**厂商信息**

**公司名：**[北京奇虎科技有限公司](https://baike.baidu.com/item/%E5%8C%97%E4%BA%AC%E5%A5%87%E8%99%8E%E7%A7%91%E6%8A%80%E6%9C%89%E9%99%90%E5%85%AC%E5%8F%B8/6471948?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E5%A5%87%E8%99%8E360/_blank)

**安全产品：**360安全卫士

**漏洞基本信息**

**漏洞名称**：Windows LSASS 进程内存非法获取漏洞

**漏洞类型**：敏感信息泄露

**影响范围**：Windows 8/10

Windows server 2012/2016/2019

**漏洞等级**：高危

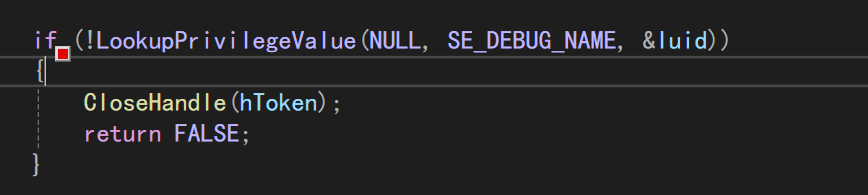
**漏洞原理**

1. **利用 SE\_DEBUG\_NAME 特权绕过进程保护，获取 LSASS 句柄。**
2. **通过内存转储获取 LSASS 中的敏感信息（NTLM 哈希、Kerberos 票据等）。**
3. **攻击者可通过 Mimikatz 等工具从转储文件中提取凭证**

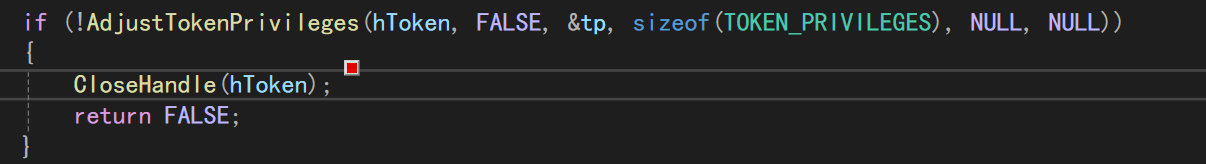
**代码功能模块审计**

**模块 1：权限提升EnableDebugPrivilege 函数（自定义）**

**关键函数（获取调试权限LUID）**

****

**关键函数（启用SE\_DEBUG\_NAME特权）**

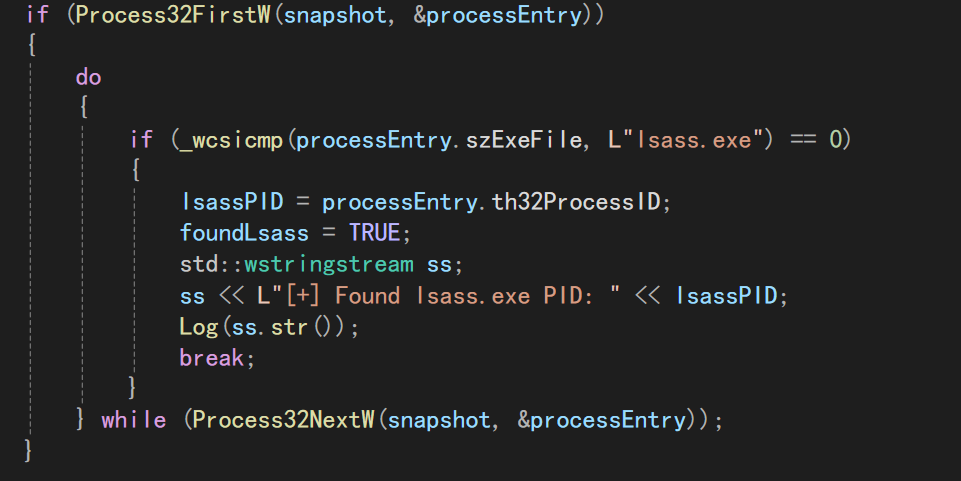
****

**模块 2：LSASS 进程定位**

**关键函数（创建进程快照）**

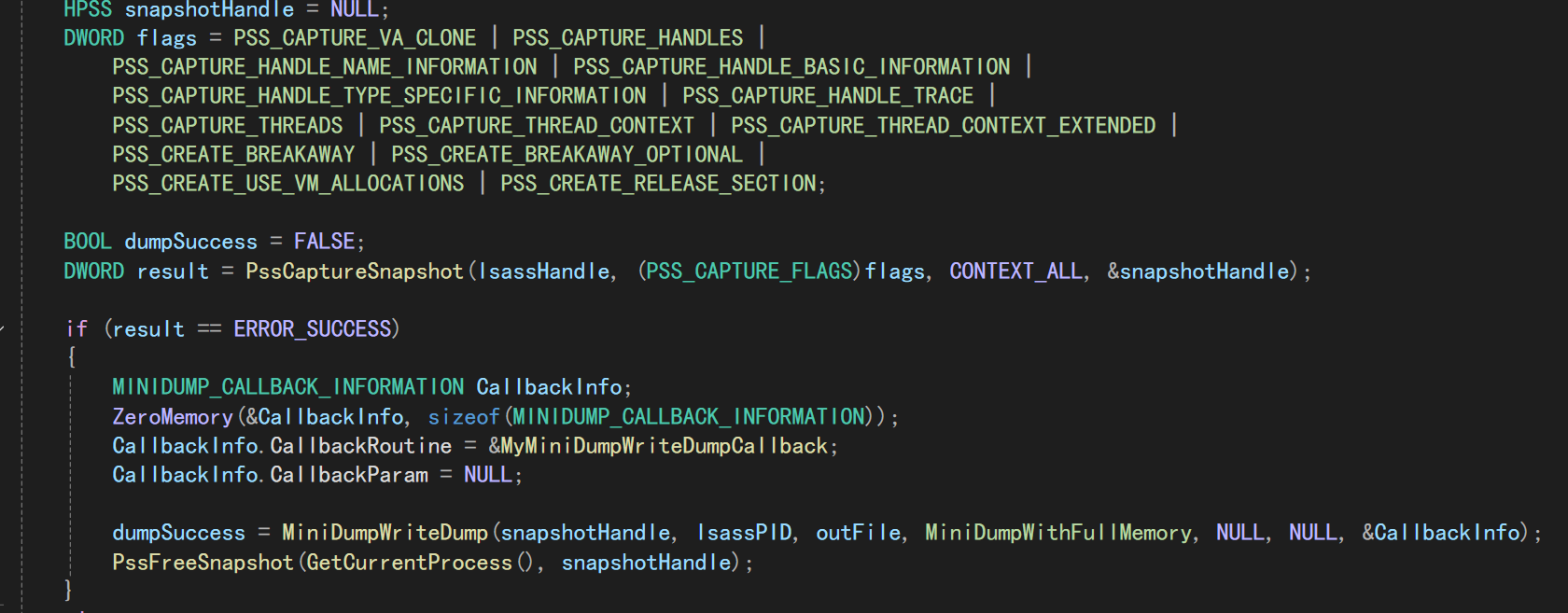
****

**关键函数（进程遍历找到lsass进程）**

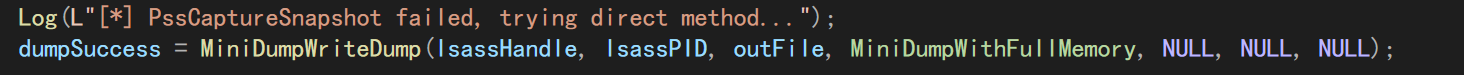
****

**模块 3：内存转储（双方法实现）**

**关键函数(方法1：PssCaptureSnapshot)**

****

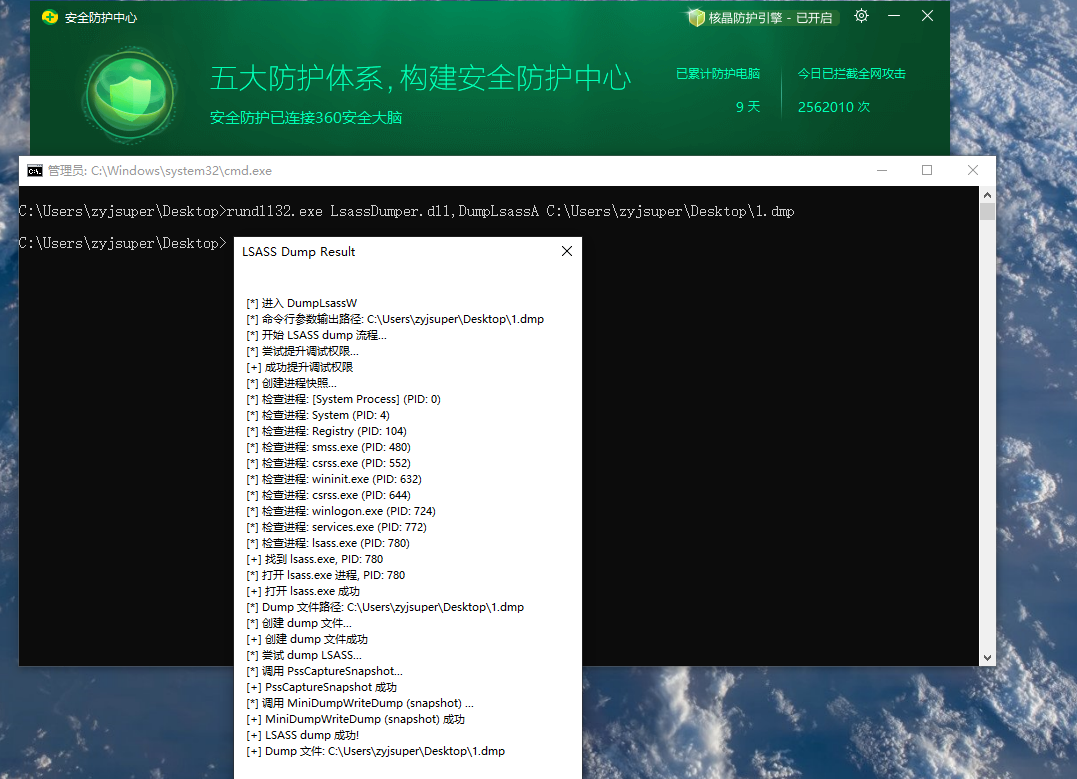
**关键函数（方法2：MiniDumpWriteDump ）**

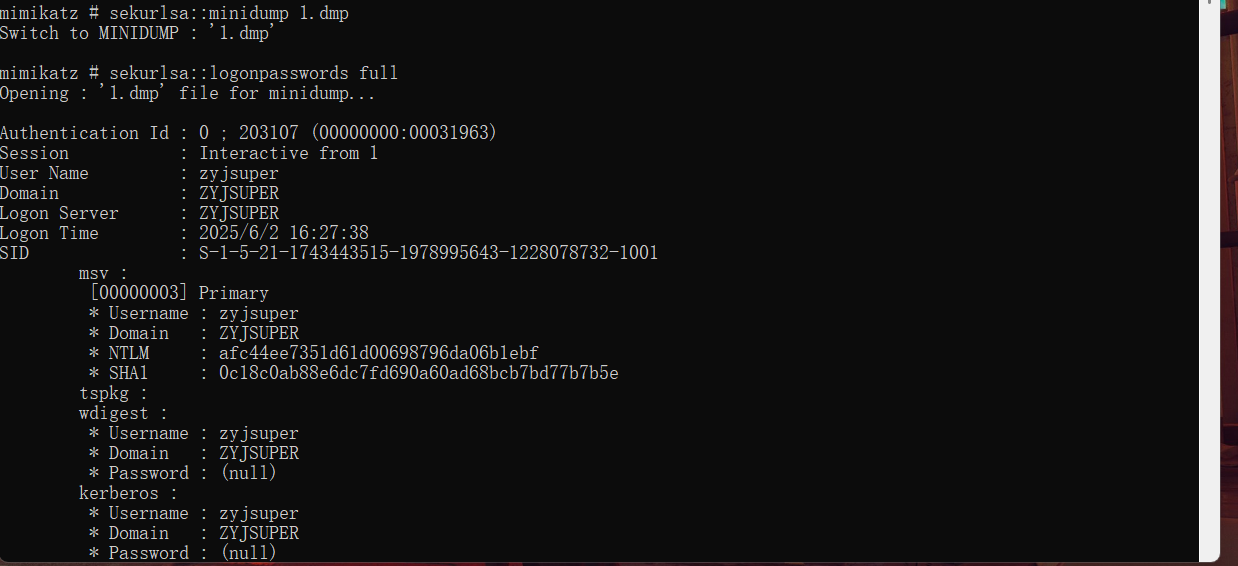
****

**代码调试运行**

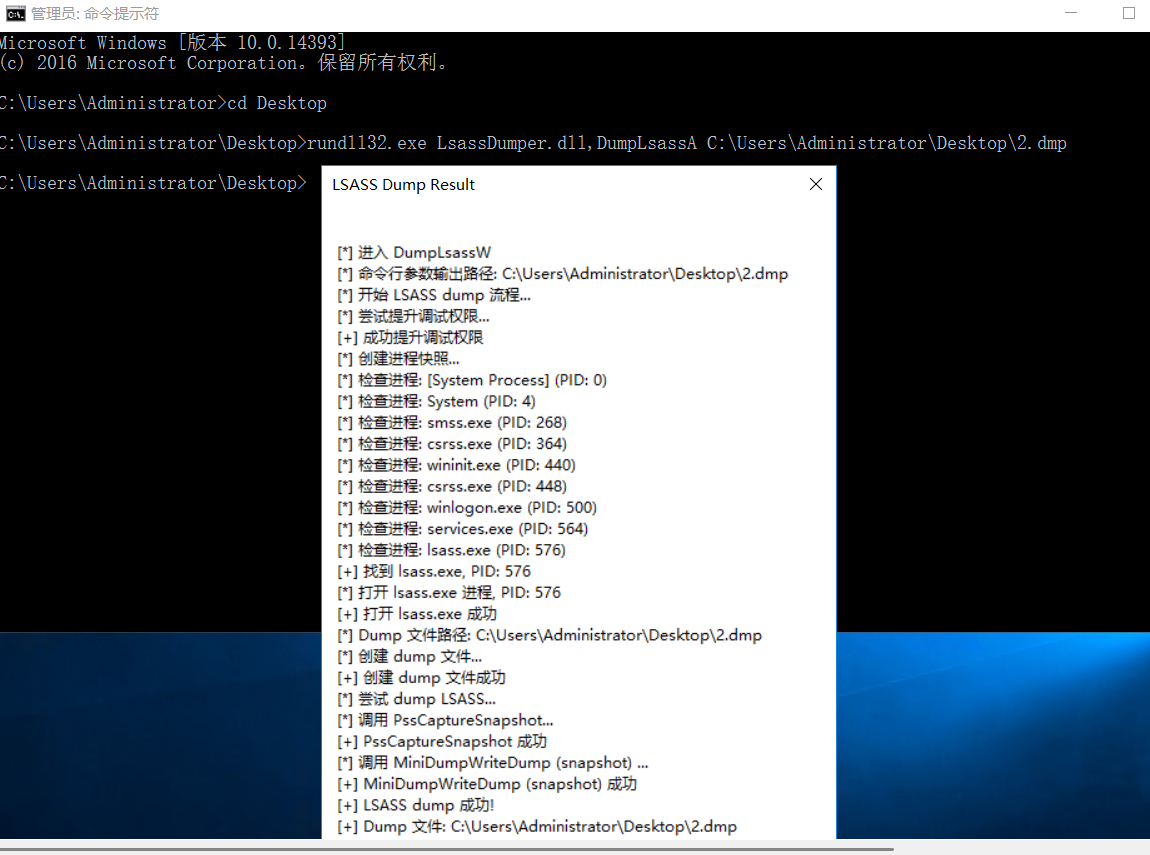
**使用弹窗调试的方法显示代码在运行过程中运行逻辑，此处演示二个环境(调试源码下载路径https://github.com/woshidaheike/360hashdump/tree/main/debug)**

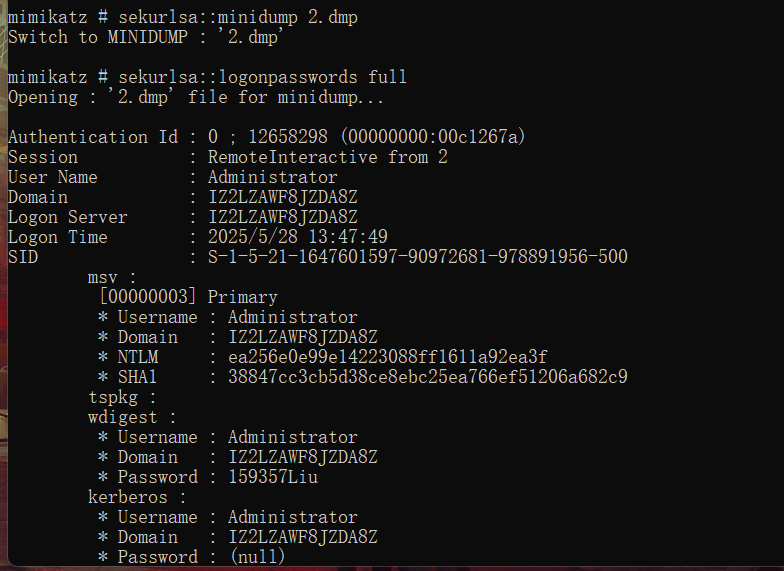
**Win10**

****

****

**Win server 2016**

****

****