测试点3-1

假设你在网站上观看视频时，你看到一个弹出窗口要求你安装定制的解码器，才能正常观看视频。如果同意安装，你的计算机有可能会面临什么威胁?

1.被安装传统病毒、蠕虫、木马等为代表的计算机病毒，计算机安全得不到保障

2.对方获取自己的ip等web信息，已收到网络威胁

3.有可能遭到欺骗类威胁，个人隐私受到攻击

以表格方式对比传统型病毒、蠕虫和木马的特点，指出各自专属的特征。

	主要特征	破坏行为	专属特征
传统型病毒	传统型病毒有一个「宿主」程序，所谓宿主程序就是指 那些让计算机病毒藏身的地方。传统型病毒通常具有 寄生性、传染性、潜伏性、触发性和破坏性。	被感染病毒的文件通过 移动存储、电子邮件等方式在主机间传播，并在被执行时，适机感染主机中的其他文件。	宿主程序被执行时，病毒代码就会获得执行的机会。
蠕虫	蠕虫是一种可以自我复制的代码，一般不需要寄生在宿主 文件中，主要通过网络传播，通常无需人为干预就能传播 。蠕虫主要具有自传播性、隐蔽性和破坏性等特性。	蠕虫病毒首先通过漏洞扫描发现网络中存在漏洞的主机、 然后利用漏洞实施攻击，攻击成功后，将该蠕虫程序迁移至被控制主机，该主机会成为新增的传染源源头，同时在 本机实施破坏行为。	利用漏洞实施攻击
木马	一种特殊的后门程序，可以用来远程控制另一台主机， 隐蔽性和非授权性是特洛伊木马的最显著特点。	基于客户端和服务端的通信、监控程序。客户端的程序 用于远程控制，可以发出控制命令，接收服务端传来的信息。服务端程序运行在被控计算机上，一般隐藏在被 控计算机中，可以接收客户端发来的命令并执行，将客户端需要的信息发回	基于客户端和服务端

测试点3-2

通过查阅资料，进一步对APT攻击进行了解，并以一种APT攻击的流程为例 ，对APT攻击的特点进行阐述。

当今，网络系统面临着越来越严重的安全挑战，在众多的安全挑战中，一种具有组织性、特定目标以及长时间持续性的新型网络攻击日益猖獗，国际上常称之为**APT（Advanced Persistent Threat高级持续性威胁）攻击**

Ping是系统提供的用于检测网络连通性的程序，有人认为这样的程序不会对 计算机系统的安全造成损害，因此没有危害性，谈谈你自己的观点，并加以 说明

不对，有的服务器会选择禁ping，这一定程度上在互联网上隐藏自己防止一些批量扫描软件探测主机，减少被入侵的几率

测试点3-3

防火墙和网闸都能提供在网络边界上的安全防护作用，请分析两者在功能上的相同与不同之处。

相同：

都可以保证高强度的安全，都起到了隔离的作用

不同：

防火墙是位于两个或多个网络之间，执行访问控制策略的一个或一组 系统，是一类防范措施的总称。网闸是在两个***不同安全域***之间，通过协议转换的手段，**以信息摆渡的方式实现数据交换**，且只有被系统明确要求传输的信息才可以通过，其信息流一般为通用应用服务。

漏报率和误报率是入侵检测系统（IDS）重要的性能指标，有人认为采用异常检测技术的IDS误报率很高，没有实用价值，请给出你的判断并说明判断理 由。

不正确，即使误报率很高，也是有一定的使用价值。异常检测是一种与系统相对无关、通用性较强的入侵检测技术。异常检测主要针对用 户行为数据、系统资源使用情况进行分析判断。