中国海洋大学 2020 年硕士研究生招生考试试题

科目代码： 940 **科目名称：** 计算机网络与安全

一、选择题（共 20 题，每题 2 分，共 40 分）

1. 在 OSI 参考模型中，自下而上第一个提供端到端服务的层次是（ ）。

   A. 物理层　　B. 数据链路层　　C. 传输层　　D. 会话层

2. 以下不属于电路交换技术优点的是（ ）。

   A. 通信时延小　　B. 有序传输数据

   C. 既适用于模拟信号、又适用于数字信号　　D. 建立连接时间短

3. 下列说法中错误的是（ ）。

   A. CSMA/CD 是一种适用于总线型结构的分布式媒体访问控制方法

   B. CSMA/CD 网络中的每个站点都可以独立决定是否发送消息

   C. CSMA/CD 在重负载情况下性能明显下降

   D. CSMA/CD 适用于无线网络，以实现无线链路共享

4. 下列关于数据链路层差错控制的叙述中，错误的是（ ）。

   A. 数据链路层只能提供差错检测，不提供差错纠正

   B. CRC 校验码可以检测出所有的单比特错误

   C. 奇偶校验码只能检测出奇数个比特错误

   D. 带 r 个校验位的多项式编码可以检测到所有长度小于或等于 r 的突发性错误

5. 高层互连是指传输层及其以上各层协议不同的网络之间的互连。实现高层互连的设备是（ ）。

   A. 中继器　　B. 网桥　　C. 路由器　　D. 网关

6. 下列地址中，属于单播地址的是（ ）。

   A. 172.31.128.255/18　　B. 10.255.255.255

   C. 192.168.24.59/30　　D. 224.105.5.211

7. 以下叙述不正确的是（ ）。

   A. BGP 报文封装在 TCP 报文中传送

   B. BGP4 支持 CIDR 技术

特别提醒：答案必须写在答题纸上，若写在试卷或草稿纸上无效。

C. ICMP 报文放在 IP 数据报的数据字段中传送

D. RIP 规定，15 跳为一条不可达路径

8. 以下（　　）字段包含在 TCP 首部中，但不包含在 UDP 首部。

A. 目的端口号　　B. 序列号　　C. 校验和　　D. 目的 IP 地址

9. 下列关于 SMTP 协议的叙述中，错误的是（　　）。

A. 支持从邮件服务器向用户代理发送邮件

B. 支持在邮件服务器之间发送邮件

C. 支持从用户代理向邮件服务器发送邮件

D. 只支持传输 7 bit ASCII 码内容

10. 以下说法错误的是（　　）。

A. UDP 不需要计算 RTT

B. TCP 是面向字节的

C. UDP 只是在 IP 数据报服务基础上增加了端口功能

D. 如果 TCP 采用“两次握手”可能发生死锁

11. 采用 base64 编码对 45 字节数据进行编码，编码后数据的大小为（　　）字节。

A. 45　　B. 60　　C. 75　　D. 90

12. 网页接收到无法处理的输入而崩溃并显示“404”错误，被损害的是（　　）。

A. 机密性　　B. 完整性　　C. 可用性　　D. 非否认性

13. RSA、ECC 等非对称加密算法会生成一个私钥和一个公钥，公钥公开而私钥保密，以下关于二者之间关系描述，正确的是（　　）。

A. 利用公钥，可在有限步骤内计算出私钥　　B. 公钥和私钥都常被用来加密消息

C. 公钥通常既用来加密，也用来签名　　D. 私钥用来加密，公钥用来签名

14. 按惯例，Linux 系统中用户账户和组的相关信息保存在/etc/（　　）和/etc/group 文件。

A. passwd　　B. account　　C. accounts　　D. user

15. 沙箱机制主要遵循了以下哪类安全原则（　　）。

A. 绝对中介　　B. 隔离原则　　C. 封装原则　　D. 开放式设计原则

16. canary 是一种防范栈溢出的机制，通过在栈中的局部变量和返回地址之间插入一个标记，当该标记被覆盖时，程序就会停止执行。该机制最有效的实施的方式为（　　）。

特别提醒：答案必须写在答题纸上，若写在试卷或草稿纸上无效。

A. CPU 增加一个寄存器，保存 canary

B. 编译时在程序中插入 canary 相关的指令

C. 程序运行前，操作系统在栈中插入 canary

D. 由程序员在 C 或 C++代码中实现

17. X.509 证书是基于（　　）的证书。

A. AES　　B. 流密码　　C. 对称密码　　D. 公钥密码

18. HTTPS 是在（　　）协议的安全保护下的 HTTP 协议。

A. SSL 或 TLS　　B. SSL 或 IPSec　　C. TLS 或 IPSec　　D. IPSec

19. 以下哪一条是数据库加密的缺点？（　　）

A. 缺乏灵活性　　B. 缺乏完整性

C. 缺乏机密性　　D. 不能使用对称加密技术

20. 就目前的进展来看，MD5、SHA-1 等散列函数算法是（　　）的。

A. 单向可逆　　B. 单向不可逆　　C. 双向可逆　　D. 双向不可逆

二、填空题（共 30 空，每空 1 分，共 30 分）

1. 在计算机网络中，（　　）子网负责信息处理，（　　）子网负责网络中的信息传递。
2. 某系统的信道带宽为 3000Hz，信噪比为 20dB，则该系统的最大数据传输率为（　　）。
3. 物理层接口特性中，用于描述完成每种功能的事件发生顺序的是（　　）。
4. 数据链路层中，位错指帧中某些位出现了差错，通常采用（　　）方式发现位错，通过（　　）方式来重传出错的帧。
5. 设 TCP 的门限窗口的初始值为 6（报文段）。当拥塞窗口上升到 8 时，网络发生了超时，TCP 使用慢开始和拥塞避免，则第 10 次和第 15 次传输的各拥塞窗口的大小分别是（　　）、（　　）。
6. RIP 路由协议是典型的基于（　　）的路由选择协议，而（　　）是使用分布式的链路状态协议。
7. 两个计算机进程要互相通信，不仅必须知道对方的 IP 地址，而且还需要知道对方的（　　）。
8. 在组播中，主机使用一个称为（　　）的协议加入组播组。
9. PPP 的帧格式中标志字段分别在首部和尾部各占 1 个字节，规定为（　　）。
10. 对于一个无序接收的滑动窗口协议，若序号位数为 n，则发送窗口的最大尺寸为（　　）。

特别提醒：答案必须写在答题纸上，若写在试卷或草稿纸上无效。

11. HDLC 协议使用（　　）方法来保证数据的透明传输。

12. 在子网 192.168.4.0/30 中，能接收目的地址为 192.168.4.3 的 IP 分组的最大主机数是（　　）。

13. 两个子网 202.118.133.0/24 和 202.118.130.0/24 进行路由聚合，得到的网络地址是（　　）。

14. 数据链路层的可靠传输机制包括（　　）、后退 N 帧协议和选择重传协议。

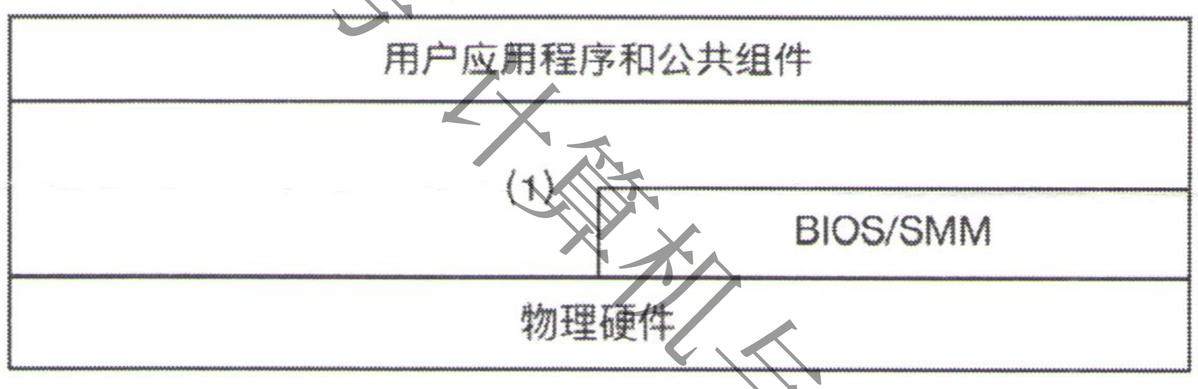
15. （　　）技术是一种分布式账本技术。2019 年 10 月，习总书记在政治局集体学习时强调，这项技术的集成应用在新的技术革新和产业变革中起着重要作用，我们要把它作为核心技术自主创新的重要突破口，明确主攻方向，加大投入力度，着力攻克一批关键核心技术，加快推动技术和产业创新发展。

16. 计算机安全是指保证信息系统资产的机密性、完整性和可用性的措施和控制方法。其中完整性包括数据完整性和（　　）完整性。

17. 解密算法本质上是（　　）算法的逆运算，输入密文和秘密密钥可以恢复明文。

18. 设置在网关位置，对进入网络的数据包进行检查和过滤的网络安全设备叫做（　　）。

19. 如下图所示，系统安全分为若干层，最底层是物理硬件，最顶层是用户应用程序和实用组件。（1）处是（　　），包含拥有特权的内核代码、API 和服务。



20. 以下代码中可能存在（　　）攻击漏洞。

```
<?php
    $userName=$_GET['userName'];
    echo "<b>".$userName."</b>";
?>
```

21. SSL 记录协议为 SSL 连接提供了两种服务（　　）性和消息完整性。

22. IPSec 安全关联是 IPSec 协议中数据包发送方和接收方之间的（　　）向关系，为二者之间的通信提供安全服务。

23. 入侵防御系统（IPS）是对 IDS 的扩展，按所处位置分为基于主机的 IPS 和基于（　　）的 IPS。

特别提醒：答案必须写在答题纸上，若写在试卷或草稿纸上无效。

24. 系统的攻击面包括（　　）攻击面、软件攻击面和人为攻击面。

25. 常用的身份认证方式包括 Know Sth、Have Sth 和 Be Sth，指纹属于其中的（　　）方式。

26. 某公司在互联网上开放了一个网络服务，查询者通过 UDP 包发送整数值 i 给该服务，该服务就会使用 UDP 包返回比特币第 i 个区块的内容给该查询者。该服务最易受到（　　）攻击。

三、问答与计算题（共 11 题，共 80 分）

1. （6 分）简述 ARP 协议的工作过程。

2. （6 分）长度为 1km、数据传输率为 10Mbps 的 CSMA/CD 以太网，信号在电缆中的传播速度为 200000km/s，试求能够使该网络正常运行的最小帧长。

3. （8 分）某单位分配到一个 B 类 IP 地址，其 net-id 为 129.250.0.0。该单位有 4000 台机器，平均分布在 16 个不同的地点。如选用子网掩码为 255.255.255.0，试给每一地点分配一个子网号码，并计算出每个地点主机号码的最小值和最大值。

4. （8 分）一个数据报长度为 5000 字节（固定首部长度）。现在经过一个网络传送，此网络能够传送的最大数据长度为 1500 字节，试问应当划分为几个短些的数据报片？各数据报片的数据字段长度、片偏移字段和 MF 标志应为何数值？

5. （10 分）一个 UDP 用户数据报的首部的十六进制表示为 07 21 00 45 00 2C E8 27。1）试求源端口、目的端口、用户数据报总长度、数据部分长度。2）这个用户数据报是从客户端发送给服务器的还是服务器发送给客户端的？使用 UDP 的这个服务器程序是什么？

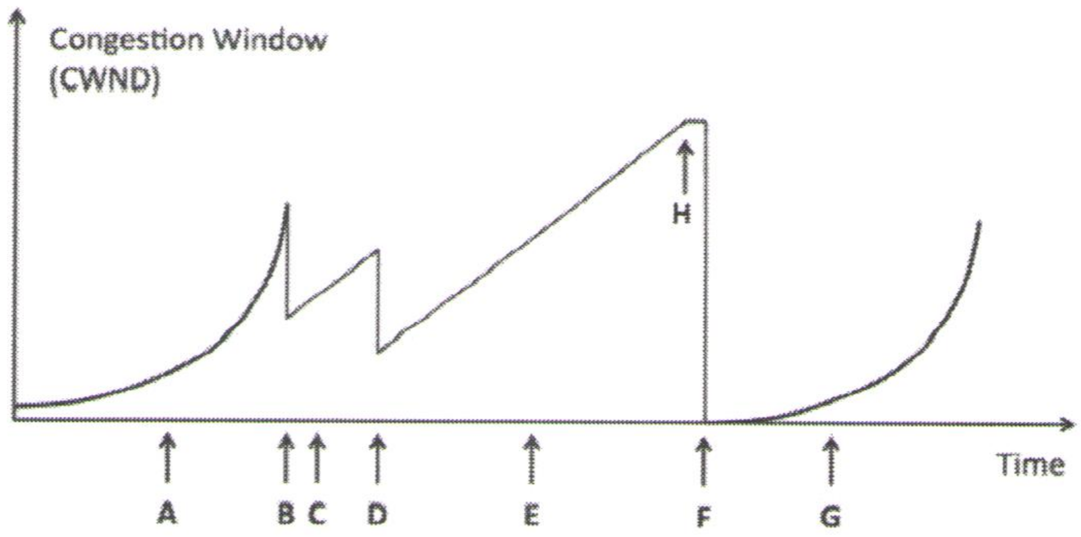
6. （10 分）针对下图中的 TCP 发送端的拥塞窗口的随时间的变化情况，回答以下问题：

（1）说明 TCP 拥塞控制中的“慢开始”、“拥塞避免”、“乘法减小”、“快重传”和“快恢复”等五项措施的含义，并结合图中的具体情况说明每项措施发生的所有时间段或时间点。

（2）说明在 B、D、F、H 等 4 个时刻，发送端所检测的事件。

（3）很多网络专家说“许多 Internet 上的 TCP 传输从来没有进入拥塞避免阶段”。请判断该论点的真伪，并说明理由。（注：据统计，WWW 上超过 90%的 Web 对象都小于 10Kbytes）。

特别提醒：答案必须写在答题纸上，若写在试卷或草稿纸上无效。



7. （10 分）考虑如下访问文件的代码：

```
const int PASSED=0;
const int DENIED=1;
char FileName[128];
int i=0;
gets(FileName); //c 标准库函数，获取用户输入的用户名
i=GetPrivilege(user,FileName); //判断该用户是否可以访问该文件
if(i==DENIED)
{
    给出提示并退出程序;
}
else
{
    执行文件访问;
}
```

（1）程序有一处系统设计上的安全缺陷，它违反了什么原则？如何违反的？如何改写来避免这个安全缺陷？

（2）程序有一处实现上的安全缺陷，它是什么漏洞？为什么会产生这个漏洞？如何改写来避免这个安全缺陷？

8. （6 分）以下为存在漏洞的 PHP 代码，请说明该代码存在哪种漏洞？这种漏洞有什么危害？举例说明如何利用这种漏洞？如何防范？

```
$name = $_REQUEST['name'];
```


特别提醒：答案必须写在答题纸上，若写在试卷或草稿纸上无效。

```
$query = "SELECT * FROM suppliers WHERE name = ' " . $name . " ' ; ";
$result = mysql_query($query);
```

9. （6 分）小明是 A 报社的一名驻外记者，为防止窃听者假冒他，创建了一种身份认证方式。出国前，他会跟同事约定一个密钥 K；出国后，每次需要跟同事联络时，他们都使用以下方式验证小明身份：同事生成一个与 K 长度相同的随机字符串 A 发给小明，小明将 A 与 K 异或得到 B 后发回，同事将 B 再次与 K 异或，如果结果是 A，就认为认证成功。

（1）请问以上认证方式有什么缺陷？

（2）小明还使用这个密钥 K 往总部发送新闻稿，他将 K 不断重复，直到形成与新闻稿一样长度的字符串，然后与新闻稿异或后发回。总部用同样的方法解密，这样在第二天新闻见报之前就不会被窃听者破解。小明每个月用这种方式发送至少 10 条新闻，请问这种加密方式有什么缺陷？

（3）你能给小明的认证和加密提供什么建议？

10. （5 分）在操作系统安全方面，通常要求管理员：1）移除不必要的服务、应用和协议；2）设置操作系统口令的强制更换（如 45 天必须更换）；3）尽可能不使用管理员或 root 身份来运行服务器程序。说明三种做法分别有什么意义。

11. （5 分）什么是高级持续性威胁（APT）？只依赖防火墙或杀毒软件能有效防范 APT 威胁吗？为什么？

特别提醒：答案必须写在答题纸上，若写在试卷或草稿纸上无效。