**信息安全导论段考试题答案**

1. 单选题（每题4分，共5题20分）

ADBCB

1、IP地址是（A ）。

A. 计算机设备在网络上的地址 B. 计算机设备在网络上的物理地址

C. 以上答案都不对 D. 计算机设备在网络上的共享地址

2、以下不是木马程序具有的特征是（A或D ）。

A. 感染性 B. 欺骗性 C. 隐蔽性 D. 繁殖性

3、不属于被动攻击的是（B ）。

A. 欺骗攻击 B. 截获并修改正在传输的数据信息

C. 窃听攻击 D. 拒绝服务攻击

4、要安全浏览网页，不应该（C ）。

A. 定期清理浏览器缓存和上网历史记录

B. 定期清理浏览器Cookies

C. 在他人计算机上使用“自动登录”和“记住密码”功能

D. 禁止使用ActiveX控件和Java 脚本

5、网络安全协议包括（ B）。

A. SMTP B. SSL、TLS、IPSec、Telnet、SSH、SET等

C. POP3和IMAP4 D. TCP/IP

二、多选题（每题4分，共5题20分，多选，错选，漏选该小题都不能得分）

1、信息安全主要包括哪些内容？（ ABCD）

A. 系统可靠性和信息保障 B. 计算机安全和数据（信息）安全

C. 物理（实体）安全和通信保密 D. 运行安全和系统安全

2、计算机感染恶意代码的现象有（ABCD ）。

A. 计算机运行速度明显变慢 B. 无法正常启动操作系统

C. 磁盘空间迅速减少 D. 正常的计算机经常无故突然死机

3、为了避免被诱入钓鱼网站，应该（ACD ）。

A. 不要轻信来自陌生邮件、手机短信或者论坛上的信息

B. 使用搜索功能来查找相关网站

C. 检查网站的安全协议

D. 用好杀毒软件的反钓鱼功能

4、文件型病毒能感染的文件类型是（ACD ）。

A. COM类型 B. HTML类型 C. SYS类型 D. EXE类型

5、为了保护个人电脑隐私，应该（ABCD ）。

A. 删除来历不明文件 B. 使用“文件粉碎”功能删除文件

C. 废弃硬盘要进行特殊处理

D. 给个人电脑设置安全密码，避免让不信任的人使用你的电脑

三、简单题（每题10分，共60分）

1、如何安装一个安全的操作系统?

答：安装一个安全的操作系统可以采用以下几步: 1) 拔掉网线。 2) 安装操作系统。 3) 安装软件防火墙， 如 Norton 防火墙、 天网防火墙、 瑞星防火墙等。 4) 安装防病毒软件， 如 Norton、 瑞星、 江民、 金山等。 5) 安装防恶意软件的软件， 如 360 安全卫士、 瑞星卡卡、 超级兔子等。 6) 给操作系统进行安全设置， 如添加审核策略、 密码策略、 对账户进行管理等。 7) 插上网线， 给操作系统打补丁。 可以采用 360 安全卫士等软件来打补丁。 8) 更新防火墙、 防病毒、 防恶意软件， 包括病毒库、 恶意软件库等。 9) 安装数据恢复软件如 Easyrecovery。 10) 安装其他操作系统的应用软件。

1. 在 UNIX 系统中， 什么是 SUID， 什么是 SGID?

答：UNIX 中的 SUID (Set User ID) / SGID (Set Group ID) 设置了用户 ID 和分组 ID 属性， 允许用户以特殊权限来运行程序， 这种程序执行时具有宿主的权限。 当用户执行一个 SUID 文件时， 用户 ID 在程序运行过程中被置为文件拥有者的用户 ID。 如果文件属于 root， 那用户就成为超级用户。 同样， 当一个用户执行 SGID 文件时， 用户的组被置为文件的组。

3、企业为什么要引入 VPN?

答：企业员工在外出差或在家里需要连接公司服务器; 或者有第三方需要接入公司服务器 (如电子商务); 或者企业数据需要进行异地灾备; 还有的企业分支机构需要连接总公司等。

4、什么是DDoS攻击?

答：分布式拒绝服务 (Distributed Denial of Service， DDoS) 攻击手段是在传统的 DoS 攻击基础之上产生的一类攻击方式。如果说计算机与网络的处理能力加大了 10 倍， 用一台攻击机来攻击不再起作用的话， 攻击者就使用 10 台、 100 台或 1000 台攻击机同时攻击目标。 DDoS 就是利用更多的傀儡机来发起进攻， 以比从前 DoS 更大的规模来进攻受害者。

5、入侵检测系统的作用是什么?

答：入侵检测系统 (Intrusion Detection System， IDS) 就是能够完成入侵检测功能的计算机软硬件系统。 它通过对计算机网络或计算机系统中若干关键点收集信息并对其进行分析， 从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。

或者：

监控、分析用户和系统的活动；

 评估关键系统和数据文件的完整性；

 识别攻击的活动模式；

 对异常活动进行统计分析

 对操作系统进行审计跟踪管理，识别违反政策的用户动

1. 什么是计算机病毒， 它是怎么产生的?

答：计算机病毒， 是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据， 影响计算机使用， 并能自我复制的一组计算机指令或者程序代码。究其产生的原因有：开个玩笑， 一个恶作剧；产生于个别人的报复心理；用于版权保护；用于特殊目的。