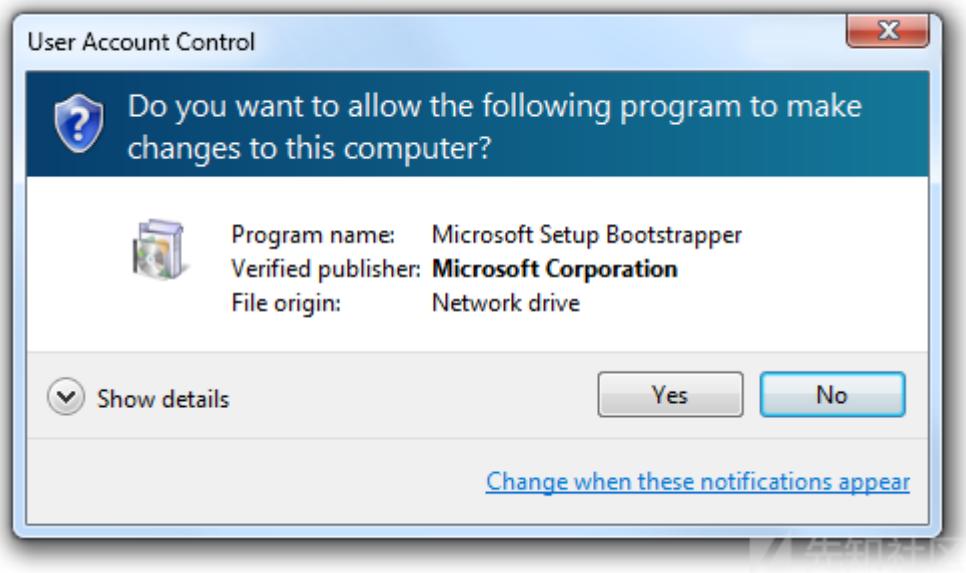
Windows 7、8、10的权限提升研究

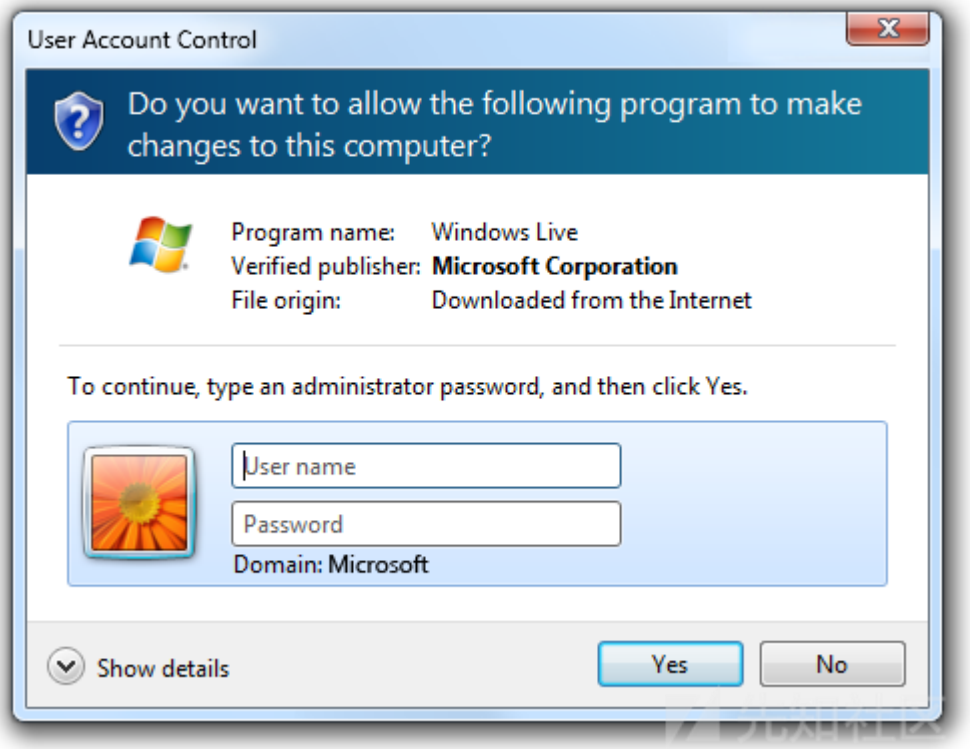
惊鸿一瞥最是珍贵 / 2019-01-20 07:38:00 / 浏览数 5318

UAC简介

在完全启用用户帐户控制(UAC)的情况下，交互式管理员通常以最小的用户权限运行，但是他们可以通过使用Consent UI提供显式准许来提升权限以执行管理任务。此类管理任务包括安装软件和驱动程序、更改系统范围的设置、查看或更改其他用户帐户以及运行管理工具。
在以最小特权运行时，管理员称为受保护的管理员，除此之外，还有超级管理员。相比之下，标准用户不能自己提升权限，但他们可以要求管理员使用Credential UI来提升他们的权限。内置管理员帐户不需要提升权限。



Contest UI，提升受保护的管理员从而获得管理权限。

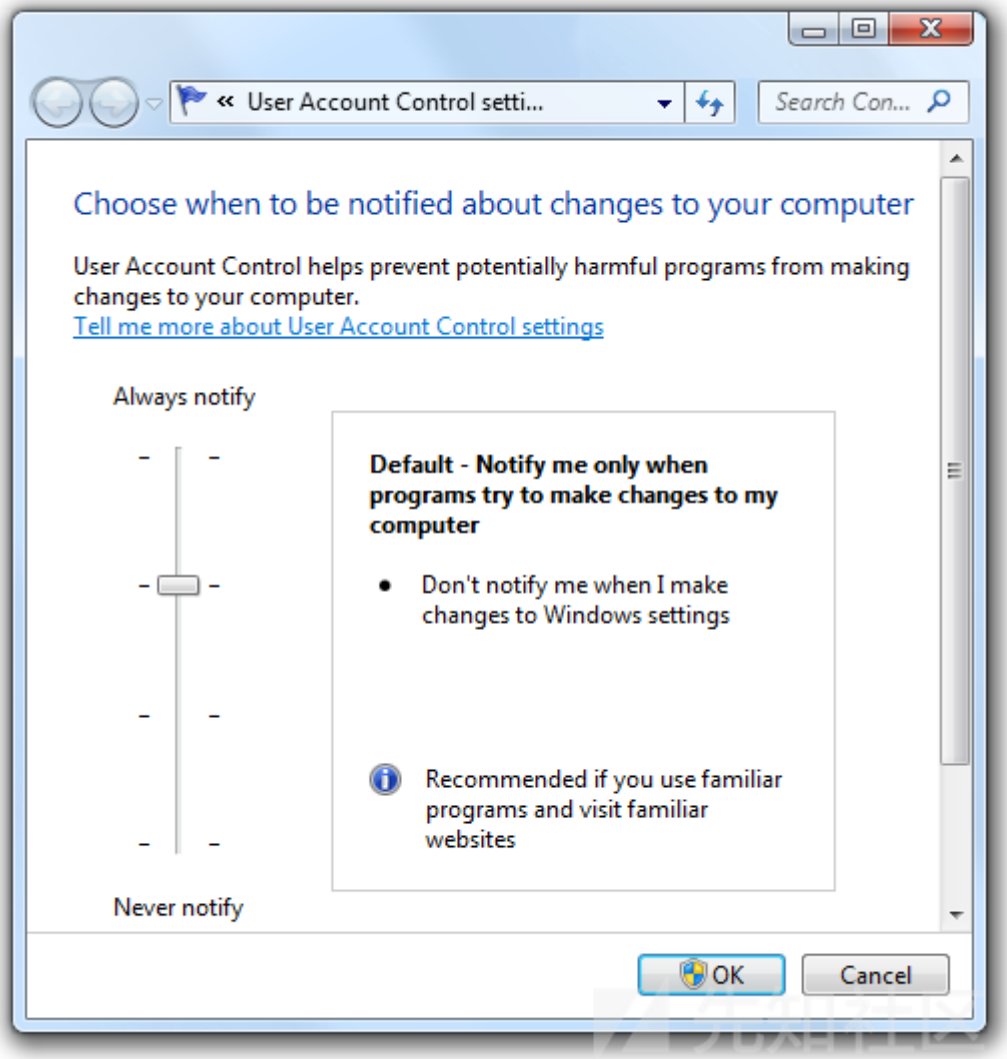


Credential UI，用于提升标准用户权限。

UAC的好处

它减少了以较高的权限运行的程序数量，因此有助于防止用户意外更改其系统设置，并有助于防止"恶意软件"获得系统范围的访问权限。拒绝提升权限，恶意软件只能影响当
与Windows Vista一样，受保护的管理员有权力决定是否收到有关所有系统更改的通知。UAC默认设置是通知所有管理员用户关于系统的更改。

收到通知后，您的桌面将变暗，您必须在UAC对话框中批准或拒绝该请求，然后才能在计算机上执行任何其他操作。桌面变暗称为安全桌面，因为其他程序在变暗时无法运行
除了Windows Vista中的两个设置外，Windows
7还为受保护的管理员引入了两个中间UAC设置。第一种方法是仅在程序进行更改时通知用户，因此管理员在自己更改程序时会自动提升权限。这是Windows
7中的UAC默认设置，它还会使用安全桌面。
Windows7中的第二个中间设置与第一个相同，只是它不使用安全桌面。



Windows7引入了两个中间UAC设置。

因此，简而言之，UAC是所有windows操作系统中存在的一个非常重要的功能，它将确保您的系统避免一些攻击，并且每次操作执行都要经过管理员权限的批准。[2]

击败Windows用户帐户控制

1.UACMe: https://github.com/hfiref0x/UACME
2.系统要求：x86-32/x64 Windows 7/8/8.1/10(TH1/TH2/RS1/RS2/RS3/RS4)(客户端，但某些方法也适用于服务器版本)。
3.需要UAC设置为默认的管理员帐户。
第一个参数是要使用的方法数量，第二个参数是要运行的可选命令(可执行文件名，包括完整路径)。第二个参数可以是空的，在这种情况下，程序将从System32文件夹执行c

No	Works in	Type	Target File(s)	Fixed in
1	Windows 7 (7600)	Dll Hijack	• \system32\sysprep\sysprep.exe • Component: cryptbase.dll	Windows 8.1 (9600)
2	Windows 8.1(9600)	Dll Hijack	• \system32\sysprep\sysprep.exe • Component: ShCore.dll	Windows 10 TP (> 9600)
3	Windows 7	Dll Hijack	• \system32\oobe\setupsqm.exe • Component:WdsCore.dll	Windows 10 TH2 (10558)
4	Windows 7 (7600)	AppCompat	• \system32\cliconfg.exe • Component: NA	Windows 10 TP (> 9600)
5	Windows 7 (7600)	Elevated COM interface	• HKLM registry keys	Windows 10 TH1 (10147)
6	Windows 7 (7600)	Dll Hijack	• \ehome\mcx2prov.exe, \system32\migwiz\migwiz.exe • Components: WdsCore.dll, CryptBase.dll, CryptSP.dll	Windows 10 TH1 (10147)
7	Windows 7 (7600)	Dll Hijack	• \system32\cliconfg.exe • Component(s): ntwdblib.dll	Windows 10 TH1 (10147)
8	Windows 7 (7600)	Dll Hijack	• \system32\sysprep\sysprep.exe	Windows 8.1 (9600)
9	Windows 7 (7600)	Dll Hijack	• IFEO registry keys, \system32\cliconfg.exe	Windows 10 TH1 (10147)
10	Windows 7 (7600)	Dll Hijack	• \system32\{New}or{Existing}\{autoelevated}.e	Windows 10 TH2 (10548)

			xe, e.g. winsat.exe • Attacker defined dll, e.g. PowProf.dll, DevObj.dll	
11	Windows 7 (7600)	Dll Hijack	• \system32\iscsicli.exe • Component(s): Attacker prepared shellcode	Windows 8.1 (9600)
12	Windows 10 TH1 (10240)	Dll Hijack	• \system32\sysprep\sysprep.exe • Component(s): dbgcore.dll	Windows 10 TH2 (10565)
13	Windows 7 (7600)	Dll Hijack	• \system32\mmc.exe EventVwr.msc • elsext.dll	Windows 10 RS1 (14316)
14	Windows 7 (7600)	Dll Hijack	• \system\credwiz.exe, \system32\wbem\oobe.exe • Component(s): netutils.dll	Windows 10 TH2 (10548)
15	Windows 7 (7600)	Dll Hijack	• \system32\cliconfg.exe • Component(s): ntwdblib.dll	Windows 10 RS1 (14316)
16	Windows 7 (7600)	Dll Hijack	• \system32\GWX\GWXUXWorker.exe,\system32\inetsrv\inetmgr.exe • Component(s): SLC.dll	Windows 10 RS1 (14316)
17	Windows 8.1 (9600)	Dll Hijack (Import forwarding)	• \system32\sysprep\sysprep.exe • Component(s): unbcl.dll	Windows 10 RS1 (14371)
18	Windows 7 (7600)	Dll Hijack (Manifest)	• \system32\taskhost.exe,\system32\tzsync.exe (any ms exe without manifest) • Component(s): Attacker defined dll	Windows 10 RS1 (14371)

19	Windows 7 (7600)	Dll Hijack	• \system32\inetsrv\inetmgr.exe • Component(s): MsCoree.dll	Windows 10 RS1 (14376)
20	Windows 7 (7600)	Dll Hijack	• \system32\mmc.exe, Rsop.msc • Component(s): WbemComn.dll	Windows 10 RS3 (16232)
21	Windows 7 (7600)	Dll Hijack	• \system32\sysprep\sysprep.exe • Component(s): comctl32.dll	Windows 10 RS3 (16232)
22	Windows 7 (7600)	Dll Hijack	• \system32\consent.exe • Component(s): comctl32.dll	Unfixed
23	Windows 7 (7600)	Dll Hijack	• \system32\pkgmgr.exe • Component(s): DismCore.dll	Unfixed
24	Windows 7 (7600)	Shell API	• \system32\CompMgmtLauncher.exe • Component(s): Attacker defined application	Windows 10 RS2 (15031)
25	Windows 7 (7600)	Shell API	• \system32\EventVwr.exe,\system32\CompMgmtLauncher.exe • Component(s): Attacker defined application	Windows 10 RS2 (15031)
26	Windows 10 TH1 (10240)	Race Condition	• %temp%\GUID\dismhost.exe • Component(s): LogProvider.dll	Windows 10 RS2 (15031)
27	Windows 7 (7600)	Elevated COM interface	• Attacker defined application • Component(s): Attacker defined components	Windows 10 RS3 (16199)

28	Windows 7 (7600)	Whitelisted component	• Attacker defined application • Component(s): Attacker defined components	Windows 8.1 (9600)
29	Windows 10 TH1 (10240)	Shell API	• \system32\sdctl.exe • Component(s): Attacker defined application	Windows 10 RS3 (16215)
30	Windows 7 (7600)	Dll Hijack	• \syswow64\{any elevated exe, e.g wusa.exe} • Component(s): wow64log.dll	unfixed
31	Windows 10 TH1 (10240)	Shell API	• \system32\sdctl.exe • Component(s): Attacker defined application	unfixed
32	Windows 7 (7600)	Dll Hijack	• \Program Files\Windows Media Player\osk.exe,\system32\EventVwr.exe,\system32\mmc.exe • Component(s): duser.dll, osksupport.dll	unfixed
33	Windows 10 TH1 (10240)	Shell API	• \system32\fodhelper.exe • Component(s): Attacker defined application	unfixed
34	Windows 8.1 (9600)	Shell API	• \system32\svchost.exe via \system32\schtasks.exe • Component(s): Attacker defined application	unfixed

35	Windows 7 (7600)	Impersonation	• Auto-elevated applications • Component(s):Attacker defined applications	unfixed
36	Windows 7 (7600)	Race condition	• Wusa.exe • Component(s): dcomcnfg.exe, mmc.exe, ole32.dll, MsCoree.dll	unfixed
37	Windows 7 (7600)	Dll Hijack	• \system32\dccw.exe • Component(s):GdiPlus.dll	unfixed
38	Window 7 (7600)	Whitelisted component	• \system32\dccw.exe • Component(s): Attacker defined components	unfixed
39	Windows 7 (7600)	Dll Hijack	• \system32\mmc.exe • Component(s):Attacker defined components	unfixed
40	Windows 7 (7600)	COM Handler hijack	• \system32\mmc.exe,\System32\recdisc.exe • Component(s): Attacker defined components	unfixed
41	Windows 7 (7600)	Elevated COM interface	• Attack defined • Component(s): Attacker defined	unfixed

运行实例

akagi32.exe 1

akagi64.exe 3

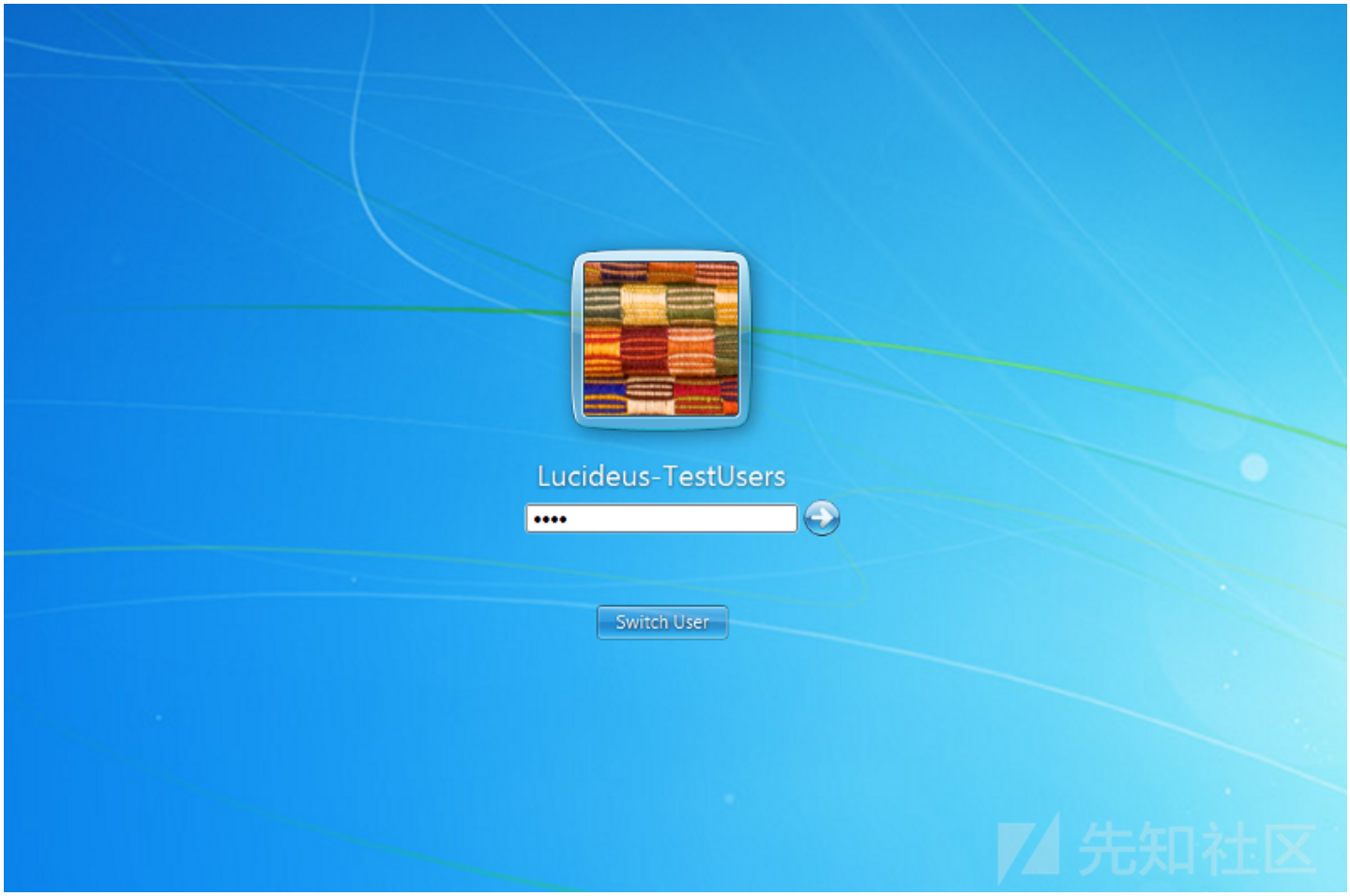
akagi32 1 c:\windows\system32\calc.exe

akagi64 3 c:\windows\system32\charmap.exe

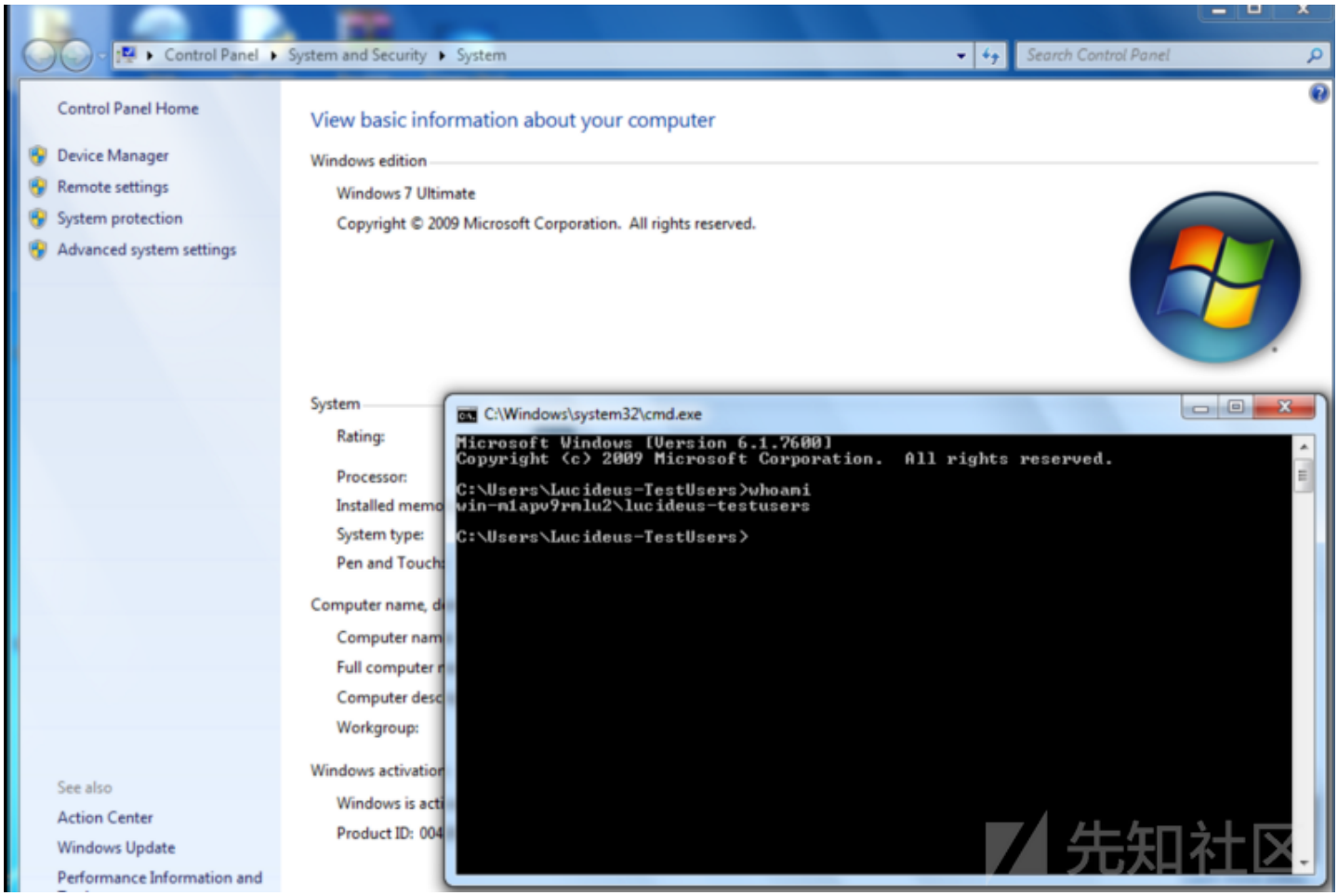
Proof of Concept

POC：1：Windows 7：64位：旗舰版 UAC绕过
用户名：Lucideus-TestUser

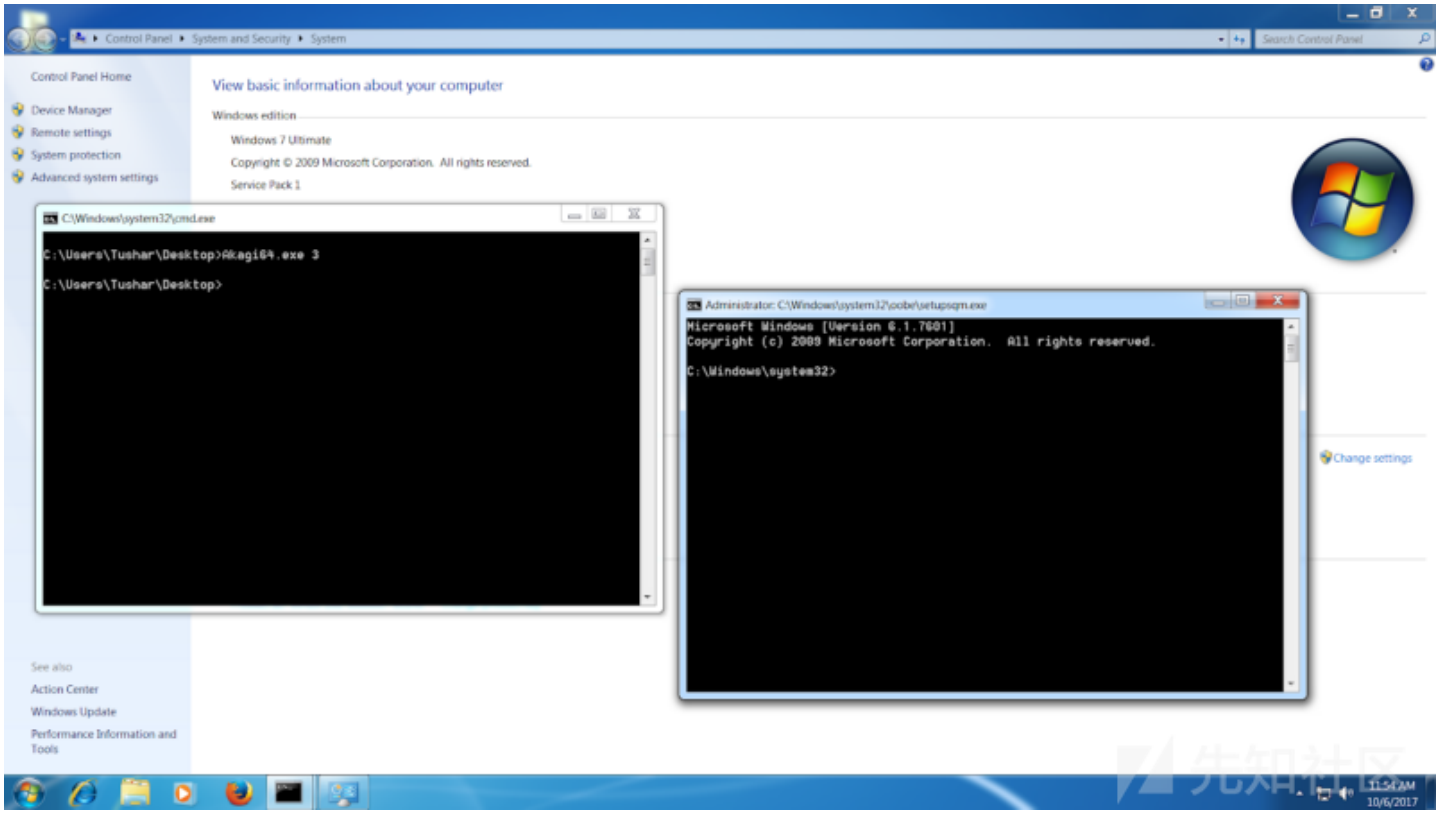
特权：标准用户



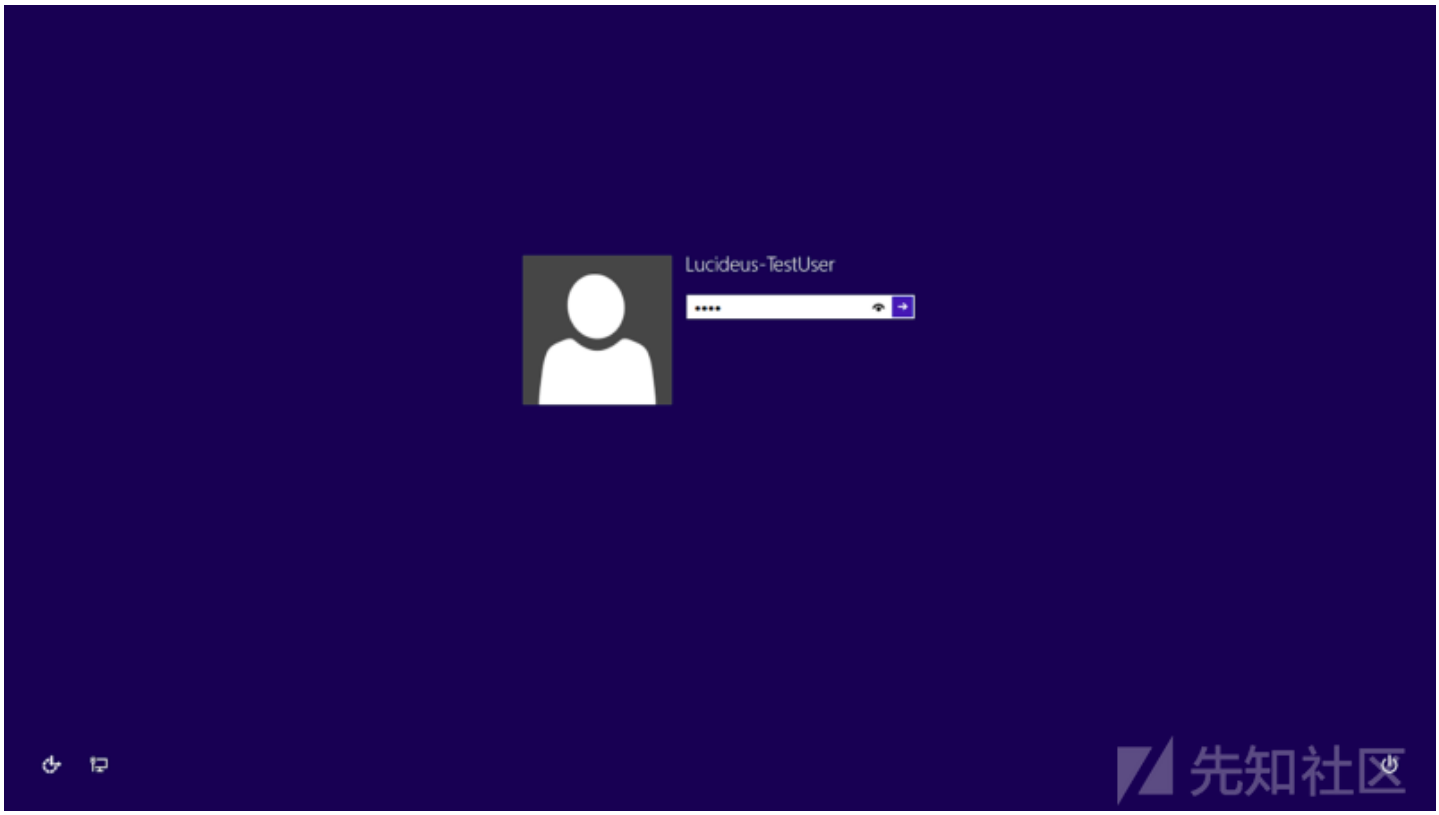
whoami命令的输出结果表明，我们只能使用有限的权限进入用户模式。



从命令行运行可执行文件：`akagi32 [Key] [Param]` 或 `akagi64 [Key] [Param]`。有关更多信息，请参见下面的“运行示例”。

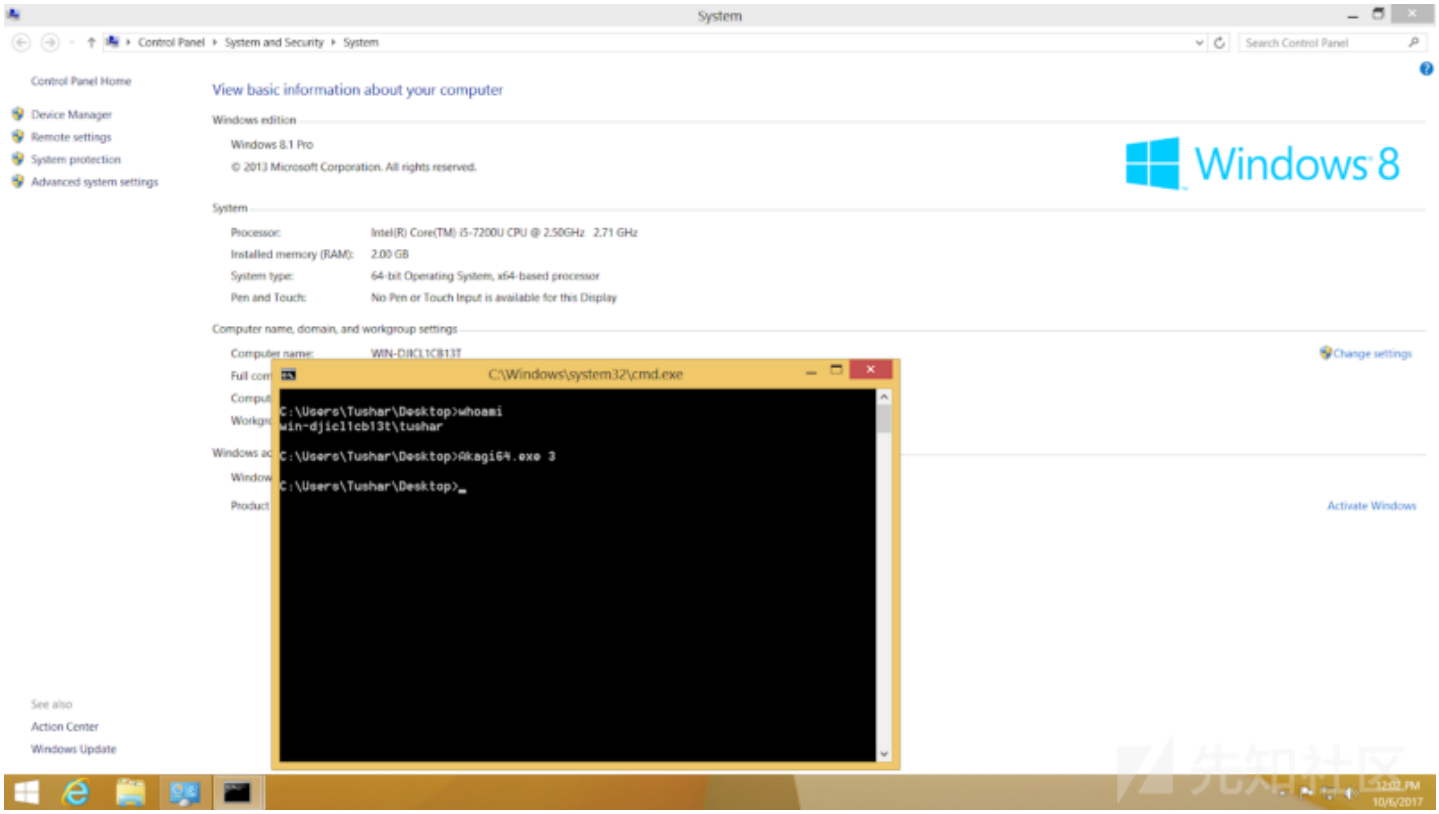


POC 2：Windows 8.1 Pro



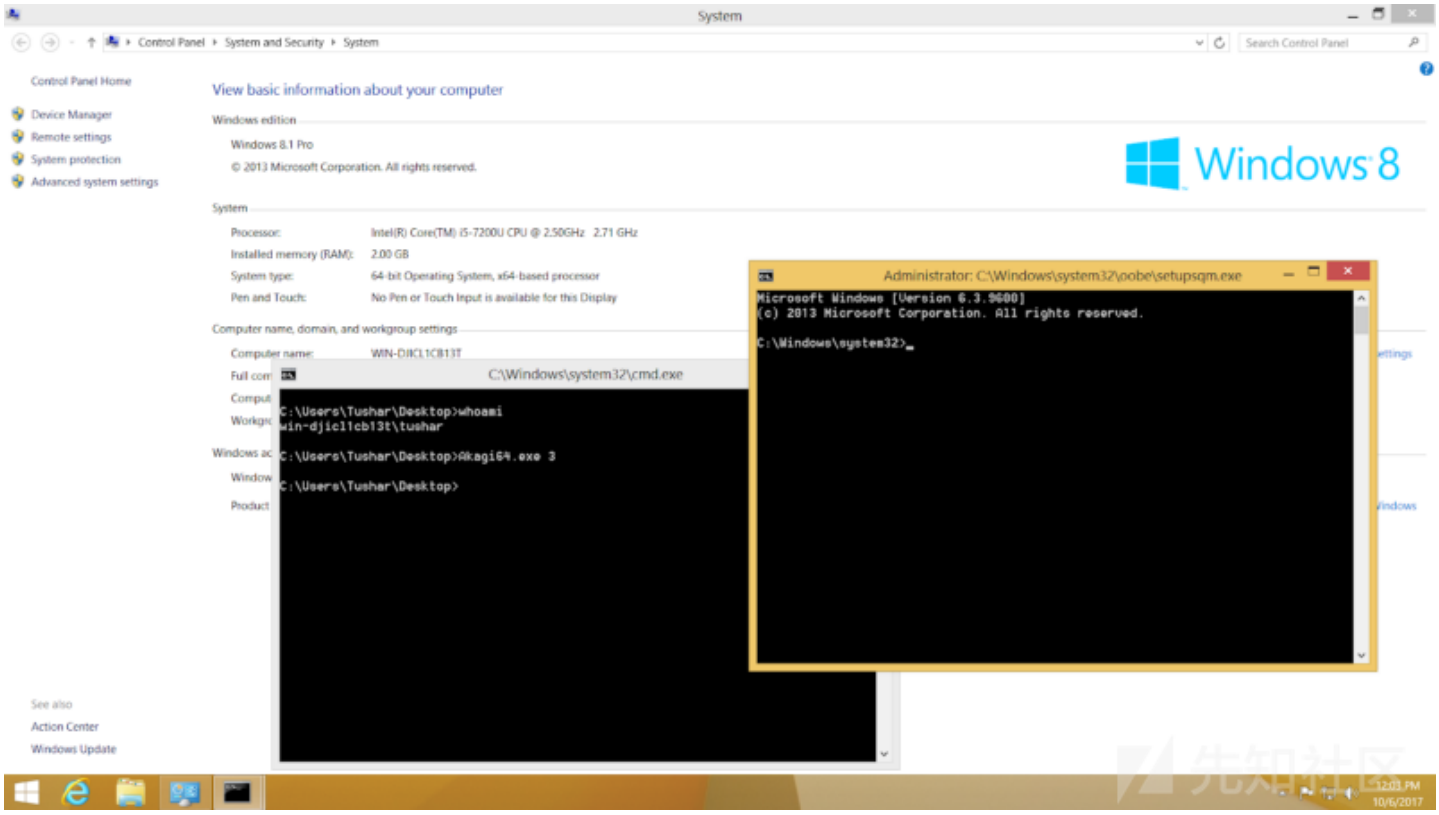
在我们输入密码后，我们不会得到管理员特权。

您可以通过以下方式进行检查：-whami(cmd中输入)



从命令行运行可执行文件：`akagi32 [Key] [Param]`或`akagi64 [Key] [Param]`。

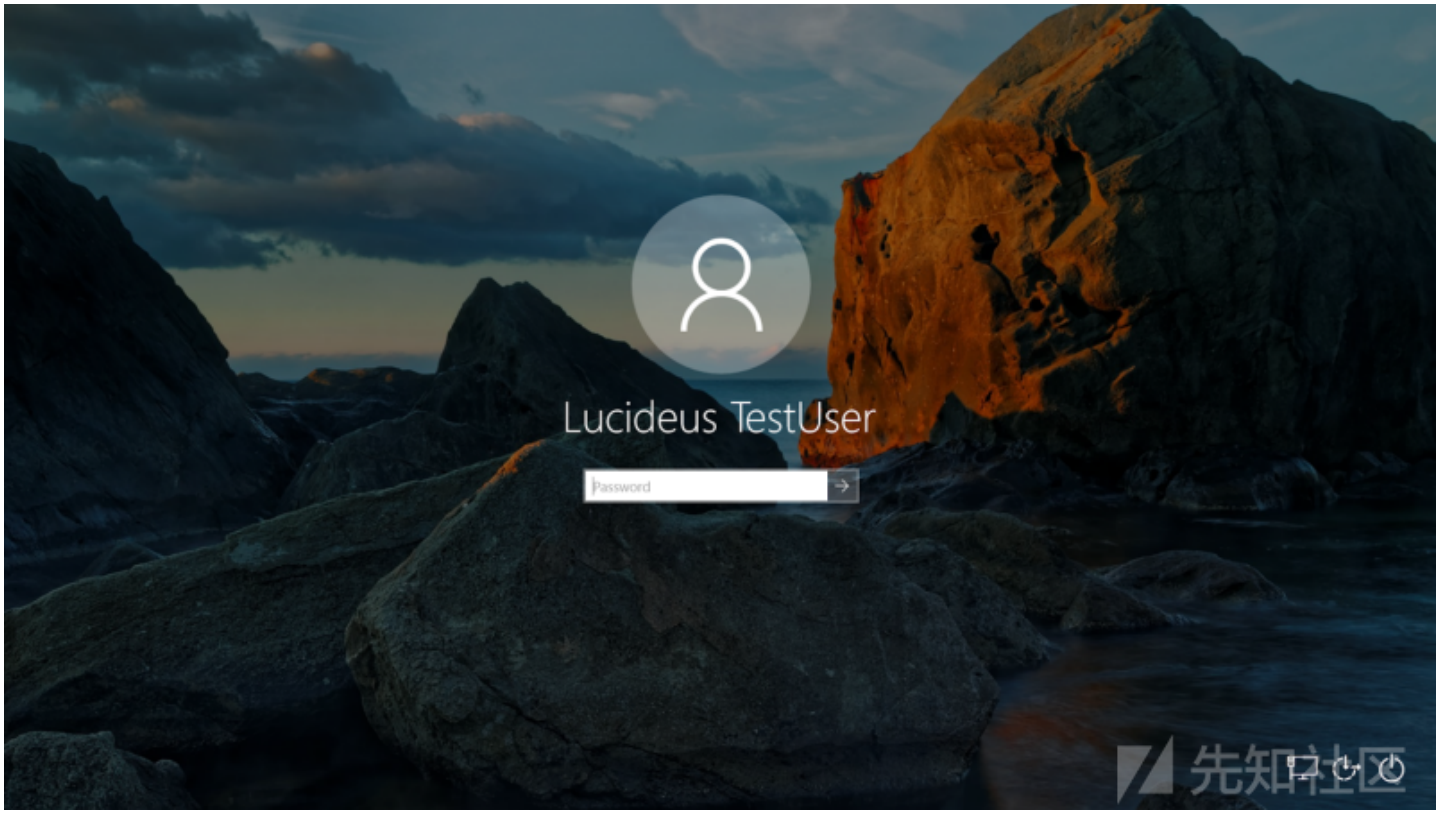
有关详细信息，请参阅下面的“运行示例”。



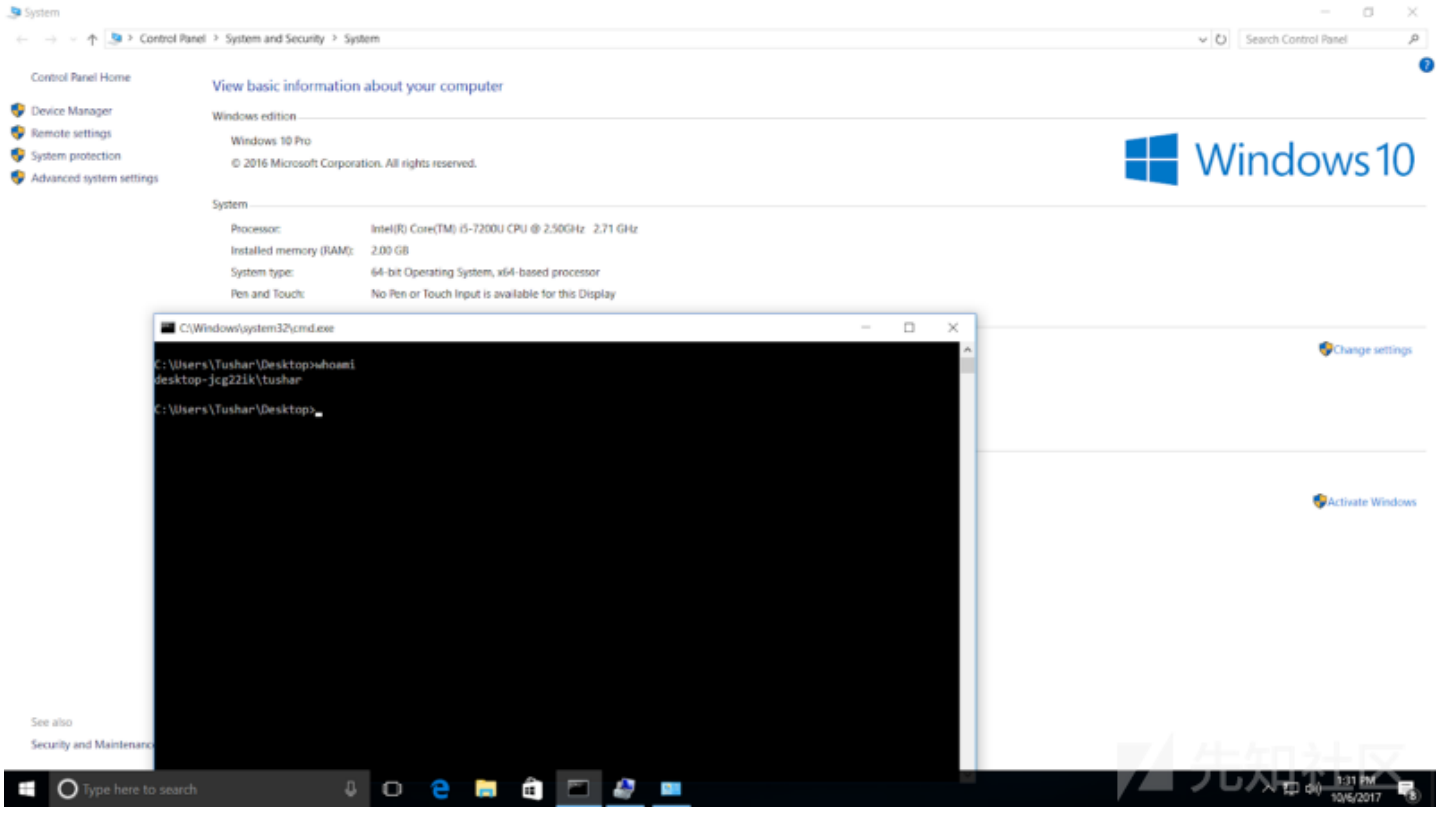
在Windows8.1专业版中与Windows7旗舰版相同。

在这里，我们也获得了管理特权，而不需要任何密码或任何特殊许可。

POC 3 : Windows 10 Pro

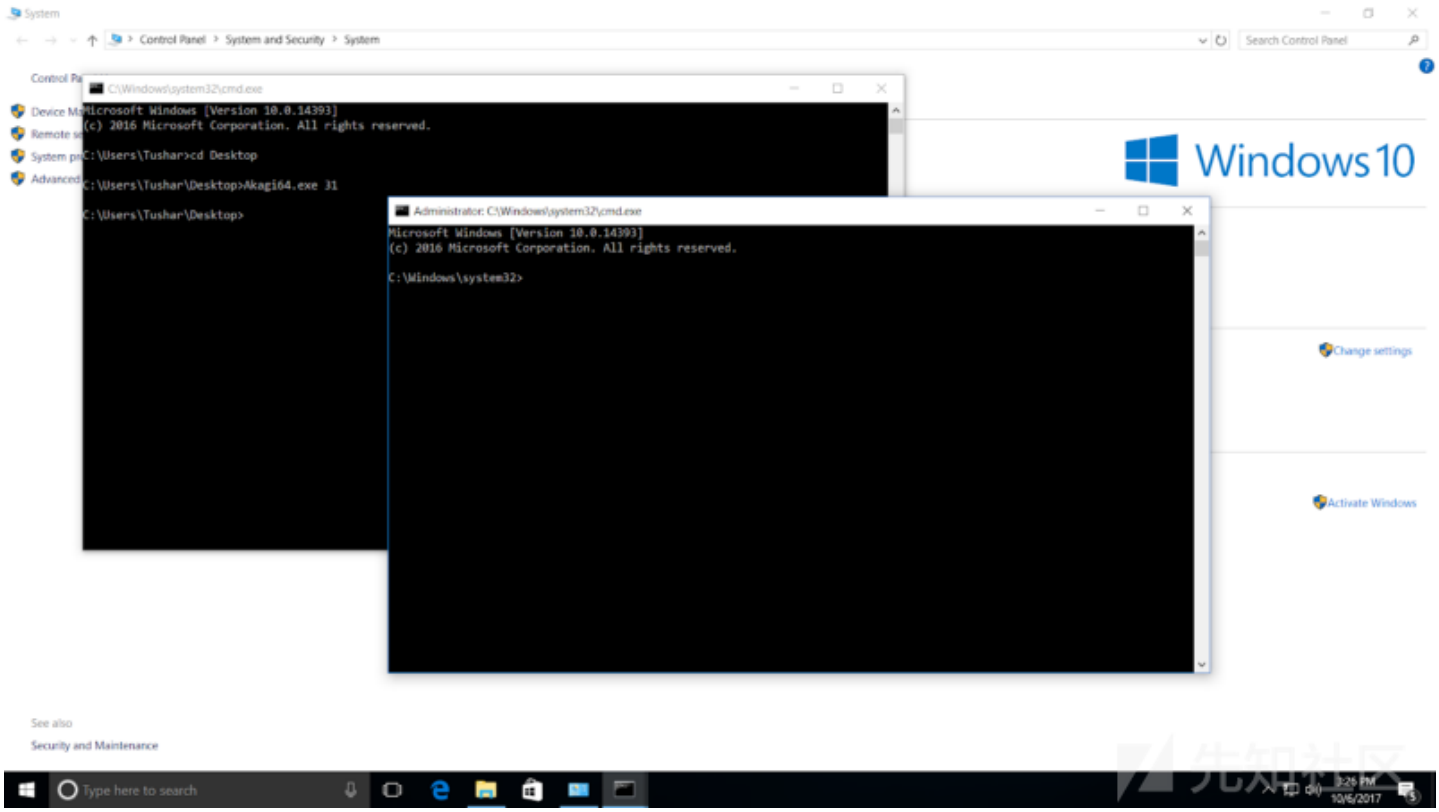


在我们输入密码后，我们无法获得管理员权限
您可以通过以下方式检查： - whoami（cmd中输入）



如您所见，我们不是管理员

然后运行 ——> `akagi32 [Key] [Param]`或`akagi64 [Key] [Param]`



我们无需任何密码或任何特殊许可即可获得管理员特权。

解决方案：自定义规则集组策略编辑

组策略设置

可以为用户帐户控制(UAC)配置10个组策略设置。下表列出了每个策略设置的默认设置，以下各节解释了不同的UAC策略设置并提供了建议。这些策略设置位于"本地安全策
https://docs.microsoft.com/en-gb/windows/security/identity-protection/user-account-control/user-account-control-group-policy-and-registry-key-settings

■■■■■https://medium.com/@lucideus/privilege-escalation-on-windows-7-8-10-lucideus-research-c8a24aa55679