1.对抗反汇编

分析下述代码实际在做什么？

74 03 jz short near ptr loc\_4011C4+1

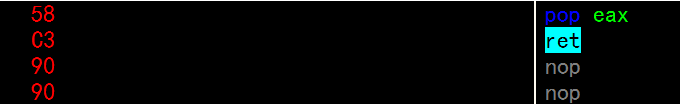
75 01 jnz short near ptr loc\_4011C4+1

loc\_4011C4:

E8 58 C3 90 90 call near ptr 90D0D521h

（提示：需自行查询机器码对应的汇编指令）

花指令auti静态反编译 实际上跳转到4011C5 执行 pop eax; ret



2.反调试

请列举出至少三个恶意代码中常见的用于反调试的API函数，并阐述原理。

IsDebuggerPesent 判断是否处于调试

CheckRemoteDebuggerPresent 判断是否处于调试（远程调试）

NtQueryInformationProcess + 参数ProcessDebugPort查询调式端口 存在则处于调试

3.反虚拟机

请列举出至少两种通用的反虚拟机技术（对VMware，VirtualBox等常见虚拟机软件都有效）。

1. GDT基址位于0xFFXXXXXX时说明处于虚拟机中
2. 扫描进程列表，是否存在敏感进程VmwareTools.exe、VMwareUser.exe等
3. TR读取的地址，当地址等于0x0040xxxx时，说明处于虚拟机中