**信息安全工程师每日一练（2016/8/20）**

第**1**题： 基于网络的入侵检测系统的输入信息源是（）。
A、系统的审计日志  B、系统的行为数据 C、应用程序的事务日志文件     D、网络中的数据包

第**2**题： 对应 telnet服务的 tcp端口是()。
A、20 B、21 C、23 D、25

第**3**题： IDS可以利用的信息来源不包括()。
A、逻辑形式的入侵信息B、网络和系统日志文件C、目录和文件中不期望的改变D、物理形式的入侵信息

第**4**题： 下列哪一个不是常见恶意电子邮件攻击？()
A、Outlook vCard缓冲区溢出B、恶意电子邮件---MIME扩展
C、VBS地址簿蠕虫D、cgi漏洞

第**5**题： 关于数据库安全的说法错误的是？（）
A.数据库系统的安全性很大程度上依赖于DBMS的安全机制
B.许多数据库系统在操作系统一下文件形式进行管理，因此利用操作系统漏洞可以窃取数据库文件
C.为了防止数据库中的信息被盗取，在操作系统层次对文件进行加密是唯一从根本上解决问题的手段
D.数据库的安全需要在网络系统、操作系统和数据库管理系统三个方面进行保护

第**6**题： 通常意义上的网络黑客是指通过互联网利用非正常手段\_\_\_\_\_。
A、上网的人B、入侵他人计算机系统的C、在网络上行骗的人

第**7**题： Windows nt/2k中的.pwl文件是？（）
A、路径文件 B、口令文件 C、打印文件 D、列表文件

第**8**题： 周期性行为，如扫描，会产生哪种处理器负荷?()
A、Idle Ioad   B、Usage Ioad C、Traffic load  D、以上都不对

第**9**题： 设置Cisco设备的管理员账号时，应（）。
A、多人共用一个账号     B、多人共用多个账号    C、一人对应单独账号     D、一人对应多个账号

第**10**题： 在WEB应用软件的系统测试技术中，下面不属于安全性测试内容的是（）。
A、客户端的内容安全性 B、服务器的内容安全性 C、数据库的内容安全性 D、Cookie安全性

**信息安全工程师每日一练（2016/8/21）**

第**1**题： 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（ ）
A、破坏B、抵赖C、截取D、窃取

第**2**题： 两个公司希望通过Internet传输大量敏感数据，从信息源到目的地之间的传输数据以密文形式出现，而且不希望由于在传输结点使用特殊的安全单元而增加开支，最合适的加密方式是  （1）  ，使用会话密钥算法效率最高的是  （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
第**3**题： 计算机病毒为了隐蔽起见,首先依靠它的()实现自身与合法的系统程序连接在一起。
A、系统调用部分B、启动部分C、破坏部分D、传染部分

第**4**题： 漏洞扫描攻击和端口扫描攻击的关系()
A、漏洞扫描攻击应该比端口扫描攻击更早发生。
B、漏洞扫描攻击应该和端口扫描攻击同时发生。
C、漏洞扫描攻击应该比端口扫描攻击更晚发生。
D、漏洞扫描攻击与端口扫描攻击没有关系。

第**5**题： Snort是一个跨平台、轻量级的()入检测系统。
A、实时B、综合C、网络D、主机

第**6**题： 以下哪一项属于计算机用户策略？()
A、计算机所有权B、信息所有权C、计算机的使用许可D、以上都是

第**7**题： 硬盘主引导记录的英文简称是()。
A、MBR B、DBR C、FAT D、FDT

第**8**题： 在OSI模型中，主要针对远程终端访问，任务包括会话管理、传输同步以及活动管理等以下是哪一层（）
A、应用层    B、物理层     C、会话层     D、网络层

第**9**题： 以下是对层次数据库结构的描述，请选择错误描述的选项。（）
A、层次数据库结构将数据通过一对多或父节点对子节点的方式组织起来
B、一个层次数据库中，根表或父表位于一个类似于树形结构的最上方，它的字表中包含相关数据
C、它的优点是用户不需要十分熟悉数据库结构
D、层次数据库模型的结构就像是一棵倒转的树

第**10**题： 防雷保安器：防止()破坏计算机信息系统的保安装置，可分为两大类：电源线防雷保安器（简称电源防雷保安器）和信号传输线防雷保安器（简称通道防雷保安器）。
A、直击雷            B、感应雷      C、雷暴          D、雷电电磁脉冲

**信息安全工程师每日一练（2016/8/19）**

第**1**题： 目前，主流的安全数据库系统一般使用( )来实现其访问控制安全机制.
A.访问控制矩阵(ACM) B.访问控制表(ACLs)
C.授权关系表(Authorization Relations) D.能力表(Capabilities)

第**2**题： 安全电子邮件协议PGP不支持  （ ）  。
A、确认发送者的身份 B、确认电子邮件未被修改  C、防止非授权者阅读电子邮件  D、压缩电子邮件大小

第**3**题： 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

第**4**题： 有关计算机病毒的传播途径，不正确的说法是()。
A、共用软盘B、软盘复制C、借用他人的软盘D、和带毒盘放在一起

第**5**题： 从安全分析员的观点来看，Windows2000可以监视三种主要事件来确保安全。其中不属于监视范围的是（ ）。
A、登录注销B、对象访问C、进程追踪D、上网追踪

第**6**题： 在风险评估中进行定量的后果分析时，如果采用年度风险损失值的方法进行计算，应当使用一下哪个公式？（）
A．SLE（单次损失预期值）x  ARO（年度发生率）
B．ARO（年度发生率）x  EF(暴露因子)
C．SLE（单次损失预期值）x  EF(暴露因子) x  ARO（年度发生率）
D．SLE（单次损失预期值）x  ARO（年度发生率）—EF(暴露因子)

第**7**题： 下面哪一项安全控制措施不是用来检测未经授权的信息处理活动的：()
A．设置网络连接时限B．记录并分析系统错误日志
C．记录并分析用户和管理员日志D．时钟同步

第**8**题： 为了保护企业的知识产权和其它资产，当终止与员工的聘用关系时下面哪一项是最好的方法？（）
A、进行离职谈话，让员工签署保密协议，禁止员工账号，更改密码
B、进行离职谈话，禁止员工账号，更改密码
C、让员工签署跨边界协议
D、列出员工在解聘前需要注意的所有责任

第**9**题： 《国家保密法》对违法人员的量刑标准是（）。
A、国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重的，处三年以下有期徒刑或者拘役；情节特别严重的，处三年以上七年以下有期徒刑
B、国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重的，处四年以下有期徒刑或者拘役；情节特别严重的，处四年以上七年以下有期徒刑
C、国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重的，处五年以下有期徒刑或者拘役；情节特别严重的，处五年以上七年以下有期徒刑
D、-国家机关工作人员违法保护国家秘密的规定，故意或者过失泄露国家秘密，情节严重，处七年以下有期徒刑或者拘役；情节特别严重的，处七年以下有期徒刑

第**10**题： 网络营业厅提供相关服务的可用性应不低于（）。
A、99.99%  B、99.9% C、99%  D、98.9%

**信息安全工程师每日一练（2016/8/22）**

第**1**题： 信息安全的级别划分有不同的维度，以下级别划分正确的是（ ）。
A.系统运行安全和保密有5个层次，包括设备级安全、系统级安全、资源访问安全、功能性安全和数据安全
B.机房分为4个级别：A级、B级、C级、D级
C.根据系统处理数据划分系统保密等级为绝密、机密和秘密
D.根据系统处理数据的重要性，系统可靠性分A级和B级

第**2**题： 应用系统运行中涉及的安全和保密层次包括系统级安全、资源访问安全、功能性安全和数据域安全。通常，系统级安全策略不包括
A.访问IP地址段的限制B.特定时间段内登录次数的限制
C.上传附件不能超过指定大小D.敏感系统的隔离

第**3**题： 安全制度是信息安全的重要保障，以下关于信息系统安全管理制度说法不正确的是（ ）。
A、安全管理制度需要建设单位、监理、承建单位三方人员共同执行
B、安全管理制度需要由监理单位制定，并报建设单位批准后执行
C、安全管理制度包括出入管理、系统升级、人事管理、应急等相关制度
D、安全管理制度的有效执行是系统安全建设成功实施的关键

第**4**题： 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

第**5**题： 计算机病毒传播速度最快、最广的途径是()。
A、用软盘复制来传播文件时B、用 U盘复制来传播文件时
C、安装系统软件时D、用网络传播文件时

第**6**题： 目前使用的防病毒软件的作用是()。
A、查出己感染的任何病毒B、查出已知名的病毒，清除部分病毒
C、清除任何己感染的病毒D、查出并清除任何病毒

第**7**题： 对于提供网络服务的内部网络，通常选择下列哪种防火墙对服务效率影响最大()。
A、包过滤防火墙B、双宿主机防火墙C、屏蔽主机防火墙D、屏蔽子网防火墙

第**8**题： 基于网络的入侵检测系统利用()作为数据源。
A、审计记录B、日志记录C、网络数据包D、加密数据

第**9**题： 当你感觉到你的Win2003运行速度明显减慢，当打开任务管理器后发现CPU使用率达到了100%，你认为你最有可能受到了（）攻击。
A、缓冲区溢出攻击 B、木马攻击 C、暗门攻击 D、DOS攻击

第**10**题： 针对一台对外提供Web服务的Windows服务器，下列关于账户权限控制，哪些项是不合理的？（）
A、限制匿名账户对Web内容的目录写权限B、从Everyone组中删除“从网络访问此计算机” 用户权限
C、禁用IUSR-MACHE和IWAN\_MACHINE账户 D、本地登录时必须使用Administrators账户

**信息安全工程师每日一练（2016/8/23）**

第**1**题： 信息安全策略的设计与实施步骤是（ ）
A.定义活动目录角色、确定组策略管理安全性、身份验证、访问控制和管理委派
B.确定标准性、规范性、可控性、整体性、最小影响、保密性原则，确定公钥基本结构
C.确定安全需求、制订可实现的安全目标、制订安全规划、制订系统的日常维护计划
D.确定安全需求、确定安全需求的范围、制订安全规划、制订系统的日常维护计划

第**2**题： 关于RSA 算法的叙述不正确的是（ ） 。
A. RSA 算法是一种对称加密算法B. RSA 算法的运算速度比DES慢
C. RSA 算法可用于某种数字签名方案D. RSA 的安全性主要基于素因子分解的难度

第**3**题： 使用网上银行卡支付系统付款与使用传统信用卡支付系统付款，两者的付款授权方式是不同的，下列论述正确的是（ ）。
A．前者使用数字签名进行远程授权，后者在购物现场使用手写签名的方式授权商家扣款
B．前者在购物现场使用手写签名的方式授权商家扣款，后者使用数字签名进行远程授权
C．两者都在使用数字签名进行远程授权
D．两者都在购物现场使用手写签名的方式授权商家扣款

第**4**题： 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

第**5**题： IIS6.0支持的身份验证安全机制有4种验证方法，  其中安全级别最高的验证方法是( )。
A、匿名身份验证 B、集成Windows身份验证 C、基本身份验证 D、摘要式身份验证

第**6**题： 《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（）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

第**7**题： 认证(Authentication)是防止(  )攻击的重要技术。
A：主动B：被动C：黑客D：偶然

第**8**题： 基于网络系统的漏洞库大体包括()。
A、CGI漏洞扫描、POP3漏洞扫描、FTP漏洞扫描、SSH漏洞扫描
B、CGI漏洞扫描、POP3漏洞扫描、SSH漏洞扫描、HTTP漏洞扫描
C、CGI漏洞扫描、FTP漏洞扫描、SSH漏洞扫描、HTTP漏洞扫描
D、CGI漏洞扫描、POP3漏洞扫描、FTP漏洞扫描、SSH漏洞扫描、HTTP漏洞扫描

第**9**题： 下面哪一个情景属于授权（Authorization）()
A、用户依照系统提示输入用户名和口令
B、用户在网络上共享了自己编写的一份Office文档，并设定哪些用户可以阅读，哪些用户可以修改
C、用户使用加密软件对自己编写的Office文档进行加密，以阻止其他人得到这份拷贝后看到文档中的内容
D、某个人尝试登录到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登录过程纪录在系统日志中

第**10**题： 以下哪个不包含在证书中？（）
A、密钥采取的算法    B、公钥及其参数    C、私钥及其参数    D、签发证书的CA名称

**信息安全工程师每日一练（2016/8/24）**

第**1**题： 在构建信息安全管理体系中，应建立起一套动态闭环的管理流程，这套流程指的是（ ）。
A．评估—响应—防护—评估
B．检测—分析—防护—检测
C．评估—防护—响应—评估
D．检测—评估—防护—检测

第**2**题： 某公司使用包过滤防火墙控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

第**3**题： 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

第**4**题： 下列哪一项不是攻击者通常使用下载文件的方法()。
A、SMB B、FTP C、TFTP  D、TELNET
第**5**题： 通过网络将文件备份到与本地计算机物理上相分离的存储介质上的备份称为()。
A、异地备份B、本地备份C、可更新备份D、动态备份

第**6**题： 信息系统开发一般不包括以下哪个阶段（）
A、系统分析B、系统设计C、系统实施D、系统维护

第**7**题： 网络隔离技术的目标是确保把有害的攻击隔离，在保证网络内部信息不外泄的前提下，完成网络间数据的安全交换。下列隔离技术中，安全性最好的是（）。
A、多重安全网关     B、防火墙     C、Vlan隔离    D、物理隔离

第**8**题： DBS是采用了数据库技术的计算机系统。DBS是一个集合体，包含数据库、计算机硬件、软件和（）。
A、系统分析员     B、程序员     C、数据库管理员     D、操作员

第**9**题： 电子邮件的机密性与真实性是通过下列哪一项实现的？（）
A、用发送者的私钥对消息进行签名，用接受者的公钥对消息进行加密
B、用发送者的公钥对消息进行签名，用接受者的私钥对消息进行加密
C、用接受者的私钥对消息进行签名，用发送者的公钥对消息进行加密
D、用接受者的公钥对消息进行签名，用发送者的私钥对消息进行加密

第**10**题：

以下关于口令安全的说法，错误的是：（     ）

A. 一般情况下，设置口令时，应保证口令最小长度为6位

B. 为避免遗忘，应将口令设置为生日、电话号码等容易记忆的内容

C. 口令应至少包含数字、大小写字母及特殊符号中的任意两种字符

D. 最长90天进行一次口令更改

**信息安全工程师每日一练（2016/8/25）**

第**1**题：

下图是发送者利用不对称加密算法向接收者传送信息的过程，图中  k1是（ ）。

A.  接收者的公钥 B. 接收者的私钥C. 发送者的公钥 D. 发送者的私钥
第**2**题： 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”

第**3**题： Fdisk软件运行后，在磁盘中创建的记录是()。
A、MBR B、DBR C、FAT D、FDT

第**4**题： 在UNIX系统中输入命令“LS-al  test”显示如下;-rwxr-xr-x  3  root root  1024  Sep  13 11:58  test”对他的含义解释错误的是：()
A、这是一个文件，而不是目录   B、文件的拥有者可以对这个文件读、写和执行的操作
C、文件所属组的成员有可以读它，也可以执行它 D、其他所有用户只可以执行它

第**5**题： 保证计算机信息运行的安全是计算机安全领域中最重要的环节之一，以下（）不属于信息运行安全技术的范畴。
A、风险分析 B、审计跟踪技术 C、应急技术 D、防火墙技术

第**6**题： Windows NT的安全标识符(SID)是由当前时间、计算机名称和另外一个计算机变量共同产生的，这个变量是:()。
A、击键速度 B、当前用户名C、用户网络地址 D、处理当前用户模式线程所花费CPU的时间

第**7**题： SQL Sever的默认通讯端口有哪些？（）
A、TCP 1025   B、TCP 1433    C、UDP 1434    D、TCP 14333    E、TCP 445

第**8**题： 在计算机机房或其他数据处理环境中，较高的潮湿环境会带来如下哪些弊端？ ()
A、产生静电        B、计算机部件腐蚀            C、有污染物                 D、B+A

第**9**题： ()是由权威机构CA发行的一种权威性的电子文档，是网络环境中的一种身份证。
A、认证机构    B、密码    C、票据    D、数字证书

第**10**题： 网络窃听（Sniffer）可以捕获网络中流过的敏感信息，下列说法错误的是（）
A、密码加密后，不会被窃听   B、Cookie字段可以被窃听
C、报文和帧可以窃听   D、高级窃听者还可以进行ARPSpoof，中间人攻击

**信息安全工程师每日一练（2016/8/26）**

第**1**题： 公钥体系中，私钥用于　（1）　，公钥用于　（2）　。
（1）A、解密和签名  B、加密和签名  C、解密和认证  D、加密和认证
（2）A、解密和签名  B、加密和签名  C、解密和认证  D、加密和认证
第**2**题： 下列攻击方式中，（）不是利用TCP/IP漏洞发起的攻击。
A．SQL注入攻击 B．Land攻击 C．Ping of Death D．Teardrop攻击

第**3**题： 执行密码变换之前的原始消息称为()。
A、明文B、密文C、密钥D、密码

第**4**题： 传统的安全方案要取得成功依赖于系统正确的设置和完善的()。
A、防御手段B、安全体系C、安全标准D、信息保护

第**5**题：  一个恰当的灾难恢复计划应考虑各种故障的级别：单个系统、()、整个系统。
A、单个设备B、数据中心C、多点热备D、业务集合

第**6**题： 在Windows 2003下netstat的哪个参数可以看到打开该端口的PID?()（格式到此）
A、a B、n   C、o D 、p

第**7**题： 接入控制方面，路由器对于接口的要求包括：（）。
A、串口接入    B、局域网方式接入     C、Internet方式接入     D、VPN接入
第**8**题： 下列哪种方法不能有效的防范SQL进入攻击（）？
A、对来自客户端的输入进行完备的输入检查
B、把SQL语句替换为存储过程、预编译语句或者使用ADO命令对象
C、使用SiteKey技术
D、关掉数据库服务器或者不使用数据库

第**9**题： 作为一台运行IIS 在Internet发布站点的Windows  Web服务器，下面哪项服务不是必需的？（）
A、IIS  Admin B、Net  Logon
C、Performance  Logs  and  Alerts D、World  Wide  Web  Publishing

第**10**题： 数字签名可以解决（）。
A、数据被泄露    B、数据被篡改    C、未经授权擅自访问    D、冒名发送数据或发送后抵赖

**2016/8/20 1~5 D C A D C 6~10 B B A C C**

**2016/8/21 1~5 C CB B C C 6~10 D A A C B**

**2016/8/19 1~5 C D D D D 6~10 A D A A A**

**2016/8/22 1~5 C C B D D 6~10 B B C D C**

**2016/8/23 1~5 C A A C B 6~10 D A D B C**

**2016/8/24 1~5 A B A D A 6~10 D D C A B**

**2016/8/25 1~5 A C A D B 6~10 D B B D A**

**2016/8/26 1~5 AD A A A B 6~10 C D C B D**