计算机网络第七章：网络安全 单元测试3

单选题

1. [单选]
确保授权用户能够及时访问和使用网络资源及服务，这属于网络安全的哪个核心概念？
（A）机密性　　（B）完整性
（C）可用性　　（D）不可否认性

2. [单选]
恶意软件（如病毒、蠕虫、木马）属于网络安全面临的哪类威胁？
（A）主动攻击　　（B）被动攻击
（C）社会工程　　（D）其他威胁

3. [单选]
通过欺骗用户获取敏感信息（如密码、银行账号），这属于哪种类型的网络安全威胁？
（A）恶意软件　　（B）拒绝服务
（C）社会工程　　（D）数据篡改

4. [单选]
网络安全的内容之一是网络防御，其主要手段包括：
（A）身份认证　　（B）数据加密
（C）防火墙、入侵检测系统（IDS）　　（D）安全策略制定

5. [单选]
对称加密算法的特点是：
（A）适合密钥交换　　（B）计算开销大，速度慢
（C）使用同一密钥进行加密解密　　（D）基于公钥基础设施

6. [单选]
非对称加密算法的特点是：
（A）速度快，适合大数据量加密　　（B）使用同一密钥进行加密解密
（C）适合用于数字签名和密钥交换　　（D）密钥分发简单

7. [单选]
数字签名的工作原理是基于哪种加密技术？
（A）对称加密　　（B）非对称加密
（C）哈希函数　　（D）数据压缩

8. [单选]
数字签名的哪个特点确保发送者无法否认发送过该数据？
（A）完整性　　（B）认证性
（C）不可否认性　　（D）机密性

9. [单选]
基于知识、基于持有、基于生物特征是哪种网络安全技术的方法？
（A）数据加密技术　　（B）数字签名技术
（C）身份认证技术　　（D）防火墙技术

10. [单选]
Kerberos协议是一种身份认证协议，它基于什么机制？
（A）公钥证书
（B）对称密钥和票据
（C）生物特征识别
（D）一次性密码

11. [单选]
防火墙根据什么来决定是否允许或拒绝进出网络的流量？
（A）流量的负载大小
（B）预定义的过滤规则
（C）数据内容的随机性
（D）网络拓扑结构

12. [单选]
哪种类型的防火墙通过跟踪连接状态来提高安全性，例如记住TCP连接的三次握手状态？
（A）包过滤防火墙
（B）状态检测防火墙
（C）应用层网关
（D）下一代防火墙

13. [单选]
以下哪个不是计算机防病毒技术中常用的检测技术？
（A）特征码检测
（B）行为检测
（C）网络流量分析
（D）沙箱技术

14. [单选]
防病毒软件的“行为检测”技术主要用于检测：
（A）已知的病毒变种
（B）未知或新型病毒的恶意行为
（C）文件中的病毒特征码
（D）网络连接是否加密

15. [单选]
防病毒措施中，定期更新病毒库的目的是：
（A）提高扫描速度
（B）减少误报
（C）应对新的病毒和变种
（D）降低系统资源占用

判断题

1. [判断]
网络安全的目标是保护网络免受所有可能的威胁。（ ）

2. [判断]
社会工程是一种主动攻击，因为攻击者会与用户互动并进行欺骗。（ ）

3. [判断]
身份认证技术用于限制用户对网络资源的访问权限。（ ）

4. [判断]
对称加密算法因其计算效率高，常用于VPN等需要大量数据加密的场景。（ ）

5. [判断]
数字签名过程使用了发送者的私钥和发送者的公钥。（ ）

6. [判断]
数字签名可以用于验证软件是否被篡改过。（ ）

7. [判断]
基于持有（如智能卡）的身份认证比基于知识（如密码）的安全性通常更高。（ ）

8. [判断]

包过滤防火墙的优点是速度快，但安全性相对较低。（　　）

9. [判断]

防病毒软件的实时防护功能可以监控文件和网络活动，实时拦截威胁。（　　）

10. [判断]

用户教育在防病毒中不重要，所有安全都应依赖技术措施。（　　）

简答题

1. [简答]

请简述网络安全的核心概念“机密性”、“完整性”和“可用性”。

2. [简答]

请简述对称加密和非对称加密的主要区别。