# 第十三章测试题

1. 选择题
2. 以下关于宏病毒说法正确的试:( B )
3. 宏病毒主要感染可执行文件
4. 宏病毒仅向办公自动化程序编制的文件进行传染
5. 宏病毒主要感染软盘、硬盘引导扇区或主引导扇区
6. CIH病毒属于宏病毒
7. 下列选项中不属于计算机病毒防御技术的是？（D）
8. 基于特征的扫描技术
9. 基于线索的扫描技术
10. 基于行为的扫描技术
11. 基于保密性检测的扫描技术

二、名词解释

1．什么是病毒植入

病毒植入是指通过移动媒体，可以将包含病毒的宿主程序或宿主文件，独立、完整的病毒程序复制到主机系统中，作为该主机系统的某个文件。

2. 防毒墙

防毒墙是一种用于防御病毒的网关，能够对流经该网关的HTTP消息、FTP消息、SMTP消息、POP3消息进行深度检测，发现包含在消息中的各种类型的病毒，阻止病毒植入内部终端网络。

三、简述题

简述网络入侵检测系统阻止蠕虫病毒传播的方法？

网络入侵检测系统通过检测流经关键网段的信息流，发现可能存在的蠕虫病毒传播过程并予以制止。通过对流经探测器的信息流进行实时监控，鉴别出和蠕虫病毒传播有关的IP分组并予以丢弃。鉴别和蠕虫病毒传播有关的IP分组的机制主要有两种，一是通过分析已有的蠕虫病毒传播机制，提取出蠕虫病毒传播的操作特征，即传播蠕虫病毒过程需要且有别于正常信息交换过程的操作序列。二是建立正常情况下特定流量的阈值，如电子邮件的平均流量。