《软件安全之恶意代码机理与防护》课程 C2 学习任务

1. 重点理解和掌握：
   a) 系统启动过程以及恶意代码可能的自启动方法（可使用 Sysinternals 工具集中的 AutoRuns 查看启动项）
   b) 熟悉二进制程序在内存中的布局情况（PE 程序本身以及在运行过程中装载的 DLL 动态链接库的开始位置和大小）
   c) 理解分页机制，熟悉 32 位及 64 位系统下 32 位及 64 位虚拟地址向物理地址转换的具体机制
   d) 熟悉磁盘的引导与分区机制（熟悉 Winhex 工具的基本用法（打开磁盘、打开分区、模板解析、扇区定位等），利用 Winhex 工具查看 MBR 分区以及 GPT 分区格式，解析自己电脑的磁盘分区，列出每一个分区的开始位置和大小），对于 MBR 分区格式下的拓展分区的解析机制，需要深入理解。
   e) 熟悉 Fat32 和 NTFS 文件系统的文件存储机制，对于 Fat32 分区，能够使用 Winhex 对已删除文件进行精准还原【文件目录项、簇链表等手工修复】，对于 NTFS 分区，能够解析具体文件的各属性，理解“数据运行（DataRun）”的概念

2. **大家在学习过程中需要回答的问题列表**
   a) 恶意软件如何在系统重启、系统重装、以及硬盘更换之后继续获得控制权？
   b) 给出在系统重启时恶意软件可以获得控制权的至少 5 种启动方式（并实践）。哪些方式不需要系统管理员权限？
   c) 每个进程可用 4GB 内存空间，但有的电脑内存才 2G！系统如何做到的？
   d) 两个进程的可执行程序映像加载地址都是 00400000H，但同一地址对应的数据却不一样，为什么？
   e) PAE 模式下，虚拟地址依然只有 32 位地址，为何可以寻址 64G 范围内的物理内存？
      i. 内存管理：物理地址扩展（PAE）分页机制 https://blog.csdn.net/trochiluses/article/details/12853027
      ii. PAE 分页模式详解：https://www.cnblogs.com/ck1020/p/6078214.html
   f) 如果硬盘分区表被完全破坏，如何重构分区表？
   g) FAT32 系统下文件被删除时，系统具体做了哪些修改？
   h) 数据擦写（安全删除）的原理什么？
   i) 在使用数据恢复软件时，为什么标准格式文件（如 doc、jpg 等）比非格式文件更容易被恢复？
   j) 在进行数据恢复时，为何有时候恢复出来的大文件只有前半部分是正确的？
   k) 恶意代码一定要在文件系统中以文件的方式出现么？它还可以隐藏在哪些区域以躲避被发现和查杀？
3. **大家在学习过程中需要进行的实际操作**
   a) 运行 hello25.exe，使用 Ollydbg（OD）查看内存布局，并进入 user32.dll 内存区域，查看 MessageBoxA 函数开始处的代码。
   b) 在自己电脑上使用 Windbg 解析 hello25.exe 程序运行时虚拟地址 0x00403000h 对应的物理地址（验证条件：物理地址与虚拟地址对应的数据应一致）。【给出操作过程的文档和操作视频】
   c) 使用 Winhex 打开自己的磁盘或者虚拟机的磁盘，对自己磁盘的分区表进行解析，给出目标电脑每个分区的开始位置与结束位置，并验证。

d) 在 FAT32 系统下删除 hello25.exe，使用 Winhex 手工恢复该程序。(可参考 C2.5.4 视频)

e) 在 NTFS 系统下，定位 Winhex.exe 在磁盘中的存储位置，定位并解析该程序的 FR 属性。

4. 本章涉及的工具列表：

a) 调试器：OllyDbg（用户态调试器），Windbg（内核调试器）

b) 编辑器：Winhex（磁盘编辑、文件编辑，注意低版本可能无法自动解析 GPT 分区格式），UltraEdit (优秀的 16 进制编辑器)，010Editor (功能强大的 16 进制编辑器)

c) 启动项枚举工具：AutoRuns

d) 虚拟磁盘：TrueCrypt（不要下载最新版本，最新版本没有创建磁盘功能）或 StrongDisk，如果自己电脑没有 FAT32 分区，可用于创建 FAT32 的虚拟分区用于实验。

e) 虚拟机软件：VMWare，如果自己磁盘不是 MBR 分区不是 32 位系统，自己可以创建一个 WinXP 的虚拟机，用于相关实验，后续也会用到 XP 虚拟机。

f) 虚拟机镜像：“恶意代码分析实战”一书提供了一个虚拟机 Win2008 镜像。