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. 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。
5. 下列防止ARP欺骗的方法，正确的是：（ ）
6. 网关建立静态IP/MAC对应关系，各主机建立MAC数据库。
7. 建立DHCP服务器。C. IDS监听网络安全 D.以上三者都正确。
8. 扫描技术的主要目的不包括：（ ）
9. 查看目标网络中哪些主机是存活的；
10. 查看哪些对资源的访问没有被授权。
11. 查看存活的主机运行了哪些服务；
12. 查看主机提供的服务有漏洞。
13. 哪些证书的序列号应该出现在CRL上（ ）
14. 有效期内的正常证书
15. 相应私钥泄露的、有效期内的CA证书
16. 尚未生效的证书
17. 过期的证书
18. 包过滤型防火墙工作在 （ ）
19. 会话层 B.应用层 C.网络层 D.数据链路层
20. 关于消息摘要的说法错误的是（ ）
21. 输入的信息越长，计算出的消息摘要越长
22. 输入的信息不同，产生的消息摘要也不同，相同的输入必会产生相同的输出
23. 消息摘要只能进行正向的消息摘要，无法从摘要恢复任何的消息。
24. 好的摘要算法，无法找到两条信息，它们的摘要相同
25. 数字证书生命周期的三个阶段不包括（ ）

A.证书初始化注册 B.颁发使用 C.证书撤销 D.证书恢复

8. 下面那个选项不是扫描的目的（ ）

A.查看目标网络那些主机存活 B.查看存活的主机运行那些服务

C.进行Ping攻击 D.查看主机提供的服务有无漏洞

9. ARP欺骗的主要环境是（ ）

1. 局域网 B.个域网 C.城域网 D.广域网
2. 下面哪个选项不属于恶意代码的传播机制（ ）

A.互联网 B.局域网 C.计算机 D.移动硬盘

11. 以下不属于网络安全的四层含义的是（ ）

A.网络上信息传播的安全 B.运行系统安全

C.网络上系统信息的安全 D.网络线路的安全

12. 以下不属于现代加密技术的是（ ）

1. 凯撒算法加密 B、对称加密 C、非对称加密 D、消息摘要技术
2. 不是Hash函数应满足的条件的是（ ）
3. 输入长度任意 B、计算哈希值容易

C、输出长度任意 D、哈希值唯一

1. 以下不属于认证方法的分类的是（ ）
2. 单向认证 B、自我认证 C、双向认证 D、第三方认证
3. 以下不属于Kerberos的设计目的的是（ ）

A、对用户保密 B、安全性 C、可靠性 D、可伸缩

16. 以下不属于PKI提供的安全服务的是（ ）

A、不可否认性 B、认证 C、完整性 D、可控性

17. 数字证书的认证过程不包括（ ）

A、撤销列表查询 B、序列号验证 C、证书加密 D、有效期验证

18. 以下不属于扫描的主要目的的是（ ）

A、查看主机总数 B、哪些主机存活

C、存活主机运行的服务 D、服务的漏洞

19. 以下不属于漏洞技术的防范的是（ ）

A、安装ARP防火墙 B、及时打补丁 C、对敏感数据加密 D、关闭本机监控

20. 不能防范缓冲区溢出的是（ ）

A、编写严格的代码 B、执行堆栈数据段

C、利用程序编译器的边界检查 D、指针完整性检查

**二 填空题（每空1分，共计20分）**

1. 网络安全的实现不仅仅取决于某项技术，更依赖于 。

2. ISO安全体系结构包括了三部分内容：安全服务、 和安全管理。

3. 不同的密码算法具有不同的安全等级，包括 、 。

4. 是在不知道密钥的情况下恢复出明文或密钥，也可以通过发现密码体制的弱点，最终得到明文或密钥。

5. 在公钥密码体制中， 是可以公开的信息，而 是需要保密的。

6. 是指攻击者想办法让目标机器停止提供服务或资源访问。

7. PKI的主要目的是为了解决 问题，PMI的主要目的是为了解决 问题。

8. 交叉认证被分为 和 两种。

9. 缓冲区溢出分为 溢出、 溢出和其他溢出类型三种。

10. 常见的扫描技术有 ， ， 。

11. 防止重放攻击最常用的方法是 。

12. 数字签名应满足的要求有： ， ， 签名是不可复制的，签名的消息是不可改变的， 签名是不可抵赖的。

**三、判断题（每小题1分，共10分）**

1.VPN的主要特点是通过加密使信息能安全的通过Internet传递。

2.对于一个计算机网络来说,依靠防火墙即可以达到对网络内部和外部的安全防护

3.在堡垒主机上建立内部DNS服务器以供外界访问，可以增强DNS服务器的安全性。

4.统计表明，网络安全威胁主要来自内部网络，而不是Internet

5.蠕虫、特洛伊木马和病毒其实是一回事

6.目前入侵检测系统可以及时的阻止黑客的攻击。

7.带VPN的防火墙一旦设置了VPN 功能，则所有通过防火墙的数据包都将通过VPN通道进行通讯。

8. 计算机信息系统的安全威胁同时来自内、外两个方面。

9.对称密钥没有非对称密钥安全性高。

10.SSL必须要求应用服务器提供数字证书。

**四 问答题（20分，每道小题分数在题后标注）**

1、访问控制策略有哪几种？（2分）说明其优缺点。（2分）

2、说明VPN具体几种连接方式？（4分）

3、恶意代码有哪几种传播机制？（4分）

1. 在局域网中，如何通过ARP欺骗，获得其他主机的数据包？（4分）

5、入侵检测的检测模式有哪些？（2分）各有什么优缺点？（2分）

**五 设计与分析题（20分，每道小题分数在题后标注）**

1. 网页挂马是目前最常见的攻击，如何防止网页挂马？（5分）
2. 攻击的准备工作有哪些？（3分）这些准备工作的目的是什么？（2分）
3. 为了防止发送的文件被泄露和篡改，如何对文件处理？请从收发双方协商密钥开始处理。（5分）

4、说明区块链安全中为何要保护交易隐私？如何保护说明防御措施。（5分）

**六 综合题（10分）**

在一个无线上网的实验室中，如何获得上163邮箱用户的用户名和密码，设计一个实验环境，说明配置方法。

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√