**一、选择题（共20分，共10题，每题2分）**

1、 病毒的（ ）是指当病毒通过引导功能进入内存后的状态。当满足一定的触发条件时开始进行传播和破坏，构成对计算机系统和资源的威胁和损坏。

A、 静态 B、 动态 C、触发态 D、破坏态

2、寄生在文件中的病毒常用（ ）实现寄生。

A、替代法 B、覆盖法 C、链接法 D、隐藏法

3、在Windows32位操作系统中，DLL文件中的特殊标示为（ ）状态。

A、MZ B、PE C、LE D、NE

4、木马与合法远程控制软件(如pcAnyWhere、dameware)的主要区别在于是否具有（ ）。

A、寄生性 B、隐藏性 C、触发性 D、连接性

5、以下不具备破坏性的是（ ）。

A、木马 B、文件型病毒 C、蠕虫 D、脚本病毒

1. 下列结构中属于蠕虫病毒程序中必备的模块是（ ）。

A、扫描模块 B、破坏模块 C、 引导模块 D、 触发模块

1. 下列病毒中（ ）计算机病毒是文件型病毒。

A、 冲击波 B、 震荡波 C、 CIH D、 红色代码

1. 脚本病毒入住内存的方法是利用( )。

A、 漏洞 B、 寄生文件运行 C、 WSH环境 D、修改注册表

9、下列计算机病毒防治方法中，能够检测加密加壳病毒的是（ ）

A、 特征值检测 B、 广谱特征检测 C、 虚拟机 D、 校验和

10、下列（ ）行为属于病毒shellcode常用的行为。

A、占用INT 13H B、 搜索API函数地址

C、对可执行文件做写入动作 D、 不直接搜索其他可执行程序进行修改

**二、填空题（共20分，共20空，每空1分）**

1、计算机病毒的引导过程一般包括 ， 和

3个步骤态。

2、现代杀毒软件一般是以 为主， 为辅。

3、常见的计算机病毒的技术特征有 ， ， ，

， ， ， 等，因此可以通过这些技术特征来区分病毒程序和普通程序。

1. 一般情况下，病毒是依据其能够 的特点而定义的 ，木马主要是根

据它的 来定义的。

5. 启发式代码扫描技术源于人工智能技术，是基于给定的 和 的扫描技术

6. 计算机病毒免疫技术是通过定义 的特征规则，不满足定义特征规则的程

序可以判断为 。

7、红色代码病毒属于 病毒。

8、蠕虫程序和传统病毒程序采用的复制机制分别是 和 。

1. **阅读代码回答问题（共20分，共2题，每题10分）**
2. mov eax,fs,0x30 //PEB

mov eax,[eax+0x0c] //PROCESS\_ MODAULE\_INFO

mov esi,[eax+0x1c] //InInitOrder.flink

lodsd //eax=InInitOrder.flink

mov ebp,[eax+8]

1. 描述以上程序是实现什么的代码。（2分）
2. 该代码是怎么实现（4分）
3. 该病毒代码一般运用在哪种病毒中，为什么需要？（4分）

2、set fso=createobject("scripting.filesystemobject")

set self=fso.opentextfile(wscript.scriptfullname,1)

vbscopy=self.readall

set ap=fso.opentextfile(目标文件.path,2,true)

ap.write vbscopy

ap.close

set cop=fso.getfile(目标文件.path)

cop.copy(目标文件.path & ".vbs")

目标文件.delete(true)

1. 叙述以上程序实现过程。（4分）
2. 代码实现了什么功能？（2分）
3. 如果以上代码是病毒代码，它获得了什么权限，为什么？（4分）

**四、简答题（共20分，共2题，每题10分）**

1、简述传统病毒的结构特征和运行机制。

2、多态病毒的防治方法有哪些？说明防治原理。

**五、综合分析题（共20分，共1题）**

* + - 1. 比较文件型病毒，木马病毒及蠕虫程序的特征。根据它们的特征设计防治策略。