成都信息工程大学考试试卷

2023 —— 2024学年第1学期

课程名称： 区块链安全基础 使用班级： 区块链22 试卷形式：开卷 闭卷√．

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 试题 | 一 | 二 | 三 | 四 | 五 | 六 | 七 | 八 | 九 | 十 | 总分 |
| 得分 |  |  |  |  |  |  |  |  |  |  |  |

一**选择题（每小题1分，共计20分）**

1. 定期对系统和数据进行备份，在发生灾难时进行恢复。该机制是为了满足信息安全的（ ）属性。

A 真实性 B 完整性 C 不可否认性 D 可用性

2. 数据在存储过程中发生了非法访问行为，这破坏了信息安全的（ ）属性。

A 保密性 B 完整性 C 不可否认性 D 可用性

1. 网上银行系统的一次转账操作过程中发生了转账金额被非法篡改的行为，这破坏了信息安全的（ ）属性。

A 保密性 B 完整性 C 不可否认性 D 可用性

1. 对网络层数据包进行过滤和控制的信息安全技术机制是（ ）。

A 防火墙 B IDS C Sniffer D IPSec

5．对口令进行安全性管理和使用，最终是为了（ ）。

A 口令不被攻击者非法获得 B 防止攻击者非法获得访问和操作权限

C 保证用户帐户的安全性 D 规范用户操作行为

6. 公钥密码基础设施PKI解决了信息系统中的（ ）问题。

A 身份信任 B 权限管理 C 安全审计 D 加密

7．链路加密技术是在OSI协议层次的第二层，数据链路层对数据进行加密保护，其处理的对象是（ ）。

A 比特流 B IP数据包 C 数据帧 D 应用数据

8. IPSec协议中涉及到密钥管理的重要协议是（ ）。

A IKE B AH C ESP D SSL

9. 入侵检测技术可以分为误用检测和（ ）两大类。

A 病毒检测 B 详细检测 C 异常检测 D 漏洞检测

10. PKI中进行数字证书管理的核心组成模块是（ ）。

A 注册中心RA B 证书中心CA C 目录服务器 D 证书作废列表

11. 对称密码体系的优点是。（ ）

1. 计算快 B、密钥管理容易

C、可以进行数字认证 D、适合多人通信

12. DES算法的过程为（ ）。

A、初始置换、迭代过程，逆置换 B、初始置换、逆置换、迭代过程

C、迭代过程、初始置换、逆置换 D、迭代过程、逆置换、初始置换

13. DES用多少位密钥加密64位明文。（ ）

A、16 B、56 C、64 D、32

14. 公钥密码体制的优点不包括（ ）。

1. 密钥少便于管理 B、计算快

C、密钥分配简单 D、可以实现数字签名

15. 一个好的密钥管理系统不需要满足（ ）。

A、密钥难以被窃取。

B、在一定条件下密钥被窃取也没有用，密钥有使用范围和时间限制。

C、密钥的分配和更换过程对用户透明，用户不一定要亲自管理密钥｡

D、最好使用对称密钥管理系统。

16.关于PKI和PMI的说法正确的是（ ）

A、PKI解决权限问题 B、PKI既能解决权限问题又能解决身份问题

C、PMI解决身份问题 D、PMI解决权限问题

17.Kerberos系统的四个基本实体不包括（ ）

A、Kerberos客户机 B、认证服务器

C、服务许可票据 D、票据许可服务器

18.关于栈溢出特点以下正确的是（ ）

A、覆盖函数的返回地址 B、拷贝的数据过长

C、缓冲区在堆中分配 D、覆盖了堆管理结构

19.下列关于误用和异常的说法正确的是（ ）

A、误用是根据已知特征和未知统计进行入侵匹配

B、误用仅根据已知特性进行匹配

C、异常是根据已知特征和未知统计进行入侵匹配

D、异常仅根据已知特性进行匹配

20.关于入侵检测的分类错误的是（ ）

A、基于主机的入侵检测 B、集中式的入侵检测

C、分布式的入侵检测 D、集中发式的入侵检测

**二 填空题（每空1分，共计20分）**

1. 网络安全的主要特征为 、 、 、 。
2. 密钥可以分为一般 和密钥加密密钥。
3. 密钥管理的目的是确保密钥的 。
4. PKI是指用 的技术来实施和提供安全服务的具有 的安全基础设施。
5. 防火墙是设置在 和 之间的一道屏障。
6. PKI系统安全的核心是 。
7. 对称密码技术的密钥分配分为哪两种方案 和 。
8. 防火墙系统的体系结构分为双宿主体系结构、 、屏蔽子网体系结构
9. 实现证书撤销的方法有证书撤销列表和 。
10. 扫描技术一般包括 和端口扫描。
11. 恶意代码的分析方法有多种，按照分析时的目标程序是否在内存中拥有私有空间，可以分为静态分析法和
12. IP欺骗就是一其他主机的IP作为 向目标主机发送数据包。
13. Kerberos中有两种票据 和 。

**三 问答题（25分，每道小题分数在题后标注）**

**1.** 什么是计算安全？什么是无条件安全？（4分）

2.古典密码学和现代密码学的区别？公钥密码理论与技术解决了什么重大问题？（4分）

3. 简述公钥密码的分发方式？（4分）

4. 防火墙的体系结构有哪些？（5分）

5. 入侵检测的检测模式有哪些？各有什么优缺点？（4分）

6. 为什么要采用PKI技术？PKI和PMI的区别和关系？（4分）

**四 设计与分析题（20分，每道小题分数在题后标注）**

1、根据所学知识设计一种在不安全信道、安全地分发会话密钥。（5分）

1. 发送方如何保证在网络上所传信息秘密地、不被篡改地发送到接收方？（5分）

3、在局域网中，如何通过ARP欺骗，获得其他主机的数据包？（5分）

4、攻击的准备工作有哪些？这些准备工作的目的是什么？（5分）

**五 综合题（15分）**

1. 针对一个未知WIFI，如何更改WIFI的配置，如禁止某些用户上网，请列出详细步骤。（5分）

2、设计一个发现周围网络用户进行数字货币交易的具体人，写出详细步骤。（15分）