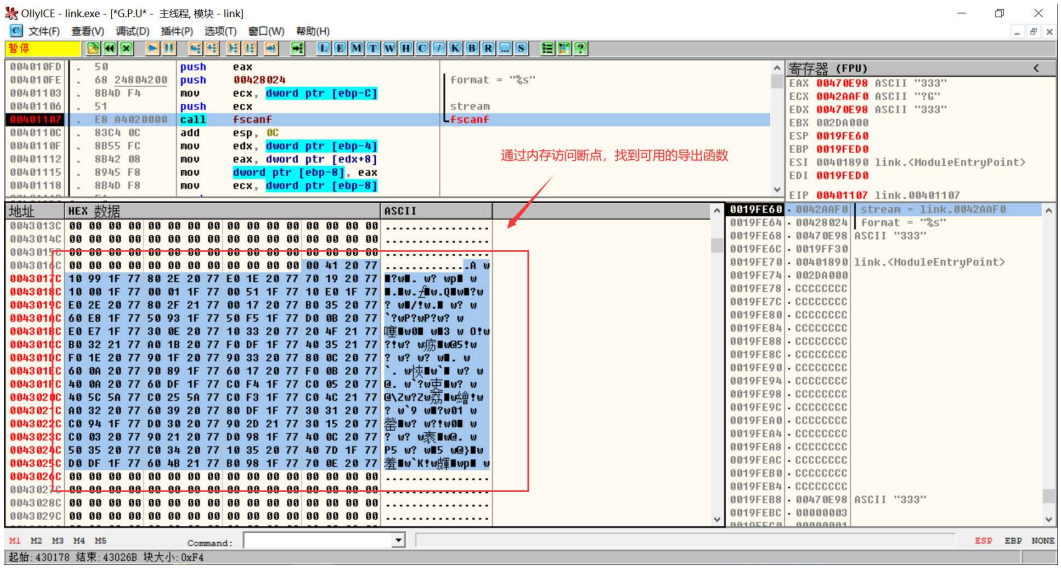
2021/04/08_shellcode_第3课_堆溢出、com漏洞挖掘

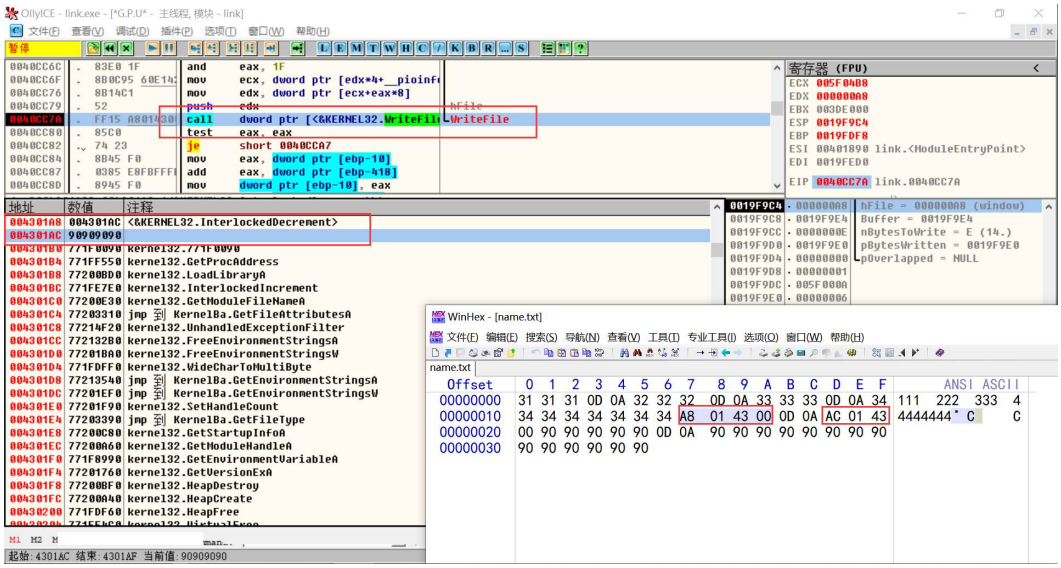
笔记本： shellcode
创建时间： 2021/4/8 星期四 10:01
作者： ileemi

堆溢出

> 堆溢出漏洞的利用相对栈溢出漏洞的利用的难度大，堆上没法锁定地址，需要根据程序上下文的环境具体分析：

- 在特定条件下，需要进可能的利用堆溢出去覆盖栈上返回地址（栈上的数据不固定）
- 通过IAT表，在程序的上下文中找到离目标点最近的API调用，将缓冲区数据进行溢出到IAT表项对应的地址，之后并将后续的IAT填为shellcode代码（此时的IAT需要可写可执行权限）。



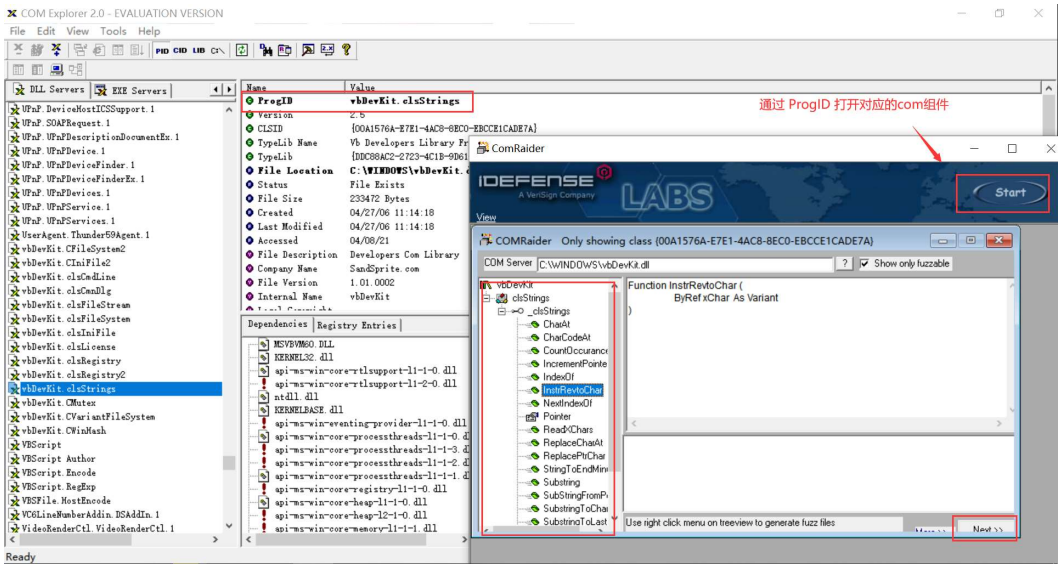


com漏洞挖掘

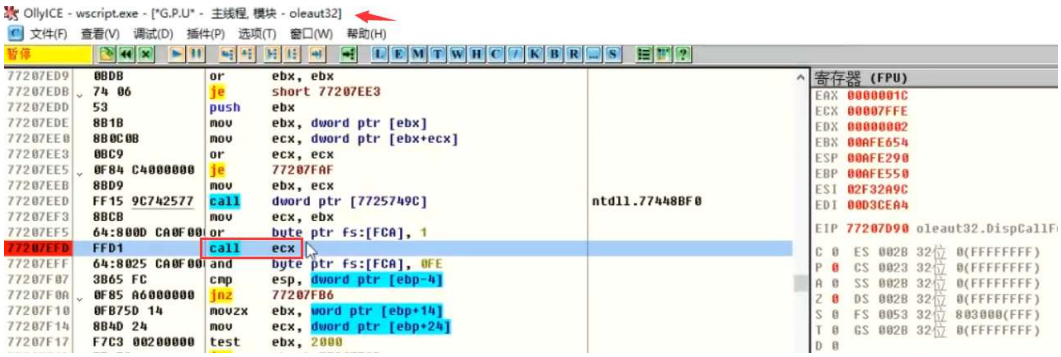
> 通过工具自动测试目标com组件，加载com组件，所有接口进行调用并传递不同长度的参数（fuzz 测试）来检测接口的稳定性。

工具：COM Explorer、COMRaider

所有的com组件都会在注册表中进行注册，通过 "COM Explorer" 可知道电脑中所有有效的com组件。



生成的 "**.wsf**" 脚本可通过 "**wscript.exe**" 程序运行。通过调试器打开 "**wscript.exe**" 程序，并将脚本作为参数对其进行调试。通过 "**oleaut32.dll**" 中的 "**DispCallFunc**" 函数内部的一个 "**call reg**" 调用，执行这条指令时，会进入到对应的com组件代码实现中。



> 《0day安全:软件漏洞分析技术》第20章有详细的使用介绍。