

19. 入侵检测技术的发展趋势不包括 【 】
A. 智能化入侵检测 B. 全面的安全防御方案
C. 分布式入侵检测 D. 集中式入侵检测
20. 下列关于可信嵌入式安全模块 ESM 的说法错误的是 【 】
A. 可以用 J2810 芯片来充当可信安全计算机中的 TBB
B. ESM 的 CPU 是一个 16 位的 RISC CPU, 具有速度快、程序精简等特点
C. 嵌入式操作系统 JetOS 是 ESM 资源的管理者, 是 ESM 和整个系统安全的关键之一
D. I/O 管理模块是操作系统 JetOS 的核心和基础, 用来实现卡与 ESM 之间的相互认证等安全保密功能
21. 下列不属于现行系统详细调查内容的是 【 】
A. 需求调查 B. 业务调查 C. 信息调查 D. 处理调查
22. 下列不属于 Kerberos 协议存在的安全缺陷的是 【 】
A. 不能很好地防止口令猜测式攻击
B. 用时间戳防止重放攻击代价偏高
C. 时间同步问题是一个薄弱环节
D. 不能有效地防止旁路控制
23. 防火墙的发展经历了五个阶段, 第一代防火墙是基于____上 【 】
A. 网关 B. 路由器 C. 服务器 D. 主机
24. 下列哪项不属于系统转换方式 【 】
A. 直接转换 B. 间接转换
C. 平行运行方式 D. 试运行方式
25. 报文认证中____是解决重放攻击的 【 】
A. 报文的时间性认证 B. 报文宿的认证
C. 报文内容的认证 D. 报文源的认证
26. 下列说法错误的是 【 】
A. 防火墙就是一种能够限制网络访问的设备或软件
B. 防火墙的出现有效地限制了数据在网络内外的自由流动
C. 防火墙自身对网络入侵不免疫
D. 防火墙能为所有的访问做出日志记录
27. 下列哪项不属于第 2 层隧道协议 【 】
A. IPSec B. PPTP C. L2F D. L2TP
28. 安全隔离与信息交换系统不包括 【 】
A. 专用隔离硬件交换单元 B. 专用隔离软件交换单元
C. 内网处理单元 D. 外网处理单元

29. 下列不属于文件数字摘要分析技术的作用的是 【 】
A. 寻找已知的异常文件 B. 排除已知的正常文件
C. 发现被篡改的文件 D. 恢复被篡改的文件
30. 下列不属于 PGP 实际操作所包括的服务的是 【 】
A. 数字签名 B. 消息加密 C. 访问控制 D. 压缩

得分	评卷人	复查人

二、多项选择题 (每小题 2 分, 共 20 分)
在每小题的五个备选答案中选出二至五个正确答案, 并将其代码写在题干后面的括号内。多选、少选、不选或错选者, 该题无分。

1. 下列属于可信安全计算机采用的关键技术的是 【 】
A. 信任机制 B. BIOS 安全增强 C. 两级日志管理
D. 防火墙技术 E. 基于智能卡的用户身份认证
2. 信息安全系统的系统设计内容包括 【 】
A. 信息安全系统的体系结构设计
B. 网络结构设计
C. 资源配置设计
D. 用户配置设计
E. 安全风险分析
3. 网络通信中的密码协议按照其完成的功能可以分成 4 类, 其中包括 【 】
A. 密钥交换协议 B. 管理协议 C. 认证协议
D. 电子商务协议 E. 纠错协议
4. 信息安全的基本属性包括 【 】
A. 可用性 B. 可共享性 C. 可控性
D. 可行性 E. 可靠性
5. 下列关于数字签名的说法正确的是 【 】
A. 数字签名算法 DSA 安全性基于计算离散对数的难度, 是一种分组技术, 它只能用于数字签名
B. 基于对称密码体制的数字签名方案的本质是共享密钥的验证
C. 基于公钥密码算法的数字签名方案本质上并不是公钥密码加密算法的逆应用
D. 数字签名根据其本身实现目的的不同, 一般分为直接数字签名和间接数字签名两种
E. 一个数字签名方案有两部分组成, 即签名算法和验证算法
6. 网络安全技术中, 访问控制安全策略的主要内容包括 【 】
A. 最小特权策略 B. 全面防御原则 C. 最小覆盖原则
D. 多级安全策略 E. 最小泄漏原则