测试点 3-1

(1)这个解码器可能是一个被伪装的木马程序，下载安装后在计算机杀毒软件对其不起作用的情况下，可能致使计算机感染病毒，从而危机资金安全、信息安全等。

(2)

<table>
<tr><th>传统型病毒</th><th>主要特征</th><th>破坏行为</th><th>专属特征</th></tr>
<tr><td>蠕虫</td><td rowspan="2">寄生性、传染性、潜伏性、触发性和破坏性</td><td>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。</td><td>可自我复制，不需要寄生在宿主文件中，</td></tr>
<tr><td>木马</td><td>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。</td><td>隐蔽性和非授权性</td></tr>
</table>

测试点 3-2

(1) APT 攻击，即高级可持续威胁攻击,也称为定向威胁攻击，指某组织对特定对象展开的持续有效的攻击活动。这种攻击活动具有极强的隐蔽性和针对性,通常会运用受感染的各种介质、供应链和社会工程学等多种手段实施先进的、持久的且有效的威胁和攻击。

实例：超级工厂病毒攻击(震网攻击)：著名的超级工厂病毒攻击为人所知主要源于 2010 年伊朗布什尔核电站遭到 Stuxnet 蠕虫的攻击的事件曝光。遭遇超级工厂病毒攻击的核电站计算机系统实际上是与外界物理隔离的，理论上不会遭遇外界攻击。坚固的堡垒只有从内部才能被攻破，超级工厂病毒也正充分的利用了这一点。超级工厂病毒的攻击者并没有广泛的去传播病毒，而是针对核电站相关工作人员的家用电脑、个人电脑等能够接触到互联网的计算机发起感染攻击**（针对性强、组织严密）**，以此为第一道攻击跳板，进一步感染相关人员的移动设备，病毒以移动设备为桥梁进入“堡垒”内部，随即潜伏下来。病毒很有耐心的逐步扩散，一点一点的进行破坏**（持续时间长）**。这是一次十分成功的 APT 攻击，而其最为恐怖的地方就在于极为巧妙的控制了攻击范围，攻击十分精准。

在 2011 年，一种基于 Stuxnet 代码的新型的蠕虫 Duqu 又出现在欧洲，号称“震网二代”。 Duqu 主要收集工业控制系统的情报数据和资产信息，为攻击者提供下一步攻击的必要信息。攻击者通过僵尸网络对其内置的 RAT 进行远程控制，并且采用私有协议与 CC 端进行通讯，传出的数据被包装成 jpg 文件（**高隐蔽性**）和加密文件。

(2)

Ping 命令是一个专用于 TCP/IP 协议的网络测试命令，在监测网络正常运行。测试网络故障点、判断故障原因等方面作用不凡，它为网络管理人员在网络维护中带来了很大的方便，深受网络管理人员的欢迎。然后 Ping 命令被人非法使用就能变成一个攻击工具，阻塞网路通道，造成主机宕机或重启等严重问题。

攻击原理：在 Ping 命令中-t 是连续发测试包，-l 可以指定包的大小，结合起来就可以对目的机攻击；另一方面 ICMP 协议有一个特点——只要发送端完成 ICMP 报文的封装并传递给路由器，这个报文将会像邮包一样自己去寻找目的地址这个特点带来个致命的缺陷——易伪造，任何人都可以伪造一个 ICMP 报文并发送出去，伪造者可以利用 SOCK_RAW 编程直接改写报文的 ICMP 首部和 IP 首部，这样的报文所携带的源地址是伪造的，在目的端根本无法追查，且由于发送的包是可以分解和重新组装，所以发送一个非法的超过 65507 字节的包是完全可能的。当系统收到这样的包，就有可能使得一个 16 位的变量溢出，引起死机、重启等问题。

测试点 3-3

(1) 防火墙与网闸都是为了保证主机的安全而采取的防护措施。防火墙最终目的是为了内网的安全防护，防止外网对内网的攻击，同时对内网访问互联网的行为进行控制。而网闸的工作原理是信息摆渡，也就是可以实现完全隔离的不同网段之间的有条件访问，这是防火墙实现不了的。举个例子说，如果你有两个网段想互相访问，通过防火墙设置的话只是通过策略和路由实现，而通过网闸的话是用它自己的协议重新封装 IP 包再进行访问。网闸因为是用自己的协议重新封装 IP 包，所以处理数据多，速度慢。

(2)我认为虽然误报率很高，但在某种程度上也说明了安全性很高。而侵检测系统主要有误用型和异常型两种检测技术，根据这两种检测技术各自的优点，以及它们的互补性，可以将两种检测技术结合起来的方案越来越多地应用于 IDS 中。比如基于统计的异常检测技术和基于模式匹配的误用检测技术相结合的 tDS 模型，减少了单纯使用某种入侵检测技术时的漏报率和误报率，从而提高系统的安全性。这说明了异常检测技术还是有一定的应用价值