

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

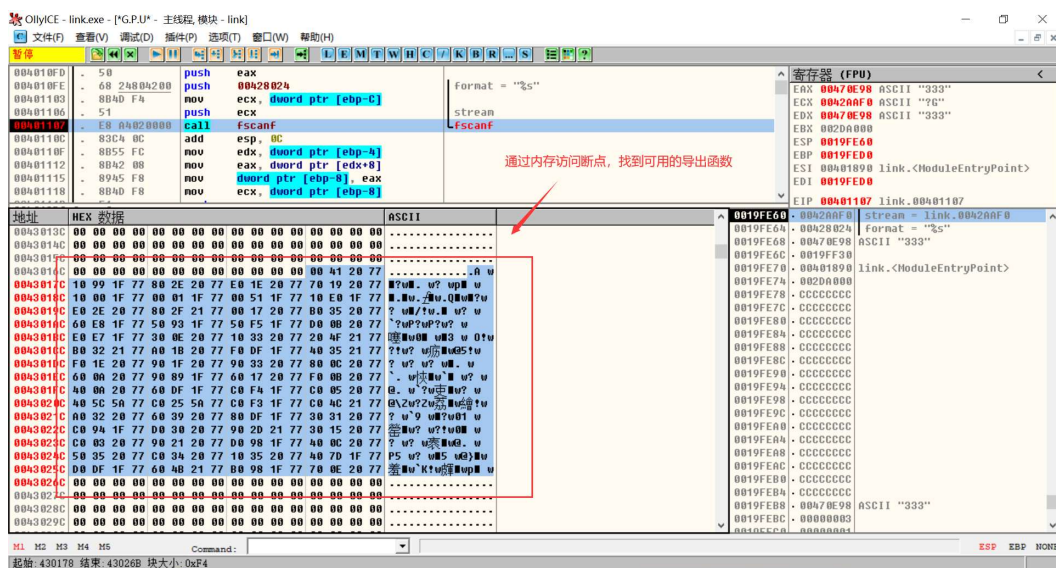
作者: ileemi

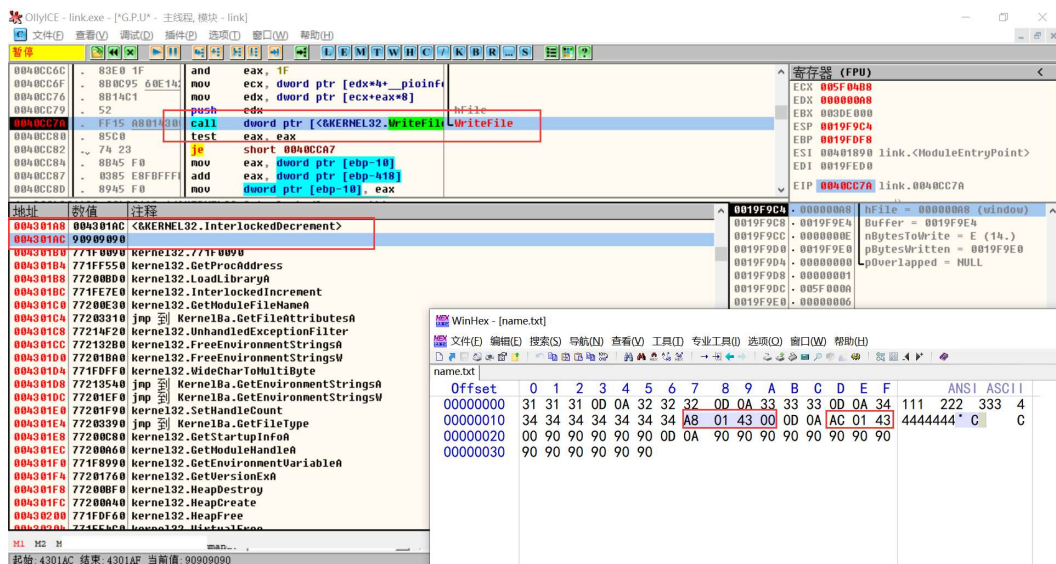
- [堆溢出](#)
- [com漏洞挖掘](#)

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，需要尽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）。



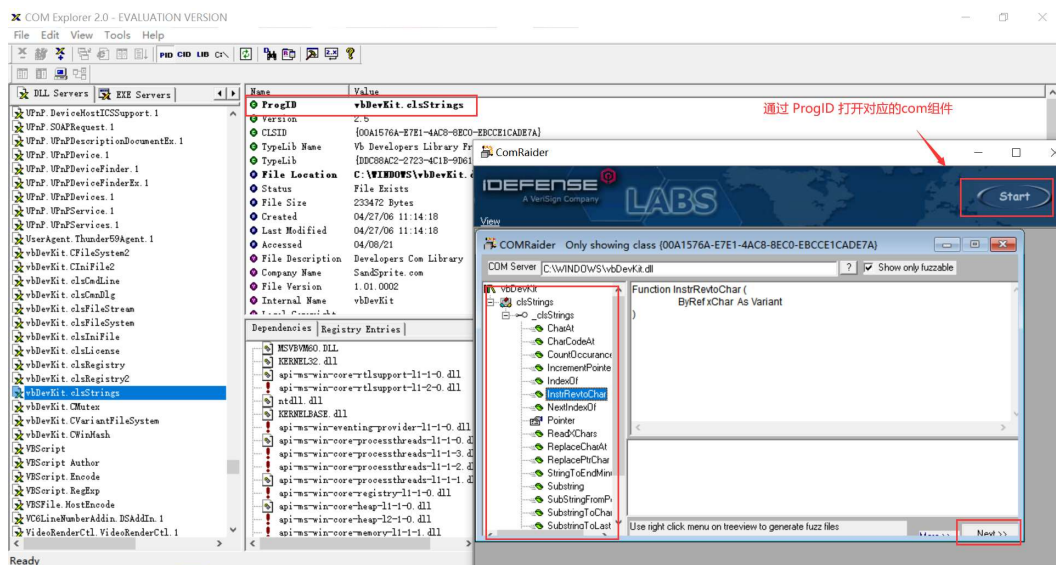


com漏洞挖掘

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。

OllyICE - wscript.exe - [G.P.U* - 主线程, 模块 - oleaut32]

文件(F) 查看(V) 调试(D) 插件(P) 选项(T) 窗口(W) 帮助(H)

77207ED9 00D8 or ebx, ebx
77207EDB 74 06 je short 77207EE3
77207EDD 53 push ebx
77207EDE 8B1B mov ebx, dword ptr [ebx]
77207EE0 8B0C0B mov ecx, dword ptr [ebx+ecx]
77207EE3 0BC9 or ecx, ecx
77207EE5 0F84 C4000000 je 77207FAF
77207EEB 8B09 mov ebx, ecx
77207EED FF15 9C742577 call dword ptr [7725749C]
77207EF3 8BCB mov ecx, ebx
77207EF5 64:800D CA0F0000 or byte ptr fs:[FCA], 1
77207EF7 FF01 call ecx
77207EFF 64:8025 CA0F0000 and byte ptr fs:[FCA], 0FE
77207F07 3B65 FC cmp esp, dword ptr [ebp+4]
77207F0A 0F85 A6000000 jnz 77207FB6
77207F10 0FB75D 14 movzx ebx, word ptr [ebp+14]
77207F14 8B4D 24 mov ecx, dword ptr [ebp+24]
77207F17 F7C3 00200000 test ebx, 2000

寄存器 (FPU)
EAX 0000001C
ECX 00007FFE
EDX 00000002
EBX 00AFE654
ESP 00AFE290
EBP 00AFE550
ESI 02F32A9C
EDI 0003CEA4
EIP 77207090 oleaut32.DispCallF
C 0 ES 002B 32 0(FFFFFFFF)
P 0 CS 002B 32 0(FFFFFFFF)
A 0 SS 002B 32 0(FFFFFFFF)
Z 0 DS 002B 32 0(FFFFFFFF)
S 0 FS 0053 32 803000(FFF)
T 0 GS 002B 32 0(FFFFFFFF)
D 0

《0day安全:软件漏洞分析技术》第20章有详细的使用介绍。