武汉大学 周子榆

软件安全之恶意代码机理与防护

首页 统计 通知 作业 考试 讨论

C1-C4测试

返回

姓名：周子榆 班级：16级信安3-4班 成绩： 90.0分

一、多选题 （题数：1，共 5.0 分）

1 以下哪个安全问题属于Security的范畴？ **5.0** 分

（5.0分）

A、 计算机病毒防护

B、 雷电防护

C、 网络黑客防护

D、 电磁防护

E、 桥梁安全

F、 地震防护

正确答案： AC 我的答案：AC

二、单选题 （题数：19，共 38.0 分）

1 可执行程序的图标数据存储在PE文件的哪个节？ **2.0** 分

（2.0分）

A、 引出函数节

B、 数据节

C、 引入函数节

D、 代码节

E、 资源节

正确答案： E 我的答案：E

2 80X86处理器的常态工作处理模式是？ **2.0** 分

（2.0分）

A、 实模式、保护模式以及虚拟86模式

B、 虚拟86模式

C、 实模式

D、 保护模式

正确答案： D 我的答案：D

3 **2.0** 分

PE文件以下哪个字段指向程序首条指令执行的位置？

（2.0分）

A、 SizeOfImage

B、 SectionAlignment

C、 AddressOfEntryPoint

D、 ImageBase

E、 BaseofCode

正确答案： C 我的答案：C

4 当文件被放入回收站之后，该文件目录项中的以下哪部分数据将发生变化? 2.0 分

（2.0分）

A、 首簇高位

B、 文件名的第一个字节

C、 首簇低位

D、 文件大小

正确答案： B 我的答案：B

5 以下说法错误的是? 2.0 分

（2.0分）

A、 相对而言，小文件比大文件更容易被恢复。

B、 相对而言，标准格式文件比非标准格式文件更容易被恢复。

C、 分区被格式化之后，其中的数据将无法被恢复。

D、 文件被误删除之后，不应该继续对该文件所在的分区进行直接和间接的写操作。

正确答案： C 我的答案：C

6 以下关于计算机Windows系统引导过程的顺序，正确的是? 2.0 分

（2.0分）

A、 BIOS ->NTLDR->DBR->MBR

B、 BIOS -> MBR ->DBR ->NTLDR

C、 MBR->DBR->NTLDR->BIOS

D、 MBR ->BIOS ->DBR ->NTLDR

E、 BIOS->MBR->NTLDR->DBR

正确答案： B 我的答案：B

7 在你看来，信息系统存在的安全问题的本质原因是： 0.0 分

（2.0分）

A、 信息系统缺乏充分安全测试

B、 信息系统存在漏洞

C、 信息资产具有价值

D、 信息系统开发未遵循安全开发流程（如SDL-IT）

E、 恶意软件数量急剧增加

正确答案： C 我的答案：B

8 以下哪个工具常用来进行PE程序调试? 2.0 分

（2.0分）

A、 UltraEdit

B、 Ollydbg

C、 PEView

D、 IDA

正确答案： B 我的答案：B

9 以下哪一类恶意软件是在应用程序执行阶段获得控制权? 2.0分

（2.0分）

A、 MBR木马

B、 DOS引导区病毒

C、 文件感染型病毒

D、 BIOS木马

正确答案： C 我的答案：C

10 NTFS文件系统下，如果一个文件较大，NTFS将开辟新空间存放File的具体数据，其通过文件记录（File Record）中的_____指明各部分数据的起始簇号和占用簇的个数? 0.0分

（2.0分）

A、 FR头

B、 $DATA

C、 Data Run

D、 MFT记录号

E、 FAT表项中的簇链表

正确答案： C 我的答案：D

11 NTFS文件系统中，文件内容的存放位置是? 0.0分

（2.0分）

A、 MFT或数据区

B、 MFT

C、 数据区

D、 DBR

正确答案： A 我的答案：C

12 硬盘中PE文件各节之间的空隙（00填充部分）大小，与以下哪个参数的大小息息相关? 2.0分

（2.0分）

A、 SizeOfImage

B、 FileAlignment

C、 SizeofHeaders

D、 SectionAlignment

E、 SizeofImage

正确答案： B 我的答案：B

13 本课程C3章节使用的test.exe示例程序，VA地址403000H处的数据在文件中对应的地址是? 2.0分

（2.0分）

A、 400H

B、 600H

C、 200H

D、 800H

正确答案： D 我的答案：D

14 以下哪个扇区不包含可执行代码? 2.0 分

（2.0分）

A、 硬盘主分区表所在扇区

B、 操作系统引导扇区（DBR）

C、 磁盘主引导扇区（MBR）

D、 扩展分区表所在扇区（EBR）

正确答案： D 我的答案：D

15 DLL文件可能加载到非预期的ImageBase地址，PE文件使用_____解决该问题。 2.0 分

（2.0分）

A、 函数引入机制

B、 资源动态分配机制

C、 重定位机制

D、 函数引出机制

E、 资源节

正确答案： C 我的答案：C

16 DLL被引出函数的函数名字符串的RVA存储在引出函数节下的哪个字段指向的表中? 2.0 分

（2.0分）

A、 AddressOfFunctions

B、 AddressOfNames

C、 AddressOfNameOrdinals

D、 Name

正确答案： B 我的答案：B

17 本课程C3章节使用的test.exe示例程序在内存中的节对齐粒度是? 2.0 分

（2.0分）

A、 4000H

B、 500H

C、 200H

D、 1000H

E、 2000H

正确答案： D 我的答案：D

18 当文件通过Shift + Del的方式删除之后，以下哪个部分将发生变化? 2.0分

（2.0分）

A、 目录项中的文件名首字节，首簇高位，文件对应的FAT表项，以及文件内容

B、 目录项中的文件名首字节，首簇高位，以及文件对应的FAT表项

C、 仅目录项中的文件名首字节和文件对应的FAT表项

D、 仅首簇高位和文件对应的FAT表项

正确答案： B 我的答案：B

19 硬盘中线性逻辑寻址方式（LBA）的寻址单位是? 2.0分

（2.0分）

A、 簇

B、 柱面

C、 磁道

D、 扇区

E、 磁头

正确答案： D 我的答案：D

三、判断题 （题数：20，共 40.0 分）

1 当文件被误删除之后，不应继续往该文件所在的分区继续写入数据，否则可能造成被删除的文件被覆盖导致无法恢复。 2.0分

（2.0分）

正确答案： √ 我的答案： √

2 当一个PE可执行文件装载到内存之后，引入地址表（IAT表）指向的数据将被对应函数在内存中的VA地址所代替。 2.0分

（2.0分）

正确答案： √ 我的答案： √

3 DLL文件中，所有引出的API函数都有一个函数名。 2.0分

（2.0分）

正确答案： × 我的答案： ×

4 电脑被感染计算机病毒之后，通过更换硬盘可以彻底防止任何病毒再生。 2.0分

（2.0分）

正确答案： × 我的答案： ×

5 扩展分区表有四个分区项，但通常只会使用到前面两项。 2.0分

（2.0分）

正确答案： √ 我的答案： √

6 熟练掌握PE文件结构，对于理解PE文件病毒感染机理具有重要意义 2.0分

（2.0分）

正确答案：√ 我的答案：√

7 Windows环境下，每个进程均可以直接访问其他进程的用户区内存空间。 2.0分

（2.0分）

正确答案：× 我的答案：×

8 FAT32文件系统进行文件空间分配的最小单位是簇，一个簇通常包含多个扇区。 2.0分

（2.0分）

正确答案：√ 我的答案：√

9 并口硬盘的数据线比串口硬盘的数据线宽，显然其传输速度更快。 2.0分

（2.0分）

正确答案：× 我的答案：×

10 硬盘主引导扇区最后两个字节必须以“55AA”作为结束 2.0分

（2.0分）

正确答案：√ 我的答案：√

11 一个具有图标和菜单的可执行文件通常都具有资源节。 2.0分

（2.0分）

正确答案：√ 我的答案：√

12 只有以电子形式存在的才是信息。 2.0分

（2.0分）

正确答案：× 我的答案：×

13 磁盘MBR扇区的分区表数据被破坏之后将无法恢复，因此要及时备份MBR扇区所有数据。 2.0分

（2.0分）

正确答案：× 我的答案：×

14 内存内核中的所有数据是所有进程共享的，用户模式代码可以直接访问。 2.0分

（2.0分）

正确答案：× 我的答案：×

15 每一个PE文件都必须有一个数据节和代码节，且这两个节不可以合并为一个节。 2.0分

（2.0分）

正确答案：× 我的答案：×

16 服务器机房的防潮防断电措施，不应属于信息安全防护的考虑范围。 **2.0** 分

（2.0分）

正确答案： × 我的答案： ×

17 Stud_PE是一款常见的PE程序动态调试软件。 **2.0** 分

（2.0分）

正确答案： × 我的答案： ×

18 在FAT32文件系统中，文件分配表有两份，即FAT1和FAT2，当一个文件被我们误删除之后，我们还可以直接从FAT2中找到对应的簇链表对FAT1进行修复，从而快速恢复该文件。 **0.0** 分

（2.0分）

正确答案： × 我的答案： √

19 通过直接修改或增加目标程序的代码节中的代码，可以使得目标程序具备原本更多的功能，譬如继续寻找和感染更多的其他目标程序。 **0.0** 分

（2.0分）

正确答案： √ 我的答案： ×

20 由于DLL文件可能不能加载到预期的ImageBase，因此重定位节对DLL文件来说是非常重要的。 **2.0** 分

（2.0分）

正确答案： √ 我的答案： √

四、填空题 （题数：5，共 17.0 分）

1 引入目录表（Import Table）的开始位置RVA和大小位于PE文件可选文件头DataDirecotry结构（共16项）中的第_____项。 **4.0** 分

[请填写阿拉伯数字]

（4.0分）

正确答案

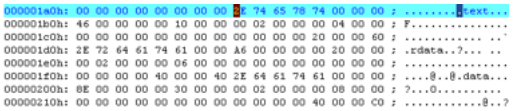
第一空:

2

我的答案:

第一空: 2

2 已知某个PE文件的ImageBase为400000H，下图是其节表部分的相关数据。某数据的VA(Virtual Address)=403006H，那么该数据在该PE文件中的文件偏移量应该是_____ H。 **3.0** 分



（3.0分）

正确答案

第一空:

806

我的答案:
第一空: 806

3 以下是某硬盘的分区表信息，通过分析可知，该硬盘的第一个主分区应为_____GB。（按1K=1000计算，小数点后保留一位，四舍五入） **3.0分**

```
00000000432 00 00 00 00 00 00 00 00  24 3F C3 8C 00 00 80 01
00000000448 01 00 07 FE FF FF 3F 00  00 00 41 39 40 06 00 FE
00000000464 FF FF 0F FE FF FF 80 39  40 06 C1 12 F8 33 00 00
00000000480 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000000496 00 00 00 00 00 00 00 00  00 00 00 00 00 00 55 AA
```

（3.0分）

正确答案
第一空:
53.7

我的答案:
第一空: 53.7

4 下图是某U盘［FAT32文件系统］下某个文件的目录项，由引导扇区参数可知该分区每个簇包含16个扇区［512字节 / 扇区］，由此可计算出该文件共占用_____个簇的存储空间？［请填写阿拉伯数字］ **3.0分**

```
000C001C0 41 41 41 20 20 20 20 20  54 58 54 20 18 0E 8B 8C
000C001D0 98 44 A4 46 00 00 AC 8C  98 44 03 00 08 D7 02 00
```

（3.0分）

正确答案
第一空:
23

我的答案:
第一空: 23

5 _____节的主要作用是将自身实现的函数对外进行引出，以便于其他程序可以动态调用本DLL文件中的函数。 **4.0分**

（4.0分）

正确答案
第一空:
引出函数

我的答案:
第一空: 引出函数

武汉大学 周子榆

软件安全之恶意代码机理与防护

首页 统计 通知 作业 考试 讨论

C5-C9单元测试

返回

姓名：周子榆 班级：16级信安3-4班 成绩： 77.0分

一、判断题 （题数：23，共 46.0 分）

1 木马程序对个人用户威胁巨大，其与计算机病毒、网络蠕虫存在的最大差别是其无法进行自我传播。 **2.0** 分

（2.0分）

正确答案：√ 我的答案：√

2 Slammer是一个非常典型的网络蠕虫，其运行时仅存在于内存之中，并不在硬盘生成文件。 **2.0** 分

（2.0分）

正确答案：√ 我的答案：√

3 任何一个网络蠕虫都会在硬盘中生成独立的文件，且其可以独立运行。 **2.0** 分

（2.0分）

正确答案：× 我的答案：×

4 APT的全称是Advanced Persistent Threat，这种威胁通常具有组织或政府背景，具有很强的可持续性和隐蔽性，并且通常具有较强的政治或军事目的，其与以获取经济利益为主要目的的传统威胁存在本质差别。 **2.0** 分

（2.0分）

正确答案：√ 我的答案：√

5 通过格式化操作系统所在盘符，可以完全清除系统中的文件型病毒。 **2.0** 分

（2.0分）

正确答案：× 我的答案：×

6 传统文件感染型病毒中的重定位技术，实际上是在目标HOST程序中增加新的重定位节，以此来完成病毒运行时的病毒代码中相关地址的自动修正。 **0.0** 分

（2.0分）

正确答案：× 我的答案：√

7 由于脚本功能非常有限，其对系统产生的破坏作用不如传统的PE病毒巨大。 **2.0** 分

（2.0分）

正确答案：× 我的答案：×

8 在蠕虫防范方面，网络运营商和网络管理部门的防护措施更为重要和关键。 **2.0** 分

（2.0分）

正确答案：√ 我的答案：√

9 只有在网络蠕虫真正爆发并获得其样本之后，才可能对其部署阻断措施。 **2.0**分

(2.0分)

正确答案：× 我的答案：×

10 远控木马分为控制端与被控制端程序，其中被控制端又被称为客户端。 **2.0**分

(2.0分)

正确答案：× 我的答案：×

11 如果一个正常程序存在可以被人恶意利用的漏洞，则其属于恶意软件。 **2.0**分

(2.0分)

正确答案：× 我的答案：×

12 按照恶意代码分类标准，灰鸽子应属于网络蠕虫。 **2.0**分

(2.0分)

正确答案：× 我的答案：×

13 漏洞利用型蠕虫比传统计算机病毒传播速度更快，是因为其利用了目标系统漏洞自动进行传播，其传播过程无须用户干预触发。 **2.0**分

(2.0分)

正确答案：√ 我的答案：√

14 StuxNet蠕虫通过利用MS10-046(lnk)漏洞，使得其可以通过可移动存储设备渗透到目标内部网络。 **2.0**分

(2.0分)

正确答案：√ 我的答案：√

15 网页挂马攻击属于典型针对特定个人的定向攻击行为。 **2.0**分

(2.0分)

正确答案：× 我的答案：×

16 无论是对于传统文件感染型PE病毒，还是PE程序自身来说，重定位的本质都是为了修正目标的实际内存地址与预期地址的差异。 **2.0**分

(2.0分)

正确答案：√ 我的答案：√

17 传统文件感染型病毒由于需要修改目标PE文件，其可能导致具有自校验功能的被感染程序无法正常运行 **0.0**分

(2.0分)

正确答案：√ 我的答案：×

18 宏病毒一种非常古老的恶意代码威胁，当前已经不可能存在这类威胁 **2.0**分

(2.0分)

正确答案： × 我的答案： ×

19 除了宏病毒威胁之外，打开数据文档是不可能存在其他安全隐患的。 **2.0** 分

(2.0分)

正确答案： × 我的答案： ×

20 漏洞利用型蠕虫的传播具有明显特点，由于在蠕虫传播初期互联网中存在的漏洞主机数量最多，因此该阶段的蠕虫传播速度最快。 **2.0** 分

(2.0分)

正确答案： × 我的答案： ×

21 相对于计算机病毒而言，网络蠕虫对网络性能形成的危害更为严重。 **2.0** 分

(2.0分)

正确答案： √ 我的答案： √

22 终端反病毒软件对于网络蠕虫防护起不到任何作用。 **0.0** 分

(2.0分)

正确答案： × 我的答案： √

23 按照Spafford的蠕虫定义，利用电子邮件传播的爱虫病毒可以被归为蠕虫。 **2.0** 分

(2.0分)

正确答案： √ 我的答案： √

二、填空题 （题数：7，共 21.0 分）

1 恶意代码为了隐藏自身，通常进行文件、进程、注册表、网络连接及端口隐藏，具备这类隐藏功能的程序，通常被称为_____。 **3.0** 分

（全英文字母，首字母大写）

(3.0分)

正确答案
第一空:
Rootkit

我的答案:
第一空: Rootkit

2 _____软件以主动收集用户个人信息、相关机密文件或隐私数据为主，搜集到的数据会主动传送到指定服务器。（汉字） **0.0** 分

(3.0分)

正确答案
第一空:
间谍

我的答案:
第一空： 木马

3 ____是指在尽量不影响目标程序（系统）正常功能的前提下，使其具有病毒自己的功能。（汉字） **0.0** 分

（3.0分）

正确答案
第一空:
感染； 传染

我的答案:
第一空： 寄生

4 远程控制型木马的连接方式通常可以分为“正向连接”和“反向连接”两大类，其中_____类木马需要被控制端开启监听端口。 **3.0** 分

（3.0分）

正确答案
第一空:
正向连接； 正向

我的答案:
第一空： 正向连接

5 1988年Morris蠕虫爆发之后，Eugene H. Spafford 为了区分蠕虫和病毒，给出蠕虫和计算机病毒的重新定义。“计算机蠕虫可以_____运行，并能把自身的一个包含所有功能的版本传播到另外的计算机上”。（汉字） **3.0** 分

（3.0分）

正确答案
第一空:
独立

我的答案:
第一空： 独立

6 为有效打击计算机犯罪，刑法修正案（七）在刑法_____**条**中增加了两款罪名，分别为非法获取计算机信息系统数据、非法控制计算机信息系统罪，以及提供侵入、非法控制计算机信息系统程序、工具罪 。（阿拉伯数字） **3.0** 分

（3.0分）

正确答案
第一空:
285

我的答案:
第一空： 285

7 _____是精心设计的用于利用特定漏洞以对目标系统进行控制的程序。（答案为全英文字母，首字母大写） **3.0** 分

（3.0分）

正确答案
第一空:
Exploit

我的答案:
第一空: Exploit

三、单选题 （题数：9，共 24.0 分）

1 目前，恶意软件数量急剧增加，其最大的驱动力是 **2.6分**

（2.6分）

A、 自我炫耀
B、 获取经济利益
C、 实现政治目的
D、 实现军事目的
E、 恶作剧

正确答案： B 我的答案：B

2 通常情况下，以下哪类恶意软件的传播速度是最快的？ **0.0分**

（2.6分）

A、 漏洞利用型蠕虫
B、 文件感染型病毒
C、 捆绑释放型病毒
D、 电子邮件蠕虫
E、 脚本病毒

正确答案： A 我的答案：D

3 远程控制型木马与远程管理软件之间的最大区别在于_____。 **2.6分**

（2.6分）

A、 是否进行版本更新
B、 是否为独立的程序
C、 是否可以传播
D、 是否获得被控制端授权
E、 是否存在远程控制功能

正确答案： D 我的答案：D

4 通过修改PE程序的_____字段，可以改变PE程序的代码执行流程。 **2.6分**

（2.6分）

A、 AddressOfEntryPoint
B、 BaseOfData

C、 BaseOfCode

D、 MZ头部的Initial Instruction Pointer IP

E、 AddressOfCode

正确答案： A 我的答案：A

5 传统文件感染型病毒在进行API函数自搜索时，主要是基于kernel32模块的何种机制进行的？ 0.0 分

（2.6分）

A、 函数引入机制

B、 资源定位机制

C、 函数引出机制

D、 重定位机制

正确答案： C 我的答案：A

6 熊猫烧香病毒采用了“Virus+Host”的感染方式，其缺陷是被感染程序的图标会发生变化。如需让被感染程序的图标保持不变，则需要对目标程序的以下哪个区域进行修改？ 2.6 分

（2.6分）

A、 图标节

B、 代码节

C、 资源节

D、 数据节

E、 资源重定位节

正确答案： C 我的答案：C

7 以下关于远程控制型木马的论述中，错误的评论项是？ 2.6 分

（2.6分）

A、 相对于正向连接木马而言，使用反向连接木马有利于攻击者第一时间控制被控主机

B、 采用反向连接方式的木马在穿透防火墙时更具优势。

C、 相对反向连接而言，采用正向连接的木马更难被定位到攻击者所在位置

D、 采用正向连接方式的木马通常需要控制端所在电脑拥有外部IP地址

正确答案： D 我的答案：D

8 以下哪种措施，不是有效的蠕虫防护措施？ 0.0 分

（2.6分）

A、 以毒攻毒，制作另外一个蠕虫来进行传播对抗

B、 补丁修补

C、 流量阻断

D、 部署终端反病毒软件进行查杀

正确答案： A 我的答案：D

9 《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》自2011年9月1日起施行，该司法解释规定：对于非法获取计算机信息系统数据、非法控制计算机信息系统罪而言，下列哪类情形，不属于该罪的“情节严重”？ **0.0** 分

（3.2分）

A、 获取支付结算、证券交易、期货交易等网络金融服务的身份认证信息十组以上的；

B、 非法控制计算机信息系统二十台以上的；

C、 明知他人实施非法获取支付结算、证券交易、期货交易等网络金融服务身份认证信息的违法犯罪行为而为其提供程序、工具五人次以上的；

D、 违法所得五千元以上或者造成经济损失一万元以上的；

E、 获取支付结算、证券交易、期货交易等网络金融服务以外的身份认证信息五百组以上的；

正确答案： C 我的答案：E

四、多选题 （题数：3，共 9.0 分）

1 在以下恶意代码中，不同类的是？ **3.0** 分

（3.0分）

A、 熊猫烧香

B、 Slammer

C、 CIH

D、 CodeRed

E、 StuxNet

F、 冲击波

正确答案： AC 我的答案：AC

2 在以下恶意代码中，不属于远程控制型木马的是： **3.0** 分

（3.0分）

A、 PCAnyWhere

B、 灰鸽子

C、 自由门

D、 冰河

E、 上兴

F、 PCShare

正确答案： AC 我的答案：AC

3 宏病毒通常通过修改自动宏的代码来获取控制权，以下不属于Word自动宏的选项是： **3.0** 分

（3.0分）

A、 AutoExec

B、 Auto_Close

C、 Auto_Open

D、 AutoExit

E、 AutoNew

正确答案： BC 我的答案：BC