全国计算机技术与软件专业技术资格（水平）考试

2017 年上半年 信息安全工程师 上午试卷与解析

（考试时间 9：00～11：30 共 150 分钟）

请按下述要求正确填写答题卡

1. 在答题卡的指定位置上正确写入你的姓名和准考证号，并用正规 2B 铅笔在你写入的准考证号下填涂准考证号。
2. 本试卷的试题中共有 75 个空格，需要全部解答，每个空格 1 分，满分 75 分。
3. 每个空格对应一个序号，有 A、B、C、D 四个选项，请选择一个最恰当的选项作为解答，在答题卡相应序号下填涂该选项。
4. 解答前务必阅读例题和答题卡上的例题填涂样式及填涂注意事项。解答时用正规 2B 铅笔正确填涂选项，如需修改，请用橡皮擦干净，否则会导致不能正确评分。

注：以下答案和解析仅供参考，最终答案以信管网和软题库考试系统答案为准

http://www.ruantiku.com

http://www.cnitpm.com/exam/

1、根据密码分析者可利用的数据资源来分类，可将密码攻击的类型分为四类，其中密码分析者能够选择密文并获得相应明文的攻击密码的类型属于（）.

A.仅知密文攻击

B.选择密文攻击

C.已知密文攻击

D.选择明文攻击

信管网参考答案：B

最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

2、《计算机信息系统安全保护等级划分准则》（GB17859——1999）中规定了计算机系统安全保护能力的五个等级，其中要求对所有主体和客体进行自主和强制访问控制的是（）

A.用户自助保护级

B.系统审计保护级

C.安全标记保护级

D.结构化保护级

信管网参考答案：C

最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

3、1949 年，（）发表了题为《保密系统的通信理论》的文章，为密码技术的研究奠定了理论基础，由此密码学成了一门科学。

A.Shannon

B.Diffie

C.Hellman

D.Shamir

信管网参考答案：A

最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

4、（）属于对称加密算法。

A.EIGantal

B.DES

C.MDS

D.RSA

信管网参考答案：B

最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

5、密码体制是一种代表性的古典密码算法，在凯撒密码体制中，设置密钥参数 k = 3，依次对密文“zhonggguo”进行加密，则相应的密文为（）

A.ckrqjjxr
B.cdrqjjxr
C.Akrqjjxr
D.Ckrqiixr
信管网参考答案：A
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

6、在信息安全防护体系设计中，保证“信息系统中数据不被非法修改、破坏、丢失等”是为了达到防护体系的（）目标。
A.可用性
B.保密性
C.可控性
D.完整性
信管网参考答案：D
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

7、下列技术中，不能预防重放攻击的是（）。
A.时间戳
B.nonce
C.明文填充
D.序号
信管网参考答案：C
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

8、计算机取证主要是对电子证据的获取、分析、归档和描述的过程，而电子证据需要在法庭上作为证据展示，进行计算机取证时应当充分考虑电子证据的真实性和电子证据的证明力，除了相关准备之外，计算机取证步骤通常不包括（）
A.保护目标计算机系统
B.确定电子证据
C.收集电子数据、保全电子证据
D.清除恶意代码
信管网参考答案：D
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

9、数字水印是通过数字信号处理的方法，在数字化的多媒体数据中，嵌入隐蔽的水印标记。其应用领域不包括（）
A.版权保护
B.票据防伪
C.证据篡改鉴定
D.图像数据
信管网参考答案：D
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

10、信息系统安全测评方法中模糊测试时一种黑盒测试技术，它将大量的畸形数据输入到目标程序中，通

过监测程序的异常来发现被测程序中可能存在的安全漏洞、关于模糊测试，以下说法错误的是（）
A.与白盒测试相比，具有更好的适用性
B.模糊测试是一种自动化的动态漏洞挖掘技术，不存在误报，也不需要人工进行大量的逆向分析工作
C.模糊测试不需要程序的源代码就可以发现问题
D.模糊测试受限于被测系统的内部实现细节和复杂度
信管网参考答案：D
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

11、下列攻击中，不能导致网络瘫痪的是（）
A.溢出攻击
B.钓鱼攻击
C.邮件炸弹攻击
D.拒绝服务攻击
信管网参考答案：B
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

12、（）是一种通过对信息进行均衡、安全的防护，提高整个系统最低安全性能的原则。
A.木桶原则
B.保密原则
C.等级化原则
D.最小特权原则
信管网参考答案：A
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

13、网站的安全协议是 https 时，该网站浏览时会进行（）处理。
A.增加访问标记
B.加密
C.身份隐藏
D.口令验证
信管网参考答案：B
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

14、被动攻击通常包含（）
A.拒绝服务攻击
B.欺骗攻击
C.窃听攻击
D.数据驱动攻击
信管网参考答案：C
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

15、以下网络攻击方式中，（）实施的攻击不是网络钓鱼的常用手段
A.利用社会工程学
B.利用虚假的电子商务网站
C.利用假冒网上银行、网上证券网站

D.利用密罐
信管网参考答案：D
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

16、数字签名是对以数字形式储存的消息就行某种处理，产生一种类似于传统手书签名功效的消息处理过程，一个数字签名体制通常包括两个部分，（）
A.施加签名和验证签名
B.数字证书和身份认证
C.身份消息加密和解密
D.数字证书和消息摘要
信管网参考答案：A
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

17、身份识别在信息安全领域有着广泛的应用，通过识别用户的生理特征来认证用户的身份是安全性很高的身份认证方法。如果把人体特征用于身份识别，则它应该具有不可复制的特点，必须具有（）
A.唯一性和保密性
B.唯一性和稳定性
C.保密性和可识别性
D.稳定性和可识别性
信管网参考答案：B
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

18、ISO 制定的安全体系结构描述了 5 种安全服务，以下不属于这 5 种安全服务的是（）
A.鉴别服务
B.数据报过滤
C.访问控制
D.数据完整性
信管网参考答案：B
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

19、在使用复杂度不高的口令时，容易产生弱口令的安全脆弱性，被攻击者利用从而破解用户账户，下列设置的口令中，（）具有最好的口令复杂度。
A.morrison
B.Wm.S*F2m5@
C.27776394
D.wangjing1977
信管网参考答案：B
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

20、工控系统广泛应用于电力、石化、医药、航天等领域，已经成为国家关键基础设施的重要组成部分。作为信息基础设施的基础，电力工控系统安全面临的主要威胁不包括（）
A.内部人为风险
B.黑客攻击
C.设备损耗

D.病毒破坏
信管网参考答案：C
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

21、对日志数据进行审计检查，属于（）类控制措施。
A.预防
B.检查
C.威慑
D.修正
信管网参考答案：B
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

22、攻击者通过对目标主机进行端口扫描，可以直接获得（）。
A.目标主机的口令
B.给目标主机种植木马
C.目标主机使用了什么操作系统
D.目标主机开放了那些端口服务
信管网参考答案：D
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

23、以下关于 NAT 的说法中，错误的是（）
A.NAT 允许一个机构专用 Intranet 中的主机透明的连接到公共域中的主机，五需每台内部主机都拥有注册的（已经越来越缺乏的）全局互联网地址
B.静态 NAT 是设置起来最简单和最容易实现的一种地址转换方式，内部网络中的每个主机都被永久映射成外部网络中的某个合法地址
C.动态 NAT 主要应用于拨号和频繁的远程连接，当远程用户连接上之后，动态 NAT 就会分配给用户一个 IP 地址，当用户断开时，这个 IP 地址就会被释放而留待以后使用
D.动态 NAT 又叫网络端口转换 NAPT
信管网参考答案：D
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

24、应用代理防火墙的主要优点是（）
A.加密强度高
B.安全控制更细化、更灵活
C.安全服务的透明性更好
D.服务对象更广泛
信管网参考答案：B
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

25、从安全属性对各种网络攻击进行分类，阻断攻击是针对（）的攻击
A.机密性
B.可用性
C.完整性
D.真实性

信管网参考答案：B
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

26、下列各种协议中，不属于身份认证协议的是（）
A. S/Key 口令协议
B. Kerberos 协议
C. X.509 协议
D. IPSec 协议
信管网参考答案：D
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

27、我国制定的关于无线局域网安全的强制标准是（）
A.IEEE 802.11
B. WPA
C. WAPI
D. WEP
信管网参考答案：C
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

28、以下恶意代码中，属于宏病毒的是（）
A. Macro.Melissa
B. Trojian.huigezi.a
C. Worm.Blaster.g
D. Backdoor.Agobot.frt
信管网参考答案：A
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

29、容灾的目的和实质是（）
A.实现对系统数据的备份
B.提升用户的安全预期
C.保持对信息系统的业务持续性
D.信息系统的必要补充
信管网参考答案：C
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

30、安卓的系统架构从上层到下层包括：应用程序层、应用程序框架层、系统库和安卓运行时、Linux 内核。其中，文件访问控制的安全服务位于（）
A.应用程序层
B.应用程序框架层
C.系统库和安卓运行时
D.Linux 内核
信管网参考答案：D
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

31、下面不属于 PKI 组成部分的是（）
A.证书主体
B.使用证书的应用和系统
C.证书权威机构
D.AS
信管网参考答案：D
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

32、SSL 协议是对称密码和公钥密码技术相结合的协议，该协议不能提供的安全服务是（）
A.保密性
B.可用性
C.完整性
D.可认证性
信管网参考答案：B
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

33、通过具有 IPScc 功能的路由器构件 VPN 的过程中，采用的应用模型是（）
A.隧道模型
B.保密模式
C.传输模式
D.压缩模式
信管网参考答案：A
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

34、安全策略表达模型是一种对安全需求与安全策略的抽象概念模型，一般分为自主访问控制模型和强制访问控制模型。以下属于自主访问控制模型的是（）
A. BLP 模型
B. HRU 模型
C. BN 模型
D.基于角色的访问控制模型
信管网参考答案：B
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

35、SHAI 算法的消息摘要长度是（）位
A.128
B.160
C.256
D.512
信管网参考答案：B
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

36、A 方有一对密钥（KA_{pub}，KA_{pri}），B 方有一对密匙（KB_{pub}，KB_{pri}），A 方给 B 方发送信息 M，对信息 M 加密为：M＇= KB_{pub}（KA_{pri}（M））。B 方收到密文，正确的解决方案是（）
A. KBpub（KApri（M＇））

B. KBpub（KApub（M‘））
C. KApub（KBpri（M‘））
D. KBpri（KApri（M‘））
信管网参考答案：C
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

37、有线等效保密协议 WEP 采用 RC4 流密码技术实现保密性，标准的 64 位标准流 WEP 用的密钥和初始向量长度分别是（）
A.32 位和 32 位
B.48 位和 16 位
C.56 位和 8 位
D.40 位和 24 位
信管网参考答案：D
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

38、文件类型病毒不能感染的文件类型是（）
A.COM 类型
B.HTML 类型
C. SYS 类型
D. EXE 类型
信管网参考答案：B
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

39、在非安全的通信环境中，为了保证消息来源的可靠性，通常采用的安全防护技术是（）
A.信息隐藏技术
B.数据加密技术
C.消息认证技术
D.数字水印技术
信管网参考答案：C
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

40、操作系统的安全审计是指对系统中有关安全的活动进行记录、检查和审核的过程，现有的审计系统包括（）三大功能模块。
A.审计事件收集及过滤、审计事件记录及查询、审计事件分析及响应报警
B.审计数据挖掘、审计事件记录及查询、审计事件分析及响应报警
C.系统日志采集与挖掘、安全事件记录及查询、安全响应报警
D.审计事件特征提取、审计事件特征匹配、安全响应报警
信管网参考答案：A
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

41、计算机病毒的生命周期一般包括（）四个阶段
A.开发阶段、传播阶段、发现阶段、清除阶段
B.开发阶段、潜伏阶段、传播阶段、清除阶段
C.潜伏阶段、传播阶段、发现阶段、清除阶段

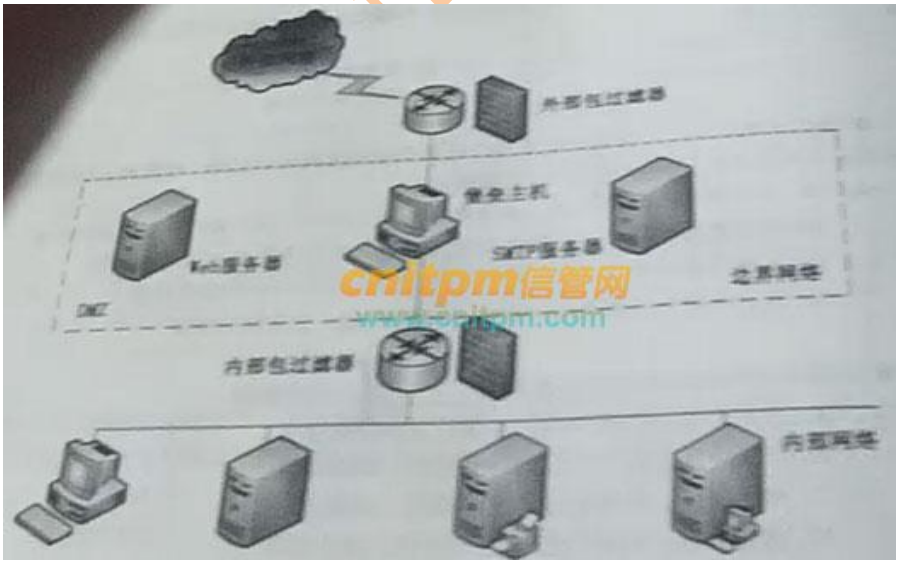
D.潜伏阶段、传播阶段、触发阶段、发作阶段
信管网参考答案：D
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

42、下面关于跨站攻击描述不正确的是（）
A.跨站脚本攻击指的是恶意攻击者向 Web 页面里插入恶意的 Html 代码
B.跨站脚本攻击简称 XSS
C.跨站脚本攻击也可称作 CSS
D.跨站脚本攻击是主动攻击
信管网参考答案：C
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

43、以下不属于信息安全风险评估中需要识别的对象是（）
A.资产识别
B.威胁识别
C.风险识别
D.脆弱性识别
信管网参考答案：C
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

44、安全漏洞扫描技术是一类重要的网络安全技术。当前，网络安全漏洞扫描技术的两大核心技术是（）
A.PINC 扫描技术和端口扫描技术
B.端口扫描技术和漏洞扫描技术
C.操作系统探测和漏洞扫描技术
D. PINC 扫描技术和操作系统探测
信管网参考答案：C
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

45、防火墙的经典体系结构主要有三种，下图给出的是（）体系结构。



A.双重宿主主机
B.（被）屏蔽主机
C.（被）屏蔽子网
D.混合模式
信管网参考答案：C
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

46、计算机系统的安全级别分为四级：D、C（C1、C2）、B（B1、B2、B3）和 A。其中被称为选择保护级的是（）
A. C1
B. C2
C. B1
D. B2
信管网参考答案：C
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

47、IP 地址欺骗的发生过程，下列顺序正确的是（）。①确定要攻击的主机 A；②发现和它有信任关系的主机 B；③猜测序列号；④成功连接，留下后门；⑤将 B 利用某种方法攻击瘫痪。
A.①②⑤③④
B.①②③④⑤
C.①②④③⑤
D.②①⑤③④
信管网参考答案：A
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

48、以下不属于网络安全控制技术的是（）
A.防火墙技术
B.数据备份技术
C.入侵检测技术
D.访问控制技术
信管网参考答案：B
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

49、以下关于认证技术的描述中，错误的是（）
A.基于生物特征认证一般分为验证和识别两个过程
B.身份认证是用来对信息系统中实体的合法性进行验证的方法
C.数字签名的结果是十六进制的字符串
D.消息认证能够确定接收方收到的消息是否被篡改过
信管网参考答案：C
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

50、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
信管网参考答案：B
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

51、能有效控制内部网络和外部网络之间的访问及数据传输，从而达到保护内部网络的信息不受外部非授权用户的访问和对不良信息的过滤的安全技术是（）
A.入侵检测
B.反病毒软件
C.防火墙
D.计算机取证
信管网参考答案：C
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

52、包过滤技术防火墙在过滤数据包时，一般不关心（）
A.数据包的原地址
B.数据包的目的地址
C.数据包的协议类型
D.数据包的内容
信管网参考答案：D
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

53、密码分析的目的是（）
A.发现加密算法
B.发现密钥或者密文对应的明文
C.发现解密算法
D.发现攻击者
信管网参考答案：B
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

54、下列关于数字签名的说法正确的是（）
A.数字签名是不可信的
B.数字签名容易被伪造
C.数字签名容易抵赖
D.数字签名不可改变
信管网参考答案：B
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

55、以下关于公钥基础设施（PKI）的说法中，正确的是（）
A. PKI 可以解决公钥可信性问题
B. PKI 不能解决公钥可信性问题
C. PKI 只能有政府来建立
D.PKI 不提供数字证书查询服务
信管网参考答案：A

最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

56、下列关于公钥体制中说法不正确的是（）
A.在一个公钥体制中，一般存在公钥和私钥两种密钥
B.公钥体制中仅根据加密密钥来去确定解密密钥在计算上是可行的
C.公钥体制中的关于可以以明文方式发送
D.公钥密码中的私钥可以用来进行数字签名
信管网参考答案：B
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

57、无线传感器网络容易受到各种恶意攻击，以下关于其防御手段说法错误的是（）。
A.采用干扰区内节点切换频率的方式抵御干扰
B.通过向独立多路径发送验证数据来发现异常节点
C.利用中心节点监视网络中其它所有节点来发现恶意节点
D.利用安全并具有弹性的时间同步协议对抗外部攻击和被俘获节点的影响
信管网参考答案：C
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

58、属于第二层的 VPN 隧道协议是（）。
A.IPSec
B.PPTP
C.GRE
D.IPv4
信管网参考答案：B
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

59、信息隐藏主要研究如何将机密信息秘密隐藏于另一公开的信息中。以下关于利用多媒体数据来隐藏机密信息的叙述中，错误的是（）。
A.多媒体信息本身有很大的冗余性
B.多媒体信息本身编码效率很高
C.人眼或人耳对某些信息由一定的掩蔽效应
D.信息嵌入到多媒体信息中不影响多媒体本身的传送和使用
信管网参考答案：B
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

60、证书授权中心（CA）的主要职责不包含（）。
A.证书管理
B.证书签发
C.证书加密
D.证书撤销
信管网参考答案：C
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

61、X.509 数字证书的内容不包括（）。

A.版本号
B.签名算法标识
C.加密算法标识
D.主体的公开密钥信息
信管网参考答案：C
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

62、如果在某大型公司本地与异地分公司之间建立一个 VPN 连接，应该建立的 VPN 类型是（）。
A.内部 VPN
B.外部 VPN
C.外联网 VPN
D.远程 VPN
信管网参考答案：D
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

63、网络密罐技术是一种主动防御技术，是入侵检测技术的一个重要发展方向，以下有关密罐说法不正确的是（）。
A.密罐系统是一个包含漏洞的诱骗系统，它通过模拟一个或者多个易受攻击的主机和服务，给攻击者提供一个容易攻击的目标
B.使用密罐技术，可以使目标系统得以保护，便于研究入侵者的攻击行为
C.如果没人攻击，密罐系统就变得毫无意义
D.密罐系统会直接提高计算机网络安全等级，是其他安全策略不可替代的
信管网参考答案：D
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

64、以下不属于代码静态分析的方法是（）。
A.内存扫描
B.模式匹配
C.定理证明
D.模型检测
信管网参考答案：A
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

65、SM4 是一种分组密码算法，其分组长度和密钥长度分别为（）。
A.64 位和 128 位
B.128 位和 128 位
C.128 位和 256 位
D.256 位和 256 位
信管网参考答案：B
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

66、设在 RSA 的公钥密码体制中，用于为（e，n）=（7,55），则私钥 d=（）。
A. 8
B. 13

C. 23
D. 37
信管网参考答案：C
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

67、DSS 数字签名标准的核心是数字签名算法 DSA，该签名算法中杂凑函数采用的是（）。
A. SHA1
B. MD5
C. MD4
D. SHA2
信管网参考答案：A
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

68、2017 年 6 月 1 日，（）开始施行。
A.中华人民共和国计算机信息系统安全保护条例
B.计算机信息系统国际联网保密管理规定
C.中华人民共和国网络安全法
D.中华人民共和国电子签名法
信管网参考答案：C
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

69、面向数据挖掘的隐私保护技术主要解决高层应用中的隐私保护问题，致力于研究如何根据不同数据挖掘操作的特征来实现对隐私的保护。从数据挖掘的角度看，不属于隐私保护技术的是（）。
A.基于数据失真的隐私保护技术
B.基于数据匿名化的隐私保护技术
C.基于数据分析的隐私保护技术
D.基于数据加密的隐私保护技术
信管网参考答案：C
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

70、强制访问控制（MAC）是一种不允许主体干涉的访问控制类型。根据 MAC 的安全基本，用户与访问的信息的读写关系有四种类型，其中能保证数据完整性的读写组合方式是（）。
A.上读-下写
B.上读-上写
C.下读-下写
D.下读-上写
信管网参考答案：A
最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm

71、There are different ways to perform IP based DoS Attacks. The most common IP based DoS attack is that an attacker sends an extensive amount of connection establishment （1）(e.g. TCP SYN requests) to establish hanging connections with the controller or a DPS. Such a way, the attacker can consume the network resources which should be available for legitimate users. In other （2）, the attacker inserts a large amount of （3）packets to the data plane by spoofing all or part of the header fields with random values. These incoming packets will trigger

table-misses and send lots of packet-in flow request messages to the network controller to saturate the controller resources. In some cases, an （4）who gains access to DPS can artificially generate lots of random packet-in flow request messages to saturate the control channel and the controller resources. Moreover, the lack of diversity among DPSs fuels fuels the fast propagation of such attacks.

Legacy mobile backhaul devices are inherently protected against the propagation of attacks due to complex and vendor specific equipment. Moreover, legacy backhaul devices do not require frequent communication with core control devices in a manner similar to DPSs communicating with the centralized controller. These features minimize both the impact and propagation of DoS attacks. Moreover, the legacy backhaul devices are controlled as a joint effort of multiple network element. For instance, a single Long Term Evilution（LTE）eNodeB is connected up to 32 MMEs. Therefore, DoS/DDoS attack on a single core element will not terminate the entire operation of a backhaul device（5）the net work.

（1）A.message B、information C、requests D、data

（2）A.methods B、cases C、hands D、sections

（3）A.bad B、real C、fake D、new

（4）A.user B、administrator C、editor D、attacker

（5）A.or B、of C、in D、to

信管网参考答案：C、B、C、D、B

最终答案以信管网题库答案为准：http://www.cnitpm.com/exam/ExamST28_707014.htm