**信息安全工程师每日一练（2016/8/27）**

第**1**题： 信息安全管理体系是指（ ）。  
A. 网络维护人员的组织体系B. 信息系统的安全设施体系  
C. 防火墙等设备、设施构建的安全体系D. 组织建立信息安全方针和目标并实现这些目标的体系  
  
第**2**题： 网吧管理员小李发现局域网中有若干台电脑有感染病毒的迹象，这时应首先（ ），以避免病毒的进一步扩散。  
A．关闭服务器B．启动反病毒软件查杀C．断开有嫌疑计算机的物理网络连接D．关闭网络交换机  
  
第**3**题： PH软件开发公司承接了ZF企业基于因特网的B2C业务系统的研发任务。ZF企业提出的业务系统安全性要求之一是防止授权侵犯和保留用户痕迹。针对这一要求，PH公司架构师给出的解决方案最可能是（）。  
A.完整性(Integrity)框架方案B.访问控制(Access Control)框架方案  
C.身份鉴别(Authentication)框架方案D.抗抵赖(Non-repudiation)框架方案  
  
第**4**题： 信息网络的物理安全要从（）两个角度来考虑。  
  A．软件安全和设备安全  B．环境安全和设备安全

C．环境安全和软件安全D．软件安全和硬件安全  
  
第**5**题： 计算机病毒主要造成()。  
A、磁盘损坏B、计算机用户的伤害C、CPU的损坏D、程序和数据的破坏   
  
第**6**题： 下列不是包过滤型防火墙的缺点的是（）。  
A、数据包的过滤规则难以准确定义B、随着过滤规则的增加，路由器的吞吐率会下降  
C、处理包的速度比代理服务器慢D、不能防范大多数类型的 IP地址欺骗   
  
第**7**题： 信息安全风险应该是以下哪些因素的函数？（）  
A、信息资产的价值、面临的威胁以及自身存在的脆弱性等  
B、病毒、黑客、漏洞等  
C、保密信息如国家密码、商业秘密等  
D、网络、系统、应用的复杂的程度  
  
第**8**题： 以下哪个不属于信息安全的三要素之一？（）  
A、机密性 B、完整性 C、抗抵赖性 D、可用性  
  
第**9**题： 应用网关防火墙的逻辑位置处在OSI中的哪一层？（）  
A、传输层     B、链路层     C、应用层     D、物理层  
  
第**10**题： MD5是按每组512位为一组来处理输入的信息，经过一系列变换后，生成一个（）为散列值。  
A、64    B、128    C、256    D、512

**信息安全工程师每日一练（2016/8/28）**

第**1**题： 一个密码系统，通常简称为密码体制。可由五元组（M,C,K,E,D）构成密码体制模型，以下有关叙述中，（ ）是不正确的。  
A．M 代表明文空间；C 代表密文空间；K 代表密钥空间；E 代表加密算法；D 代表解密算法  
B．密钥空间是全体密钥的集合，每一个密钥 K 均由加密密钥 Ke 和解密密钥 Kd 组成，即有 K=  
C．加密算法是一簇由 M 到 C 的加密变换，即有 C=（M,  Kd）  
D．解密算法是一簇由 C 到 M 的加密变换，即有 M  =（C,  Kd）  
  
第**2**题： 下面有关安全审计的说法错误的是（）  
A、安全审计需要用到数据挖掘和数据仓库技术B、安全审计产品指包括主机类、网络类及数据库类  
C、安全审计的作用包括帮助分析案情事故发生的原因  
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

第**3**题： 为了系统地、-完整地构建信息系统的安全体系框架，信息系统安全体系应当由（）共同构建。  
  A. ．技术体系、组织机构体系和管理体系B．硬件、软件、安全产品和管理制度  
  C．技术框架、产品、管理制度和标准 D．用户需求、建设内容、运维管理  
  
第**4**题： 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  
  
第**5**题： Iptables中 -A 命令参数的作用是()。  
A、添加一个规则链B、扩展一条规则链C、添加一个规则链到链尾D、添加一个规则链到链头   
  
第**6**题： 对大部分组织而言，通常将信息分成二或三级就足够了，第二级别的信息是()的，这些信息称为“私有”、“公司敏感”或“公司秘密”。  
A、公开发表B、存档处理的C、不公开发表D、禁止发表   
  
第**7**题： 如果有大量计算机需要频繁的分析，则可利用哪个命令工具进行批处理分析？()  
A、 dumpel B、 showpriv  
C、 Secedit.exe D、 gpolmig.exe    
  
第**8**题： Solaris操作系统下，下面哪个命令可以修改/n2kuser/.profile文件的属性为所有用户可读、科协、可执行？（）  
A、chmod 744 /n2kuser/.profile B、 chmod 755 /n2kuser/.profile  
C、 chmod 766 /n2kuser/.profile D、 chmod 777 /n2kuser/.profile  
  
第**9**题： 下列哪些属于WEB脚本程序编写不当造成的（）？  
A、IIS5.0  Webdav Ntdll.dll远程缓冲区一处漏洞B、apache可以通过../../../../../../../etc/passwd方位系统文件  
C、登陆页面可以用password=’a’or’a’=’a’绕过 D、数据库中的口令信息明文存放  
  
第**10**题： AES密钥长度不能是（）。  
A、128位    B、192位    C、256位    D、512位

**信息安全工程师每日一练（2016/8/29）**

第**1**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。以下关于这四个层次安全的，错误的是（ ）。  
A．按粒度从粗到细排序为系统级安全、资源访问安全、功能性安全、数据域安全  
B．系统级安全是应用系统的第一道防线  
C．所有的应用系统都会涉及资源访问安全问题  
D．数据域安全可以细分为记录级数据域安全和字段级数据域安全

第**2**题： 下列行为不属于网络攻击的是 （ ） 。  
A、连续不停Ping某台主机 B、发送带病毒和木马的电子邮件

C、向多个邮箱群发一封电子邮件 D、暴力破解服务器密码  
第**3**题： 下面有关双宿主机网关的配置说法错误的是（）。  
A、用一台装有两个网络适配器的双宿主机做防火墙  
B、双宿主机用两个网络适配器分别连接两个网络，又称堡垒主机  
C、堡垒主机上运行着防火墙软件  
D、双重宿主主机首先要开放网络层的路由功能   
  
第**4**题： MD5的输出比特数是()。  
A、64 B、128 C、160 D、256   
  
第**5**题： 一下对于Oracle文件系统描述错误的是（）？  
A、\*nix下Oracle的可执行文件在$Oracle\_HOME/bin/Oracle,$Oracle\_HOME/bin也应该包含在路径环境变量内   
B、Windows下Oracle的可执行文件在%Oracle\_HOME%\bin\Oracle.exe,其他   
C、硬件加密   
D、固件加密  
  
第**6**题： 在典型的WEB应用站点的层次结构中，“中间件”是在哪里运行的？（）  
A、浏览器客户端 B、web服务器 C、应用服务器 D、数据库服务器  
  
第**7**题： DNSSec中并未采用（）。  
A、数字签名技术    B、公钥加密技术    C、地址绑定技术    D、报文摘要技术  
  
第**8**题： “冲击波”病毒运行时会将自身复制到Windows目录下，并命名为（）  
A、Gsrss.exe        B、msbast.exe C、msblast.exe     D、lsass.exe  
  
第**9**题： 关于80年代Mirros蠕虫危害的描述，哪句话是错误的？（）  
A、占用了大量的计算机处理器的时间，导致拒绝股务B、窃取用户的机密信息，破坏计算机数据文件  
C、该蠕虫利用Unix系统上的漏洞传播D、大量的流量堵塞了网络，导致网络瘫痪  
  
第**10**题： 下面哪一项是黑客用来实施DDoS攻击的工具？()   
A、LC5       B、Rootkit       C、Icesword         D、Trinoo

**信息安全工程师每日一练（2016/8/30）**

第**1**题： 在 PKI 体系中\_\_\_\_\_\_负责管理 PKI 结构下的所有用户(包括各种应用程序)的证书，把 用户的公钥和用户的其他信息捆绑在一起，在网上验证用户的身份.  
A、RADIUS server B、ISP C、CA D、IE  
  
第**2**题： 包过虑防火墙对数据包的依据不包括（ ）  
A、源 IP 地址  B、源端口号 C、MAC 地址  D、目的 IP 地址  
  
第**3**题： MD5常用于数据（）保护  
A、校验    B、完整   C、机密   D、可靠  
  
第**4**题： 下列不属于 iptables规则策略表的是B()。  
A、filter B、forward C、mangle D、nat   
  
第**5**题： 信息网络安全的第三个时代是（）  
A、主机时代，专网时代，多网合一时代 B、主机时代，PC时代，网络时代  
C、PC时代，网络时代，信息时代 D、2001年，2002年，2003年  
  
第**6**题： 下列哪一条与操作系统安全配置的原则不符合?()  
A、关闭没必要的服务 B、不安装多余的组件   
C、安装最新的补丁程序 D、开放更多的服务  
  
第**7**题： 目前数据大集中是我国重要的大型分布式信息系统建设和发展的趋势，数据大集中就是将数据集中存储和管理，为业务信息系统的运行搭建了统一的数据平台，对这种做法认识正确的是（）？  
A、数据库系统庞大会提供管理成本 B、数据库系统庞大会降低管理效率  
C、数据的集中会降低风险的可控性 D、数据的集中会造成风险的集中  
  
第**8**题： 网络攻击的有效载体是什么？（     ）  
A．黑客    B．网络     C．病毒         D．蠕虫  
  
第**9**题： 端对端加密只需要保证消息都在哪里进行加密？（）  
A、源点和目的地节点    B、经过的每一个节点    C、源点和中间经过的每一个节点    D、所有节点  
  
第**10**题： 关于使用电脑有以下行为规范：  （      ）

①及时安装系统补丁 ②及时修改登录密码  ③使用建行分配的IP地址④保证杀毒软件病毒库为最新

在脱离建行网络环境下使用电脑时，应该注意什么？

A、①②     B、①④ C、②③ D、①②④

**信息安全工程师每日一练（2016/8/31）**

第**1**题： 我国强制性国家标准《计算机信息安全保护等级划分准则》将计算机信息系统分为5个安全保护等级，其中适用于地方各级国家机关、金融机构、邮电通信、能源与水源供给部门的信息系统适用（ ）。  
A. 安全标记保护级  B. 结构化保护级  C.访问验证保护级     D.系统审计保护级  
  
第**2**题： 应用系统运行的安全管理中心，数据域安全是其中非常重要的内容，数据域安全包括（ ）  
A、行级数据域安全，字段级数据域安全B、系统性数据域安全，功能性数据域安全  
C、数据资源安全，应用性数据安全D、组织级数据域安全，访问性数据域安全  
  
第**3**题： 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、信誉的损失D、商业及经济的利益  
  
第**4**题：  下列哪个不是常见的网络应用服务？()  
A、WEB B、MAIL C、DNS D、ARP   
  
第**5**题： 以下对Windows服务的说法错误的是（ ）  
A.为了提升系统的安全性管理员应尽量关闭不需要的服务  
B.Windows服务只有在用户成功登录系统后才能运行  
C.可以作为独立的进程运行或以DLL的形式依附在Svchost.exe  
D.windows服务通常是以管理员的身份运行的  
  
第**6**题： 主要用于加密机制的协议是()  
A、HTTP B、FTP C、TELNET D、SSL  
  
第**7**题： WindowsNT和Windows2000系统能设置为在几次无效登录后锁定帐号,这可以防止()  
A、木马B、暴力攻击C、IP欺骗;D、缓存溢出攻击  
第**8**题： 监听的可能性比较低的是（）数据链路。  
A、Ethernet     B、电话线     C、有线电视频道     D、无线电  
第**9**题： 应控制自互联网发起的会话并发连接数不超出网上营业厅设计容量的（）。  
A、60%     B、70%     C、80%     D、90%  
  
第**10**题： 以下哪一项不是流氓软件的特征？()  
A、通常通过诱骗或和其他软件捆绑在用户不知情的情况下安装B、通常添加驱动保护使用户难以卸载  
C、通常会启动无用的程序浪费计算机的资源D、通常会显示下流的言论

**信息安全工程师每日一练（2016/9/1）**

第**1**题： RSA是一种公开密钥算法，所谓公开密钥是指（ ）  
A.加密密钥是公开 B.解密密钥是公开 C.加密密钥和解密密钥都是公开 D.加密密钥和解密密钥都是相同  
  
第**2**题： 入侵检测系统执行的主要任务不包括（）。  
A、监视、分析用户及系统活动，审计系统构造和弱点B、统计分析异常行为模式  
C、评估重要系统和数据文件的完整性D、发现所维护信息系统存在的安全漏洞  
  
第**3**题： 以下哪种系统安装在主机上提供入侵检测功能？()  
A、网络嗅探器B、基于主机的入侵检测系统C、VPN D、基于网络的入侵检测系统   
  
第**4**题： 下列哪个标准本身由两个部分组成，一部分是一组信息技术产品的安全功能需要定义，另一部分是对安全保证需求的定义？()  
A、可信任计算机系统评估标准（ TCSEC）B、信息技术安全评价准则（ ITSEC）  
C、信息技术安全评价联邦准则（ FC）D、 CC标准   
  
第**5**题： 互联网电子邮件服务提供者对用户的和互联网电子邮件地址负有\_\_\_\_\_保密的义务。  
A、个人注册信息B、收入信息C、所在单位的信息  
  
第**6**题： “中华人民共和国保守国家秘密法”第二章规定了国家秘密的范围和密级，国家秘密的密级分为：（）。  
A、“普密”、“商密”两个级别           B、“低级”和“高级”两个级别

C、“绝密”、“机密”、“秘密”三个级别    D、“一密”、“二密”，“三密”、“四密”四个级别  
  
第**7**题： 为了防御网络监听，最常用的方法是：（     ）。  
A．采用物理传输（非网络）  B．信息加密  C．无线网    D．使用专线传输  
  
第**8**题： 以下各种加密算法中属于单钥制加密算法的是（）。  
A、DES加密算法    B、Caesar替代法    C、Vigenere算法    D、Diffie-Hellman加密算法  
  
第**9**题： “U盘破坏者”病毒（Worm.vhy）采用（）图标，很容易被用户误点击，点击后就会在后台破坏硬盘数据，致使中毒电脑重新启动的时候完全崩溃。  
A、网上邻居    B、我的电脑C、我的文档    D、收藏夹  
  
第**10**题： 攻击者截获并记录了从A到B的数据，然后又从早些时候所截获的数据中提取出信息重新发往B称为（）。  
A、中间人攻击    B、口令猜测器和字典攻击C、强力攻击   D、回放攻击

**信息安全工程师每日一练（2016/9/2）**

第**1**题： 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（1） ；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 （2） 病毒感染。  
（1）A、文件型 B、引导型 C、目录型 D、宏病毒  
（2）A、文件型 B、引导型 C、目录型 D、宏病毒

第**2**题： 防止计算机传染病毒的方法是()。  
A、不使用有病毒的盘片B、不让有传染病的人操作C、提高计算机电源稳定性D、联机操作   
  
第**3**题： 以下哪一项不是攻击终端服务器的方法？()  
A、缓冲区溢出B、交互式登录的密码猜测攻击C、远程桌面协议 DoS攻击D、权限提升风险   
  
第**4**题： 绿色上网软件可以自动过滤或屏蔽互联网上的\_\_\_\_，保护青少年健康成长。  
A、网络游戏B、网络聊天信息C、淫秽色情信息  
  
第**5**题： 我国的计算机年犯罪率的增长是()  
A、10% B、160 %C、60% D、300%  
  
第**6**题： SQL语言可以（）在宿主语言中使用，也可以独立地交互式使用。  
A、-极速 B、-嵌入 C、-混合 D、-并行  
  
第**7**题： 下列不属于对物理层信息窃取的是()  
A、对存储介质的盗取 B、对监视器的窃听 C、对网络线路的窃听 D、对设备屏蔽电磁干扰  
  
第**8**题： Kerberos提供的最重要的安全服务是？（）。  
A、鉴别    B、机密性    C、完整性    D、可用性  
  
第**9**题： 公钥机制利用一对互相匹配的（）进行加密，解密。  
A、私钥    B、密钥    C、数字签名    D、数字证书  
  
第**10**题： 以下哪一个最好的描述了数字证书？（）  
A、等同于在网络上证明个人和公司身份的身份证

B、浏览器的一个标准特性，它使得黑客不能得知用户的身份      
C、网站要求用户使用用户名和密码登陆的安全机制      
D、伴随在线交易证明购买的收据

**2016/8/27 1~5 D C D B D 6~10 C A C C B**

**2016/8/28 1~5 C B A B C 6~10 C C D C D**

**2016/8/29 1~5 C C D B B 6~10 C C C B D**

**2016/8/30 1~5 C C B B A 6~10 D D C A D**

**2016/8/31 1~5 A A A D B 6~10 D B B C D**

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

**2016/9/2 1~5 DC A A C C 6~10 B D A B A**