2022-2023学年《恶意代码分析与防治技术》

具体题型如下：

- 10 道单选（和课上题以及学堂在线题类似）
- 5 道多选（同上）
- 8 道简答（默写）
  - 记不太清了，只记得有写出几种恶意代码并说明
  - 虚拟机的优缺点
  - 注册表的内容和？作用？
  - 提权？
  - 存活机制
  - rootkit（SSDT IDT）
  - YARA 编写规则
- 2 道大题（需要阅读给出的代码然后进行答题）
  - 我们这届考了一个 DLL 注入（主要是要对调用的那些 API 有印象，写出来工作流程是咋回事，为什么 DLL 注入）
  - 一个 WIN dbg?（写出哪有问题然后怎么用 win dbg，好像是这样，记不清了）