**一、简要分析计算机病毒、木马、蠕虫的区别**

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，并能自我复制的代码片段，需要插入到宿主程序中运行，攻击的是本地文件。

木马是一段能实现有用的或必需的功能的程序（独立个体），但是同时还完成一些不为人知的功能用来攻击。

蠕虫是一个独立个体。蠕虫的攻击过程是对一般网络攻击过程的自动化实现，利用网络安全漏洞（主要是缓冲区溢出漏洞）使代码在远程系统上自动运行，这一点也是蠕虫与病毒、木马的本质区别，漏洞攻击也体现了蠕虫的漏洞依赖性。因此修补安全漏洞或关闭相关网络端口即可防止相应蠕虫侵入。

**二、为了提高隐蔽性，木马有哪些隐藏技术？**

1启动隐藏

隐藏自己，使得目标主机加载运行木马程序，而不被用户发现

比如前面介绍的各种木马自动加载技术；前面介绍的无文件木马，通过其它软件来触发执行；诱骗用户点击运行：如文件类型图标欺骗

2木马文件/目录隐藏

通过某种方式使用户无法发现木马文件和目录

比如隐藏在其它文件中：如无文件木马；勾选文件/目录属性中的“隐藏”，文件浏览器不可见（除非开启显示所有文件）

3进程隐藏

隐藏木马进程，使得任务管理器等工具不可见.

伪隐藏是指程序的进程仍然存在，只不过是让它消失在进程列表里。

真隐藏则是让程序彻底的消失，不以一个进程或者服务的方式工作。

设置窗口不可见 (从任务栏中隐藏)

把木马程序注册为服务 (从进程列表中隐藏)

欺骗查看进程的函数 (从进程列表中隐藏)

使用可变的高端口 (端口隐藏技术)

使用系统服务端口 (端口隐藏技术)

替换系统驱动或系统DLL (真隐藏技术)

动态嵌入技术 (真隐藏技术)

4通信隐藏

端口隐藏：现在大部分木马一般在控制主机后会在1024以上不易发现的高端口上驻留；有一些木马也会选择一些常用的端口，如80、23。有些木马利用80端口时，在收到正常的HTTP请求仍然把它交与Web服务器处理，只有收到一些特殊约定的数据包后，才调用木马程序。

木马也可以通过电子邮件，网盘等媒介传输数据。

**三、比较分析木马静态检测和动态检测技术的优缺点。**

静态检测（特征检测）：根据恶意代码的特征码（代码散列码、代码中的关键字、字节串、特定端口等）进行检测。缺点是只能检测到已知类型的木马。

动态检测技术基于定义的恶意代码异常行为规则，实时监控进程的动态行为，当发现有违犯规则的行为出现，则给出异常告警。这些行为主要包括：文件行为，进程行为，网络行为，注册表行为。与特征码静态检测技术相比，动态检测技术能够检测未知恶意代码、恶意代码的变种，不足：产生的误报率较高，且不能识别出病毒的名称和类型等。