绝密 ★ 考试结束前

全国2015年10月高等教育自学考试

计算机网络安全试题

课程代码:04751

请考生按规定用笔将所有试题的答案涂、写在答题纸上。

选择题部分

注意事项:

1. 答题前,考生务必将自己的考试课程名称、姓名、准考证号用黑色字迹的签字笔或钢笔填写在答题纸规定的位置上。

2. 每小题选出答案后,用2B铅笔把答题纸上对应题目的答案标号涂黑。如需改动,用橡皮擦干净后,再选涂其他答案标号。不能答在试题卷上。

一、单项选择题(本大题共15小题,每小题2分,共30分)

在每小题列出的四个备选项中只有一个是符合题目要求的,请将其选出并将"答题纸"的相应代码涂黑。错涂、多涂或未涂均无分。

1. 利用恶意代码属于

A. 主动攻击　　B. 被动攻击　　C. 邻近攻击　　D. 内部人员攻击

2. VPN的中文含义是

A. 局域网　　B. 虚拟专用网

C. 万维网　　D. 入侵检测系统

3. 计算机机房设计时首先要考虑的问题是

A. 照明应达到规定标准　　B. 机房内应设置更衣室和换鞋处

C. 机房进出口须设置应急电话　　D. 如何减少无关人员进入机房的机会

4. 电源对用电设备安全的潜在威胁不包括

A. 脉动　　B. 噪声　　C. 线路短路　　D. 电磁干扰

5. 关于端到端加密系统,下面叙述正确的是

A. 通常允许对消息的目的地址进行加密

B. 消息在被传输到达终点之前必须进行解密

C. 端到端加密系统的价格便宜

D. 与链路加密和节点加密相比,可靠性低

6. 数据包过滤防火墙通常安装在

A. Hub　　B. 路由器　　C. 网桥　　D. 交换机

7. 在防火墙的基本配置中，增加用户的命令是

A. adduser　　B. dns　　C. deluser　　D. route

8. 关于个人防火墙的特点，下面叙述正确的是

A. 不能抵挡内部的攻击

B. 不能为用户隐蔽暴露在网络上的信息，比如 IP 地址之类的信息等

C. 只能对单机提供保护，不能保护网络系统

D. 降低了保护级别，需要额外的硬件资源

9. 入侵检测系统的组成部分包括

A. 数据提取、入侵分析、响应处理和远程管理

B. 数据提取、分布监视、入侵分析和响应处理

C. 分布监视、入侵分析、响应处理和远程管理

D. 分布监视、入侵检测、响应处理和远程管理

10. 关于误用检测，下面叙述错误的是

A. 按照预定模式搜寻事件数据

B. 适用于对已知模式的可靠检测

C. 主要依赖于可靠的用户活动记录和分析事件的方法

D. 误用检测也称为特征提取

11. CPU 处理中断，规定了中断的优先权，优先权最高的是

A. 不可屏蔽中断　　B. 除法错　　C. 可屏蔽中断　　D. 单步中断

12. 复合型病毒是指

A. 寄生在磁盘引导区的计算机病毒

B. 寄生在主引导区的计算机病毒

C. 寄生在文件中的计算机病毒

D. 具有引导型病毒和文件型病毒寄生方式的计算机病毒

13. 指令替换法属于

A. 反跟踪技术　　B. 加密技术　　C. 模糊变换技术　　D. 自动生产技术

14. 网络安全体系结构的基本手段包括

A. 保护、检测、响应和恢复　　B. 保护、检测、响应和评估

C. 加密、检测、认证和恢复　　D. 加密、鉴别、响应和恢复

15. 关于安全需求分析，下面叙述正确的是

A. 应用层的安全需求是保护网络不受攻击，确保网络服务的可用性

B. 网络层的安全需求是针对用户和网络应用资源的

C. 用户身份假冒属于应用层的安全需求所要解决的问题

D. 非授权访问属于网络层的安全需求所要解决的问题

非选择题部分

注意事项：

用黑色字迹的签字笔或钢笔将答案写在答题纸上，不能答在试题卷上。

二、填空题（本大题共 10 小题，每小题 2 分，共 20 分）

16. OSI 参考模型从下层到上层依次是：物理层、数据链路层、网络层、_____、会话层、表示层、应用层。

17. 监视和跟踪每一个有效连接的状态，并根据这些信息决定是否允许网络数据包通过防火墙，这种防火墙技术是_____。

18. 按照网络安全漏洞的可利用方式来划分，漏洞探测技术可以分为：_____型漏洞探测和攻击型漏洞探测两种。

19. 网络安全解决方案中，实际安全风险分析一般应从网络、_____、应用等 3 个方面进行分析，同时还应从总体上对整个网络系统的安全风险进行详细分析。

20. 为提高电子设备的抗干扰能力，主要的措施有屏蔽、隔离、滤波、吸波及接地等，其中_____是应用最多的方法。

21. 恶意代码的主要关键技术有生存技术、攻击技术和_____。

22. 防火墙是位于被保护网络和_____之间执行访问控制策略的系统，以防止发生对被保护网络的不可预测的、潜在破坏性的侵扰。

23. 误用检测和异常检测各有优势和不足，考虑到两者的互补性，往往将它们结合在一起使用。通常的做法是将误用检测用于网络数据包，将异常检测用于_____。

24. 公钥基础设施主要包括认证机构 CA、_____、密钥备份（即恢复系统）、证书作废处理系统和 PKI 应用接口系统等。

25. 经过格式化后的磁盘应包括主引导记录区（硬盘）、引导记录区、文件分配表（FAT）、_____和数据区。

三、简答题(本大题共 6 小题,每小题 5 分,共 30 分)

26. 简述 OSI 安全体系结构中定义的五大类安全服务。

27. 静电对电子设备的损害具有哪些特点?

28. 简述密码学中五元组的内容。

29. 简述防火墙的五大基本功能。

30. 简述入侵检测系统需要解决的两个问题。

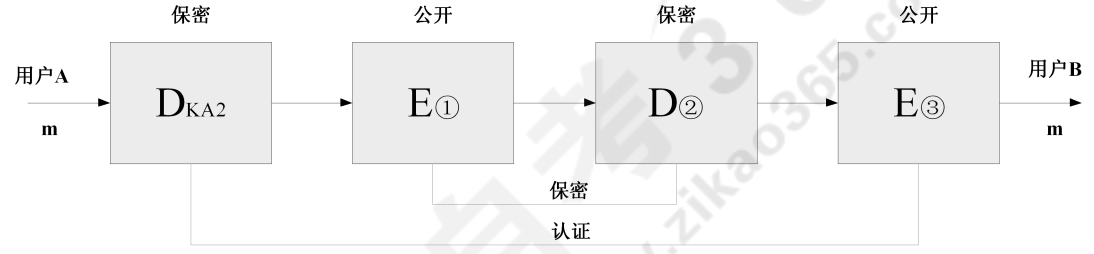
31. 计算机病毒的检测手段有哪些?

四、综合分析题(本大题共 2 小题,每小题 10 分,共 20 分)

32. 题 32 图是双钥保密和认证体制示意图。用户 A 和 B 的公开密钥,分别以 KA1 和 KB1 表示;用户 A 和 B 的私有密钥,分别以 KA2 和 KB2 表示。

(1)请写出题 32 图中①~③处所选用的密钥。

(2)试阐述题 32 图所示双钥密码的缺点,并分析改进的措施。



题 32 图

33. 端口扫描技术向目标主机的端口发送探测数据包,并记录目标主机的响应。题 33 表是 3 种端口扫描技术的扫描结果显示。请分析分别属于哪种扫描技术,并简要阐述相关的扫描原理。

题 33 表

扫描技术	扫描结果
技术 1	Initiating Connect() Scan against 192.168.100.1 [1672 ports] Discovered open port 80/tcp on 192.168.100.1
技术 2	Initiating SYN Stealth Scan against 192.168.100.1 [1672 ports] Discovered open port 80/tcp on 192.168.100.1
技术 3	Initiating UDP Scan against 192.168.100.1 [100 ports] PORT STATE SERVICE 53/udp open|filtered domain