理论技能与职业素养（100分）

**2023年全国职业院校技能大赛（高等职业教育组）**

**“信息安全管理与评估”理论技能**

【注意事项】

1.理论测试前请仔细阅读测试系统使用说明文档，按提供的账号和密码登录测试系统进行测试，账号只限1人登录。

2.该部分答题时长包含在第三阶段比赛时长内，请在临近竞赛结束前提交。

3.参赛团队可根据自身情况，可选择1-3名参赛选手进行作答，团队内部可以交流，但不得影响其他参赛队。

一、 单选题 （每题2分，共35题，共70分）

1、应急事件响应和恢复措施的目标是（ B ）。

A、保证信息安全

B、最小化事件的影响

C、找出事件的责任人

D、加强组织内部的监管

2、下列数据类型不属于静态数据提取的数据类型（ C ）。

A、系统日志

B、系统进程

C、网络数据包

D、文件元数据

3、安全评估的方法不包括（ C ）。

A、风险评估

B、威胁建模

C、减少漏洞

D、渗透测试

4、以下不属于入侵监测系统的是（ C ） 。

A、 AAFID系统

B、 SNORT系统

C、 IETF系统

D、 NETEYE系统

5、通过TCP序号猜测，攻击者可以实施下列哪一种攻击？（ D ）

A、 端口扫描攻击

B、 ARP欺骗攻击

C、 网络监听攻击

D、 TCP会话劫持攻击

6、下面不是数据库的基本安全机制的是（ D ） 。

A、 用户认证

B、 用户授权

C、 审计功能

D、 电磁屏蔽

7、假设创建了名为f的实例，如何在f中调用类的add\_food函数？（ D ）

A、 f(add\_food())

B、 f.[add\_food()]

C、 f.add\_food

D、 f.add\_food()

8、aspx 的网站配置文件一般存放在哪个文件里？（ C ）

A、 conn.asp

B、 config.php

C、 web.config

D、 index.aspx

9、一个基于特征的IDS应用程序需要下列选项中的哪一项来对一个攻击做出反应？（ B ）

A、 正确配置的DNS

B、 正确配置的规则

C、 特征库

D、 日志

10、完成数据库应用系统的设计并进行实施后，数据库系统进入运行维护阶段。下列工作中不属于数据库运行维护工作的是（ D ） 。

A、 恢复数据库数据以核查问题

B、 为了保证安全，定期修改数据库用户的密码

C、 更换数据库服务器以提高应用系统运行速度

D、 使用开发人员提供的SQL语句易始化数据库中的表

11、以下不属入侵检测中要收集的信息的是（ B ） 。

A、 系统和网络日志文件

B、 目录和文件的内容

C、 程序执行中不期望的行为

D、 物理形式的入侵信息

12、POP3服务器使用的监听端口是？（ B ）

A、 TCP的25端口

B、 TCP的110端口

C、 UDP的25端口

D、 UDP的110端口

13、目标计算机与网关通信失败，更会导致通信重定向的攻击形式是？（ D ）

A、 病毒

B、 木马

C、 DOS

D、 ARP欺骗

14、\_\_\_\_\_\_\_\_的目的是发现目标系统中存在的安全隐患，分析所使用的安全机制是否能够保证系统的机密性、完整性和可用性。（ A ）

A、 漏洞分析

B、 入侵检测

C、 安全评估

D、 端口扫描

15、以下哪一项描述不正确？（ C ）

A、 ARP是地址解析协议

B、 TCP/IP传输层协议有TCP和UDP

C、 UDP协议提供的是可靠传输

D、 IP协议位于TCP/IP网际层

16、如果想在类中创建私有方法，下面哪个命名是正确的？（ C ）

A、 \_add\_one

B、 add\_one

C、 \_\_add\_one

D、 add\_one\_\_

17、MD5的主循环有（ B ） 轮。

A、 3

B、 4

C、 5

D、 8

18、根据网络安全应急处理流程，应急启动后，应该进行哪一步（ B ） 。

A、 归类&定级

B、 应急处置

C、 信息通报

D、 后期处理

19、( )是一种架构在公用通信基础设施上的专用数据通信网络，利用 IPSec 等网络层安全协议和建立在 PKI 上的加密与签名技术来获得私有性。（ C ）

A、 SET

B、 DDN

C、 VPN

D、 PKIX

20、假设系统中有n个用户，他们使用对称加密体制实现保密通信，那么系统中共需要管理（ n(n-1)/2）个密钥，每个用户需要保存（ A ） 个密钥。

A、 n-1

B、 2n

C、 Cn2

D、 n！

21、什么是数据库安全的第一道保障（）。（ C ）

A、 操作系统的安全

B、 数据库管理系统层次

C、 网络系统的安全

D、 数据库管理员

22、下列方法中不能用来进行DNS欺骗的是？（ D ）

A、 缓存感染

B、 DNS信息劫持

C、 DNS重定向

D、 路由重定向

23、下列选项哪列不属于网络安全机制？（ C ）

A、 加密机制

B、 数据签名机制

C、 解密机制

D、 认证机制

24、部署大中型 IPSEC VPN 时，从安全性和维护成本考虑，建议采取什么样的技术手段提供设备间的身份验证。（ B ）

A、 预共享密钥

B、 数字证书

C、 路由协议验证

D、 802.1x

25、现今非常流行的SQL（数据库语言）注入攻击属于下列哪一项漏洞的利用？（ C ）

A、 域名服务的欺骗漏洞

B、 邮件服务器的编程漏洞

C、 WWW服务的编程漏洞

D、 FTP服务的编程漏洞

26、维吉利亚(Vigenere)密码是古典密码体制比较有代表性的一种密码，其密码体制采用的是（ C ） 。

A、 置换密码

B、 单表代换密码

C、 多表代换密码

D、 序列密码

27、如果VPN网络需要运行动态路由协议并提供私网数据加密,通常采用什么技术手段实现（ B ） 。

A、 GRE

B、 GRE+IPSEC

C、 L2TP

D、 L2TP+IPSEC

28、过滤所依据的信息来源不包括？（ D ）

A、 IP包头

B、 TCP包头

C、 UDP包头

D、 IGMP包头

29、bind9的日志默认保存在？（ C ）

A、 /var/log/named.log

B、 /var/log/named/named.log

C、 /var/named/data/named.run

D、 /var/log/data/named.run

30、一个完整的密码体制，不包括以下（ C ）要素。

A、 明文空间

B、 密文空间

C、 数字签名

D、 密钥空间

31、Linux系统中，添加用户的命令是？（ C ）

A、 net user test /add

B、 user add test

C、 useradd test

D、 test useradd

32、以下关于正则表达式，说法错误的是？（ D ）

A、 ‘root’表示匹配包含root字符串的内容

B、 ‘.’表示匹配任意字符

C、 [0-9]表示匹配数字

D、 ‘^root’表示取反

33、将用户user123修改为管理员权限命令是 （ C ） 。

A、 net user localgroup administrators user123 /add

B、 net use localgroup administrators user123 /add

C、 net localgroup administrators user123 /add

D、 net localgroup administrator user123 /add

34、VIM模式切换的说法中，正确的是？（ A ）

A、 命令模式通过i命令进入输入模式

B、 输入模式通过:切换到末行模式

C、 命令模式通过ESC键进入末行模式

D、 末行模式通过i进入输入模式

35、在常见的安全扫描工具中，以下（ C ） 主要用来分析Web站点的漏洞，可以针对数千种常见的网页漏洞或安全风险进行检测。

A、 SuperScan

B、 Fluxay（流光）

C、 Wikto

D、 MBSA

**二、 多选题 （每题3分，共10题，共30分）**

1、在动态易失数据提取及固定过程中，为了提高数据准确性，以下( ABC )技术不对数据传输造成影响

A、数据库触发器

B、数据加密技术

C、数据压缩校验

D、网络延迟

2、在应急响应流程中，以下( ABC )方法适合收集信息。

A、监控系统

B、系统日志分析

C、询问用户

D、随机抽样调查

3、关于函数中变量的定义，哪些说法是正确的？（ AC ）

A、 即使函数外已经定义了这个变量，函数内部仍然可以定义

B、 如果一个函数已经定义了name变量，那么其他的函数就不能再定义

C、 函数可以直接引用函数外部定义过的变量

D、 函数内部只能定义一个变量

4、下面标准可用于评估数据库的安全级别的有（ ABCD ）

A、 TCSEC

B、 IFTSEC

C、 CC DBMS.PP

D、 GB17859-1999

5、安全的网络通信必须考虑以下哪些方面？（ ABCD ）

A、 加密算法

B、 用于加密算法的秘密信息

C、 秘密信息的分布和共享

D、 使用加密算法和秘密信息以获得安全服务所需的协议

6、RC4加密算法被广泛应用，包括（ ABC ）

A、 SSL/TLS

B、 WEP协议

C、 WPA协议

D、 数字签名

7、VIM的工作模式，包括哪些？（ ABD ）

A、 命令模式

B、 输入模式

C、 高亮模式

D、 底行模式

8、在反杀伤链中，情报可以分为那几个层次？（ BCD ）

A、 战斗

B、 战略

C、 战区

D、 战术

9、我国现行的信息安全法律体系框架分为（ ABC ）三个层面。

A、信息安全相关的国家法律

B、信息安全相关的行政法规和部分规章

C、信息安全相关的地方法规/规章和行业规定

D、信息安全相关的个人职业素养

10、信息道德与信息安全问题一直存在的原因有（ ABCD ）。

A、信息系统防护水平不高

B、信息安全意识不强

C、信息安全法律法规不完善

D、网络行为道德规范尚未形成