Powerkatz.dll 的利用

1. 准备：

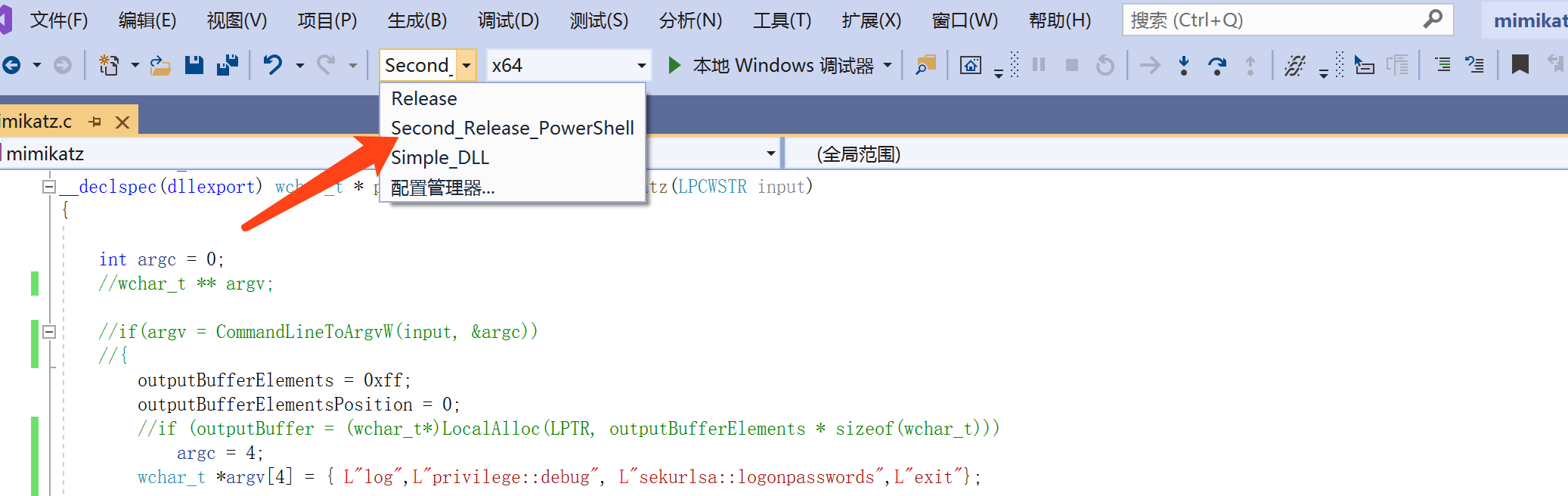
（1）mimikatz : <https://github.com/gentilkiwi/mimikatz>

(2)sRDI: <https://github.com/monoxgas/sRDI>

(3)donut:: <https://github.com/TheWover/donut>

1. 生成powerkatz.dll

VS加载mimkatz项目，作者已经预置了dll的编译方式。



在编译之前，先修改一下源代码，因为dll模式下没有交互方式，需要硬编码要执行的命令，并且没有控制台输出，需要使用 log 模式将输出保存，我修改的位置如下，就是在源代码中 dllexport的powershell\_reflective\_mimikatz函数中，添加想要执行的命令。



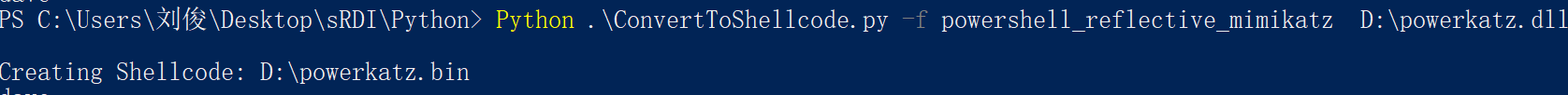
修改完保存，生成dll即可，可以用VS自带的dumpbin.exe /exports XX.dll查看导出函数。

1. 变形。

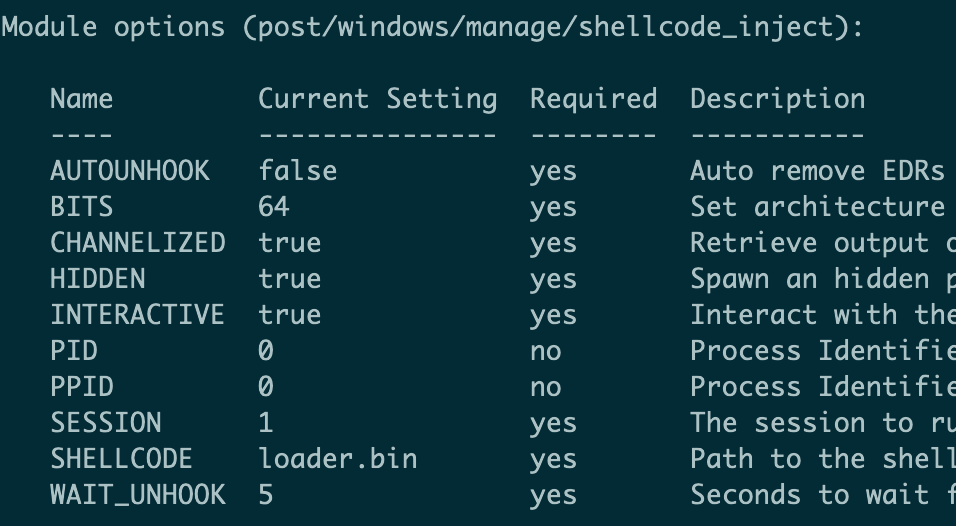
方法比较多，这里测试了sRDI（转换成反射dll注入的shellcode）和donut的shellcode转换。

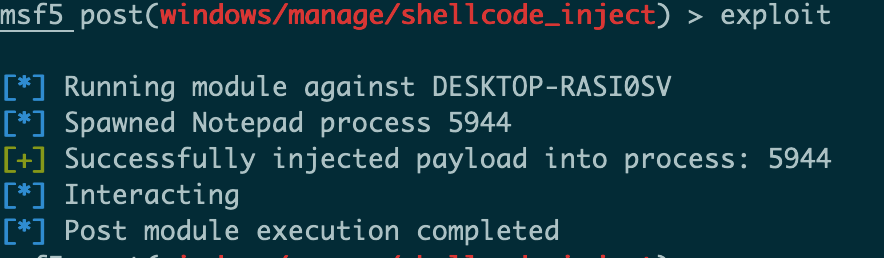
1. sRDI

使用项目中的python转换脚本，转换成shellcode



加载这个shellcode可以用sRDI项目自带的nativeloader.exe，也可以用msf 的injectshellcode

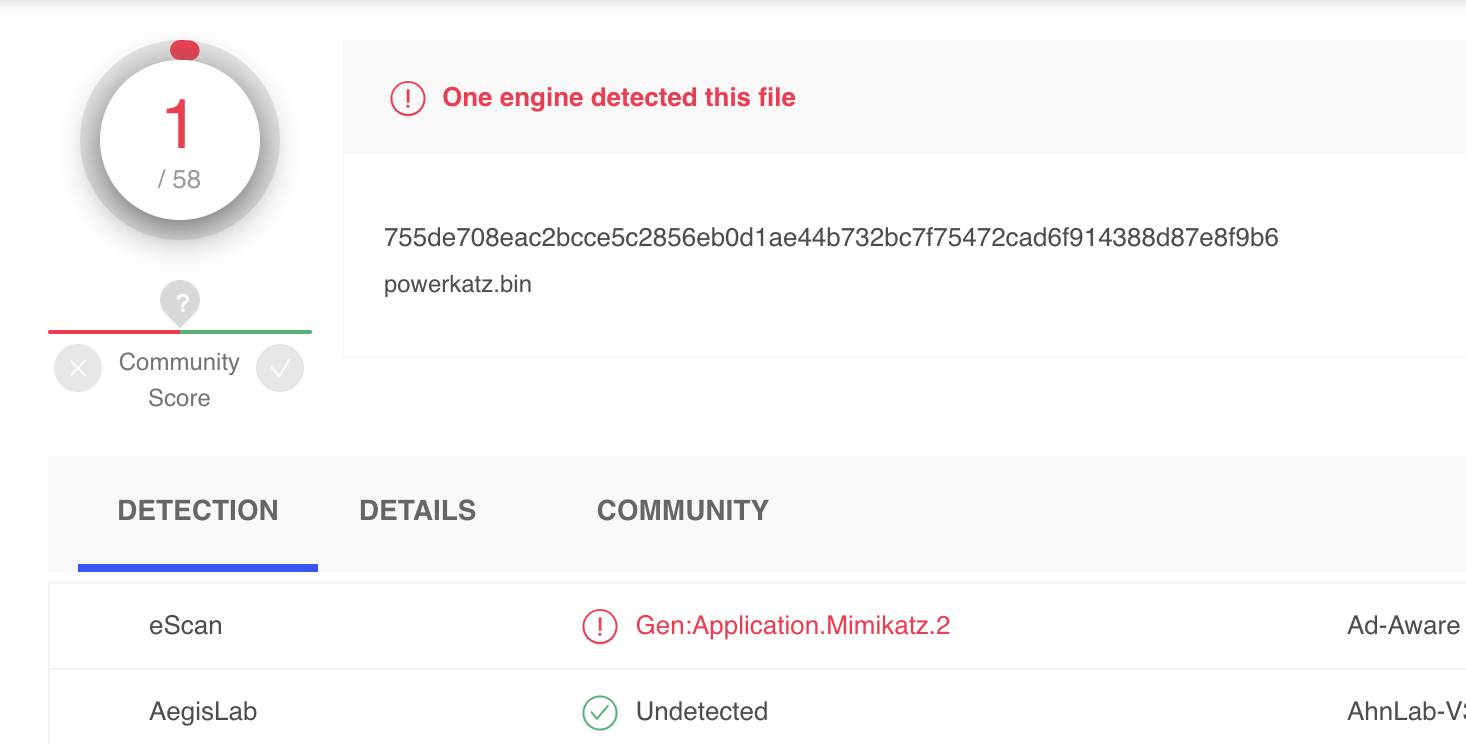




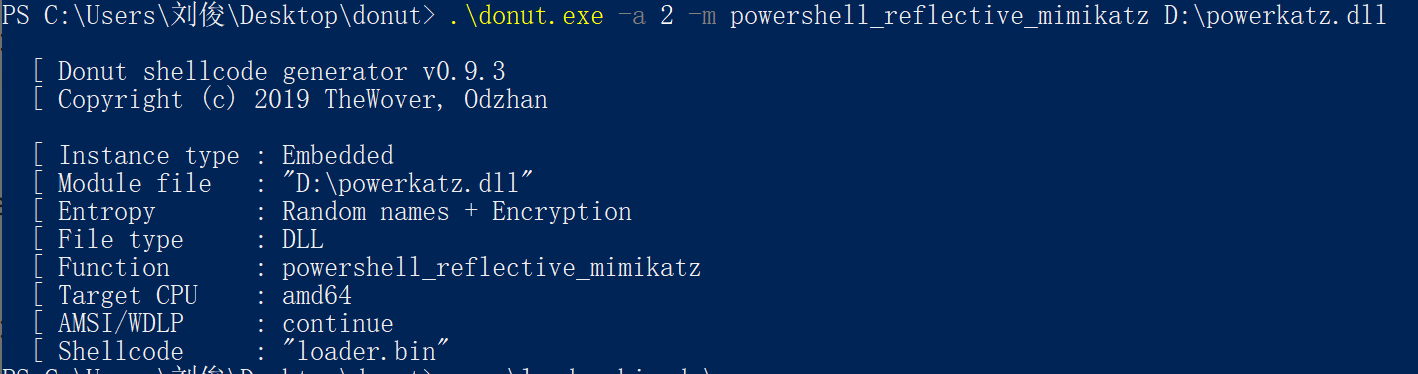
注入完成，在msf的stager文件同目录生成mimi的log文件，shell权限问题，debug模式没获取到。



Virustotal：1/58



1. donut



主要是函数名要写对。生成loader.bin后加载方式都一样，msf也可以。

Virustotal：0/57

