全国计算机等级考试（NCRE）
三级信息安全技术
样题及参考答案

➢ 样题

一、单项选择题

1、信息技术的产生与发展，大致经历的三个阶段是
A）电讯技术的发明、计算机技术的发展和互联网的使用
B）电讯技术的发明、计算机技术的发展和云计算的使用
C）电讯技术的发明、计算机技术的发展和个人计算机的使用
D）电讯技术的发明、计算机技术的发展和半导体技术的使用

2、P2DR 模型是美国 ISS 公司提出的动态网络安全体系的代表模型。该模型的四个组成部分的核心是
A）策略
B）防护
C）检测
D）响应

3、有关信息和情报的关系，表述正确的是
A）情报都是信息，信息不一定是情报
B）情报都是信息，信息也都是情报
C）信息都是情报，情报不一定是信息
D）情报不一定是信息，信息一定是情报

4、信息安全的内因和外因，不包括
A）计算机病毒的泛滥
B）组成网络的通信和信息系统的自身缺陷
C）互联网的开放性
D）人为的原因

5、以下属于分组密码算法的是

A）RSA

B）DSA

C）ECC

D）SM4

6、下列有关对称密码的描述中，说法错误的是

A）加解密处理速度快

B）保密度高

C）密钥管理和分发简单

D）数字签名困难

7、下列有关哈希函数的说法中，正确的是

A）哈希函数是一种双向密码体制

B）哈希函数将任意长度的输入经过变换后得到相同长度的输出

C）MD5 算法首先将任意长度的消息填充为 512 的倍数，然后进行处理

D）SHA 算法要比 MD5 算法更快

8、消息认证不能预防的攻击是

A）伪装

B）内容修改

C）计时修改

D）发送方否认

9、DES 加密算法采用的有效密钥的位数是

A）64

B）128

C）56

D）168

10、数字签名可以提供的安全服务，不包括

A）机密性

B）完整性

C）消息认证

D）抗抵赖

11、集中式的 AAA 管理协议，不包括

A）RADIUS

B）TACACS

C）Diameter

D）SSO

12、删除一个视图的 SQL 命令是

A）DELETE

B）DROP

C）CLEAR

D）REMOVE

13、下列关于 Unix 文件系统的描述中，错误的是

A）目录本身不是文件，而用于组织文件，它包括一组其它文件的二进制文件

B）网络连接是一种特殊类型的文件

C）/dev 目录下找到的设备文件，可以对硬件驱动器等进行信息编码

D）正规文件包括 ASCII 文本文件、二进制数据文件、二进制可执行文件等

14、下列不属于分布式访问控制的是

A）单点登录

B）Kerberos 协议

C）SESAME

D）Diameter 协议

15、同时具有强制访问控制和自主访问控制属性的模型是

A）Biba

B）Chinese Wall

C）RBAC

D）BLP

16、数据库的完整性服务，不包括

A）结构完整性

B）实体完整性

C）参照完整性

D）语义完整性

17、下列选项中，不属于 Windows 系统进程管理的方法是

A）DOS 命令行

B）任务管理器

C）Msinfo32

D）服务

18、在 Unix 系统中，文件的权限模式位的符号模式为 rwxrwxrwx，则对应的绝对模式为

A）666

B）777

C）888

D）999

19、在 Unix/Linux 中，负责日志记录和审计的进程是

A）syslogd

B）lpd

C）mail

D）crond

20、设 U1 为数据库中的角色，Student 为数据库中的基本表，将 U1 查询 Student 的权限收回的 SQL 语句为

A）REVOKE SELECT ON TABLE Student FROM U1

B）AUDIT SELECT ON TABLE Student FROM U1

C）NOAUDIT SELECT ON TABLE Student FROM U1

D）GRANT SELECT ON TABLE Student FROM U1

21、下列选项中，不属于诱骗式攻击的是

A）钓鱼网站

B）ARP 欺骗

C）网站挂马

D）社会工程

22、下列选项中，包过滤防火墙不能过滤的数据包信息是

A 目标 IP 地址

B）ICMP 协议包

C）UDP 包的目的端口、源端口

D）HTTP 包的 GET、POST 请求

23、下列选项中，属于防火墙能防范的安全威胁是

A）内网之间的恶意攻击

B）网络端口扫描攻击

C）文件病毒和内部驱动木马的攻击

D）针对防火墙开放端口的攻击

24、IPSec 协议中支持加密和完整性检验功能的协议是

A）ESP

B）AH

C）SSL

D）SET

25、下列选项中，不属于可执行代码动态安全检测技术的是

A）模糊测试

B）智能模糊测试

C）词法分析

D）动态污点分析

26、下列选项中，攻击者不能利用进行 DoS 攻击的是

A）TCP

B）ICMP

C）UDP

D）IPSec

27、下列选项中，属于软件漏洞网络攻击框架性工具的是

A）BitBlaze

B）Nessus

C）Metasploit

D）Nmap

28、下列选项中，用于进行网络异常状态的监测和诊断的是

A）SNMP

B）ICMP

C）UDP

D）ARP

29、TCP 的下列标志位中，用于表示出现差错时释放 TCP 连接重新建立新连接的是

A）RST

B）PSH

C）ACK

D）FIN

30、在 Web 系统开发时，下列技术选项中不能避免注入漏洞的出现的是

A）使用预编译语句

B）给关键 Cookie 植入 Httponly 标识

C）使用存储过程来验证用户的输入

D）在数据类型、长度、格式和范围等方面对用户输入进行过滤

31、下列选项中，不属于代码混淆技术的是

A）语法转换

B）控制流转换

C）数据转换

D）词法转换

32、下列漏洞库中，由国内机构维护的漏洞库是

A）CVE

B）NVD

C）EBD

D）CNNVD

33、下列选项中，不属于木马自身属性特点的是

A）隐藏性

B）窃密性

C）伪装性

D）感染性

34、下列选项中，误用检测技术不包括的是

A）状态转换分析

B）模型推理

C）统计分析

D）专家系统

35、下列选项中，不属于 PKI 信任模型的是

A）网状信任模型

B）链状信任模型

C）层次信任模型

D）桥证书认证机构信任模型

36、下列选项中，不属于网站挂马的主要技术手段是

A）框架挂马

B）Body 挂马

C）下载挂马

D）Js 脚本挂马

37、信息安全管理体系认证范围需考虑的问题有

A）文件化的适用性申明、地理位置

B）组织相关的活动 、信息系统的边界平台和应用

C）需要包括在内的组织范围、所包括的主旨机构支持的活动

D）以上都是

38、信息安全风险管理中的风险管理内容包括

A）资产识别与评估、风险管理术语

B）风险管理术语、威胁识别与评估

C）资产识别与评估、威胁识别与评估

D）威胁识别与评估、风险控制

39、《中华人民共和国计算机信息系统安全保护条例》中第十三条规定

A）计算机信息系统的使用单位应当建立健全管理制度，负责本单位计算机信息系统的安全保护工作

B）计算机信息系统的安全保护工作，重点维护国家事务、经济建设、国防建设、尖端科学技术等重要领域的计算机信息系统的安全

C）切实保护本单位信息系统的安全，是保护本单位权益的需要

D）计算机信息系统的使用单位应当建立健全管理制度，但不需负责本单位计算机信息系统的安全保护工作

40、信息安全管理措施中可以实现物理与环境安全的有

A）围墙与门

B）警卫、警犬
C）ID 卡和证章
D）以上都是

41、判定残留风险，下列说法正确的是
A）不需在机构内部判定
B）信息安全的目标是将残留风险降为 0
C）信息安全的目标并不是将残留风险降为 0
D）决定者发现的风险都是受控制的

42、风险缓解策略包括三类计划，IRP、DRP、BCP 分别指
A）事件响应计划、灾难恢复计划和业务持续性计划
B）事件响应计划、业务持续性计划和灾难恢复计划
C）业务持续性计划、事件响应计划和灾难恢复计划
D）灾难恢复计划、业务持续性计划和事件响应计划

43、信息安全管理体系认证的目的，不包含
A）获得最佳的信息安全运行方式
B）保证商业安全
C）降低风险、避免损失
D）保持安全竞争优势

44、“电子认证服务提供者应当妥善保存与认证相关的信息，信息保存期限至少为电子签名认证证书失效后五年”，以上条文出自
A）《网络安全法》
B）《保守国家秘密法》
C）《电子签名法》
D）《刑法》

45、审核准备工作，不包括的是
A）编制审核计划
B）加强安全意识教育
C）收集并审核有关文件
D）准备审核工作文件——编写检查表

46、依据涉密信息系统分级保护管理规范和技术标准，涉密信息系统建设使用单位将保密级

别分为三级，下列分级正确的是

A）秘密 机密 要密

B）机密 要密 绝密

C）秘密 机密 绝密

D）秘密 要密 绝密

47、下列关于风险识别的评估成果与用途的叙述中，不正确的是

A）信息资产分类表，集合了信息资产以及它们对机构的影响或价值

B）权重标准分析表，为每项信息资产分配等级值或影响权重

C）漏洞风险等级表，为每对无法控制的资产漏洞分配风险等级

D）控制策略分类表，控制了漏洞产生的风险

48、下列对 CC 标准特点的叙述中，正确的是

A）通过实例化，解决了安全特性在不同产品与系统之间存在的差异

B）不再强调功能的级别，而是强调保证的级别，注重非技术性因素的评价

C）制定了两个框架，定义了标准的主体

D）评估结果最终是一个客观参考性的结果，是一个通过或者未通过的声明，对企业的实际指导意义很强

49、下列关于信息安全管理体系认证的叙述中，不正确的是

A）信息安全管理体系第三方认证为组织机构的信息安全体系提供客观评价

B）每个组织都必须进行认证

C）认证可以树立组织机构的信息安全形象

D）满足某些行业开展服务的法律要求

50、根据《信息安全等级保护管理办法》的五个安全保护等级中，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害属于

A）第二级

B）第三级

C）第四级

D）第五级

二、填空题

1、信息安全的发展经历了 **【1】** 、计算机安全和信息保障三个阶段。

2、访问控制是在__【2】__的基础上，依据授权对提出的资源访问请求加以控制。

3、操作系统使用__【3】__机制来确保进程不会在彼此之间，或给系统的重要组件造成负面影响。

4、访问控制在准则中被分为两类：自主访问控制和__【4】__。

5、1985 年提出的 ElGamal 公钥密码体制的安全性是基于求解有限域 Zp 上__【5】____的困难性的。为了抵抗攻击，p 应该至少是 160 位以上的十进制数且 p-1 至少有一个大的素因子。

6、安全散列算法 SHA 的输出是__【6】__位。

7、消息加密本身提供了一种认证手段。在这种方法中，整个消息的__【7】__作为认证码。

8、基于矩阵的__【8】__的访问控制信息表示的是访问能力表，即每个主体都附加一个该主体可访问的客体的明细表。

9、基于角色的访问控制模型的要素包括__【9】__、角色、许可等基本定义。

10、进程管理是通过__【10】__完成的。

11、ACK-Flood 攻击属于利用__【11】__协议发起的攻击。

12、__【12】__负责接收用户的证书申请，审核用户的身份，并为用户向 CA 提出证书请求，最后将申请的证书发放给用户。

13、利用开放网络的物理链路和专用的安全协议，实现逻辑上网络安全连接的技术称为__【13】__。

14、软件防篡改技术主要是通过__【14】__检验来检测软件是否被攻击者篡改。

15、可以通过网络等途径，自动将自身的全部代码或部分代码通过网络复制，传播给其它网络中计算机的完全独立可运行程序是__【15】__。

16、处于未公开状态的漏洞被称为__【16】__漏洞。

17、当一个函数被调用时，这个被调用函数的相关信息会保存在内存的栈区，这块内存中连续的栈区域即__【17】__。

18、Web 安全检测技术包括__【18】__检测和白盒检测两种主要检测技术。

19、体系审核是为获得__【19】__，对体系进行客观的评价，以确定满足审核准则的程度所进行的系统的、独立的并形成文件的检查。

20、《网络安全法》是我国第一部关于网络安全工作的基本大法，明确了各方面维护网络安全的责任和义务，是网络管理和治理的根本依据。《网络安全法》将于__【20】__施行。

三、综合应用题

1、在一个基于公钥密码机制的安全应用系统中，假设用户 Alice 和 Bob 分别拥有自己的公钥和私钥。请回答下述问题：

（1）在产生 Alice 和 Bob 的密钥时，如果采用 RSA 的算法，选取的模数 N 至少要有__【1】__位，如果采用椭圆曲线密码，选取的参数 P 的规模应大于__【2】__位。

（2）为了预防 Alice 抵赖，Bob 要求 Alice 对其发送的信息进行签名。Alice 将使用自己的__【3】__对信息签名；如果要求对信息保密传输，Alice 将使用 Bob 的__【4】__对消息加密。

（3）实际应用中为了缩短签名长度，提高签名的速度，而且为了更安全，常对信息的__【5】__进行签名。

2、请回答有关数据库自主存取控制的有关问题：

（1）自主存取控制可以定义各个用户对不同数据对象的存取权限，向用户授予权限的 SQL 语句是__【6】__；如果指定了__【7】__子句，则获得某种权限的用户还可以把这种权限再授予其它的用户；向用户收回授予权限的 SQL 语句是__【8】__。

（2）对数据库模式的授权则由 DBA 在创建用户时实现，如果在 CREATE USER 命令中没有指定创建新的用户的权限，默认该用户拥有__【9】__权限。

（3）可以为一组具有相同权限的用户创建一个__【10】__，用其来管理数据库权限可以简化授权的过程。

3、在下述有关 ARP 攻击防护的描述中，补充其中的内容。

在下图中，内网有两台计算机 A 和 B，通过交换机连接到网关设备最后连入互联网，其中计算机 A 的 IP 地址为 192.168.1.10，MAC 地址为 MACA；计算机 B 的 IP 地址为 192.168.1.20，MAC 地址为 MACB；网关设备的 IP 地址为 59.60.1.1，MAC 地址为 MACG。

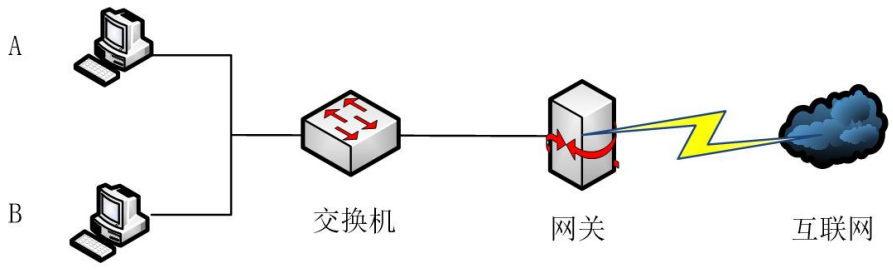

图 1 网络拓扑图

其中，B 计算机感染了 ARP 病毒，此 ARP 病毒向其它内网计算机发起伪装网关 ARP 欺骗攻击，它发送的 ARP 欺骗数据包中，IP 地址为__【11】__，MAC 地址为__【12】__。

为了防止 ARP 欺骗，需要在内网计算机和网关设备上进行 MAC 地址与 IP 地址的双向静态绑定。

首先，设置内网中的 A 计算机：

arp 【13】

arp 【14】 【15】 【16】

然后，在网关设备中对 A 计算机设置 MAC 地址与 IP 地址的绑定：

arp 【17】

arp 【18】 【19】 【20】

➢ 参考答案

一、单项选择题

1.A	2.A	3.A	4.A	5.D
6.C	7.B	8.D	9.C	10.A
11.D	12.B	13.A	14.D	15.C
16.A	17.D	18.B	19.A	20.A
21.B	22.D	23.B	24.A	25.C
26.D	27.C	28.B	29.A	30.B
31.A	32.D	33.D	34.C	35.B
36.A	37.D	38.C	39.A	40.D
41.C	42.A	43.D	44.C	45.B
46.C	47.D	48.B	49.B	50.B

二、填空题

【1】通信安全
【2】身份认证
【3】保护环
【4】强制访问控制
【5】离散对数问题
【6】160
【7】密文 或 加密
【8】行
【9】用户
【10】中断
【11】TCP
【12】RA 或 注册机构
【13】VPN 或 虚拟专用网
【14】完整性
【15】蠕虫
【16】0day 或 零日 或 0 日
【17】栈帧

【18】黑盒
【19】审核证据
【20】2017 年 6 月 1 日

三、综合应用题

【1】1024
【2】160
【3】私钥
【4】公钥
【5】摘要
【6】GRANT
【7】WITE GRANT OPTION
【8】REVOKE
【9】CONNECT
【10】角色
【11】59.69.1.1
【12】MACB
【13】-d
【14】-s
【15】59.60.1.1
【16】MACG
【17】-d
【18】-s
【19】192.168.1.10
【20】MACA