视     B、电扇     C、报警器     D、应急电话

第**9**题： PKI（公共密钥基础结构）中应用的加密方式为（）。
A、对称加密    B、非对称加密    C、HASH加密    D、单向加密

第**10**题： 以下哪一项是常见Web站点脆弱性扫描工具？()
A、Appscan   B、Nmap   C、Sniffer   D、LC

**信息安全工程师每日一练（2016/9/4）**

第**1**题： 信息安全从社会层面来看，反映在（ ）这三个方面。
A．网络空间的幂结构规律、自主参与规律和冲突规律
B．物理安全 、数据安全和内容安全
C．网络空间中的舆论文化、社会行为和技术环境
D．机密性、完整性、可用性

第**2**题： 公钥密码是（1），常用的公钥加密算法有（2），它可以是实现加密和数字签名。
（1）A、对称密钥技术，有1个密钥。B、不对称密钥技术，有2个密钥。
C、对称密钥技术，有2个密钥。D、不对称密钥技术，有1个密钥。
（2）A、DESB、IDES C、三元DES D、RSA

第**3**题： 设数据码字为10010011，采用海明码进行校验，则必须加入  （ ）  比特冗余位才能纠正一位错。
A、2 B、3 C、4 D、5

第**4**题： 下列算法中，( )属于摘要算法。
A、DES  B、MD5  C、Diffie-Hellman  D、AES

第**5**题： 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

第**6**题： 什么命令关闭路由器的finger服务？（）
A、disable finger    B、no finger    C、no finger service    、no service finger

第**7**题： 在分布式开放系统的环境中，以下哪个选项的数据库访问服务提供允许或禁止访问的能力？（）
A、对话管理服务 B、事务管理服务 C、资源管理服务 D、控制管理服务

第**8**题： 对网络中两个相邻节点之间传输的数据进行加密保护的是（）。
A、节点加密    B、链路加密    C、端到端加密    D、DES加密

第**9**题： 请从下列各项中选出不是HASH函数算法的一项。（）
A、MD5    B、SHA    C、HMAC    D、MMAC

第**10**题： 在大多数情况下，病毒侵入计算机系统以后，()。
A、病毒程序将立即破坏整个计算机软件系统
B、计算机系统将立即不能执行我们的各项任务
C、病毒程序将迅速损坏计算机的键盘、鼠标等操作部件
D、一般并不立即发作，等到满足某种条件的 时候，才会出来活动捣乱、破坏

**信息安全工程师每日一练（2016/9/5）**

第**1**题： 在（ ）中，①代表的技术通过对网络数据的封包和加密传输，在公网上传输私有数据、达到私有网络的安全级别；②代表的技术把所有传输的数据进行加密，可以代替telnet，可以为ftp提供一个安全的“通道”；③代表的协议让持有证书的Internet浏览器软件和WWW 服务器之间构造安全通道传输数据，该协议运行在TCP/IP 层之上，应用层之下。
A. ①SSH②VPN③SSL B. ①VPN②SSH③SSL C. ①VPN②SSL③SSH D. ①SSL②VPN③SSH

第**2**题： 系统运行安全的关键是管理，下列关于日常安全管理的做法，不正确的是（ ）。
A.系统开发人员和系统操作人员应职责分离
B.信息化部门领导安全管理组织，一年进行一次安全检查
C.用户权限设定应遵循“最小特权”原则
D.在数据转储、维护时要有专职安全人员进行监督

第**3**题： PH公司是一家共有45人的系统集成公司。为加强知识产权保护等安全管理，PH公司对公司内局域网采取了以下安全解决方案:安装防火墙限制对Internet的访问;安装过滤软件禁止邮件被发送到Internet;对堆叠在一起的两台24口千兆交换机的每个端口进行“端口+MAC地址+IP地址”绑定，限制无关计算机访问内部局域网;每台计算机只安装DVDROM并在BIOS中禁用USB口以防止公司重要文档被拷贝。但公司发现，这些措施没能阻止公司机密文档的泄露。
该安全解决方案存在的一个明显且主要的漏洞是( )。
A.防火墙不能阻止信息传送
B.员工可建立FTP服务器外传文档
C.没有设置进入网络的密码系统
D.没有在公司内部部署CA服务器

第**4**题： 许多黑客利用软件实现中的缓冲区溢出漏洞进行攻击，对于这一威胁，最可靠的解决方案是 （ ） 。
A、安装防火墙 B、安装用户认证系统 C、安装相关的系统补丁软件 D、安装防病毒软件

第**5**题： 具有保密资质的公司中一名涉密的负责信息系统安全的安全管理员提出了离职申请，公司采取的以下安全控制措施中，( )可能存在安全隐患.
A、立即终止其对安全系统的所有访问权限
B、收回所有相关的证件、徽章、密钥、访问控制标志、提供的专用设备等
C、离职员工办理完人事交接，继续工作一个月后离岗
D、和离职人员签订调离后的保密要求及协议

第**6**题： 公司总部与分部之间需要传输大量数据，在保障数据安全的同时又要兼顾密钥算法效率，最合适的加密算法是（）。
A. RC-5  B. RSA  C. ECC  D. MD5

第**7**题： 以下关于入侵检测设备的叙述中，（）是不正确的。
A．不产生网络流量    B．使用在尽可能靠近攻击源的地方

 C．使用在尽可能接近受保护资源的地方 D．必须跨接在链路上

第**8**题： 以下不属于防火墙技术的是 (  )。
A：IP过滤B：线路过滤C：应用层代理D：计算机病毒检测

第**9**题： 某公司财务管理数据只能提供给授权用户，通过采取安全管理措施确保不能被未授权的个人、实体或过程利用或知悉，以确保数据的（ ）
A、保密性B、完整性C、可用性D、稳定性

第**10**题： ()的误警率很高，但对于未知的入侵行为的检测非常有效。
A、滥用检测B、异常检测C、主机检测D、网络检测

第**11**题： 基于椭圆曲线上离散对数困难性的公钥算法是()。
A、DES B、RSA C、Elgamal D、ECC

第**12**题：  PKI使用的身份认证技术是（ ）。
A、数字签名B、CA C、MAC D、HMAC

第**13**题： 关于 Windows 2000 中的身份验证过程，下面哪种说法是错误的？()
A、如果用户登录一个域，则 Windows 2000将把这些登录信息转交给域控制器处理。
B、如果用户登录本机，则 Windows 2000将把这些登录信息转交给域控制器处理。
C、如果用户登录一个域，则 Windows 2000利用域控制器含有的目录副本，验证用户的登录信息。
D、如果用户登录本机，则 Windows 2000利用本机的安全子系统含有的本机安全数据库，验证用户的登录信息。

第**14**题： 安全审计是对系统活动和记录的独立检查和验证，以下哪一项不是审计系统的()
A.辅助辨识和分析未经授权的活动或攻击
B.对与己建立的安全策略的一致性进行核查
C.及时阻断违反安全策略的访问
D.帮助发现需要改进的安全控制措施

第**15**题： 计算机病毒是一种破坏计算机功能或者毁坏计算机中所存储数据的\_\_\_\_\_。
A、程序代码B、微生物病菌C、计算机专家

第**16**题： 从技术角度上看数据安全的技术特征主要包含哪几个方面？（）。
A、数据完整性、数据的方便性、数据的可用性
B、数据的完整性、数据的保密性、数据的可用性
C、数据的稳定性、数据的保密性、数据的可用性
D、数据的方便性、数据的稳定性、数据的完整性

第**17**题： 在3DES算法中，密钥最高可达到多少位？（）
A、96    B、128    C、168    D、200

第**18**题： 以下哪些软件是用于加密的软件？（）
A、PGP              B、SHA              C、EFS              D、DES

第**19**题： 防止用户被冒名所欺骗的方法是（）。
A、对信息源发放进行身份验证B、进行数据加密C、对访问网络的流量进行过滤和保护   D、采用防火墙

第**20**题： 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

**信息安全工程师每日一练（2016/10/3）**

第**1**题： 要成功实施信息系统安全管理并进行维护，应首先对系统（ ）进行评估鉴定。
A.风险 B.资产 C.威胁 D.脆弱性

第**2**题： 下列属于包过滤型防火墙优点的是（）。
A、包过滤型防火墙对用户和网络应用是透明的B、包过滤型防火墙维护简单
C、支持有效的用户身份认证D、能够对通过包过滤型防火墙的所有信息进行全面的监控

第**3**题：  灾难恢复计划是一个十分复杂的文档，因此需要测试。测试的必要性不仅在于检验其正确性，而且在于检查其是否处于()。
A、正常响应状态B、故障检测状态C、执行状态D、备用状态

第**4**题： 一个数据包过滤系统被设计成允许你要求服务的数据包进入，而过滤掉不必要的服务。这属于什么基本原则。（  ）
A、访问控制机制B、最小特权管理机制C、身份鉴别机制D、安全审计机制

第**5**题： 风险管理的重点：()
A．将风险降低到可以接受的程度B．不计代价的降低风险

C．将风险转移给第三方D．惩罚违反安全策略规定的雇员
第**6**题： 以下选项中那一项是对信息安全风险采取的纠正机制?()
A．访问控制B．入侵检测C．灾难恢复D．防病毒系统

第**7**题： “保护数据库，防止未经授权的或不合法的使用造成的数据泄露、更改破坏。”这是指数据的（   ）
A．并发控制　  　　　B．完整性 　　　C．安全性　D．恢复
第**8**题： TCP/IP协议中，负责寻址和路由功能的是哪一层？()
A、应用层B、传输层C、网络层D、数据链路层
第**9**题： 非对称加密需要 \_\_\_\_\_对密钥()
A、1或2 B、0或2 C、0或1

第**10**题： 关于全员参与原则的理解，以下哪一项说法不确切()
A、信息安全并非仅仅是IT部门的事
B、每一个员工都应该明白，时时处处都存在信息不安全的隐患
C、每一个员工都应该参与所有的信息安全工作
D、每一个员工都应该明确自己肩负的信息安全责任

**信息安全工程师每日一练（2016/10/6）**

第1题： 某公司网管员对核心数据的访问进行控制时，针对每个用户指明能够访问的资源，对于不在指定资源列表中的对象不允许访问。该访问控制策略属于（ ）。
A．自主访问控制（DAC）B．强制访问控制（MAC）
C．基于角色的访问控制（RBAC）D．访问控制列表方式（ACL）

第2题： 在信息系统安全管理中，安全协议，公证和数字签名等技术主要用于提高信息系统的（  ）。
A.保密性B.可用性C.完整性D.不可抵赖性

第3题： 《互联网信息服务管理办法》规定，互联网信息服务提供者（网站）不得制作、复制、发布、传播、迷信、赌博、暴力、恐怖\_\_\_\_\_等违法有害信息。
A、淫秽色情B、商业广告C、新闻信息

第4题： 按TCSEC标准，WinNT的安全级别是（）。
A、C2 B、B2 C、C3 D、B1

第5题： 下列哪种攻击不是针对统计数据库的（）？
A、小查询集合大查询集攻击 B、中值攻击 C、跟踪攻击 D、资源解析攻击

第6题： 以下是对客户/服务器数据库系统的描述，请选择错误描述的选项。（）
A、客户端的用户将数据进行处理可自行存放到本地，无须传送到服务器处理，从而显著减少了网络上的数据传输量，提高了系统的性能和负载能力
B、主从式数据库系统中的主机和分布式数据库系统中的每个节点都是一个通用计算机，既执行DBMS功能又执行应用程序
C、在网络中把某些节点的计算机专门用于执行DBMS核心功能，这台计算机就成为数据库服务器
D、其他节点上的计算机安装DBMS外围应用开发工具和应用程序，支持用户的应用，称为客户机

第7题： 公钥加密体制中，没有公开的是（）。
A、明文    B、密文    C、公钥    D、算法

第8题： 以下哪项不属于数据库系统实体安全？（）
A、环境安全    B、线路安全    C、设备安全    D、媒体安全

第9题： Internet组织中负责地址、号码的分配的组织是什么？()
A、Internet SocietyB、IANAC、IETFD、IESG

第10题： 在TCP/IP协议体系结构中，传输层有哪些协议？()
A、TCP和IP B、UDP和TCP C、IP 和ICMP D、TCP、IP、UDP、ICMP

第11题： 集中监控有效解决了监控\_\_\_\_\_\_要求()
A、专业性、集中控制、不间断性B、专业性、实时性、不间断性C、专业性、实时性、永久性

第12题： 网络监控目前技术上的不足主要体现在()
A、只有误报率高B、只有漏报率C、误报率和漏报率都高

第13题： 法律是由那个部门通过的？()
A、人民代表大会B、国务院C、政府部门

第14题： 我国《刑法》中第几条规定了“破坏计算机信息系统罪”()
A、第二百八十五条B、第二百八十六条C、第二百八十七条

第15题： 1985年，美国国防部公布了可信计算机系统评估准则（TCSEC-Trusted Com puter System Evaluation Criteria）俗称()
A、橘皮书B、白皮书C、黄皮书

第16题： 人是存储身份认证标识介质之一()
A、是B、否

第17题： 加密认证措施的选择依赖于信息的分级与用户的分类的结果()
A、是B、否

第18题： 世界上第一个针对IBM-PC机的计算机病毒是()
A、大麻病毒B、小球病毒C、巴基斯坦病毒D、米开朗基罗病毒

第19题： 引导型病毒可以通过哪些途径传染\_\_\_\_\_()
A、文件B、浏览器C、软盘D、电子邮件

第20题： 发现来历不明的邮件，杀毒软件又未能报警，可以将邮件转发给国家计算机病毒应急处理中心的邮箱Sos@antivirus-China.org.cn()

A、对B、错
**2016/9/3 1~5 D D C B C 6~10 C C D B A**

**2016/9/4 1~5 C BD C B C 6~10 C C A D D**

**2016/9/5 1~5 B B A C C 6~10 A D D A B**

 **11~ 15 D A B C A 16~20 B C A A C**

**2016/10/3 1~5 D A D B A 6~10 C C C C C**

**2016/10/6 1~5 A C A A D 6~10 A A B B B**

 **11~15 B C A B A 16~20 A A C C A**