第一套 信息安全管理与评估理论知识题库

一、 单选题 （每题 2 分，共 35 题，共 70 分）

1、《中华人民共和国数据安全法》已由中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议通过，现予公布，自（ ）起施行。

A、2020 年 9 月 1 日

B、2021 年 9 月 1 日

C、2020 年 1 月 1 日

D、2021 年 1 月 1 日

2、下列( )方式属于对学生进行信息道德与信息安全教育。

A、用计算机播放影片

B、用计算机为某活动搜索素材

C、用计算机处理班级照片

D、播放计算机犯罪新闻专题片

3、检查点能减少数据库完全恢复时所必须执行的日志，提高数据库恢复速度。下列有关检查点的说法，错误的是（ ）。

A、 检查点记录的内容包括建立检查点时正在执行的事务清单和这些事务最近一个日志记录的地址

B、 在检查点建立的同时，数据库管理系统会将当前数据缓冲区中的所有数据记录写入数据库中

C、 数据库管理员应定时手动建立检查点，保证数据库系统出现故障时可以快速恢复数据库数据

D、 使用检查点进行恢复时需要从"重新开始文件"中找到最后一个检查点记录在日志文件中的地址

4、下面程序的运行结果是: # i nclude<stdio.h> { int k=0; char c='A'; do {switch(c++) {case 'A':k++;break; case 'B':k--; case 'C':k+=2;break; case 'D':k=k%2;continue。

A、 k=0

B、 k=2

C、 k=3

D、 k=4

5、大学遭遇到 DDOS 攻击，那么根据网络安全应急预案，启动应急响应方案时，可以将应急预案定为哪个等级？（ ）

A、 3 级

B、 4 级

C、 2 级

D、 1 级

6、以下不属入侵检测中要收集的信息的是（ ）。

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

7、外部数据包过滤路由器只能阻止一种类型的 IP 欺骗，即（ ），而不能阻止 DNS 欺骗？

A、 内部主机伪装成外部主机的 IP

B、 内部主机伪装成内部主机的 IP

C、 外部主机伪装成外部主机的 IP

D、 外部主机伪装成内部主机的 IP

8、部署全网状或部分网状 IPSEC VPN 时为减小配置工作量可以使用哪种技术。( )
A、 L2tp+IPSEC
B、 DVPN
C、 IPSEC over GRE
D、 动态路由协议
9、在一下古典密码体制中，属于置换密码的是？( )
A、 移位密码
B、 倒叙密码
C、 仿射密码
D、 PlayFair 密码
10、数据库管理员应该定期对数据库进行重组，以保证数据库性能。下列有关数据库重组工作的说法，错误的是( )。
A、 重组工作中可能会对数据库数据的磁盘分区方法和存储空间进行调整
B、 重组工作一般会修改数据库的内模式和模式，一般不改变数据库外模式
C、 重组工作一般在数据库运行一段时间后进行，不应频繁进行数据库重组
D、 重组工作中应尤其注意频繁修改数据的表，因为这些表很容易出现存储碎片，导致效率下降
11、Skipjack 是一个密钥长度为( )位。
A、 56
B、 64
C、 80
D、 128
12、m-序列本身是适宜的伪随机序列产生器，但只有在 ( ) 下，破译者才不能破解这个伪随机序列。
A、 唯密文攻击
B、 已知明文攻击
C、 选择明文攻击
D、 选择密文攻击
13、小李在使用 nmap 对目标网络进行扫描时发现，某一个主机开放了 25 和 110 端口，此主机最有可能是什么？( )
A、 文件服务器
B、 邮件服务器
C、 WEB 服务器
D、 DNS 服务器
14、下面不是 Oracle 数据库支持的备份形式的是 ( )。
A、 冷备份
B、 温备份
C、 热备份
D、 逻辑备份
15、以下关于 TCP 和 UDP 协议的描述中，正确的是？( )
A、 TCP 是端到端的协议，UDP 是点到点的协议
B、 TCP 是点到点的协议，UDP 是端到端的协议
C、 TCP 和 UDP 都是端到端的协议
D、 TCP 和 UDP 都是点到点的协议
16、下面不是计算机网络面临的主要威胁的是? ( )
A、 恶意程序威胁
B、 计算机软件面临威胁
C、 计算机网络实体面临威胁
D、 计算机网络系统面临威胁

17、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？（ ）
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
18、关于并行数据库，下列说法错误的是（)。
A、 层次结构可以分为两层，顶层是无共享结构，底层是共享内存或共享磁盘结构
B、 无共享结构通过最小化共享资源来降低资源竞争，因此具有很高的可扩展性，适合于 OLTP 应用
C、 并行数据库系统经常通过负载均衡的方法来提高数据库系统的业务吞吐率
D、 并行数据库系统的主要目的是实现场地自治和数据全局透明共享
19、Str='heiheihei' print str[3:]将输出？（ ）
A、 hei
B、 heihei
C、 eih
D、 ihe
20、包过滤型防火墙工作在? ( )
A、 会话层
B、 应用层
C、 网络层
D、 数据链路层
21、下面是个人防火墙的优点的是? ( )
A、 运行时占用资源
B、 对公共网络只有一个物理接口
C、 只能保护单机，不能保护网络系统
D、 增加保护级别
22、关于 IP 提供的服务，下列哪种说法是正确的？（ ）
A、 IP 提供不可靠的数据投递服务，因此数据包投递不能受到保障
B、 IP 提供不可靠的数据投递服务，因此它可以随意丢弃报文
C、 IP 提供可靠的数据投递服务，因此数据报投递可以受到保障
D、 IP 提供可靠的数据投递服务，因此它不能随意丢弃报文
23、print type(2.0)将输出？（ ）
A、 <type 'long'>
B、 <type 'str'>
C、 <type 'int'>
D、 <type 'float'>
24、Open 函数中 w 参数的作用是？（ ）
A、 读文件内容
B、 写文件内容
C、 删除文件内容
D、 复制文件内容
25、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？（ ）
A、 正确配置的 DNS
B、 正确配置的规则
C、 特征库
D、 日志
26、在 RHEL5 服务器中，查看用户 vanzk 密码记录的操作及输出如下所示: [root@pc05~]#grep vanzk /etc/shadow vanzk:!!1fKuFV9X8$VxFk0Ergj4uzP9UZGnleb.:15771:0:99999:7::: 则据此可判断用户 vanzk

的账号（ ）。
A、 每次设置新的密码后，有效期为 7 天，过期后必须重设
B、 其 uid 为 0，具有与 root 用户一样的权限
C、 因密码被锁定而无法登录
D、 使用的密码长度超过 8 位，安全性较高
27、Shell 编程条件判断中，文件权限判断说法错误的是？
A、 -r 判断该文件是否存在，并且该文件是否拥有读写权限
B、 -w 判断该文件是否存在，并且该文件是否拥有写权限
C、 -x 判断该文件是否存在，并且该文件是否拥有执行权限
D、 -u 判断该文件是否存在，并且该文件是否拥有 SUID 权限
28、IPSec 包括报文验证头协议 AH 协议号（ ）和封装安全载荷协议 ESP 协议号（ ）。
A、 51 50
B、 50 51
C、 47 48
D、 48 47
29、VIM 光标操作说法中错误的是？（ ）
A、 h 光标向左移动一位
B、 2j 光标向下移动两行
C、 w 跳到下一个单词的词尾
D、 G 跳到文档的最后一行
30、Linux 软件管理 rpm 命令，说法不正确的是？（ ）
A、 -v 显示详细信息
B、 -h: 以#显示进度；每个#表示 2%
C、 -q PACKAGE_NAME：查询指定的包是否已经安装
D、 -e 升级安装包
31、部署 IPSEC VPN 时，配置什么安全算法可以提供更可靠的数据验证 ( ).
A、 DES
B、 3DES
C、 SHA
D、 128 位的 MD5
32、指数积分法（Index Calculus）针对下面那种密码算法的分析方法？
A、 背包密码体制
B、 RSA
C、 ElGamal
D、 ECC
33、Linux 的基本命令 ls，其选项-l 代表的是？
A、 显示详细信息
B、 查看目录属性
C、 人性化显示文件大小
D、 显示文件索引号
34、VIM 命令中，用于撤销的命令是？
A、 a
B、 x
C、 p
D、 u
35、你想发送到达目标网络需要经过那些路由器，你应该使用什么命令？
A、 Ping

B、 Nslookup
C、 Traceroute
D、 Ipconfig

二、 多选题 （每题 3 分，共 10 题，共 30 分）
1、数据库系统可能的潜在安全风险包括（)。
A、 操作系统安全风险，包括软件的缺陷、未进行软件安全漏洞修补工作、脆弱的服务和选择不安全的默认配置
B、 数据库系统中可用的但并未正确使用的安全选项、危险的默认设置、给用户不适当的权限、对系统配置的未经授权的改动等
C、 不及时更改登录密码或密码太过简单，存在对重要数据的非法访问以及窃取数据库内容或恶意破坏等
D、 数据库系统的内部风险，如内部用户的恶意操作等
2、SQL Server 中的预定义服务器角色有（)。
A、 Sysadmin
B、 Serveradmm
C、 Setupadmin
D、 Securityadmin
3、想使用 python 输出 im happy 下面哪些写法是正确的？
A、 print (im happy)
B、 print 'im happy'
C、 echo 'im happy'
D、 print '''im happy'''
4、以下属于多表代换的密码是？
A、 Playfair
B、 Polybius
C、 Vigenere
D、 Hill 密码
5、下列关于 SQL Server 2008 身份验证模式的说法，正确的是（)。
A、 在"Windows 身份验证模式"下，不允许 sa 登录到 SQL Server 服务器
B、 在"Windows 身份验证模式"下，所有 Windows 用户都自动具有登录到 SQL Server 服务器的权限
C、 不管是哪种身份验证模式，Windows 中的 Administrator 无需授权就可登录到 SQL Server 服务器
D、 安装好 SQL Server 之后，可以根据需要随时更改身份验证模式
6、数据库访问控制的粒度可能有（)。
A、 数据库级
B、 表级
C、 记录级（ 行级 ）
D、 属性级
7、操作系统安全主要包括（ ）等方面 。
A、 账户密码安全和文件共享安全
B、 文件权限管理和用户权限管理
C、 日志审计和远程访问权限管理
D、 文件夹选项和安全选项
8、IPSec 可以提供哪些安全服务 ( )
A、 数据机密性
B、 数据完整性
C、 数据来源认证
D、 防重放攻击

9、关于类的说法，下面哪些是错误的？
A、 私有方法和私有变量只能在类的内部使用
B、 一个类只能创建一个实例
C、 两个不同的类中的方法不能重名
D、 创建类的实例时，传入的变量类型要和类中定义的一致
10、IKE 的主要功能包括()
A、 建立 IPSec 安全联盟
B、 防御重放攻击
C、 数据源验证
D、 自动协商交换密钥

答案：

1.B 2021 年 9 月 1 日 1.B.
2.D 播放计算机犯罪新闻专题片
3.C 数据库管理员应定时手动建立检查点，保证数据库系统出现故障时可以快速恢复数据库数据
4.C、k=3
5. D.
6. D.物理形式的入侵信息
7. D、外部主机伪装成内部主机的 IP
8.C、IPSEC over GRE
9. A、移位密码
10.B、重组工作一般会修改数据库的内模式和模式，一般不改变数据库外模式
11.C、
12.A.唯密文攻击
13.B.
14.D 逻辑备份
15.D.TCP 和 UDP 都是点到点的协议
16.B、计算机软件面临威胁
17.C、WWW 服务的编程漏洞
18.D、并行数据库系统的主要目的是实现场地自治和数据全局透明共享
19.B、heihei
20.C
21. D、增加保护级别
22.A.IP 提供不可靠的数据投递服务，因此数据包投递不能受到保障
23. D.<type 'float'>
24.B.写文件内容
25.B.正确配置的规则
26.C、因密码被锁定而无法登录
27. D.-u 判断该文件是否存在，并且该文件是否拥有 SUID 权限
28.A.51 50
29.D.

30. D.
31. B、3DES
32.B、RSA
33.A、显示详细信息
34. D、U
35.C Traceroute

多选：

1. A、B、C、D
2. A、C、D
3. B、D
4. A C
5. B C
6. A、B、C、D
7. A、B、C
8. A、B、C、D
9. B、D
10. A、C、D

第二套

一、 单选题 （每题 2 分，共 35 题，共 70 分）

1、《中华人民共和国网络安全法》已由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议通过，自（ ）起施行。

A、 2019 年 6 月 1 日

B、 2018 年 6 月 1 日

C、 2017 年 6 月 1 日

D、 2016 年 6 月 1 日

2、下列( )行为属于信息道德与信息安全失范行为。

A、上网

B、朋友圈恶作剧

C、网络诈骗

D、网上购物

3、设在 RSA 的公钥密码体制中，公钥为（e,n）=（13，35），则私钥 d=？（ ）。

A、 11

B、 13

C、 15

D、 17

4、关于函数，下面哪个说法是错误的？（ ）

A、 函数必须有参数

B、 函数可以有多个函数

C、 函数可以调用本身

D、 函数内可以定义其他函数

5、以下哪一项描述不正确？（ ）

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
6、下列选项中不是 Hydra 工具中的-e 参数的值是？（ ）
A、 o
B、 n
C、 s
D、 r
7、网络监听（嗅探）的这种攻击形式破坏了下列哪一项内容？（ ）
A、 网络信息的抗抵赖性
B、 网络信息的保密性
C、 网络服务的可用性
D、 网络信息的完整性
8、下面程序的运行结果是: #i nclude <stdio. h> main() { int x,i; for(j-1;i<=100;i++) {x=i; if(++x%2==0) if(++x%3==0) if(++x%7==0) printf("%d",x); } } 。( )
A、 26 68
B、 28 70
C、 39 81
D、 42 84
9、IPSEC 包括报文验证头协议 AH 协议号（ ）和封装安全载荷协议 ESP 协议号。( )
A、 51 50
B、 50 51
C、 47 48
D、 48 47
10、在远程管理 Linux 服务器时，以下( ) 方式采用加密的数据传输。( )
A、 rsh
B、 telnet
C、 ssh
D、 rlogin
11、在 wireshark 中下列表达式能捕获设置了 PSH 位的 TCP 数据包的是？（ ）
A、 tcp[13]&4==4
B、 tcp[13]&2==2
C、 tcp[13]&16==16
D、 tcp[13]&8==8
12、什么是数据库安全的第一道保障（)。
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
13、以下不属于防火墙作用的是（)。
A、 过滤信息
B、 管理进程
C、 清除病毒
D、 审计监测
14、在数据库系统中,死锁属于（)。
A、 系统故障

B、 事务故障
C、 介质保障
D、 程序故障
15、哪个关键字可以在 python 中定义函数？（ ）
A、 dcf
B、 def
C、 class
D、 public
16、下面哪些选项可以让输出的字符串换行？（ ）
A、 print '''im Happy'''
B、 print 'im \nhappy'
C、 print 'im /nhappy'
D、 print ''im happy''
17、小李在使用 nmap 对目标网络进行扫描时发现，某一个主机开放了 25 和 110 端口，此主机最有可能是什么？（ ）
A、 文件服务器
B、 邮件服务器
C、 WEB 服务器
D、 DNS 服务器
18、手动脱压缩壳一般是用下列哪种方法？（ ）
A、 使用 upx 脱壳
B、 使用 winhex 工具脱壳
C、 使用 fi 扫描后，用 unaspack 脱壳
D、 确定加壳类型后，ollyice 调试脱壳
19、下面不是 Oracle 数据库提供的审计形式的是（ ）。
A、 备份审计
B、 语句审计
C、 特权审计
D、 模式对象设计
20、如果想在类中创建私有方法，下面哪个命名是正确的？（ ）
A、 _add_one
B、 add_one
C、 __add_one
D、 add_one__
21、POP3 服务器使用的监听端口是？（ ）
A、 TCP 的 25 端口
B、 TCP 的 110 端口
C、 UDP 的 25 端口
D、 UDP 的 110 端口
22、下列哪个工具可以进行 web 程序指纹识别？（ ）
A、 nmap
B、 openVAs
C、 御剑
D、 whatweb
23、在需求分析阶段规定好不同用户所允许访问的视图，这属于数据库应用系统的（ ）。
A、 功能需求分析
B、 性能需求分析

C、 存储需求分析
D、 安全需求分析
24、假如你向一台远程主机发送特定的数据包，却不想远程主机响应你的数据包，这时你可以使用以下哪一种类型的进攻手段？（ ）
A、 缓冲区溢出
B、 暴力攻击
C、 地址欺骗
D、 拒绝服务
25、下面那个名称不可以作为自己定义的函数的合法名称？（ ）
A、 print
B、 len
C、 error
D、 Haha
26、以下关于正则表达式，说法错误的是？（ ）
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
27、哪个关键词可以在 python 中进行处理错误操作？（ ）
A、 try
B、 catch
C、 finderror
D、 error
28、VIM 退出命令中，能强制保存并退出的是？（ ）
A、 x
B、 wq
C、 q
D、 wq!
29、下列不属于网络安全 CIA 需求属性的是哪一项？（ ）
A、 机密性
B、 可抵赖性
C、 完整性
D、 可用性
30 在一台 Cisco 路由器 R1 上进行了如下 ACL 配置: R1 (config)#access-list 1 permit any R1 (config)#access-list 1 deny 192.168.21.1 0.0.0.0 R1 (config) #interface f0/0 R1 (config) #ip access-group 1 in 以上设置可以实现在路由器 R1 的 F0/0 接口的（ ）功能。
A、 拒绝来自主机 192.168.21.1 的数据包
B、 只允许来自主机 192.168.21.1 的数据包
C、 允许所有报文通过
D、 拒绝所有报文转发
31、在 RHEL5 系统中，使用 lvextend 为逻辑卷扩容以后，还需要进行（ ）操作以便系统能够识别新的卷大小。
A、 Lvscan
B、 Partprobe
C、 Reboot
D、 resize2fs
32、Linux 软件管理 rpm 命令，说法不正确的是？（ ）
A、 -v 显示详细信息

B、 -h: 以#显示进度；每个#表示 2%
C、 -q PACKAGE_NAME：查询指定的包是否已经安装
D、 -e 升级安装包
33、SYN Flood 属于？（ ）
A、 拒绝服务攻击
B、 缓存区溢出攻击
C、 操作系统漏洞攻击
D、 社会工程学攻击
34、差分分析是针对下面那种密码算法的分析方法？（ ）
A、 DES
B、 AES
C、 RC4
D、 MD5
35、按目前的计算能力，RC4 算法的密钥长度至少应为（ ）才能保证安全强度。
A、 任意位
B、 64 位
C、 128 位
D、 256 位
二、 多选题 （每题 3 分，共 10 题，共 30 分）
1、下面标准可用于评估数据库的安全级别的有（ ）。
A、 TCSEC
B、 IFTSEC
C、 CC DBMS.PP
D、 GB17859-1999E.TD
2、Bash 编程中，常见的循环有？（ ）
A、 foreach
B、 while
C、 for
D、 until
3、关于 yum 命令，说法正确的有哪些？（ ）
A、 -y 自动应答 yes
B、 -e 静默执行
C、 -t 延迟安装
D、 -R[分钟] 设置等待时间
4、源代码泄露可能让攻击者分析出哪些其它漏洞？（ ）
A、 SQL 注入
B、 命令执行
C、 文件上传
D、 XSS
5、下列关于 SQL Server 2008 中 guest 用户的说法，正确的是（ ）。
A、 guest 用户没有对应的登录账户名
B、 通过授权语句可以启用数据库中的 guest 用户
C、 所有数据库用户都继承该数据库中 guest 用户的权限
D、 任何 SQL Server 登录账户都可以访问启用了 guest 用户的数据库
6、隐藏 Apache 服务器信息的方法包括？（ ）
A、 隐藏 HTTP 头部信息
B、 禁止显示错误信息

C、 自定义错误页面，消除服务器的相关信息
D、 修改服务 IP 地址
7、在 RHEL5 系统中，以下（ ）操作将在分区/dev/sdb7 上创建 EXT3 文件系统。
A、 mkfs –t ext3 /dev/sdb7
B、 mkfs.ext3 /dev/sdb7
C、 fdisk –t ext3 /dev/sdb7
D、 format /dev/sdb7 –t ext3
8、IKE 的主要功能包括( )
A、 建立 IPSec 安全联盟
B、 防御重放攻击
C、 数据源验证
D、 自动协商交换密钥
9、利用 Metasploit 进行缓冲区溢出渗透的基本步骤包括（)。
A、 选择利用的漏洞类型
B、 选择 meterpreter 或者 shell 类型的 payload
C、 设置渗透目标 IP、本机 IP 地址和监听端口号
D、 选择合适的目标类型
10、以下 Linux 命令中，跟目录及文件基本操作相关的命令有哪些？（ ）
A、 cd
B、 touch
C、 rm
D、 userdel

答案：

单选
1.A、2019 年 6 月 1 日
2.C、网络诈骗
3. D、17
4.A、函数必须有参数
5.C、UDP 协议提供的是可靠传输
6. D、
7.B、网络信息的保密性
8.C、39 81
9.A、51 50
10.C、ssh
11.B、tcp[13]&2==2
12.A、操作系统的安全
13.B、管理进程
14.B、事务故障
15.B、def
16. A、 print ""'im Happy""
17.D、DNS 服务器

18.C、使用 fi 扫描后，用 unaspack 脱壳
19.D、模式对象设计
20.C.add one
21.B、TCP 的 110 端口
22.D、whatweb
2ö 窭覷↔桻叁料 Π 猙燋站、安全需求分析
24.D、拒绝服务
25.A、 print
26. D、
'^root’ 表示取反
27.A、try
28.B、wq
29.B、可抵赖性
30.A、拒绝来自主机 192.168.21.1 的数据包
31.D、resize2fs
32. D、-e 升级安装包
33.A、拒绝服务攻击
34.D、MD5
35.C、128 位
多选：
1.A、TCSEC; C、CC DBMS.PP
2.B、while;C、for; D、until
3.A、-y 自动应答 yes;B、-e 静默执行
4.A、SQL 注入;B、命令执行;C、文件上传;D、XSS
5.B、通过授权语句可以启用数据库中的 guest 用户
隐藏 HTTP 头部信息;B、禁止显示错误信息;C、自定义错误页面，消除服务器的相关信息 6.A、7.A、mkfs -t ext3 /dev/sdb7;B、mkfs.ext3 /dev/sdb7
8. A.建立 IPSec 安全联盟;D、自动协商交换密钥
9.A、:选择利用的漏洞类型:B、选择 meterpreter 或者 shell 类型的 payload;C、设置渗透目标
IP、本机 IP 地址和监听端口号
10.A、cd; B、touch;C、rm

第三套

一、 单选题 （每题 2 分，共 35 题，共 70 分）
1、《中华人民共和国个人信息保护法》是为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用，根据宪法，制定的法规，自（ ）起施行。
A、 2020 年 11 月 1 日
B、 2021 年 11 月 1 日
C、 2022 年 1 月 1 日
D、 2021 年 1 月 1 日
2、下列( )方式不适合对学生进行信息道德与信息安全教育。

A、观看相关新闻
B、观看相关视频
C、信息技术课
D、一起玩游戏
3、有关数据库加密，下面说法不正确的是（ ）。
A、 索引字段不能加密
B、 关系运算的比较字段不能加密
C、 字符串字段不能加密
D、 表间的连接码字段不能加密
4、入侵检测的目的是（ ）。
A、 实现内外网隔离与访问控制
B、 提供实时的检测及采取相应的防护手段，阻止黑客的入侵
C、 记录用户使用计算机网络系统进行所有活动的过程
D、 预防、检测和消除病毒
5、\x32\x2E\x68\x74\x6D 此加密是几进制加密？（ ）
A、 二进制
B、 八进制
C、 十进制
D、 十六进制
6、现代密码学中很多应用包含散列运算，而下面应用中不包含散列运算的是？（ ）
A、 消息机密性
B、 消息完整性
C、 消息认证码
D、 数字签名
7、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？（ ）
A、 病毒
B、 木马
C、 DOS
D、 ARP 欺骗
8、设在 RSA 的公钥密码体制中，公钥为（e,n）=（13，35），则私钥 d=？（ ）
A、 11
B、 13
C、 15
D、 17
9、Shell 变量命令，说法错误的是？（ ）
A、 变量名必须以字母或下划线开头，且只能由字母、数字和下划线组成
B、 变量名的长度不得超过 100 个字符
C、 变量名在有效的范围内必须是唯一
D、 在 bash 中，变量的默认类型都是字符串型
10、SQL 的 GRANT 和 REVOKE 语句可以用来实现（ ）。
A、 自主存取控制
B、 强制存取控制
C、 数据库角色创建
D、 数据库审计
11、Str='heiheihei' print str[3:]将输出？（ ）
A、 hei
B、 heihei

C、 eih
D、 ihe
12、能修改系统引导扇区，在计算机系统启动时首先取得控制权的病毒属于（ ）。
A、 文件病毒
B、 引导型病毒
C、 混合型病毒
D、 恶意代码
13、下列哪个不是密码字典？（ ）
A、 弱口令字典
B、 社工字典
C、 彩虹表
D、 《康熙字典》
14、Skipjack 是一个密钥长度为( )位。
A、 56
B、 64
C、 80
D、 128
15、在 RSA 算法中，取 P=3，q=11,e=3，则 d 等于多少？（ ）
A、 33
B、 20
C、 14
D、 7
16、已知字母 A 的 ASCII 码为十进制数 65,且 c2 为字符型,则执行语句 c2='A'+'6'-'3';后,c2 中的值为？（ ）
A、 D
B、 68
C、 58
D、 24
17、Burp suite 是用于攻击（ ）的集成平台。
A、 web 应用程序
B、 客户机
C、 服务器
D、 浏览器
18、远程 windows 口令破解的工具是？（ ）
A、 NtScan
B、 getpass
C、 Hydra
D、 Saminside
19、如果想在文件 test.txt 中追加内容，应该使用下列哪个选项？（ ）
A、 a=open('test.txt',"a")
B、 a=open('test.txt',"r")
C、 a=open('test.txt',"d")
D、 a=open('test.txt',"w")
20、在强制存取控制机制中，当主体的许可证级别等于客体的密级时，主体可以对客体进行如下操作（ ）。
A、 读取
B、 写入
C、 不可操作
D、 读取、写入

21、关于数据库应用系统的设计，下列说法正确的是（ ）。

A、 数据库应用系统设计需要考虑数据组织与存储、数据访问与处理、应用设计等几个方面

B、 数据库概念设计阶段，采用自上而下的 E-R 设计时，首先设计局部 E-R 图，然后合并各局部 E-R 图得到全局 E-R 图

C、 在数据库逻辑设计阶段，将关系模式转换为具体 DBMS 平台支持的关系表

D、 在数据库物理设计阶段，一般需要设计视图和关系模式的完整性约束

22、如果想在类中创建私有方法，下面哪个命名是正确的？（ ）

A、 _add_one

B、 add_one

C、 __add_one

D、 add_one__

23、nmap 的-SV 是什么操作？（ ）

A、 TCP 全连接扫描

B、 FIN 扫描

C、 版本扫描

D、 全面扫描

24、扫描器之王 NMAP 中，全面扫描的命令是什么？（ ）

A、 -o

B、 -SV

C、 -sP

D、 -a

25、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？（ ）

A、 正确配置的 DNS

B、 正确配置的规则

C、 特征库

D、 日志

26、一个完整的密码体制，不包括以下（ ）要素。

A、 明文空间

B、 密文空间

C、 数字签名

D、 密钥空间

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（ ）。

A、 GRE

B、 GRE+IPSEC

C、 L2TP

D、 L2TP+IPSEC

28、在现有的计算能力条件下，对于椭圆曲线密码算法(ECC)，被认为是安全的最小密钥长度 是？（ ）

A、 128 位

B、 160 位

C、 512 位

D、 1024 位

29、在( )年，美国国家标准局 NBS 把 IBM 的 Tuchman-Meyer 方案确定数据加密标准，即 DES。

A、 1949

B、 1972

C、 1977

D、 2001

30、过滤所依据的信息来源不包括？（ ）

A、 IP 包头
B、 TCP 包头
C、 UDP 包头
D、 IGMP 包头
31、SEAL 使用了四个（ ）位寄存器。
A、 24
B、 32
C、 48
D、 56
32、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（ ）。
A、 置换密码
B、 单表代换密码
C、 多表代换密码
D、 序列密码
33、Linux 中，使用哪一个命令删除非空文件夹？（ ）
A、 mv
B、 rm
C、 rmdir
D、 del
34、下面哪一项不是 hash 函数的等价提法？（ ）
A、 压缩信息函数
B、 哈希函数
C、 单向散列函数
D、 杂凑函数
35、差分分析是针对下面那种密码算法的分析方法？（ ）
A、 DES
B、 AES
C、 RC4
D、 MD5
二、 多选题 （每题 3 分，共 10 题，共 30 分）
1、分组密码的常见的四中运行模式中，如果其中一个密文分组有一个比特的错误，不会将该错误进行传播的模式是？（ ）
A、 ECB
B、 CBC
C、 CFB
D、 OFB
2、Apache 服务器外围加固措施包括？（ ）
A、 部署 WAF
B、 部署 IPS
C、 部署 IDS
D、 部署蜜罐系统
3、Bash 编程中，常见的循环有？（ ）
A、 foreach
B、 while
C、 for
D、 until
4、netwox 工具拥有以下哪些功能？（ ）

A、 嗅探
B、 SQL 注入
C、 欺骗
D、 地址转换
5、如何在不改变原始网络拓扑和业务的前提下，消除或者避免 ICMP 重定向攻击？（ ）
A、 关掉 ip redirects
B、 代理 ARP
C、 使用访问控制表（ACL）
D、 不同掩码长度子网划分
6、移动用户常用的 VPN 接入方式是（ ）。
A、 L2TP
B、 IPSECHIKE 野蛮模式
C、 GRE+IPSEC
D、 L2TP+IPSEC
7、Linux 的 ls 命令，下列说法正确的是？（ ）
A、 -d：选项是查看目录属性
B、 -l：选项是显示详细信息
C、 -h：选项是人性化显示文件大小
D、 -i：选项是显示文件索引号
8、以下 Linux 命令中，跟网络管理相关的命令有哪些？（ ）
A、 ifconfig
B、 df
C、 lsmod
D、 netstat
9、防火墙一般需要检测哪些扫描行为？（ ）
A、 Port-scan
B、 Icmp-scan
C、 Udp-scan
D、 Tcp-synflood
10、在 RHEL5 系统中，以下（ ）操作将在分区/dev/sdb7 上创建 EXT3 文件系统。
A、 mkfs –t ext3 /dev/sdb7
B、 mkfs.ext3 /dev/sdb7
C、 fdisk –t ext3 /dev/sdb7
D、 format /dev/sdb7 –t ext3

答案

单选：
1.B、2021 年 11 月 1 日
2. D、-起玩游戏
3. A、索引字段不能加密
4.B、提供实时的检测及采取相应的防护手段，阻止黑客的入侵
5.D、十六进制

6.A、消息机密性
7. D、ARP 欺骗
8.C、15
9.B、变量名的长度不得超过 100 个字符
10.A、自主存取控制
11.B、 heihei
12.B、引导型病毒
13. D.《康熙字典》
14 C、80
15.C、14
16.B、68
17.A、web 应用程序
18.C、Hydra
19.A、a=open('test.txt',"a”）
20.D、读取、写入
21.A、数据库应用系统设计需要考虑数据组织与存储、数据访问与处理、应用设计等几个方面
22.C、add one
23.C、
24. D.-a
25.B、正确配置的规则
26.C、数字签名
27. D、L2TP+IPSEC
28 B、160 位
29.C、1977
30.D、IGMP 包头
31.B、32
32.C、多表代换密码
33.B、rm
34.C、单向散列函数
35.A、DES
多选：
1.A、ECB; D、OFB
2.A、部署 WAF;B、部署 IPS;C、部署 IDS
3.B、while; C、for; D、until
4.A、嗅探;B、SQL 注入;C、欺骗;D、地址转换
5.A、关掉 ip redirects;C、使用访问控制表(ACL)
6.A、L2TP; D、L2TP+IPSEC
7.B、-1:选项是显示详细信息;C、-h:选项是人性化显示文件大小
8.A、ifconfig; D、netstat
9.A、Port-scan; B、Icmp-scan;C、Udp-scan; D、Tcp-synflood
10.A、mkfs -t ext3 /dev/sdb7;B、 mkfs.ext3 /dev/sdb7

第四套

一、 单选题 （每题 2 分，共 35 题，共 70 分）

1、为了保护计算机信息系统的安全，促进计算机的应用和发展，保障社会主义现代化建设的顺利进行制定的条例。由中华人民共和国国务院于（ ）年 2 月 18 日发布实施《中华人民共和国计算机信息系统安全保护条例》，（ ）年 1 月 8 日修订。

A、 1994 2010

B、 1995 2011

C、 1994 2011

D、 1995 2010

2、随意下载、使用、传播他人软件或资料属于（ ）信息道德与信息安全失范行为。

A、黑客行为

B、侵犯他人隐私

C、侵犯知识产权

D、信息传播

3、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。（ ）

A、 预共享密钥

B、 数字证书

C、 路由协议验证

D、 802.1x

4、针对 Windows 系统主机，攻击者可以利用文件共享机制上的 Netbios “空会话”连接漏洞，获取众多对其攻击有利的敏感信息，获取的信息中不包含下列哪一项信息？（ ）

A、 系统的用户和组信息

B、 系统的共享信息

C、 系统的版本信息

D、 系统的应用服务和软件信息

5、IP 数据报分片后的重组通常发生在？（ ）

A、 源主机和数据报经过的路由器上

B、 源主机上

C、 数据报经过的路由器上

D、 目的主机上

6、下面不属于 SYN FLOODING 攻击的防范方法的是？（ ）

A、 缩短 SYN Timeout（连接等待超时）时间

B、 利用防火墙技术

C、 TCP 段加密

D、 根据源 IP 记录 SYN 连接

7、当数据库系统出现故障时，可以通过数据库日志文件进行恢复。下列关于数据库日志文件的说法，错误的是（ ）。

A、 数据库出现事务故障和系统故障时需使用日志文件进行恢复

B、 使用动态转储机制时，必须使用日志文件才能将数据库恢复到一致状态

C、 在 OLTP 系统中，数据文件的空间使用量比日志文件大得多，使用日志备份可以降低数据库的备份空间

D、 日志文件的格式主要有以记录为单位的日志文件和以数据块为单位的日志文件两种

8、SQL 的 GRANT 和 REVOKE 语句可以用来实现（　）。

A、 自主存取控制

B、 强制存取控制

C、 数据库角色创建

D、 数据库审计

9、下面对于数据库视图的描述正确的是（　）。

A、 数据库视图也是物理存储的表

B、 可通过视图访问的数据不作为独特的对象存储，数据库内实际存储的是 SELECT 语句

C、 数据库视图也可以使用 UPDATE 或 DELETE 语句生成

D、 对数据库视图只能查询数据，不能修改数据

10、有一种攻击不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统显影减慢甚至瘫痪。它影响正常用户的使用，甚至使合法用户被排斥而不能得到服务。这种攻击叫做（　）。

A、 可用性攻击

B、 拒绝性攻击

C、 保密性攻击

D、 真实性攻击

11、16 模 20 的逆元是？（　）

A、 3

B、 4

C、 5

D、 不存在

12、PKZIP 算法广泛应用于（　）程序。

A、 文档数据加密

B、 数据传输加密

C、 数字签名

D、 文档数据压缩

13、下列选项哪列不属于网络安全机制？（　）

A、 加密机制

B、 数据签名机制

C、 解密机制

D、 认证机制

14、一个 C 程序的执行是从哪里开始的？（　）

A、 本程序的 main 函数开始，到 main 函数结束

B、 本程序文件的第一个函数开始，到本程序 main 函数结束

C、 本程序的 main 函数开始，到本程序文件的最后一个函数结束

D、 本程序文件的第一个函数开始，到本程序文件的最后一个函数结束

15、检查点能减少数据库完全恢复时所必须执行的日志，提高数据库恢复速度。下列有关检查点的说法，错误的是（　）。

A、 检查点记录的内容包括建立检查点时正在执行的事务清单和这些事务最近一个日志记录的地址

B、 在检查点建立的同时，数据库管理系统会将当前数据缓冲区中的所有数据记录写入数据库中

C、 数据库管理员应定时手动建立检查点，保证数据库系统出现故障时可以快速恢复数据库数据

D、 使用检查点进行恢复时需要从"重新开始文件"中找到最后一个检查点记录在日志文件中的地址

16、下列不属于口令安全威胁的是？（　）

A、 弱口令

B、 明文传输

C、 MD5 加密

D、 多账户共用一个密码

17、在远程管理 Linux 服务器时，以下（ ）方式采用加密的数据传输。
A、 rsh
B、 telnet
C、 ssh
D、 rlogin
18、在 C 语言中（以 16 位 PC 机为例），5 种基本数据类型的存储空间长度的排列顺序为?（ ）
A、 char<int<long int<=float<double
B、 char=int<long int<=float<double
C、 char<int<long int=float=double
D、 char=int=long int<=float<double
19、下列方法中不能用来进行 DNS 欺骗的是？（ ）
A、 缓存感染
B、 DNS 信息劫持
C、 DNS 重定向
D、 路由重定向
20、以下对 DoS 攻击的描述，正确的是？（ ）
A、 不需要侵入受攻击的系统
B、 以窃取目标系统上的机密信息为目的
C、 导致目标系统无法正常处理用户的请求
D、 若目标系统没有漏洞，远程攻击就不会成功
21、通过 TCP 序号猜测，攻击者可以实施下列哪一种攻击？（ ）
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
22、下面不是保护数据库安全涉及到的任务是（)。( )
A、 确保数据不能被未经过授权的用户执行存取操作
B、 防止未经过授权的人员删除和修改数据
C、 向数据库系统开发商索要源代码，做代码级检查
D、 监视对数据的访问和更改等使用情况
23、下面不是 Oracle 数据库提供的审计形式的是（)。
A、 备份审计
B、 语句审计
C、 特权审计
D、 模式对象设计
24、在一下古典密码体制中，属于置换密码的是？（ ）
A、 移位密码
B、 倒叙密码
C、 仿射密码
D、 PlayFair 密码
25、一个基于网络的 IDS 应用程序利用什么来检测攻击？（ ）
A、 正确配置的 DNS
B、 特征库
C、 攻击描述
D、 信息包嗅探器
26、下列工具中可以对 web 表单进行暴力破解的是?（ ）
A、 Burp suite

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：https://d.book118.com/228106126070006057