2023-2024学年《恶意代码分析与防治技术》

- 选择（2 分一个）
  - 涉及到沙盒的缺点等。是每个选项混合很多，考的比较明显，认真看过了应该都没啥问题，不是非常细致。
  - 异或计算 (给定 A 和 a 的起始 ASCII 码，挂起进程)。
  - 简单的 Yara。
- 多选（2 分一个）
  - 涉及到虚拟机的优势
  - 还有一个印象很深注册表操作的 API，有的后面有 Ex，有的没有。具体而言是 Get 没有 Ex 等任何后缀，Set 和 Open 应该是有 Ex，但没有 W。
  - 有二选和三选，没有四选应该。
- 简答（5 分一个）
  - 恶意代码分析的目的
  - 击键记录器的三种实现方式（内核 1 + 用户 2）
  - 内核态与用户态代码区别
  - 简单加密算法有哪三个及原理 + 数据识别方法
  - 写一个 Yara。涉及到十六进制表示 $a={AA ...}，文件大小，PE 文件判断还有一个和课后题很类似的 for i in (1..#a) : (@a [i]< 多少多少)
  - 进程挂起和进程注入的原理
  - 五个驻留化技术方法及原理
  - IDS,IPS,DNS 沉洞，Web 和 Email Proxy 的原理。和 DPI 相关
- 大题（一个 15 分）
  - 进程注入（DLL 注入）的代码。问你注入的进程是 svchost，为什么注入他？注入流程等。大部分代码都有。分析也很简单
  - SSDT 和 IDT 的原理，以及实现挂钩原理。+ 一个 Rootkit 定位 NtCreateFile（挂钩函数）和对应 Rootkit 模块【比较简单其实，稍微看眼实验报告就行，就找在对应地址范围内的就 ok】