计算机信息安全技术课程期末考试试卷​

一、单项选择题（每题 1 分，共 20 分）​

1. 以下关于信息安全的定义，准确的是（ ）​

A. 信息不被泄露​

B. 信息系统稳定运行​

C. 保护信息的保密性、完整性和可用性，以及信息系统的安全​

D. 防止信息被篡改​

1. 以下哪种算法属于哈希函数（ ）​

A. DES​

B. SHA - 256​

C. Diffie - Hellman​

D. ElGamal​

1. 以下关于防火墙的描述，错误的是（ ）​

A. 可以部署在内部网络和外部网络之间​

B. 能完全防止病毒入侵​

C. 可基于 IP 地址、端口号进行包过滤​

D. 有状态检测防火墙、应用代理防火墙等类型​

1. 在数字证书体系中，负责验证用户身份并颁发数字证书的是（ ）​

A. 证书注册机构（RA）​

B. 证书颁发机构（CA）​

C. 证书信任机构（TA）​

D. 证书存储机构（SA）​

1. 以下哪种攻击是通过向目标系统发送大量虚假请求，耗尽系统资源，导致其无法正常服务（ ）​

A. 口令攻击​

B. 中间人攻击​

C. 分布式拒绝服务（DDoS）攻击​

D. 缓冲区溢出攻击​

1. 数据库安全中，通过设置用户只能访问特定视图中的数据，实现的安全措施是（ ）​

A. 数据加密​

B. 访问控制​

C. 视图机制​

D. 审计追踪​

1. 生物特征认证中，具有方便快捷、非接触式优点，但受环境光线等因素影响较大的是（ ）​

A. 指纹识别​

B. 掌纹识别​

C. 人脸识别​

D. 静脉识别​

1. 以下关于安全协议 SSL/TLS 的说法，正确的是（ ）​

A. SSL 是 TLS 的升级版本​

B. 主要用于保障电子邮件的安全传输​

C. 能在客户端和服务器之间建立安全的加密通道​

D. 不支持身份认证功能​

1. 以下哪种不属于恶意软件（ ）​

A. 病毒​

B. 间谍软件​

C. 操作系统补丁​

D. 勒索软件​

1. 信息安全风险评估流程中，在识别出风险后，下一步是（ ）​

A. 风险处理​

B. 风险监控​

C. 风险分析​

D. 风险规避​

1. 以下关于对称加密和非对称加密结合使用的描述，正确的是（ ）​

A. 先用对称加密算法加密数据，再用非对称加密算法加密对称密钥​

B. 先用非对称加密算法加密数据，再用对称加密算法加密非对称密钥​

C. 对称加密和非对称加密不能结合使用​

D. 结合使用会降低加密效率​

1. 入侵检测系统按照数据源分类，不包括（ ）​

A. 基于主机的入侵检测系统​

B. 基于网络的入侵检测系统​

C. 基于应用的入侵检测系统​

D. 基于特征的入侵检测系统​

1. 以下哪种技术用于将内部私有 IP 地址转换为外部公有 IP 地址（ ）​

A. DNS​

B. DHCP​

C. NAT​

D. ARP​

1. 为了防止重放攻击，在认证过程中通常会使用（ ）​

A. 随机数​

B. 数字证书​

C. 哈希值​

D. 对称密钥​

1. 以下关于操作系统安全的描述，错误的是（ ）​

A. 及时更新系统补丁可修复安全漏洞​

B. 设置用户权限能限制非法访问​

C. 关闭不必要的服务不会提高系统安全性​

D. 审计功能可记录用户操作行为​

1. 以下哪种安全技术可用于检测和阻止针对 Web 应用的攻击，如 SQL 注入、跨站脚本攻击（ ）​

A. 防火墙​

B. Web 应用防火墙（WAF）​

C. 入侵检测系统（IDS）​

D. 防病毒软件​

1. 数字签名的核心作用不包括（ ）​

A. 验证消息来源​

B. 保证消息完整性​

C. 实现消息加密​

D. 防止消息抵赖​

1. 以下关于虚拟专用网络（VPN）的说法，正确的是（ ）​

A. 只能在局域网内使用​

B. 不具备数据加密功能​

C. 通过公用网络构建安全的专用网络通道​

D. 无法隐藏用户真实 IP 地址​

1. 信息安全管理中，风险应对策略不包括（ ）​

A. 风险降低​

B. 风险转移​

C. 风险忽视​

D. 风险接受​

1. 以下哪种认证方式属于 “所有” 因素认证（ ）​

A. 指纹认证​

B. 短信验证码认证​

C. 智能卡认证​

D. 口令认证​

二、填空题（每空 1 分，共 15 分）​

1. 信息安全的三个基本目标**保密性**、**完整性**和可用性。​
2. RSA 加密算法的安全性基于**大数分解的困难性**。​
3. 防火墙的访问控制策略通常包括**允许策略**和拒绝策略。​
4. 常见的网络攻击类型包括主动攻击和**被动攻击**。​
5. 数字证书中包含用户的公钥、身份信息以及**证书颁发机构的数字签名**。​
6. 数据库安全防护措施包括访问控制、数据加密、**视图机制**和审计等。​
7. 入侵检测系统的两种主要检测技术是异常检测和**误用检测**。​
8. 安全协议 SSH 主要用于实现**安全的远程登录和文件传输**。​
9. 恶意软件的传播途径主要有网络传播、**移动存储设备传播**和文件下载传播等。​
10. 信息安全风险评估的方法主要有定性评估、**定量评估**和综合评估。​
11. 为防止数据在传输过程中被窃取，可采用**数据加密**技术。​
12. 基于角色的访问控制（RBAC）模型中，权限与**角色**相关联，用户通过扮演不同角色获得相应权限。​
13. 哈希函数的特点包括输入长度可变、输出长度固定、**单向性**和抗碰撞性。​

三、计算题（每题 10 分，共 20 分）​

1. 假设使用凯撒密码对明文 “COMPUTER” 进行加密，偏移量为 3，请写出加密后的密文，并简要说明凯撒密码的原理及安全缺陷。​

凯撒密码原理：一种简单的替换密码，将字母偏移。

缺陷：密钥空间小、缺乏混淆/扩散​​

1. 某企业有 500 名员工，采用基于角色的访问控制（RBAC）模型，将员工划分为 10 个不同角色。企业有 20 个数据库表，每个表有增、删、改、查 4 种操作权限。若每个角色被分配不同的权限组合，计算该企业在 RBAC 模型下最多需要管理的权限 - 角色映射关系数量。

角色数量×权限总数=10（角色）×80（权限）=800个映射关系

四、简答题（每题 5 分，共 25 分）​

1. 阐述防火墙在网络安全中的作用，并说明其主要的工作模式。​

作用：

安全屏障：隔离内外网，阻止非法访问，保护内网资源与数据安全。

流量管控：监控过滤流量，防御恶意攻击与数据泄露。

结构隐藏：屏蔽内网拓扑，提升安全性。

访问限制：约束内网用户访问高危外网，降低风险。

工作模式：

包过滤：基于网络/传输层（IP、端口等）分析过滤数据包。

应用代理：代理应用层请求，深度检查处理数据。

状态检测：跟踪连接状态，结合上下文提供动态防护。

1. 什么是数字签名？说明数字签名在信息安全中的作用。​

定义：发送方用私钥加密消息摘要生成签名，与原始消息一并发送。接收方用发送方公钥解密验证，确保消息真实、完整。

作用：身份认证（确认发送方身份）完整性验证（防止消息篡改）不可抵赖（发送方无法否认签名行为）

1. 简述入侵检测系统的工作原理和主要功能。​

工作原理：入侵检测系统收集网络流量、主机日志等数据并预处理后，采用异常检测（建正常模型对比）或误用检测（匹配特征库）分析，触发则按策略响应。

主要功能：****实时监测，分析记录，主动防御****

1. 分析信息安全风险评估的重要性，并说明风险评估的主要步骤。​

五、分析题（每题 10 分，共 20 分）​

1. **案例**：某学校的教务系统遭到黑客攻击，学生成绩数据被篡改。经调查发现，系统存在弱口令问题，且未对用户输入进行有效验证。请分析该事件中存在的信息安全问题，并提出相应的防范措施。

​问题：**弱口令问题、未对用户输入进行有效验证、缺乏安全意识和管理**

措施：**加强口令管理、防止 SQL 注入攻击、提高安全意识和管理水平**

* **存在的信息安全问题**：​
* **弱口令问题**：系统允许用户设置简单易猜的口令，如生日、连续数字等，攻击者可以通过暴力破解或字典攻击获取用户账号密码，从而非法访问系统。​
* **未对用户输入进行有效验证**：黑客可以利用这一漏洞进行 SQL 注入攻击，构造恶意的 SQL 语句，篡改数据库中的数据，如学生成绩数据 。​
* **缺乏安全意识和管理**：学校可能没有对教务系统的安全给予足够重视，没有制定严格的安全管理制度和规范，也没有对系统进行定期的安全检查和维护 。​
* **防范措施**：​
* **加强口令管理**：强制要求用户设置复杂的口令，如包含字母、数字、特殊字符，且长度不少于 8 位；定期更换口令；启用多因素认证，如口令结合短信验证码或动态令牌，增加认证的安全性 。​
* **防止 SQL 注入攻击**：对用户输入进行严格的验证和过滤，采用参数化查询、输入验证函数等技术，确保输入的数据符合预期格式，防止恶意 SQL 语句的注入；对数据库进行安全加固，限制数据库用户的权限，只授予必要的操作权限 。​
* **提高安全意识和管理水平**：对系统管理员和相关工作人员进行信息安全培训，提高安全意识和技能；建立完善的信息安全管理制度，定期对教务系统进行安全评估和漏洞扫描，及时发现和修复安全问题 。​

1. **案例**：一家公司的员工在使用公共 WiFi 时，其手机连接的企业邮箱账号被盗，邮件内容被窃取。请分析该事件可能的攻击方式，并说明企业和员工应采取哪些措施来防止此类事件发生。​

**攻击方式：中间人攻击、WiFi 嗅探、恶意软件攻击**

**企业措施：加强网络安全防护、提供安全的远程访问方式、加强员工培训**

**员工措施：谨慎使用公共 WiFi、启用设备安全防护、使用多因素认证**

* **可能的攻击方式**：​
* **中间人攻击**：黑客在公共 WiFi 网络中搭建恶意的接入点，伪装成合法的 WiFi 热点。当员工连接该热点时，黑客可以截获员工手机与企业邮箱服务器之间的通信数据，获取账号密码等信息；还可以篡改通信内容，进行钓鱼攻击 。​
* **WiFi 嗅探**：黑客使用专门的工具在公共 WiFi 网络中监听网络流量，捕获未加密的邮件通信数据，从中提取账号密码和邮件内容 。​
* **恶意软件攻击**：员工在连接公共 WiFi 时，可能不小心下载或安装了恶意软件，这些软件可以在后台运行，窃取手机中的敏感信息，包括企业邮箱账号密码 。​
* **企业应采取的措施**：​
* **加强网络安全防护**：对企业邮箱服务器进行安全加固，启用 SSL/TLS 加密协议，确保邮件在传输过程中的保密性和完整性；部署入侵检测系统和防火墙，实时监测和阻止网络攻击 。​
* **提供安全的远程访问方式**：为员工提供 VPN 服务，员工通过 VPN 连接企业内部网络访问邮箱，在公共 WiFi 环境下建立安全的专用网络通道，防止信息泄露 。​
* **加强员工培训**：定期对员工进行信息安全培训，提高员工在公共网络环境下的安全意识，如不随意连接陌生的 WiFi 热点，谨慎处理网络请求和下载文件等 。​
* **员工应采取的措施**：​
* **谨慎使用公共 WiFi**：尽量避免在公共 WiFi 环境下进行敏感操作，如登录企业邮箱、进行网上银行交易等；如果必须使用，优先选择有密码保护且官方认证的 WiFi 热点 。​
* **启用设备安全防护**：在手机等设备上安装可靠的安全防护软件，及时更新系统和软件补丁，开启设备的安全防护功能，如防火墙、病毒查杀等 。​
* **使用多因素认证**：为企业邮箱账号启用多因素认证，即使账号密码被窃取，攻击者没有其他认证因素也无法登录邮箱 。

参考答案​

一、单项选择题​

1. C​
2. B​
3. B​
4. B​
5. C​
6. C​
7. C​
8. C​
9. C​
10. C​
11. A​
12. D​
13. C​
14. A​
15. C​
16. B​
17. C​
18. C​
19. C​
20. C​

二、填空题​

1. 保密性、完整性​
2. 大数分解的困难性​
3. 允许策略​
4. 被动攻击​
5. 证书颁发机构的数字签名​
6. 视图机制​
7. 误用检测​
8. 安全的远程登录和文件传输​
9. 移动存储设备传播​
10. 定量评估​
11. 数据加密​
12. 角色​
13. 单向性​

三、计算题​

1. **答案**：​

* 加密后的密文：“FRPSXWHU”。​
* 凯撒密码原理：凯撒密码是一种简单的替换密码，将明文中的每个字母按照指定的偏移量在字母表中进行移动，从而得到密文。例如，偏移量为 3 时，A 替换为 D，B 替换为 E，以此类推。​
* 安全缺陷：凯撒密码的密钥空间非常小，只有 26 种可能的偏移量（不考虑偏移量为 0 的情况），攻击者可以通过穷举法在短时间内破解密码。而且它没有混淆和扩散特性，明文的统计特性很容易在密文中体现出来，安全性较低 。​

1. **答案**：​

* 每个数据库表有 4 种操作权限，企业有 20 个数据库表，那么每个表的权限组合数为从 4 种权限中选取不同组合的情况。根据组合数学知识，每个表的权限组合数为​

24−1=15

（减去全不选的情况）。​

* 20 个数据库表的总权限组合数为​

1520

种。​

* 企业有 10 个角色，每个角色可分配不同的权限组合，所以最多需要管理的权限 - 角色映射关系数量为​

10×1520

。​

四、简答题​

1. **答案**：​

* **主要区别**：对称加密算法使用相同的密钥进行加密和解密，加密速度快，效率高，但密钥管理困难，适合加密大量数据；非对称加密算法使用一对密钥，即公钥和私钥，公钥加密的信息只能用对应的私钥解密，私钥加密的信息只能用对应的公钥解密，密钥管理相对方便，可实现数字签名和身份认证，但加密速度慢，适合加密少量数据。​
* **常见算法**：对称加密算法如 AES（高级加密标准）；非对称加密算法如 RSA 。​

1. **答案**：​

* **作用**：防火墙是网络安全的屏障，通过制定访问控制策略，隔离内部网络和外部网络，阻止非法的网络访问，保护内部网络的资源和数据安全；对网络流量进行监控和过滤，防止恶意攻击和数据泄露；隐藏内部网络结构，提高网络的安全性；限制内部网络用户对外部危险网络的访问，降低安全风险 。​
* **工作模式**：包过滤模式，在网络层和传输层对数据包的头部信息（如源 IP、目的 IP、端口号等）进行分析和过滤；应用代理模式，在应用层对用户的请求进行代理转发，对应用层数据进行检查和处理；状态检测模式，能检测数据包的上下文信息，跟踪连接状态，提供更高级的安全防护 。​

1. **答案**：​

* **定义**：数字签名是指发送方使用自己的私钥对消息摘要进行加密，生成的一段数据。将原始消息和数字签名一起发送给接收方，接收方用发送方的公钥对数字签名进行解密，验证消息的真实性和完整性 。​
* **作用**：身份认证，确认消息确实是由声称的发送方发送的；消息完整性验证，确保消息在传输过程中没有被篡改；不可抵赖性，发送方不能否认自己发送过该消息，因为只有发送方的私钥才能生成有效的数字签名 。​

1. **答案**：​

* **工作原理**：入侵检测系统通过收集网络流量、主机日志、系统调用等多种数据源的信息，对这些数据进行预处理，去除噪声和冗余信息。然后运用异常检测或误用检测等技术进行分析，异常检测是通过建立系统正常行为的模型，将当前行为与模型对比，发现偏离正常模型的行为视为异常；误用检测是基于已知的攻击模式（特征库），查找与之匹配的行为。当检测到可疑行为时，按照预先设定的策略进行响应 。​
* **主要功能**：实时监测网络和系统中的攻击行为，及时发现潜在的安全威胁；对攻击行为进行分析和记录，为后续的安全事件调查和处理提供依据；在检测到攻击时，采取主动响应（如阻断攻击源）或被动响应（如发出警报通知管理员）措施，降低攻击造成的损失 。​

1. **答案**：​

* **重要性**：信息安全风险评估能够识别组织面临的各种信息安全风险，了解风险的来源、发生的可能性和可能造成的影响，为制定合理的信息安全策略和措施提供依据；帮助组织确定信息安全防护的重点和优先级，合理分配安全资源，提高信息安全投资的效益；通过风险评估，可发现信息系统和管理过程中的安全漏洞和薄弱环节，及时采取措施进行改进和完善，降低安全风险，保障信息系统的安全运行 。​
* **主要步骤**：风险识别，确定信息资产、威胁、脆弱性等；风险分析，评估风险发生的可能性和影响程度；风险评价，将风险分析结果与风险准则进行比较，确定风险等级；根据风险评价结果，选择合适的风险应对策略，如风险规避、风险降低、风险转移或风险接受 。​

五、分析题​

1. **答案**：​

* **存在的信息安全问题**：​
* **弱口令问题**：系统允许用户设置简单易猜的口令，如生日、连续数字等，攻击者可以通过暴力破解或字典攻击获取用户账号密码，从而非法访问系统。​
* **未对用户输入进行有效验证**：黑客可以利用这一漏洞进行 SQL 注入攻击，构造恶意的 SQL 语句，篡改数据库中的数据，如学生成绩数据 。​
* **缺乏安全意识和管理**：学校可能没有对教务系统的安全给予足够重视，没有制定严格的安全管理制度和规范，也没有对系统进行定期的安全检查和维护 。​
* **防范措施**：​
* **加强口令管理**：强制要求用户设置复杂的口令，如包含字母、数字、特殊字符，且长度不少于 8 位；定期更换口令；启用多因素认证，如口令结合短信验证码或动态令牌，增加认证的安全性 。​
* **防止 SQL 注入攻击**：对用户输入进行严格的验证和过滤，采用参数化查询、输入验证函数等技术，确保输入的数据符合预期格式，防止恶意 SQL 语句的注入；对数据库进行安全加固，限制数据库用户的权限，只授予必要的操作权限 。​
* **提高安全意识和管理水平**：对系统管理员和相关工作人员进行信息安全培训，提高安全意识和技能；建立完善的信息安全管理制度，定期对教务系统进行安全评估和漏洞扫描，及时发现和修复安全问题 。​

1. **答案**：​

* **可能的攻击方式**：​
* **中间人攻击**：黑客在公共 WiFi 网络中搭建恶意的接入点，伪装成合法的 WiFi 热点。当员工连接该热点时，黑客可以截获员工手机与企业邮箱服务器之间的通信数据，获取账号密码等信息；还可以篡改通信内容，进行钓鱼攻击 。​
* **WiFi 嗅探**：黑客使用专门的工具在公共 WiFi 网络中监听网络流量，捕获未加密的邮件通信数据，从中提取账号密码和邮件内容 。​
* **恶意软件攻击**：员工在连接公共 WiFi 时，可能不小心下载或安装了恶意软件，这些软件可以在后台运行，窃取手机中的敏感信息，包括企业邮箱账号密码 。​
* **企业应采取的措施**：​
* **加强网络安全防护**：对企业邮箱服务器进行安全加固，启用 SSL/TLS 加密协议，确保邮件在传输过程中的保密性和完整性；部署入侵检测系统和防火墙，实时监测和阻止网络攻击 。​
* **提供安全的远程访问方式**：为员工提供 VPN 服务，员工通过 VPN 连接企业内部网络访问邮箱，在公共 WiFi 环境下建立安全的专用网络通道，防止信息泄露 。​
* **加强员工培训**：定期对员工进行信息安全培训，提高员工在公共网络环境下的安全意识，如不随意连接陌生的 WiFi 热点，谨慎处理网络请求和下载文件等 。​
* **员工应采取的措施**：​
* **谨慎使用公共 WiFi**：尽量避免在公共 WiFi 环境下进行敏感操作，如登录企业邮箱、进行网上银行交易等；如果必须使用，优先选择有密码保护且官方认证的 WiFi 热点 。​
* **启用设备安全防护**：在手机等设备上安装可靠的安全防护软件，及时更新系统和软件补丁，开启设备的安全防护功能，如防火墙、病毒查杀等 。​
* **使用多因素认证**：为企业邮箱账号启用多因素认证，即使账号密码被窃取，攻击者没有其他认证因素也无法登录邮箱 。