成都信息工程大学考试试卷

2023 —— 204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级 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.网络信息安全的主要特征不包括（ ）。

1. 保密性 B.完整性 C.可用性 D.真实性

2.在DES加密方法中，每一组数据加密分组的长度是（ ）。

A.64位 B.56位 C.48位 D.32位

1. 数字证书是用（ ）签名的。

A.CA的公钥 B.CA的私钥 C.用户的私钥 D.用户的公钥

1. 用于实现身份鉴别的安全机制是（ ）。

A.加密机制和数字签名机制  B.加密机制和访问控制机制

C.数字签名机制和路由控制机制     D.访问控制机制和路由控制机制

5.假若A想和B进行通讯，且A已经拿到B的公钥，要确定B公钥不是伪造的可采用什么技术验证？（ ）

1. 数字签名技术 B.数字摘要技术 C.数字证书技术 D.对称密钥加密技术

6.（ ）最好地描述了数字证书。

A.等同于在网络上证明个人身份的身份证

B.浏览器的一标准特性，它使得黑客不能得知用户的身份

C.网站要求用户使用用户名和密码登陆的安全机制

D.伴随在线交易证明购买的收据

1. 数字证书的生命周期不包括哪个阶段？（ ）

A.初始化注册阶段 B.颁发投入工作阶段 C.撤消阶段 D.失效阶段

1. IPSec协议工作在（ ）层次。

A.数据链路层       B.网络层          C.应用层         D.传输层

1. IP扫描主要是用来判断主机的什么情况的？（ ）

A主机是否存活 B.主机开了哪些服务

1. 主机有哪些漏洞 D.主机的IP地址

10. 将获得的信息再次发送以在非授权情况下进行传输，这属于( ).

A 窃听 B篡改 C 伪装 D 重放

11. 在下列密码体制中，加密密钥k1 解密密钥k2 是相同的。（ ）

A、传统密码体制 B、非对称密码体制 C、对称密码体制 D、公开密码体制

1. 防止发送方否认的方法是（ ）

Ａ、消息认证 Ｂ、保密 Ｃ、日志 D、数字签名

13.以下不是包过滤防火墙主要过滤的信息？ （ ）

A. 源IP地址 B. 目的IP地址 C. TCP源端口和目的端口 D. 时间

14.关于密码系统中密钥层次的相关说法，正确的是（ ）。

1. 主密钥位于密码系统中整个密钥层次的最高层，可以保护密钥加密密钥，但不能直接加密会话秘钥。
2. 会话秘钥又称基本密钥，即两个通信终端用户在一次通话或交换数据时使用的密钥。

C.保密存储方法包括基于密钥的软保护和基于硬件的物理保护。

D.用于数据加密的密钥称为二级密钥。

15.密钥的管理是整个加密系统中最薄弱的环节，以下的说法正确的是（ ）。

1. 好的密钥具有：易记难猜、真正的随机性、使用特定算法、采用散列函数、双密钥系统的密钥必须满足一定的关系等特点。
2. 所有的密钥都有生存期，密钥的生存周期是指授权使用该密钥的周期。
3. 密钥加密密钥数量大（N(N-1)/2），因此只能由伪随机数发生器产生。
4. 在实际中，最不安全的密钥保护方法是将密钥存放在物理上安全的地方。

16.关于VPN的描述，不正确的是（ ）。

1. 成本高
2. 易于安装和使用
3. 网络结构灵活
4. VPN是一种连接。

17.下列防止ARP欺骗的方法，正确的是：（ ）

1. 网关建立静态IP/MAC对应关系，各主机建立MAC数据库。
2. 建立DHCP服务器。
3. IDS监听网络安全
4. 以上三者都正确。

18.扫描技术的主要目的不包括：（ ）

1. 查看目标网络中哪些主机是存活的；
2. 查看哪些对资源的访问没有被授权。
3. 查看存活的主机运行了哪些服务；
4. 查看主机提供的服务有漏洞。
5. 哪些证书的序列号不应该出现在CRL上（ ）
6. 有效期内的正常证书
7. 相应私钥泄露的、有效期内的CA证书
8. 尚未生效的证书
9. 过期的证书

20.下列有关防火墙的说法，错误的是（ ）

1. 防火墙有能力控制对主机系统的访问。
2. 防火墙是设置在保护网络和外部网络之间的一道屏障，用于阻断来自外部的对本网络的威胁和入侵。
3. 代理服务器可以在无任何应用的前提下将内外网隔断。
4. 防火墙不能防范利用服务器系统漏洞进行攻击。

**二 填空题（每空1分，共计20分）**

1.密钥的分配是指产生并使使用者获得 的过程。

2.防火墙是位于两个网络之间，一端是 ，另一端是 。

3.网络安全的主要特征有： **，** **，** **，** **。**

4.在一个保密通信系统中，通信双方任意一方都有可能进行欺骗，用 技术可以有效解决这个问题。

5**.** 是电子商务中各实体的网上身份证明，它证明实体所声明的身份与其公钥的匹配关系，使得实体身份与证书上的公钥相绑定。

6.网络攻击的第一步是 **。**

7.对称密码技术的分配方案分为 和 。

8.Kerberos系统涉及的四个基本实体是 、 、 、 。

9.数字证书的认证过程：1. 2.

3. 4. 。

**三、判断题（每小题1分，共10分）**

1、网络交易的信息风险主要来自冒名偷窃、篡改数据、信息丢失等方面的风险。（ ）

2、基于公开密钥体制（PKI）的数字证书是电子商务安全体系的核心。（ ）

3、入侵检测的信息分析方法中模式匹配法的优点是能检测到从未出现过的黑客攻击手段。（ ）

4、TCP FIN属于典型的端口扫描类型。（ ）

5、复合型防火墙是内部网与外部网的隔离点，起着监视和隔绝应用层通信流的作用，同时也常结合过滤器的功能。（ ）

6、漏洞只可能存在于操作系统中，数据库等其他软件系统不会存在漏洞。（ ）

7、x-scan 能够进行端口扫描。（ ）

8、网络钓鱼的目标往往是细心选择的一些电子邮件地址。（ ）

9、防火墙规则集的内容决定了防火墙的真正功能。（ ）

10、Windows 系统中，系统中的用户帐号可以由任意系统用户建立。用户帐号中包含着用户的名称与密码、用户所属的组、用户的权利和用户的权限等相关数据。（ ）

**四 问答题（25分，每道小题分数在题后标注）**

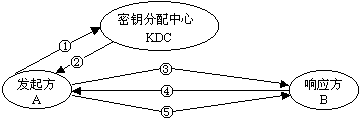
1.请简述一下在PKI技术支持下，一个获取其他用户公钥的大概过程。（5分）

1. 什么是PKI？（2分）简述PKI的原理。（3分）
2. 简述SSL的工作原理。（5分）
3. Kerberos用的是什么密码技术？（1分）简述其基本原理。（4分）

5、什么是密码体制？（2分）描述密码的体系结构，（2分）密钥管理的目的是什么？。（1分）

**五 设计与分析题（15分，每道小题分数在题后标注）**

1、下图就是具有密钥分配中心的密钥分配方案。图中假定A和B分别与KDC有一个共享的密钥Ka和Kb，A希望与B建立一个逻辑连接，并且需要一次性会话密钥来保护经过这个连接传输的数据。



1. 用形式化语言描述具体过程（3分）
2. 第一步为什么用随机数？一般采用什么随机数？为什么？（3分）
3. 一间网络实验室拥有20多台三层交换机，40台二层交换机，当每天开始实验时会出现什么状况？如何防范？（4分）

3、请说明自私挖矿的目的和具体步骤（5分）

**六 综合题（10分）**

找到一个WIFI的SSID，然后更改WIFI的配置，禁止某些用户上网，请列出详细步骤。

成都信息工程大学考试草稿纸

2016 —— 2017学年第 1 学期

课程名称： 信息安全理论与技术 使用班级： 物联网14级1、2班 试卷形式：开卷 闭卷√