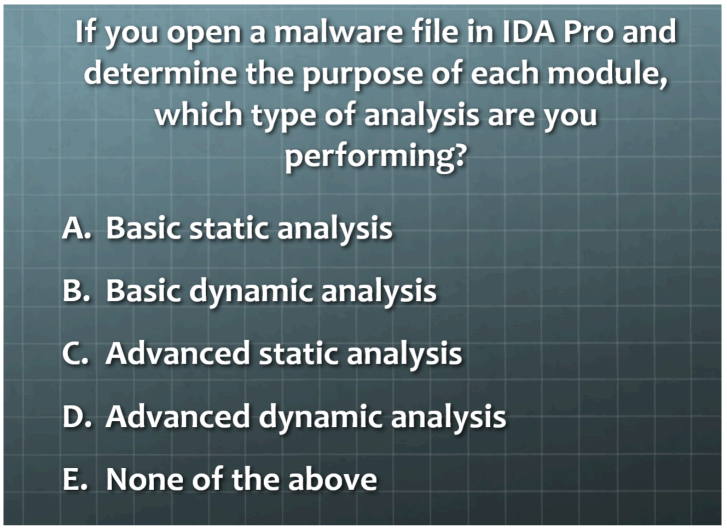
2024-2025学年《恶意代码分析与防治技术》期末考试

1　单选题(2分一个,共10个)

1.通过查看反汇编，是什么分析技术？——静态高级分析



这题应该是说，将每个模块的功能都分析了一下，所以应该是静态分析。然后不光光是看了一下文件，把文件的模块都看了，说明是静态高级技术

选C

2.原题

3.原题

18.单选题 (1分)

如何截获进程内部的消息?

A. 本地钩子（Local Hook）

B. 高级远程钩子（High-level Remote Hook）

C. 低级远程钩子（Low-level Remote Hook）

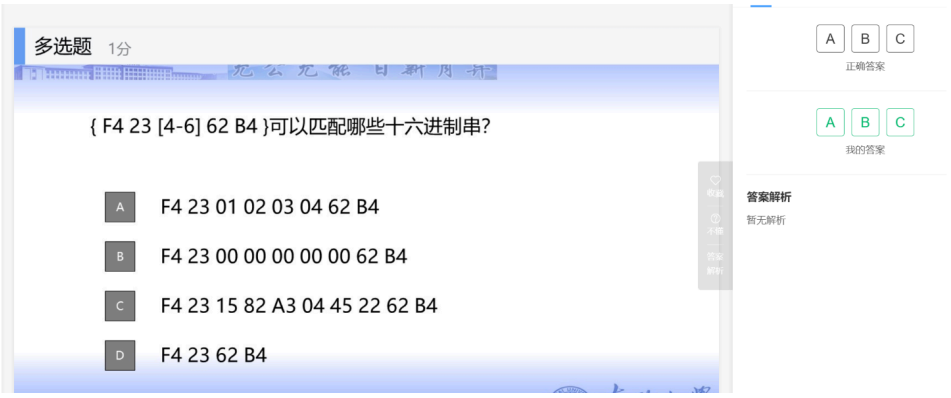
D. 键盘记录器（Keylogger）

本题得分： 0分

正确答案： B

4.哪个攻击用到了可警告的等待状态？——APC注入

5.一个简单的yara，涉及到[]的使用，没其他啥知识点，类似于下面这样：



6.考了一个base64自定义解密，不难，要了解base64的加密机制

7.下面哪个不是混淆技术的目的？——选隐藏动态行为那个，也是基本原题了

8.考察驱动程序

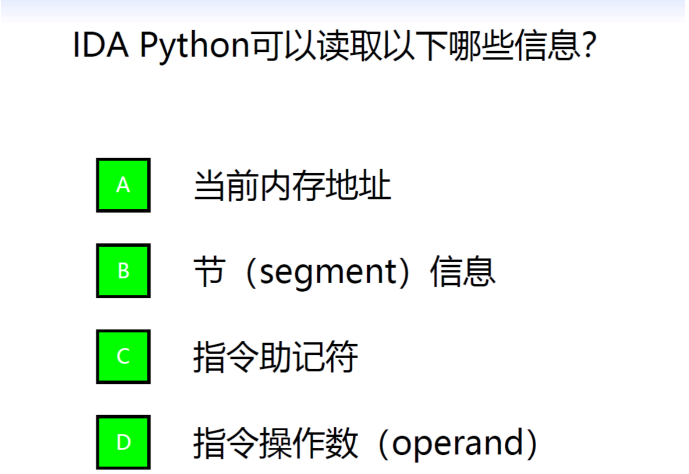
选错误的那个，选 只能有一个过滤驱动程序，这个是错的

9-10：还有两个题想不起来了，但是不难反正是

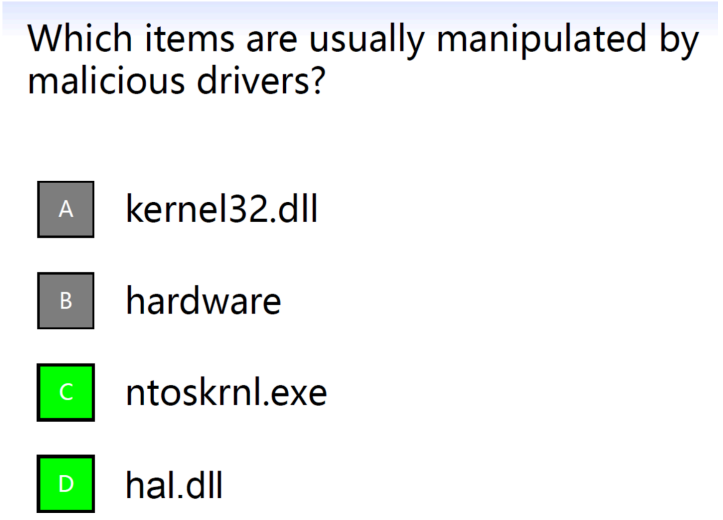
2　多选题(2分一个,共5个)

1.考了一个yara分析，涉及到nocase，#，@等

2.IDA Python的功能，原题



3.恶意驱动程序的攻击目标？原题!



4.虚拟机的缺点，很明显的一个题，有一个选项说的是优点，算是送分了

虚拟机进行计算机病毒动态分析的安全风险?

A 计算机病毒检测虚拟机，改变其动态行为

B 虚拟机软件的漏洞

C 虚拟机逃逸

D 可控性好

5.svchost.exe不能用在哪些地方?

A.OWN

B.KERNEL

C.SHARE

D.COM

这题不知道选啥，我选了OWN和KERNEL，考完之后有人说COM也不行。。。

13.单选题 (1分)

svchost.exe使用的服务类型是（）

A KERNEL_DRIVER

B WIN32_SHARE_PROCESS

C WIN32_OWN_PROCESS

D Component Object Model

本题得分： 1分

正确答案： B

3 简答题(5分一个,共8个)

1.写出常见的5种恶意代码类型，并简单解释其攻击方式

2.涉及到SEH异常处理

```
    push next
    push fs:[0]
    mov fs:[0], esp
    int3
    ...
next:
```

int3中断之后，程序会如何执行?

这个代码怎么执行的？写出原理

3.为什么要使用简单数据加密？简单数据加密的优点？写出三种简单数据加密的方式

4.写出HOOK注入，APC注入，进程注入的简要说明

5.写一个yara。涉及到PE文件，地址出现位置，所有的含a的字符串的地址都小于1000，第二次出现的字符串的地址等于3000，文件大小在20KB到2MB之间

$a每次在文件或内存中出现位置，都必须小于100。
（使用for-in表达方式来描述）

yara规则：

```
for all i in (1..#a):(@[i]<100)
```

#a代表的是a字符串出现的次数，所以刚好帮我们完成了遍历

类似于上面这个（）

6.默写DNS沉洞，IDS，IPS，网页代理和邮件代理的原理

7.五种持久化机制，写出名字和对应的原理

8.解释设备栈，驱动栈，以及设备和驱动的关系。防火墙是什么类型的驱动程序?

4　分析题(15分一个,共2个)

1.进程替换相关，和PPT基本一样，提供API函数的作用，不用硬背

```
CreateProcess(...,"svchost.exe",...,CREATE_SUSPENDED,...);
ZwUnmapViewOfSection(...);
VirtualAllocEx(...,ImageBase,SizeOfImage,...);
WriteProcessMemory(...,headers,...);
for (i=0; i < NumberOfSections; i++) {
 ❶ WriteProcessMemory(...,section,...);
}
SetThreadContext();
...
ResumeThread();
```

给了一个这个代码：

- 说出这个代码使用的恶意行为方式?
- 恶意代码攻击了主机中的哪个进程?
- 简单说明一下攻击的流程（解释代码！）
- 被感染的程序涉及到什么状态？（不太懂要写啥）
- 为什么要攻击这个进程?

2.简单的SSDT和IDT，和21级考的几乎一模一样

- 解释一下SSDT和IDT是什么
- 恶意代码如何完成SSDT和IDT的注入?
- 分析代码

类似于给了这种代码：

```
kd> dd nt
...
8050122c  805c9928 805c98d8 8060aea6 805aa334
8050123c  8060a4be 8059cbbc 805a4786 805cb406
8050124c  804feed0 8060b5c4 8056ae64 805343f2
8050125c  80603b90 805b09c0 805e9694 80618a56
8050126c  805edb86 80598e34 80618caa 805986e6
8050127c  805401f0 80636c9c 805b28bc 80603be0
8050128c  8060be48 1f7ad94a4 8056bc5c 805ca3ca
8050129c  805ca102 80618e86 8056d4d8 8060c240
805012ac  8056d404 8059fba6 80599202 805c5f8e
```

我们发现，有一个地址不在我们的范围之内，所以确实发生了挂钩的现象！

我们可以通过检测系统SSDT并根据偏移量找出对应的函数，来识别挂钩，我们可以通过lm命令打开模块：

```
kd>lm
...
f7ac7000 f7ac8580   intelide   (deferred)
f7ac9000 f7aca700   dmload     (deferred)
f7ad9000 f7ada680   Rootkit    (deferred)
f7aed000 f7aee280   vmmouse    (deferred)
...
```

分析对应的挂钩过程，分析哪个rootkit的模块挂钩了哪个SSDT的函数，看PPT就行