**信息安全工程师每日一练（2016/7/20）**

第**1**题： "需要时，授权实体可以访问和使用的特性"指的是信息安全的（ ）。
A．保密性B．完整性C．可用性D．可靠性

第**2**题： 下面关于防火墙的说法，正确的是 （ ） 。
A、防火墙一般由软件以及支持该软件运行的硬件系统构成
B、防火墙只能防止未经授权的信息发送到内网
C、防火墙能准确地检测出攻击来自哪一台计算机
D、防火墙的主要支撑技术是加密技术

第**3**题： 以下人员中，谁负有决定信息分类级别的责任？（）
A、用户 B、数据所有者 C、审计员 D、安全官

第**4**题： 下列情形之一的程序，不应当被认定为《中华人民共和国刑法》规定的“计算机病毒等破坏性程序”的是：（）。
A、能够盗取用户数据或者传播非法信息的
B、能够通过网络、存储介质、文件等媒介，将自身的部分、全部或者变种进行复制、传播，并破坏计算机系统功能、数据或者应用程序的
C、能够在预先设定条件下自动触发，并破坏计算机系统功能、数据或者应用程序的
D、其他专门设计用于破坏计算机系统功能、数据或者应用程序的程序

第**5**题： 随着安全要求的提高、技术的演进，（）应逐步实现物理隔离，或者通过采用相当于物理隔离的技术（如MPLSVPN）实现隔离。
A、局域网     B、广域网及局域网     C、终端    D、广域网

第**6**题： 在建立堡垒主机时，（）。
A、在堡垒主机上应设置尽可能少的网络服务
B、在堡垒主机上应设置尽可能多的网络服务
C、对必须设置的服务给予尽可能高的权限
D、不论发生任何入侵情况，内部网始终信任堡垒主机

第**7**题： EFS可以用在什么文件系统下（）。
A、FAT16    B、FAT32    C、NTFS    D、以上都可以

第**8**题： 发送消息和用发送方私钥加密哈希加密信息将确保消息的：（）。
A、真实性和完整性    B、真实性和隐私    C、隐私和不可否认性    D。隐私和不可否性

第**9**题： 以下关于CA认证中心说法正确的是（）。
A、CA认证时使用对称密钥机制的认证方法
B、CA认证中心支负责签名，不负责证书的产生
C、CA认证中心负责证书的颁发和管理、并依靠证书证明一个用户的身份
D、CA认证中心不用保持中立，可以随便找一个用户来作为CA认证中心

第**10**题： PGP加密算法是混合使用（）算法和IDEA算法，它能够提供数据加密和数字签名服务，主要用于邮件加密软件。
A、DES              B、RSA              C、IDEA             D、AES

**信息安全工程师每日一练（****2016/7/21）**

第**1**题： 为了保障数据的存储和传输安全，需要对一些重要数据进行加密。由于对称密码算法（1），所以特别适合对大量的数据进行加密。国际数据加密算法IDEA的密钥长度是（2）位。
（1）A、比非对称密码算法更安全 B、比非对称密码算法密钥长度更长
C、比非对称密码算法效率更高 D、还能同时用于身份认证
（2）A、56 B、64 C、128 D、256

第**2**题： 下列安全协议中（）是应用层安全协议。
A．IPSec B．L2TP C．PAP D．HTTPS

第**3**题： <a href=“错误!超链接引用无效。% 72%61%74%69%6F%6E%61%69%72%2E%63%6F%6D%2F%72%65%71%2E%61% 73%70………………………………………….>中 www.microsoft.com是什么信息？()
A、服务器的域名B、用户名C、文件名D、主机名

第**4**题： 关于DDoS技术，下列哪一项描述是错误的()。
A、一些DDoS攻击是利用系统的漏洞进行攻击的
B、黑客攻击前对目标网络进行扫描是发功DDoS攻击的一项主要攻击信息来源
C、对入侵检测系统检测到的信息进行统计分析有利于检测到未知的黑客入侵和更为复杂的DDoS攻击入侵
D、DDoS攻击不对系统或网络造成任何影响

第**5**题： 若有多个Oracle数据需要进行集中管理，那么对sysdba的管理最好选择哪种认证方式（）？
A、系统认证 B、password文件认证方式 C、域认证方式 D、以上三种都可

第**6**题： 下列应用服务器中，不遵循J2EE规范的是（）？
A、MTS B、WebLogic C、Oracle 9iApplication Server D、WebSpere

第**7**题： AES属于哪种加密方式？（）。
A、流加密    B、分组加密    C、异或加密    D、认证加密

第**8**题： DES属于哪种加密方式？（）
A、流加密    B、块加密    C、异或加密    D、认证加密

第**9**题： 在高级加密标准AES算法中，区块大小为（）。
A、128位         B、192位         C、256位            D、512位

第**10**题： 与RSA（Rivest,Shamir,Adleman）算法相比，DDS（Digital Signature Standard）不包括（）
A、数字签名     B、鉴别机制     C、加密机制     D、数据完整性

**信息安全工程师每日一练（****2016/7/22）**

第**1**题： （ ）属于保证数据的完整性。
A、 保证传送的数据信息不被第三方监视和窃取
B、 保证数据信息在传输过程中不被篡改
C、 保证电子商务交易各方身份的真实性
D、 保证发送方不能抵赖曾经发送过某数据信息

第**2**题： 下面关于漏洞扫描系统的叙述，错误的是 （ ） 。
A、漏洞扫描系统是一种自动检测目标主机安全弱点的程序
B、黑客利用漏洞扫描系统可以发现目标主机的安全漏洞
C、漏洞扫描系统可以用于发现网络入侵者
D、漏洞扫描系统的实现依赖于系统漏洞库的完善

第**3**题： MySQL服务器通过 MySQL数据库里()向我们提供了一套灵活的权限控制机制。
A、视图表B、权限表C、数据表D、用户信息表

第**4**题：  CA在数字签名当中扮演的主要角色是()。
A、签名者B、仲裁C、验证者D、攻击者

第**5**题： 下列哪一个不是 ISAPI的缓冲区溢出？()
A、格式化字符串缓冲区溢出B、ida.dll 缓冲区溢出C、红色代码蠕虫病毒D、IPP缓冲区溢出

第**6**题： 目前我国颁布实施的信息安全相关标准中，以下哪一个标准属于强制执行的标准？（）
A、GB/T 18336-2001 信息技术安全性评估准则
B、GB 17859-1999 计算机信息系统安全保护等级划分准则
C、GB/T 9387.2-1995 信息处理系统开放系统互联安全体系结构
D、GA/T 391-2002 计算机信息系统安全等级保护管理要求

第**7**题： 以下属于4A策略管理模块可以管理的为（）。
A、访问控制策略     B、信息加密策略     C、密码策略     D、防火墙策略

第**8**题： 非对称密钥的密码技术具有很多优点，其中不包括：（）。
A、可提供数字签名、零知识证明等额外服务
B、加密/解密速度快，不需占用较多资源
C、通信双方事先不需要通过保密信道交换密钥
D、密钥持有量大大减少

第**9**题： 从技术角度，以下不是漏洞来源的是（）
A、软件或协议设计时候的瑕疵     B、软件或协议实现中的弱点
C、软件本身的瑕疵     D、显示卡内存容量过低

第**10**题： SSL主要利用数据加密技术，以确保数据在网络传输过程中不会被截取及窃听。该协议运行在网络的（）。
A．数据链路层   B．传输层与应用层之间C．传输层   D．应用层与会话层之间

**信息安全工程师每日一练（****2016/7/23）**

第**1**题： WindowsNT和Windows2000系统能设置为在若干次无效登录后锁定账号，此技术可以防止（  ）。
A、暴力攻击 B、木马病毒 C、缓存溢出攻击 D、IP欺骗

第**2**题： 某网站向CA申请了数字证书。用户通过 （1） 来验证网站的真伪。在用户与网站进行安全通信时，用户可以通过 （2） 进行加密和验证，该网站通过 （3） 进行解密和签名。
（1）A、CA的签名 B、证书中的公钥  C、网站的私钥  D、用户的公钥
（2）A、CA的签名  B、证书中的公钥  C、网站的私钥  D、用户的公钥
（3）A、CA的签名  B、证书中的公钥  C、网站的私钥  D、用户的公钥

第**3**题： 以下关于加密算法的叙述中，正确的是  （ ）  。
A、DES算法采用128位的密钥进行加密
B、DES算法采用两个不同的密钥进行加密
C、三重DES算法采用3个不同的密钥进行加密
D、三重DES 算法采用2个不同的密钥进行加密

第**4**题： HTTPS的安全机制工作在  (1)  。而S-HTTP的安全机制工作在  (2)  。
（1）A、网络层  B、传输层  C、应用层  D、物理层
（2）A、网络层  B、传输层 C、应用层  D、物理层

第**5**题： 当今IT的发展与安全投入，安全意识和安全手段之间形成()
A、安全风险屏障B、安全风险缺口C、管理方式的变革D、管理方式的缺口

第**6**题： 在NT中，怎样使用注册表编辑器来严格限制对注册表的访问？（）
A、HKEY\_CURRENT\_CONFIG,连接网络注册、登录密码、插入用户ID
B、HKEY\_CURRENT\_MACHINE,浏览用户的轮廓目录，选择NTUser.dat
C、HKEY\_USERS,浏览用户的轮廓目录，选择NTUser.dat
D、HKEY\_USERS,连接网络注册，登录密码，插入用户ID

第**7**题： 账户口令管理中4A的认证管理的英文单词为：（）
A、Account     B、Authentication     C、Authorization     D、Audit

第**8**题： 当IPS遇到软件/硬件问题时，强制进入直通状态，以避免网络断开的技术机制称为（）。
A、pass     B、bypass     C、watchdog     D、HA

第**9**题： 病毒在感染计算机系统时，一般（）感染系统的。
A、病毒程序都会在屏幕上提示，待操作者确认（允许）后
B、实在操作者不觉察的情况下
C、病毒程序会要求操作者制定存储的磁盘和文件夹后
D、在操作者为病毒制定存储的文件名以后

第**10**题： 下列措施中，()不是减少病毒的传染
和造成的损失的好办法。
A、重要的文件要及时、定期备份，使备份能反映出系统的最新状态
B、外来的文件要经过病毒检测才能使用，不要使用盗版软件
C、不与外界进行任何交流，所有软件都自行开发
D、定期用抗病毒软件对系统进行查毒、杀毒

**信息安全工程师每日一练（****2016/7/24）**

第**1**题： 下面有关加密技术的叙述中，（ ）是错误的。
A、IDEA是一种对称加密算法B、公钥加密技术和单向陷门函数密不可分
C、IKE是一种消息摘要算法D、公钥加密的一个重要应用是数字签名

第**2**题： 网络隔离技术的目标是确保把有害的攻击隔离，在保证可信网络内部信息部不外泄的前提下，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**3**题： 采用CRC进行差错校验，生成多项式为G(X)=X4+X+1，信息码字为10111，则计算出的CRC校验码是  （ ）  。
A、0000 B、0100 C、0010 D、1100

第**4**题： 发生()后，磁盘上的物理数据和日志文件被破坏，这是最严重的一种故障，恢复方法是重装数据库，然后重做已完成的事务。
A、系统故障B、事故故障C、介质故障D、软件故障

第**5**题： 那类 TCP扫描不带任何标志位？()
A、SYN扫描B、ACK扫描C、FIN扫描D、NULL扫描

第**6**题： 以下哪一种是入侵检测系统所通常采用的：()
A、基于网络的入侵检测系统
B、基于 IP的入侵检测系统
C、基于服务的入侵检测系统
D、基于域名的入侵检测系统

第**7**题： 对于信息安全发展历史描述正确的是：()
A.信息安全的概念是随着计算机技术的广泛应用而诞生的
B.目前信息安全己经发展到计算机安全的阶段
C.目前信息安全不仅仅关注信息技术，人们意识到组织、管理、工程过程和人员同样是促进 系统安全性的重要因素
D.我们可以将信息安全的发展阶段概括为，由“计算机安全”到“通信安全”，再到“信息 安全”，直至现在的“信息安全保障”

第**8**题： 信息产业部将以世界电信日主题纪念活动为契机，广泛进行宣传和引导，进一步增强电信行业和全社会的\_\_\_\_\_不意识。
A、国家安全B、网络与信息安全C、公共安全

第**9**题： 网络安全在多网合一时代的脆弱性体现在（）。
A、网络的脆弱性    B、软件的脆弱性   C、管理的脆弱性     D、应用的脆弱性

第**10**题： 交换机转发以太网的数据基于：（）。
A、交换机端口号     B、MAC地址     C、IP地址     D、数据类别

**信息安全工程师每日一练（****2016/7/25）**

第**1**题： 关于kerberos 和PKI 两种认证协议的叙述中正确的是（1），在使用kerberos 认证时，首先向密钥分发中心发送初始票据（2）来请求会话票据，以便获取服务器提供的服务。.
（1）A．kerberos   和PKI 都是对称密钥 B．kerberos 和PKI 都是非对称密钥
C．kerberos 是对称密钥，而PKI 是非对称密钥D．kerberos 是非对称密钥，而PKI 是对称密钥
（2）A．RSA B．TGT C．DES D．LSA

第**2**题： 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（）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

第**3**题： 关于状态检测技术，说法错误的是()。
A、跟踪流经防火墙的所有通信
B、采用“状态监视”模块，执行网络安全策略
C、对通信连接的状态进行跟踪分析
D、状态检测防火墙工作在协议的最底层，所以不能有效的监测应用层的数据

第**4**题： 关于 ICMP协议扫描的正确说法是哪个？()
A、根据目标主机对查询报文和差错报文的响应来判断目标系统的相关信息
B、能穿越防火墙C、能判断服务端口D、能识别主机名

第**5**题： 对称加密体制中，不公开的信息是（ ）。
A、密钥B、算法C、密文空间D、明文空间

第**6**题： BMA访问控制模型是基于()
A.健康服务网络 B.ARPANET C.ISP D.INTERNET

第**7**题： 主动方式FTP服务器要使用的端口包括（）。
A、TCP 21 TCP 20   B、TCP21 TCP大于1024的端口
C、TCP 20、TCP 大于1024端口     D、都不对

第**8**题： 为了防止电子邮件中的恶意代码，应该由（）方式阅读电子邮件。
A、纯文本 B、网页 C、程序 D、会话

第**9**题： 链路加密要求必须先对链路两端的加密设备进行（）。
A、异步    B、重传    C、同步    D、备份

第**10**题： 在以下隧道协议中，属于三层隧道协议的是（）。
A、L2F         B、PPTP            C、L2TP           D、IPSec

2016/7/20 1~5 C A B A D 6~10 A C A C B

2016/7/21 1~5 CC D B D B 6~10 C B B A C

2016/7/22 1~5 B C B B A 6~10 B C B D B

2016/7/23 1~5 A ABC D BC B 6~10 C B B B C

2016/7/24 1~5 C D D C D 6~10 A C B C B

2016/7/25 1~5 CB C D A A 6~10 A A A C D