Chapter 1

单选题 (5分)

木马与病毒的重大区别是（）。

A 木马会自我复制

B 木马具有隐蔽性

C 木马不具感染性

D 木马通过网络传播

作答区

A B C D

正确答案

C

下一题

单选题 (5分)

恶意代码指的是（）。

A 计算机病毒

B 间谍软件

C 内核嵌套

D 任何对用户、计算机或网络造成破坏的软件

作答区

A B C D

正确答案

D

下一题

单选题 (5分)

网络黑客产业链是指黑客们运用技术手段入侵服务器获取站点权限以及各类账户信息并从中谋取（）的一条产业链。

A 非法经济利益

B 经济效益

C 效益

D 利润

作答区

A B C D

正确答案

A

下一题

单选题 (5分)

以下不是恶意代码分析目标的是（）。

A 对可疑程序进行深入分析，确定该程序是否有恶意行为

B 定位被感染的机器或者文件

C 恶意代码的优化和改进

D 衡量并消除恶意代码对系统造成的破坏

作答区

A B C D

正确答案

C

下一题

单选题 (5分)

蠕虫与普通病毒相比特有的性质为（）。

A 传播性

B 隐蔽性

C 不利用文件寄生

D 破坏性

作答区

A B C D

正确答案

C

下一题

单选题 (5分)

蠕虫病毒的传染目标是（）。

A 计算机内的文件系统

B 计算机内的病毒

C 计算机内的木马

D 互联网内的所有计算机

作答区

A B C D

正确答案

D

下一题

单选题 (5分)

轰动全球的震网病毒是（）。

A 木马

B 蠕虫病毒

C 后门

D 寄生型病毒

作答区

A B C D

正确答案

B

下一题

单选题 (5分)

下列属于高级静态分析技术的描述是（）。

A 检查可执行文件但不查看具体指令的一些分析技术

B 通过运行恶意代码来观测和分析系统中的动态行为

C 主要是对恶意代码内部机制的逆向工程，通过将可执行文件装载到反汇编器中，查看反汇编指令，来分析恶意代码到底做了什么

D 使用调试器来检查恶意代码运行时的内部状态

作答区

A B C D

正确答案

C

下一题

单选题 (5分)

下列对Rootkit的描述正确的是（）。

A 允许攻击者远程访问被感染的计算机

B 用来下载其它恶意代码的程序

C 用来启动其它恶意程序的程序

D 用来隐藏其它恶意代码的程序

作答区

A B C D

正确答案

D

下一题

单选题 (5分)

以下哪些方法是恶意代码分析过程中不建议使用的（）

A 在进入细节分析之前对恶意代码要有一个概要性的理解

B 尝试多从不同角度，使用不同工具和方法来分析恶意代码

C 对全部反汇编指令直接进行逐行分析

D 先使用基本的动态和静态分析工具，定位可疑的静态和动态特征。

作答区

A B C D

正确答案

C

下一题

单选题 (5分)

以下不是恶意代码分析目标的是（）

A 对可疑程序进行深入分析，确定该程序是否有恶意行为

B 定位被感染的机器或者文件

C 恶意代码的优化和改进

D 衡量并消除恶意代码对系统造成的破坏

作答区

A B C D

正确答案

C

下一题

单选题 (5分)

计算机病毒数量的变化趋势是（）

A 不断增多

B 逐渐减少

C 保持基本稳定

D 趋于消失

作答区

A B C D

正确答案

A

查看解析

下一题

判断题 (5分)

病毒能够自我执行和自我复制。

作答区

正确答案

下一题

判断题 (5分)

蠕虫是利用文件寄生来通过网络传播的恶性病毒。

作答区

正确答案

下一题

判断题 (5分)

木马不具有欺骗性，而具有隐蔽性和非授权性。

作答区

正确答案

下一题

判断题 (5分)

病毒特征码关注是恶意代码对系统做什么，而主机特征码关注恶意代码本身的特性。

作答区

正确答案

下一题

判断题 (5分)

网络特征码可以在没有进行恶意代码分析时创建，但在恶意代码分析帮助下提取的特征码往往更加有效的，可以提供更高的检测率和更少的误报。

作答区

正确答案

下一题

判断题 (5分)

基础静态分析技术的分析速度快，但针对复杂的恶意代码时很大程度上是无效的，而且它可能会错过一些重要的行为。

作答区

正确答案

下一题

判断题 (5分)

Mass恶意代码比APT恶意代码具有更大的安全威胁，杀毒软件很难检测到Mass恶意代码。

作答区

正确答案

下一题

多选题 (5分)

以下哪些系统或设备可能被计算机病毒感染（）

A 计算机、智能手机

B 打印机、网络路由器

C 摄像头、智能家具设备

D 智能汽车、智能电网、智慧城市

作答区

正确答案

A B C D

查看解析

查看答题卡

Chapter 2

单选题 (5分)

以下不是哈希值做的事是（）

A 杀毒软件使用哈希值作为计算机病毒的文件特征

B 病毒分析报告中使用哈希值标识病毒样本

C 通过哈希值计算文件的生成日期

D 在线搜索哈希值，查看哈希值对应的文件是否已经被杀毒软件公司检测到病毒

作答区

A B C D

正确答案

C

下一题

单选题 (5分)

PE文件中，通常哪个节包含可执行代码（）

A .rdata

B .text

C .data

D .rsrc

作答区

A B C D

正确答案

B

下一题

单选题 (5分)

PE文件中，以下哪个节中包含程序所使用的资源（）

A .rdata

B .text

C .data

D .rsrc

作答区

A B C D

正确答案

D

下一题

单选题 (5分)

当一个库被链接到可执行程序时，这个库中所有代码都复制到可执行程序中去，这种链接方法是（）

A 静态链接

B 动态链接

C 运行时链接

D 转移链接

作答区

A B C D

正确答案

A

下一题

单选题 (5分)

操作系统在程序被装载到内存时，搜索程序所需的库文件并装载到程序的内存空间中，这种链接方式是（）

A 静态链接

B 动态链接

C 运行时链接

D 转移链接

作答区

A B C D

正确答案

B

下一题

单选题 (5分)

当单击Resource Hacker工具中分析获得的条目时，看不到的是

A 字符串

B 二进制代码

C 图标

D 菜单

作答区

A B C D

正确答案

B

下一题

判断题 (5分)

哈希值是一种用来唯一标识恶意代码文件的常用方法。

作答区

正确答案

下一题

判断题 (5分)

Strings程序检测到的一定是真正的字符串。

作答区

正确答案

下一题

判断题 (5分)

当加壳的程序运行时，会首先运行一段脱壳代码，来还原被加壳代码所修改的程序代码和数据，然后再运行程序的代码。

作答区

正确答案

下一题

判断题 (5分)

PE头部可以获得的关键信息有时间戳、节表。

作答区

正确答案

下一题

判断题 (5分)

使用运行时链接的可执行程序，只有当需要使用函数时，才链接到库，而并不是像动态链接模式一样在程序启动时就会链接。

作答区

正确答案

下一题

判断题 (5分)

与导入函数类似，DLL和EXE的导出函数，是用来与其它程序和代码进行交互时所使用的。

作答区

正确答案

下一题

判断题 (5分)

加壳的目的是使计算机病毒更难被检测和分析

作答区

正确答案

下一题

判断题 (5分)

URLDownloadToFile() 一般提示该计算机病毒会从Internet上下载一个文件

作答区

正确答案

下一题

多选题 (5分)

以下哪些内容是计算机病毒基本静态分析的对象（）

A URL

B 文件哈希值

C 注册表键值

D API函数名

作答区

A B C D

正确答案

A B C D

下一题

多选题 (5分)

加壳和混淆技术的目的是（）

A 压缩文件的体积

B 隐藏URL和IP地址信息

C 隐藏重要的字符串信息

D 隐藏程序的行为

作答区

A B C D

正确答案

A B C

下一题

多选题 (5分)

以下哪些信息可以在PE文件头中找到（）

A 程序的入口点地址

B 程序的类型（EXE 或者 DLL）

C 调用的Windows API函数信息

D 程序所需要的内存空间大小

作答区

A B C D

正确答案

A B C D

下一题

多选题 (5分)

以下哪些函数被加壳代码用来装载其它API函数（）

A LoadLibrary

B GetProcessAddress

C FindFirstFile

D FindNextFile

作答区

A B C D

正确答案

A B

下一题

主观题 (10分)

列举5个杀毒软件公司的名字。

作答详情

待批改

我的答案 全屏查看

火绒，CAT-QuickHeal, McAfee, Cyren, 360, Zillya

查看答题卡

Chapter 3

单选题 (10分)

以下哪种联网模式在宿主机（Host Machine）和客户机（Guest Machine）之间创建了一个隔离的私有局域网

A Bridge

B NAT

C Host-only

D Custom

作答区

A B C D

正确答案

C

下一题

单选题 (10分)

以下哪种网络连接方式使虚拟机和宿主机共用一个IP地址?

A NAT

B Bridge

C Host-only

D Custom

作答区

A B C D

正确答案

A

下一题

单选题 (10分)

以下哪种网络连接模式使虚拟机与物理机连接到相同的局域网中，各有一个独立的IP地址?

A Bridge

B NAT

C Host-only

D Custom

作答区

A B C D

正确答案

A

下一题

判断题 (10分)

Vmware的快照管理器可以在任何时间返回系统的快照

作答区

正确答案

下一题

判断题 (10分)

VMware虚拟机可以对系统快照进行分支

作答区

正确答案

下一题

判断题 (10分)

虚拟机是运行在ring0级

作答区

正确答案

下一题

多选题 (10分)

在隔离的物理机器上面进行恶意代码的动态分析过程有哪些风险（）

A 恶意代码可能会破坏物理计算机系统

B 有些恶意代码的行为需要网络连接才会被执行

C 恶意代码难以清除

D 环境容易搭建

作答区

正确答案

A B C

下一题

多选题 (10分)

恶意代码动态分析环境的构建，可以使用哪些虚拟机软件（）

A VMware Player

B VMware Station

C VMware Fusion

D VirtualBox

作答区

正确答案

A B C D

下一题

多选题 (10分)

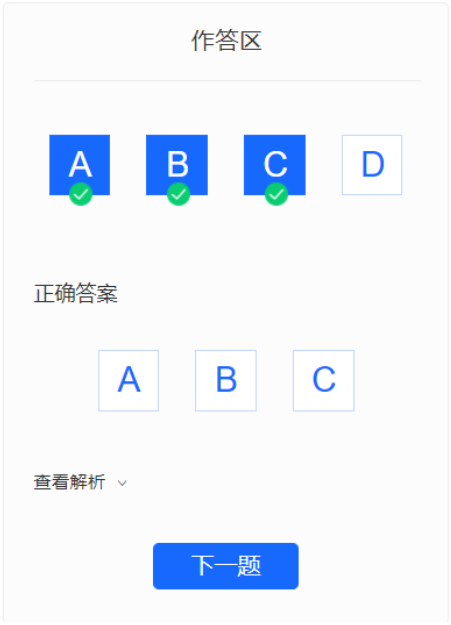
使用虚拟机进行恶意代码动态分析的优点有哪些（）

A 与物理系统隔离

B 恶意代码的执行过程是高度可控的

C 恶意代码的清除比较容易

D 虚拟机有逃逸漏洞



多选题 (10分)

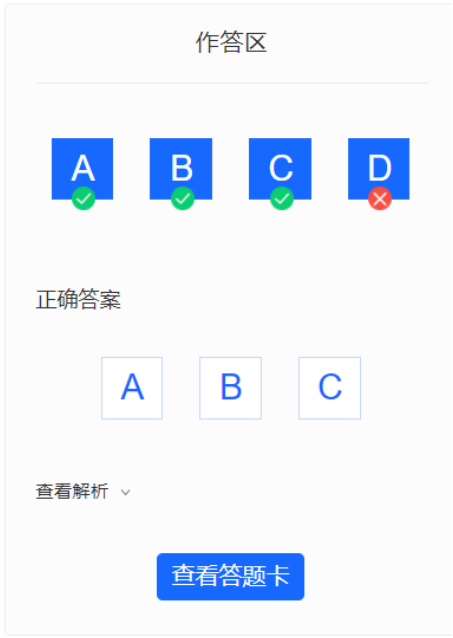
使用虚拟机进行恶意代码动态分析的风险有哪些（）

A 恶意代码可能会探测虚拟机，并改变其行为

B 虚拟机软件本身具有漏洞

C 恶意代码有可能从虚拟机中逃逸，进入物理机器中

D 恶意代码执行过程高度可控



Chapter 4

单选题 (5分)

使用沙箱进行恶意代码动态分析的优点是（）

A 沙箱只能简单地运行可执行程序，缺少命令行选项

B 沙箱中的运行环境是固定的，可能与恶意代码需要的运行环境不匹配

C 沙箱可以快速提供一份较全面的恶意代码的动态分析报告

D 恶意代码如果检测到了沙箱环境，将会停止运行，或者表现异常。

作答区

A B C D

正确答案

C

下一题

单选题 (5分)

以下哪个工具可以列出当前系统所有活跃的进程、进程载入的DLL列表、进程间的创建关系?

A Process Monitor

B Process Explorer

C 沙箱

D Regshot

作答区

A B C D

正确答案

B

下一题

```
1 ![image-20210927102625824](C:\Users\Nirvana\AppData\Roaming\Typora\typora-user-images\image-20210927102625824.png)
```

多选题 (10分)

INetSim可以模拟的网络服务有（）

A HTTP

B FTP

C IRC

D DNS

作答区

A B C D

正确答案

A B C D

下一题

单选题 (10分)

下列工具中，哪一个是网络抓包工具（）

A ApateDNS

B Netcat

C INetSim

D Wireshark

作答区

A B C D

正确答案

D

下一题

单选题 (10分)

以下哪一个工具可以模拟常见的网络服务（）

A ApateDNS

B Netcat

C INetSim

D Wireshark

作答区

A B C D

正确答案

C

下一题

判断题 (10分)

Process Monitor是Windows系统下的高级监视工具，整合了文件监视器FileMon和注册表监视器RegMon的功能，可以监控注册表、文件系统、网络、进程和线程的动态行为。

作答区

正确答案

下一题

判断题 (10分)

进程替换技术为恶意代码提供了和其他进程一样的特权，恶意代码看起来就像一个合法执行的进程一样，它在内存中的镜像会和磁盘上的一样。

作答区

正确答案

下一题

判断题 (10分)

INetSim模拟的Dummy网络服务可以记录从客户端收到的数据。

作答区

正确答案

下一题

判断题 (10分)

ApateDNS在本机上通过监听UDP的80端口，对用户指定的IP地址给出虚假的DNS响应。

作答区

正确答案

下一题

多选题 (10分)

保护进程安全的机制有哪些?

A ASLR

B DEP

C 文件镜像特征（File Image Signature）

D 内存镜像特征（Memory Image Signature）

作答区

正确答案

A C B

查看答题卡

Chapter 5

单选题 (5分)

以下哪一层是由十六进制形式的操作码和操作数组成?

A 微指令

B 机器码

C 低级语言

D 高级语言

作答区

A B C D

正确答案

B

单选题 (5分)

在获取不到高级语言源码时，（）是从二进制机器码中能可靠还原得到的最高一层语言。

A 机器指令

B 微指令

C 汇编语言

D 机器码

作答区

A B C D

正确答案

C

单选题 (5分)

内存中的（）节用于函数的局部变量和参数，以及控制程序执行流。

A 数据

B 堆

C 代码

D 栈

作答区

A B C D

正确答案

D

单选题 (5分)

而0x52000000对应0x52这个值使用的是（）字节序。

A 小端

B 大端

C 终端

D 前端

作答区

A B C D

正确答案

A

单选题 (5分)

在以下寄存器中用于定位内存节的寄存器是（）。

A 通用寄存器

B 段寄存器

C 状态寄存器

D 指令指针

作答区

A B C D

正确答案

B

单选题 (5分)

在以下寄存器中用于定位要执行的下一条指令的寄存器是（）。

A 通用寄存器

B 段寄存器

C 状态寄存器

D 指令指针

作答区

A B C D

正确答案

D

单选题 (5分)

若栈依次压入数字1、2、3、4，则最先弹出来的数字是（）

A 1

B 2

C 3

D 4

作答区

A B C D

正确答案

D

判断题 (5分)

IP地址127.0.0.1在小端字节序下，表示为0x7F000001。

作答区

正确答案

判断题 (5分)

操作数指向感兴趣的值所在的内存地址，一般由方括号内包含值、寄存器或方程式组成，如[eax]。

作答区

正确答案

判断题 (5分)

nop指令什么事情都不做。当它出现时，直接执行下一条指令。

作答区

正确答案

判断题 (5分)

sub指令会修改两个重要的标志：ZF和CF。如果结果为零，CF被置位；如果目标操作数比要减去的值小，则ZF被置位。

作答区

正确答案

判断题 (5分)

cmp指令的执行结果不影响ZF和CF标志位。

作答区

正确答案

单选题 (5分)

以下不是解释型语言的是

A Java

B Perl

C NET

D C

作答区

A B C D

正确答案

D

单选题 (5分)

在通用寄存器中，（）是数据寄存器。

A EAX

B EBX

C ECX

D EDX

作答区

A B C D

正确答案

D

单选题 (5分)

在通用寄存器中，（）是基址寄存器。

A EAX

B EBX

C ECX

D EDX

作答区

A B C D

正确答案

B

判断题 (5分)

在x86汇编语言中，一条指令由一个助记符，以及零个或多个操作数组成。

作答区

正确答案

单选题 (5分)

存储栈顶内存地址的CPU寄存器是（）

A EBP

B ESP

C EIP

D EDX

作答区

A B C D

正确答案

B

判断题 (5分)

栈顶的内存地址比栈底的内存地址大

作答区

正确答案

单选题 (5分)

mov eax, 0xFFFFFFFF
inc eax
指令执行之后CPU标志寄存器的值是（）

A cf=0, zf=0

B cf=0, zf=1

C cf=1, zf=0

D cf=1, zf=1

作答区

A B C D

正确答案

B

多选题 (5分)

以下哪些指令会对栈进行操作?

A call

B ret

C push

D pop

作答区

A B C D

正确答案

D C B A

Chapter 6

单选题 (10分)

以下哪个窗口是操作和分析二进制的主要位置，也是反汇编代码所在的地方

A 函数窗口

B 结构窗口

C 反汇编窗口

D 二进制窗口

作答区

A B C D

正确答案

C

多选题 (10分)

IDA pro 有以下哪些功能?

A 识别函数

B 标记函数

C 划分出局部变量

D 划分出参数

作答区

A B C D

正确答案

A B C D

单选题 (10分)

用IDA Pro对一个程序进行反汇编时，字节偶尔会被错误的分类。可以对错误处按（）键来取消函数代码或数据的定义。

A C键

B D键

C shift+D键

D U键

作答区

A B C D

正确答案

D

单选题 (10分)

可以按（）键重新定义原始字节为代码。

A C键

B D键

C shift+D键

D U键

作答区

A B C D

正确答案

A

判断题 (10分)

当重命名时，只需要在一个地方重命名，新名字会自动扩展到被引用的地方

作答区

正确答案

判断题 (10分)

除非有上下文，否则通常情况下，数据在IDA Pro中以八进制格式显示。

作答区

正确答案

多选题 (10分)

在IDA Pro中可以搜索一下哪些内容?

A 字符串（String）

B 立即数（Immediate）

C 字节（Byte）

D 字节序列（Byte Sequence）

作答区

正确答案

A B C D

判断题 (10分)

如果一个函数被调用，函数的局部变量的内存地址相对于epb的偏移是一个正整数。

作答区

正确答案

查看解析

多选题 (10分)

IDA Pro支持下面哪些数据的显示格式?

A 二进制

B 八进制

C 十进制

D 十六进制

作答区

正确答案

A B C D

判断题 (10分)

Windows API函数的调用约定（Calling Convention）是__cdecl

作答区

正确答案

查看解析

Chapter 7

单选题 (10分)

下列汇编代码中，使用了全局变量的是（）

A mov eax,dword_40CF60

B mov eax,[ebp-4]

C mov eax,[ebp+var_4]

D add eax,1

作答区

A B C D

正确答案

A

单选题 (10分)

以下语句不正确的是（）

A 比较（cmp）语句的结果可以决定后面条件跳转的结果

B 条件跳转指令jnz可以判断cmp指令比较的两个值是否不相等，如果两个值不相等，这个跳转就会发生

C 跳转指令jump不会产生代码路径的分支

D 对于一个if语句必定有一个条件跳转指令，所有条件跳转指令也都对应一个if语句结构

作答区

A B C D

正确答案

D

多选题 (10分)

微软__fastcall约定备用的寄存器是（）

A EAX

B EBX

C ECX

D EDX

作答区

A B C D

正确答案

C D

多选题 (10分)

() 是Windows API使用的调用约定

A __cdecl

B __stdcall

C __fastcall

D 压栈与移动

作答区

A B C D

正确答案

B C

单选题 (10分)

参数从右到左按序压入栈，当函数完成时由调用者(Caller)清理栈的调用约定是（）

A __cdecl

B __stdcall

C __fastcall

D 压栈与移动

作答区

A B C D

正确答案

A

单选题 (10分)

以下代码分析错误的是（）。

A jnz为条件跳转，jmp为无条件跳转

B while循环与for循环的汇编代码非常相似，唯一的区别在于while循环缺少一段递增代码

C while循环停止重复执行的唯一方式，就是那个期望发生的条件跳转

D while循环总要进入一次

作答区

A B C D

正确答案

D

单选题 (10分)

下列论述错误的是（）

A 数组是相似数据项的有序集合

B 结构体和数组相似，但是结构体可以包括不同类型的元素

C 链表的访问次序必须与链表数据在内存上的存储次序一致

D 在汇编代码中，数组是通过使用一个基地址作为起始点来进行访问的。

作答区

A B C D

正确答案

C

判断题 (10分)

微软Visual Studio编译器和GNU GCC编译器对函数参数的传递使用了不同的CPU指令。VS将函数参数通过PUSH指令压到栈上，GCC将函数参数通过MOV指令移动到栈上。

作答区

正确答案

判断题 (10分)

switch语句被程序员用来做一个基于字符或者整数的决策。例如，后门通常使用单一的字节值从一系列动作中选择一个。switch语句通常以两种方式被编译；使用if方式或使用跳转表。

作答区

正确答案

判断题 (10分)

结构体通过一个作为起始指针的基地址来访问。要判断附近的数据字节类型是同一结构的组成部分，还是只是凑巧相互挨着是比较困难的，这依赖于这个结构体的上下文。

作答区

正确答案

Chapter 8

单选题 (10分)

在Win32编程中，DWORD数据类型对应的C++数据类型是（）

A int

B unsigned int

C float

D char

作答区

正确答案

B

下一题

多选题 (10分)

以下哪些数据类型的长度是4个字节（）？

A BOOL

B HANDLE

C DWORD

D BOOLEAN

作答区

正确答案

A B C

查看解析

下一题

单选题 (10分)

使用匈牙利命名法（Hungarian Notation Convention）的Win32编程中，一个变量名为pszMyString，根据前缀信息可以判断该变量的数据类型为（）

A 句柄

B 注册表键值

C 字符串指针

D 类

作答区

A B C D

正确答案

C

查看解析

下一题

多选题 (1分)

每个Windows句柄都对应一个系统资源，Win32编程中对句柄的操作有（）

A 存储句柄

B 使用API访问句柄对应的系统资源

C 对句柄进行算数运算

D 将句柄作为指针使用

作答区

A B C D

正确答案

A B

查看解析

下一题

单选题 (10分)

注册表键值
“HKEY_LOCAL_MACHINE\Software\Microsoft\Windows”
中，根键（Root Key）是（）

A HKEY_LOCAL_MACHINE

B Software

C Microsoft

D Windows

作答区

A B C D

正确答案

A

下一题

单选题 (10分)

Windows API函数名的后缀可以表示函数参数的数据类型，以下哪个后缀表示函数可以输入宽字符字符串作为参数（）

A A

B W

C Ex

作答区

A B C

正确答案

B

下一题

多选题 (10分)

互联网是黑客控制远程被病毒感染机器的主要通道，一般被感染的计算机会调用的网络函数有（）

A connect ()

B listen ()

C accept ()

D socket ()

作答区

A B C D

正确答案

A D

下一题

单选题 (10分)

动态链接库的主函数名是（）

A main ()

B DriverEntry ()

C DllMain ()

D WinMain

作答区

A B C D

正确答案

C

下一题

单选题 (10分)

分配时间片的最小对象是（）

A 应用程序

B 进程

C 线程

D 函数

作答区

A B C D

正确答案

C

下一题

单选题 (10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

作答区

A B C D

正确答案

B

查看答题卡

Chapter 9

多选题 (10分)

以下哪个工具可以看到恶意代码CPU指令的执行过程?

A 源码级调试器

B 反汇编级调试器

C ProcessMonitor

D IDA Pro

作答区

A B C D

正确答案

B

下一题

多选题 (10分)

下面哪种调试过程需要使用两台连接到一起的电脑?

A 源码级调试过程

B 内核模式的反汇编调试过程

C 用户模式的反汇编调试过程

作答区

A B C

正确答案

B

下一题

多选题 (10分)

下面哪种恶意代码的动态调试操作可能会错过重要的恶意行为?

A 单步执行 single-step

B 单步步入 step-into

C 单步步过 step-over

D 执行到函数返回 step-out

作答区

A B C D

正确答案

C D

下一题

多选题 (10分)

下面哪种恶意代码的动态调试操作可以进入到被调用函数的入口地址?

A 单步执行 single-step

B 单步步入 step-into

C 单步步过 step-over

D 执行到函数返回 step-out

作答区

A B C D

正确答案

A B

下一题

多选题 (10分)

以下哪种断点（breakpoint）类型使用的是中断3?

A 软件断点

B 硬件断点

C 条件断点

D 内存断点

作答区

A B C D

正确答案

A C

下一题

多选题 (10分)

下面哪种断点的设置需要修改二进制代码?

A 软件断点

B 硬件断点

C 条件断点

D 内存断点

作答区

A B C D

正确答案

A C

下一题

多选题 (10分)

基于DR寄存器的硬件断点，最多可以设置几个?

A 1

B 4

C 8

D 任意多个

作答区

A B C D

正确答案

B

下一题

多选题 (10分)

当恶意代码在被动态调试过程中，如果触发了系统异常，下面哪些异常处理过程会被启动?

A 调试器的第一次调试（first chance）

B 调试器的第二次调试（second chance）

C SEH异常处理

D INT3中断

作答区

A B C D

正确答案

A B C

下一题

9/10

进度：已完成 9/10 题 答题卡

多选题 (10分)

调试器使用的单步执行操作，是基于哪种系统异常机制来实现的?

A INT3中断

B 内存访问权限

C DR寄存器

D CPU标志寄存器的Trap Flag

作答区

A B C D

正确答案

D

下一题

10/10

进度：已完成 10/10 题 答题卡

多选题 (10分)

以下哪些操作可以基于调试器的二进制代码修改来实现?

A 跳过一个函数的执行

B 修改一个函数执行时的参数

C 软件破解（software cracking）

D 代码复用（code reuse）

作答区

A B C D

正确答案

A B C D

查看答题卡

Chapter 10

单选题 (10分)

下列关于OllyDbg运行恶意代码说法错误的是（）。

A OllyDbg有几种调试恶意代码的方法，可以直接加载可执行文件，也可以加载DLL程序

B 如果恶意代码已经在系统上运行，可以通过附加进程的方式调试它

C OllyDbg是一个灵活的调试器，可以用命令行选项运行恶意代码，支持执行DLL中某个函数

D 可以在加载恶意代码程序之前给OllyDbg传入命令行参数

作答区

A B C D

正确答案

D

下一题

单选题 (10分)

多数DLL会在PE头的（）打包一个修订位置的列表。

A .text节

B .data节

C .rsrc节

D .reloc节

作答区

A B C D

正确答案

D

下一题

单选题 (10分)

OllyDbg最多同时设置（）个内存断点。

A 1个

B 2个

C 4个

D 任意多个

作答区

A B C D

正确答案

A

下一题

单选题 (10分)

OllyDbg使用了一个名为（）的虚拟程序来加载DLL。

A rundll32.exe

B user32.dll

C kernel32.dll

D loaddll.exe

作答区

A B C D

正确答案

D

下一题

单选题 (10分)

以下说法错误的是（）。

A OllyDbg可以很容易修改实时数据，如寄存器和标志。它也可以将汇编形式的修补代码直接插入到一个程序

B OllyDbg可以使用00项或nop指令填充程序

C 键单击高亮的条件跳转指令，然后选择Binary→Fill with NOPs，该操作产生的结果时NOP指令替换了JNZ指令，这个过程会把那个位置上的NOP永久保存在磁盘上，意味着恶意代码以后会接受任意输入的密钥

D 当异常发生时，OllyDbg会暂停运行，然后你可以使用进入异常、跳过异常、运行异常处理 等方法，来决定是否将异常转移到应用程序处理

作答区

A B C D

正确答案

C

下一题

上一单元：10.9插件、脚本调试
下一单元：实验报告

多选题 (10分)

OllyDbg提供了多种机制来帮助分析，包括下面几种（）。

A 日志（Log）

B 监视（Watch）

C Patch

D 标注（Label）

作答区

A B C D

正确答案

A B C D

下一题

多选题 (10分)

以下哪项支持Python脚本编程功能?

A OllyDump

B 调试器隐藏插件

C 命令行

D ImmDbg

作答区

A B C D

正确答案

D

下一题

多选题 (10分)

以下哪一种追踪方式可以直接恢复到单步跳过（step over）之前的状态?

A 标准回溯跟踪

B 堆栈调用跟踪

C 运行跟踪

D 内存访问跟踪

作答区

A B C D

正确答案

A

下一题

9/10

进度：已完成 9/10 题 答题卡

多选题 (10分)

以下对个各个插件说法正确的是（）。

A OllyDump是OllyDbg最常使用的插件，它能够将一个被调试的进程转储成一个PE文件

B 为了防止恶意代码使用反调试技术，恶意代码分析人员通常在分析恶意代码期间，一直运行调试器隐藏插件

C OllyDbg的命令行插件允许你用命令行来使用OllyDbg

D OllyDbg默认情况下自带书签插件，书签插件可以将一个内存位置加到书签中，利用书签，下次不需要记住就可以轻松获取那个内存地址

作答区

A B C D

正确答案

A B C D

下一题

10/10

进度：已完成 10/10 题 答题卡

多选题 (10分)

以下哪个选项可以缓解dll程序装载时的地址冲突问题?

A 确定dll的内存装载顺序

B dll程序编译时不使用编译器默认的基地址，指定一个不同的内存装载地址

C 添加.reloc节，调整因重定位（rebasing）引起的地址问题

D 所有dll都使用相同的内存装载地址

作答区

A B C D

正确答案

B C

查看答题卡

Chapter 11

单选题 (10分)

WinDbg支持通过命令来浏览内存，以下WinDbg读选项中，（）选项的命令可以读取内存数据并以ASCII文本显示。

A da

B du

C dd

D dc

作答区

A B C D

下一题

单选题 (10分)

在WinDbg中，　（）命令可以用通配符来搜索函数或者符号。

A bu

B x

C Ln

D dt

作答区

A B C D

下一题

判断题 (10分)

WinDbg支持在命令行中使用简单的算数操作符，对内存和寄存器的值进行直接的操作，如加减乘除。

作答区

下一题

判断题 (10分)

Rootkit通过修改操作系统内部函数，来隐藏自己的存在痕迹。

作答区

提交

判断题 (10分)

恶意代码与驱动通信最常使用的请求是DeviceIoControl。

作答区

提交

多选题 (10分)

下面那个选项可以被用户空间的应用程序直接访问?

A 物理设备 physical hardware

B Windows系统内核

C 设备驱动 device driver

D 设备对象 device object

作答区

A B C D

提交

多选题 (10分)

WinDbg支持以下哪些功能?

A 用户模式下的调试

B 内核模式下的调试

C rootkit病毒动态分析

D 应用程序的动态分析

作答区

A B C D

提交

多选题 (10分)

以下哪些对驱动的描述是错误的?

A 驱动负责创建和销毁设备对象（Device Object）

B 驱动被装载到内核空间中

C 应用程序可以直接访问驱动

D 驱动程序的入口函数是DriverEntry

作答区

A B C D

提交

9/10

进度：已完成 8/10 题 答题卡

多选题 (10分)

下面哪些选项是恶意Rootkit的主要攻击目标?

A kernel32.dll

B user32.dll

C ntoskrnl.exe

D hal.dll

作答区

A B C D

提交

10/10

进度：已完成 9/10 题 答题

多选题 (10分)

以下哪个选项对设备（Device）的描述是正确的?

A 物理硬件

B 由驱动程序创建

C 用户空间的应用程序不可以直接访问

D 用户空间的应用程序可以直接访问

作答区

A B C D

提交

Chapter 13

单选题 (10分)

APC可以让一个线程在它正常的执行路径运行之前执行一些其它的代码。每一个线程都有一个附加的APC队列，它们在线程处于（）时被执行。

A 阻塞状态

B 计时等待状态

C 可警告的等待状态

D 被终止状态

作答区

A B C D

正确答案

C

多选题 (10分)

Lancher的功能通常包括哪些?

A 解密、解压缩

B 隐蔽启动恶意代码

C 提升恶意代码的执行权限

D 下载恶意代码

作答区

A B C D

正确答案

A B C

多选题 (10分)

Lancher通常将要释放的恶意代码隐藏在PE文件的哪个节中?

A .text

B .data

C .resc

D .detour

作答区

A B C D

正确答案

C

多选题 (10分)

以下哪种技术需要用到CreateRemoteProcess函数?

A DLL注入

B 直接注入

C Hook注入

D APC注入

作答区

A B C D

正确答案

A B

多选题 (10分)

以下哪种隐蔽执行技术需要修改PE文件的节表?

A 进程注入

B APC注入

C Hook注入

D Detours

作答区

A B C D

正确答案

D

多选题 (10分)

以下哪种Hook技术的Hook Procedure在DLL中，需要操作系统将DLL映射到进程空间?

A Local Hooks

B High-Level Remote Hooks

C Low-Level Remote Hooks

D Rootkit

作答区

A B C D

正确答案

B

多选题 (10分)

下面对Hooks的描述哪些是错误的?

A 对所有的线程进行Hook，会增加系统的执行开销，容易被安全软件检测到

B 对一个常用的消息进行Hook，容易被安全软件发现。恶意代码一般Hook不常用的系统中不常用的消息

C 恶意代码执行起来后，会尽快调用UnhookWindowsHookEx函数，将之前的Hook从系统中删除，隐蔽其行为。

D Hook一个指定的线程比Hook全部线程实现起来更加容易

作答区

A B C D

正确答案

D

查看解析

多选题 (10分)

以下哪种注入技术需要以SUSPENDED状态启动进程?

A 进程注入

B Hook注入

C 进程替换

D APC注入

作答区

A B C D

正确答案

C

多选题 (10分)

以下哪种注入技术可以在内核空间使用?

A 进程注入

B Detours

C 进程替换

D APC注入

作答区

A B C D

正确答案

D

多选题 (10分)

进程注入需要用到的API函数有哪些?

A VirtualAllocEx

B WriteProcessMemory

C OpenProcess

D CreateRemoteThread

作答区

A B C D

正确答案

A B C D