**MS-EXP:**

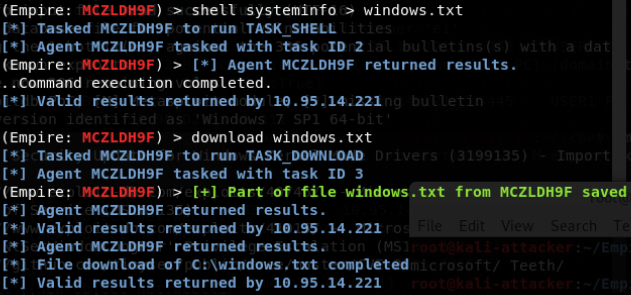
https://github.com/FuzzySecurity/PowerShell-Suite/blob/master/Invoke-MS16-032.ps1

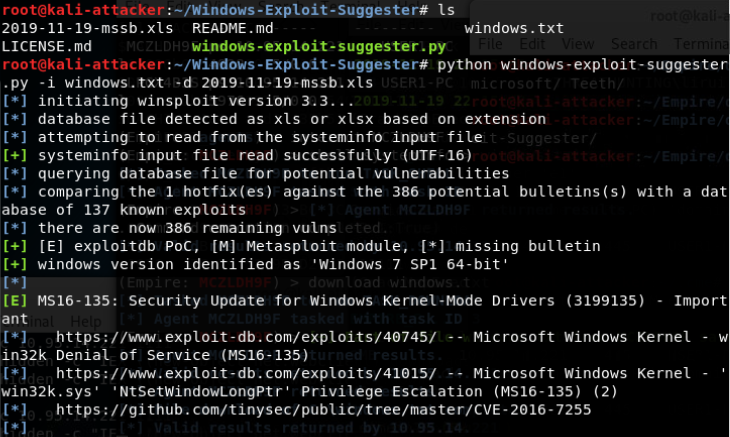
https://github.com/FuzzySecurity/PSKernel-Primitives/tree/master/Sample-Exploits/MS16-135

**check漏洞工具:**

Windows 自带默认命令systeminfo 将提取任何给定的 Windows 主机的所有补丁安装史记录。可以拿回这个输出结果，将其复制到Kali 系统并运行 Windows Exploit Suggester 以查找已知的漏洞然后针对性的进行漏洞利用从而提升权限

https://github.com/AonCyberLabs/Windows-Exploit-Suggester





**第三方软件提权、系统0day提权:**

当处在一个已经打好所有补丁的 Windows 主机环境中时，将重点关注第三方软件中的不同权限提升漏洞或操作系统的任何 0day 漏洞

https://insecure.org/search.html?q=privilege%20escalation

https://bugs.chromium.org/p/project-zero/issues/list?can=1&q=escalation&colspec=ID+Type+Status+Priority+Milestone+Owner+Summary&cells=ids

**PASS THE CACHE(MS14068)：**

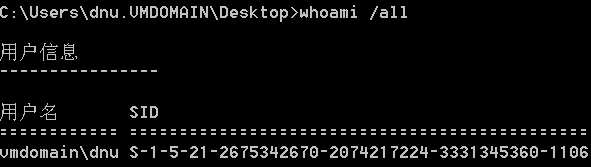
PTC:

MS14068是一个能够使普通用户提权到域控权限的权限提升漏洞，攻击者可以通过构造特定的请求包来达到提升权限的目的。

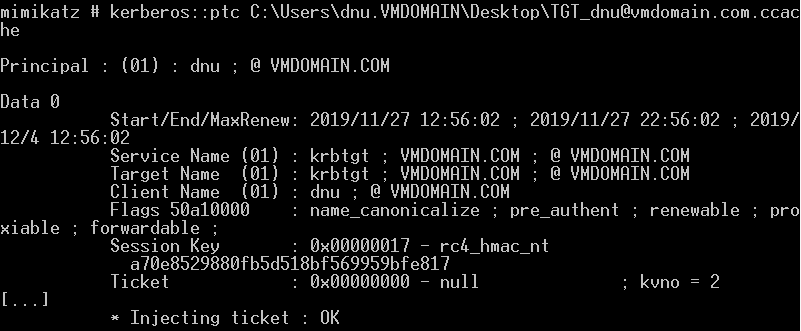
KB3011780





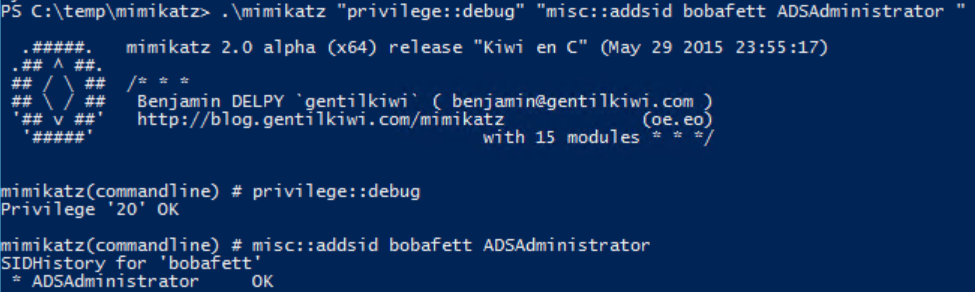


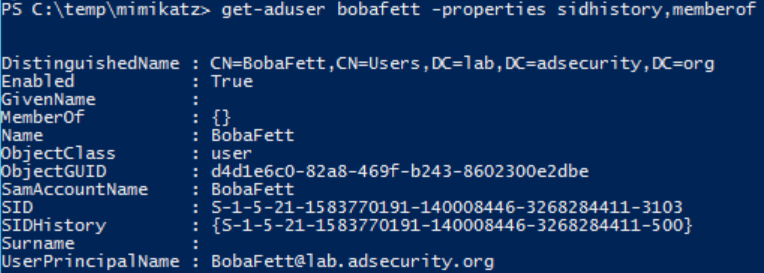






**修改域用户SID历史记录提权:**



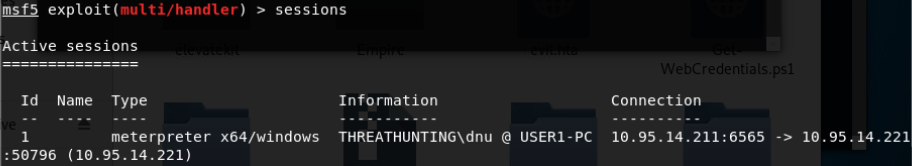


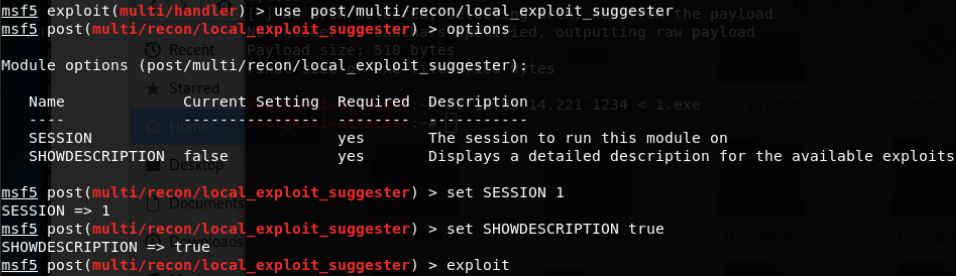
**MSF框架提权模块**

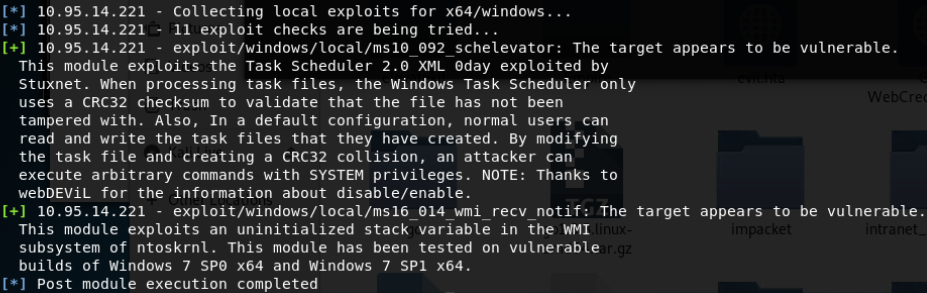
**Windows内核提权-MSF**

1.辅助提权模块

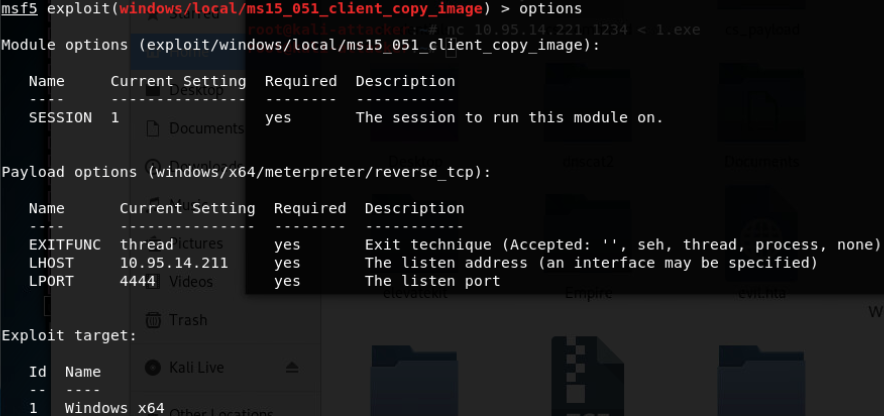
Local Exploit Suggester

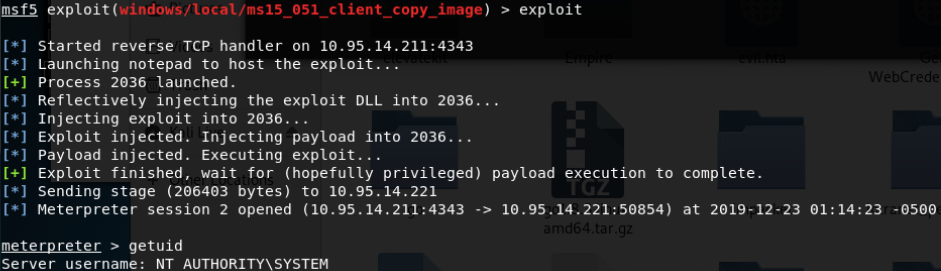




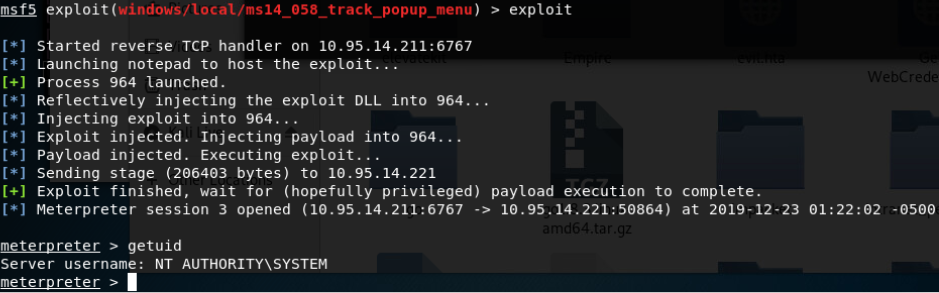
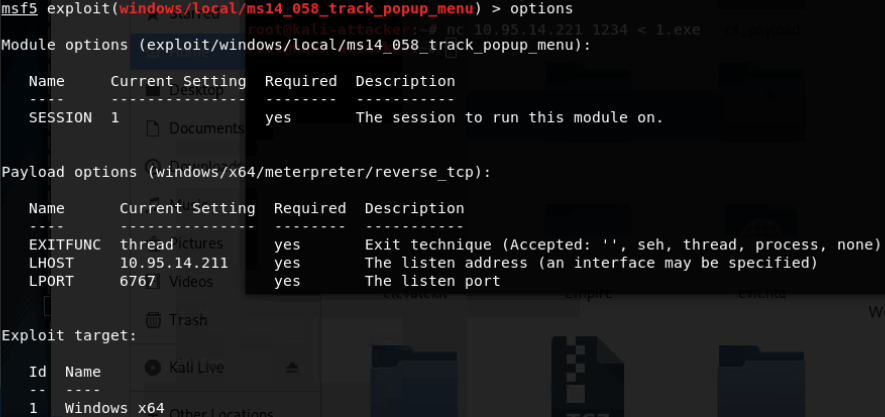


2. Windows ClientCopyImage Win32k漏洞利用(win7 32/64位/win2008R2 SP1 64位)

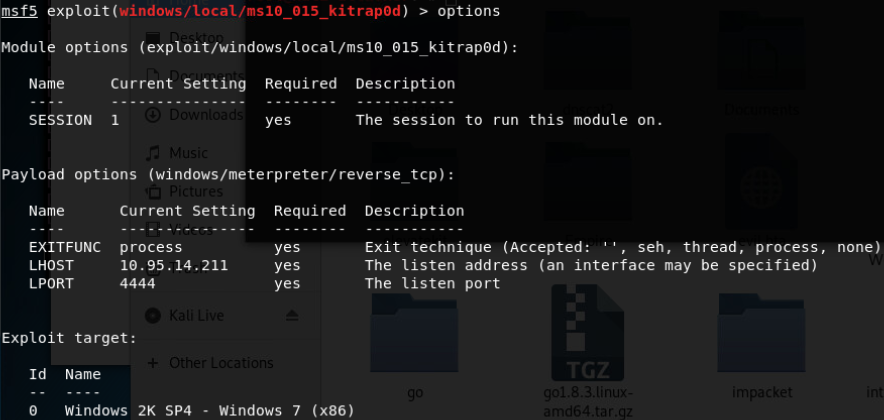




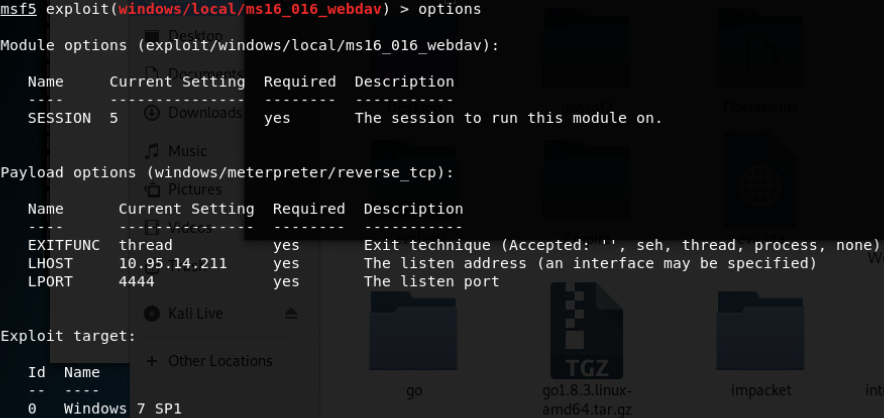
3.Windows TrackPopupMenu Win32k NULL Pointer Dereference(Windows XP SP3/Windows Server 2003 SP2/Windows7 SP1/Windows Server2008 32位/Windows Server2008R2 SP1 64位)



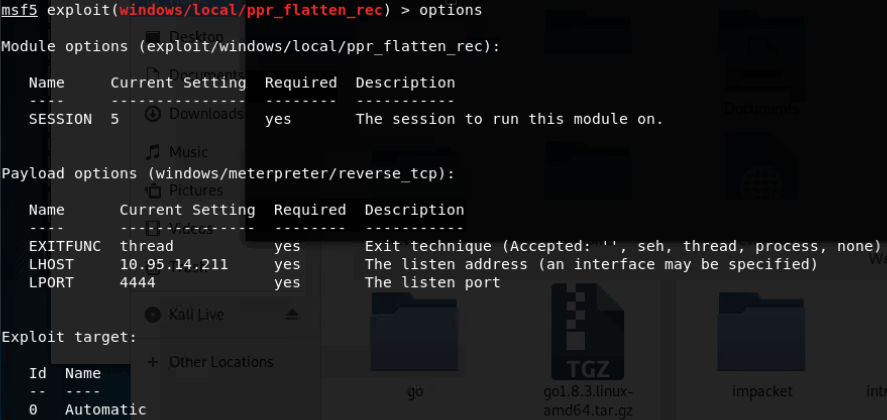
4. KiTrap0D(Windows Server 2003 32/Windows Server 2008 32位/Windows7 32位/XP 32位)



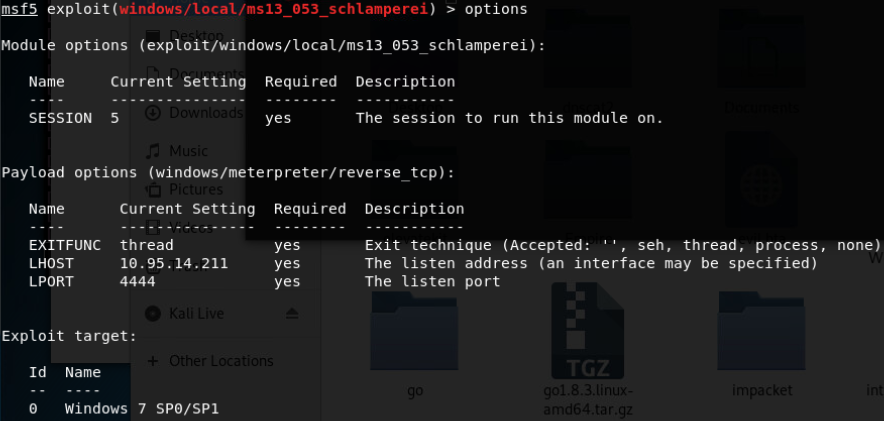
5. MS16-016 mrxdav.sys WebDav Local Privilege Escalation(win7 SP1 32位)



6. EPATHOBJ::pprFlattenRec本地提权(Windows XP SP3/Windows2003 SP1/Windows7 SP1/32位)



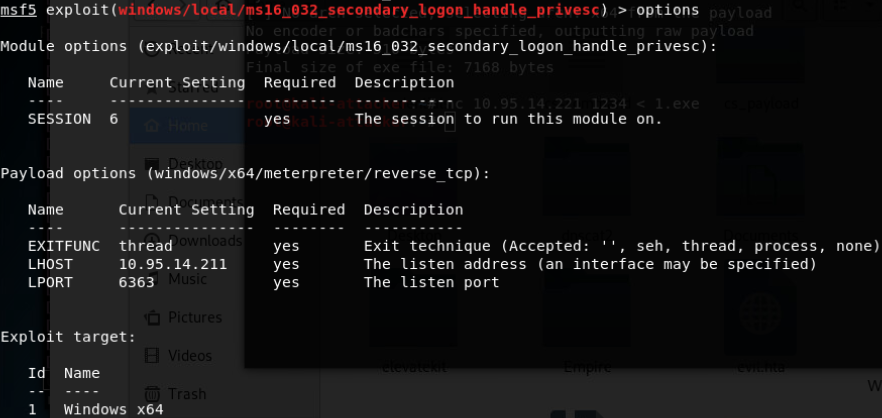
7. MS13-053：NTUserMessageCall Win32k内核池溢出(win7 32位)



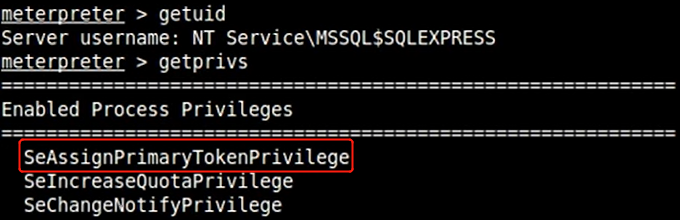
8. MS16-032 Secondary Logon Handle提权(Windows7-10/Windows Server2008/2012 32

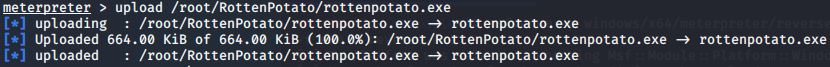
位和64位)

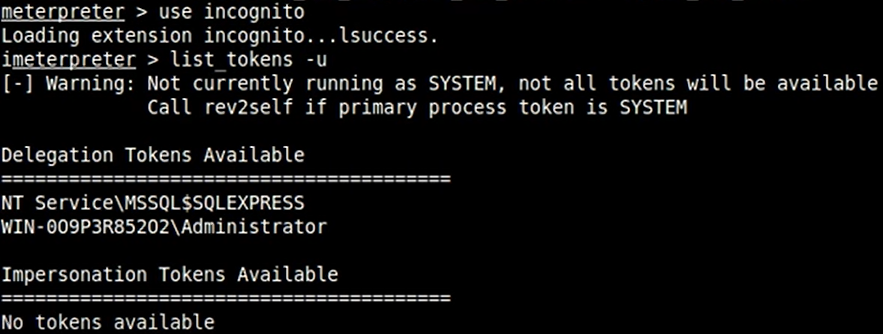
只对集成了 powershell2.0 或更高版本的Windows且具有多个CPU内核的系统有效



9. RottenPotato提权(Local Privilege Escalation from Windows Service Accounts to SYSTEM)







需要.net4.0以上环境:

https://support.microsoft.com/zh-cn/help/4054530/microsoft-net-framework-4-7-2-offline-installer-for-windows



