**使用CobaltStrike窃取伪造指定进程的用户访问令牌:**

windows中通常关注两种令牌:

1.授权令牌(delegation token)

这种令牌通常用于本地及远程RDP登录

2.模拟令牌(impersonation token)

这种令牌通常用于各种非交互式的登录，比如net use,wmi,winrm等

这两种令牌都会在系统重启以后被清除, 否则将会一直驻留在内存中,而授权令牌则会在用户注销以后自动被转为模拟令牌,但仍然可利用

利用前提:

默认情况下,当前用户肯定是只能看到当前用户自己和比自己权限低的所有访问令牌,这无可厚非,现代操作系统在早期就是这样来设计用户空间 ACL 的,所以,如果你想看到系统中所有用户的访问令牌,那就务必要将自己当前用户的权限提到一个特权用户的身份上,比如,windows 的 system 或者 administrator,这样你才能看到当前系统中所有用户的访问令牌

思路:

对于一般性的域渗透来讲,在前期我们绝大部分的时间可能都会花在如何去搞到域管密码或者密码 hash 随后登到域控拿下整个目标域中的机器权限, 此处想说明的主要还是另一种不需要域管密码或者密码 hash 也能拿下域控权限的常用方式,具体是这样,先尝试提权拿下当前机器,假设在当前机器中就有域管进程[也就是说在这些进程中有域管的访问令牌],那么,此时我们就可以通过窃取伪造域管令牌的方式去直接以域管的身份访问域控,这个效果其实是跟你拿着域管的密码或者 hash 直接 wmi 或者 net use 过去的效果是一模一样的

要想看到当前机器中的所有用户访问令牌,必须要先把自己提到一个系统特权身份上[对于windows来讲,一般情况下,都是指system权限],所以我们要先来尝试提下权beacon> elevate ms14-058 system,提成功以后,就会弹回一个 system 权限的 shell

直接去 dir 域控机器的 windows 目录,你会发现它提示没权限,这很正常,因为你当前还没有提供任何的认证凭据 [比如,域管的账号密码或者密码 hash,再或者域管令牌]

首先,你得先去找下当前机器中的任意一个域管进程并确定其进程 id,因为我们现在已有了当前机器的 system 权限,所以,理论上你应该可以看到机器中的所有用户进程,这其中就包括域管的, 当一台机器加到某个域中时会自动往当前机器的 administrators 组添加一个域管用户,这也就是为什么域管可以随意管理当前域内的任意一台机器的关键原因之一

beacon 内置的 steal\_token 工具,来尝试窃取上面那个 java 进程中的域管令牌,当看到提示模拟域管令牌成功后,此时我们再直接去 dir 域控的 windows 目录,发现就可以正常访问了,这也就是我前面一直在说的,当前拥有什么样的访问令牌直接决定了你能访问到当前或远程机器中的哪些系统资源,

beacon> steal\_token 1892

beacon> getuid

beacon> shell dir \\2008R2-DCSERVER\c$

beacon> rev2self 撤回令牌

注意,当我们用完某个用户的访问令牌以后,一定要记得再把它顺手还原回去,在 beacon 也内置了一个叫 rev2self 工具,直接执行即可把当前令牌还原为原来的用户令牌,因为是在提到 system 以后才做的操作,所以就直接给还原到了 system 下

msf : use post/multi/recon/local\_exploit\_suggester

dcsync 从dc中提取密码哈希

hashdump 转储密码哈希值

logonpasswords 使用mimikatz转储凭据和哈希值

mimikatz

pth

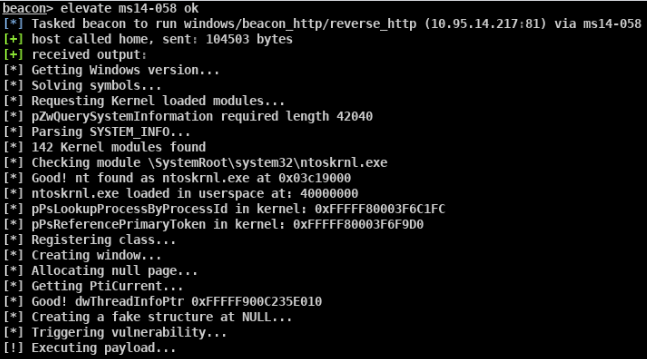
wdigest 使用mimikatz转储明文凭据

实验记录

java -XX:+AggressiveHeap -XX:+UseParallelGC -jar cobaltstrike.jar

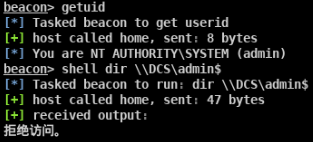
./teamserver ip password

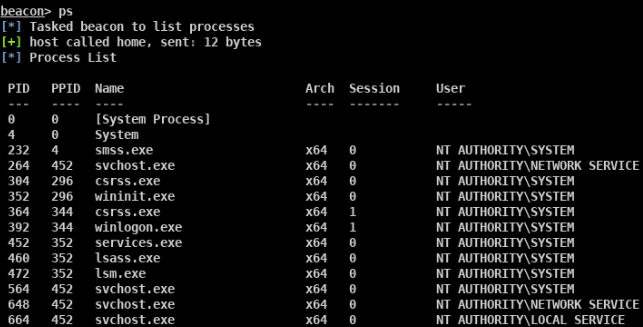


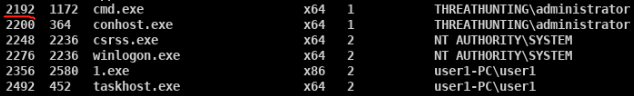


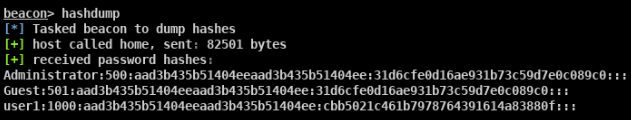


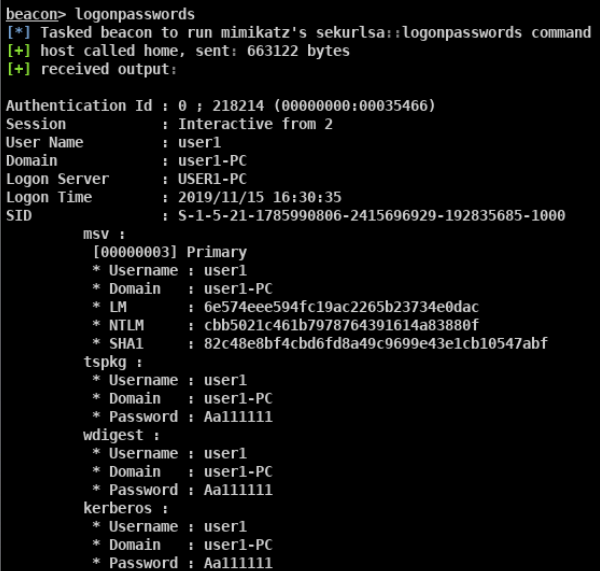
本机system权限无法访问域控共享文件夹

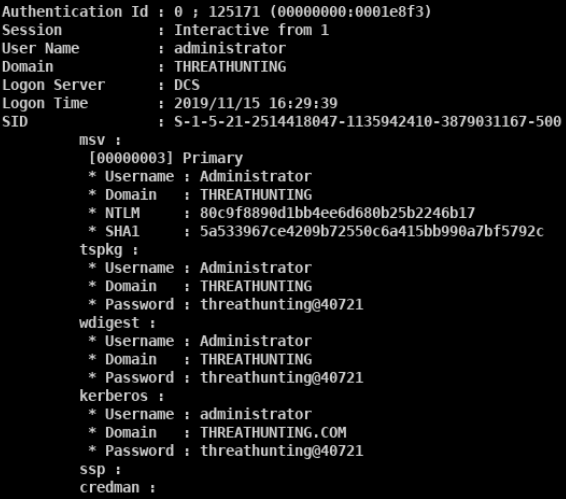




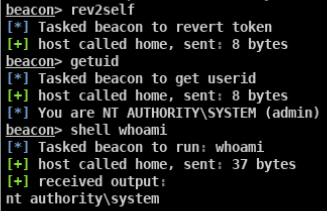


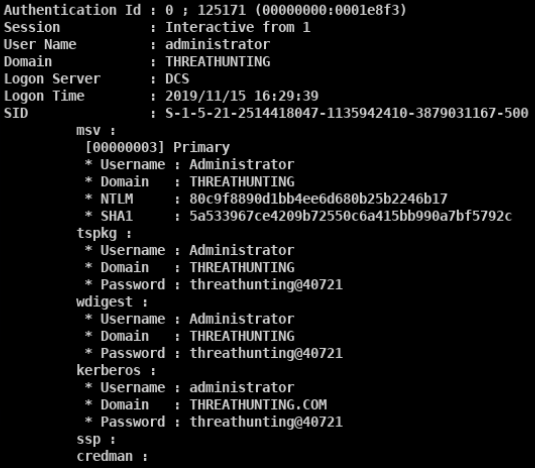




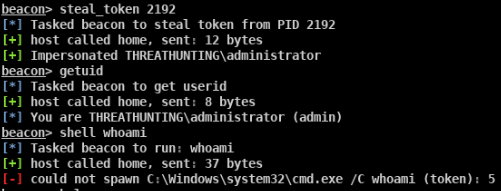


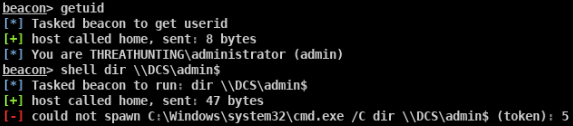






问题



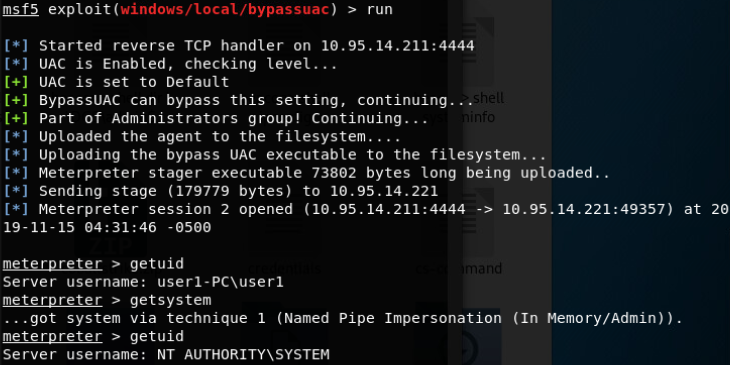


**使用 meterpreter 中 incognito 模块窃取伪造指定进程的用户访问令牌:**

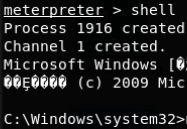
use exploit/windows/local/bypassuac win32 64都可

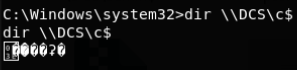
getsystem

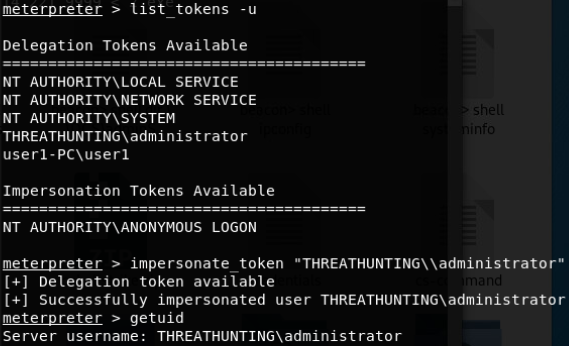
实验记录

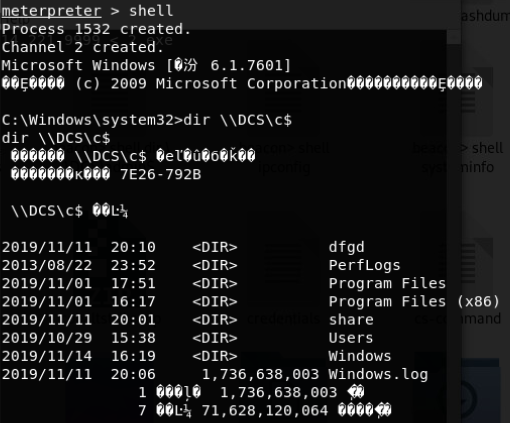


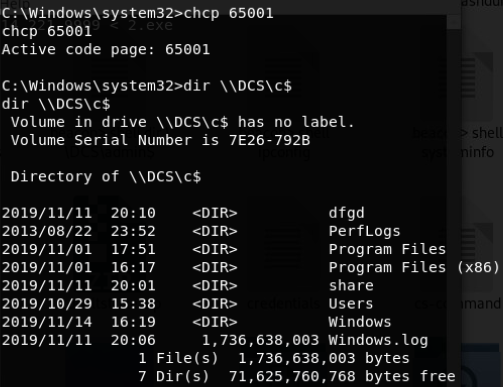




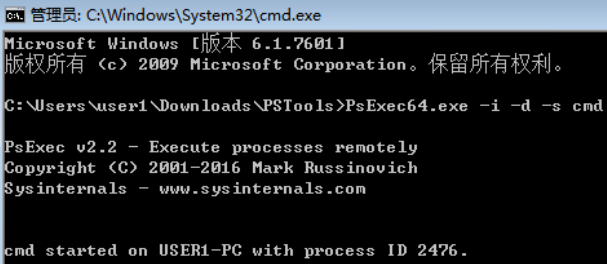


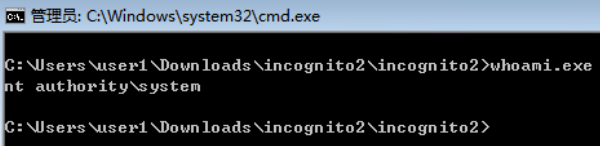


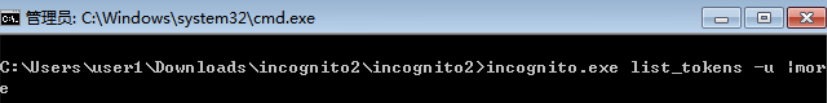


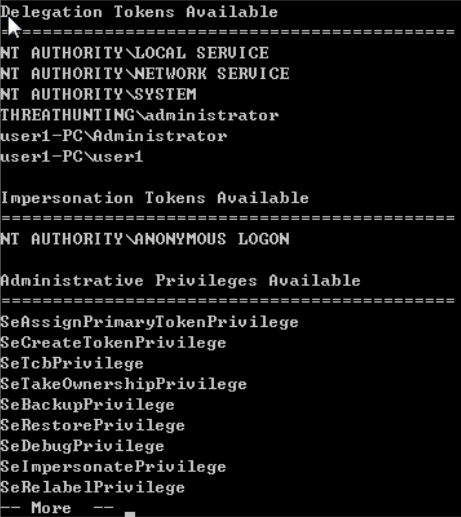


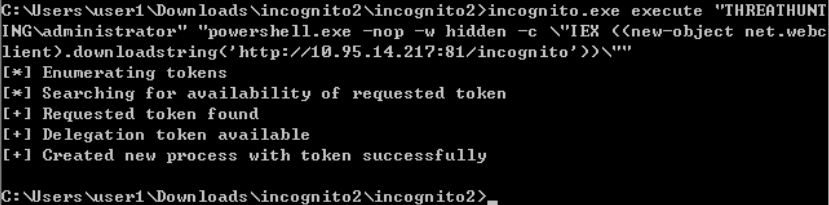
**使用 incognito 伪造任意用户身份的访问令牌执行payload:**



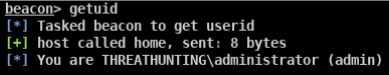




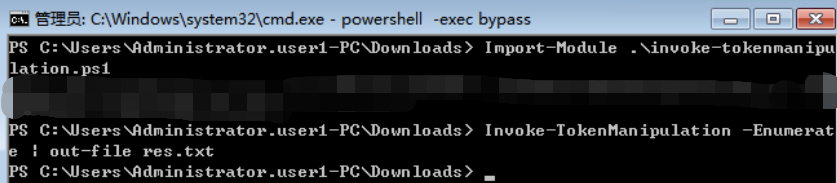


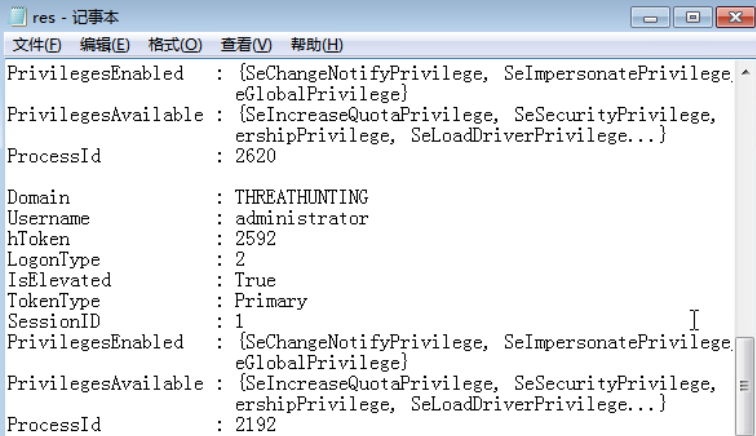


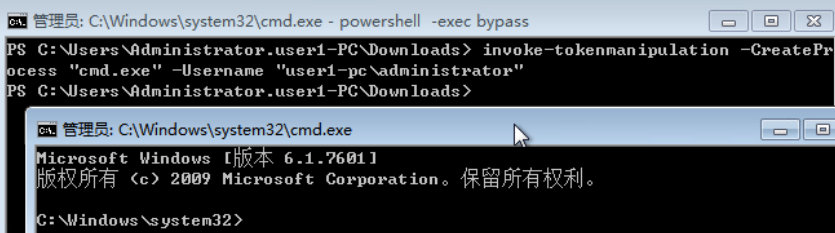


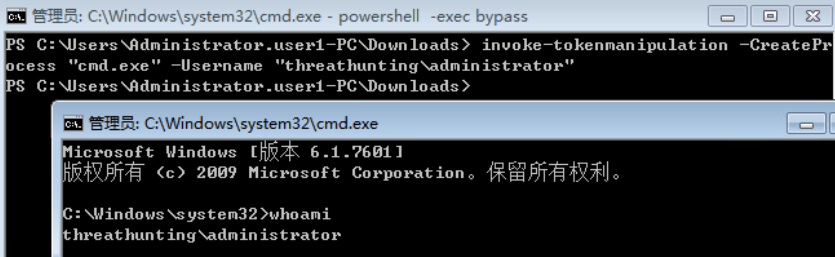


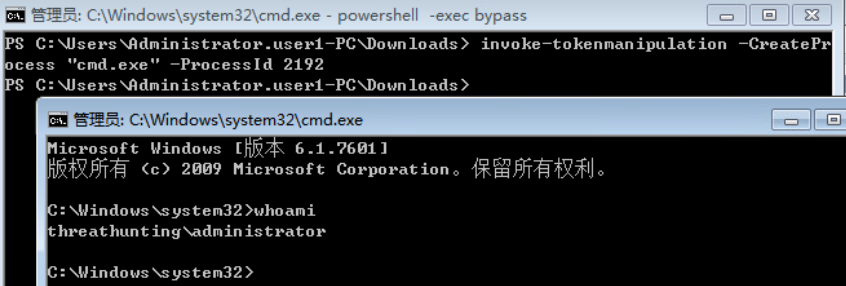
**使用 Invoke-TokenManipulation.ps1 脚本伪造指定用户身份令牌执行 payload:**



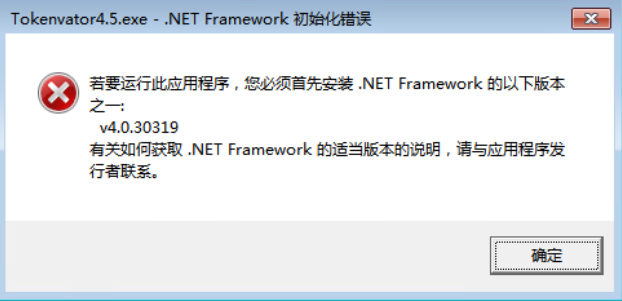


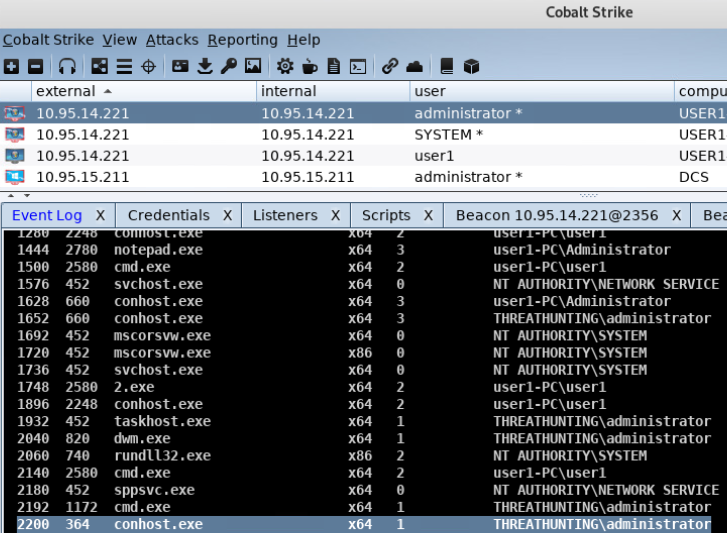


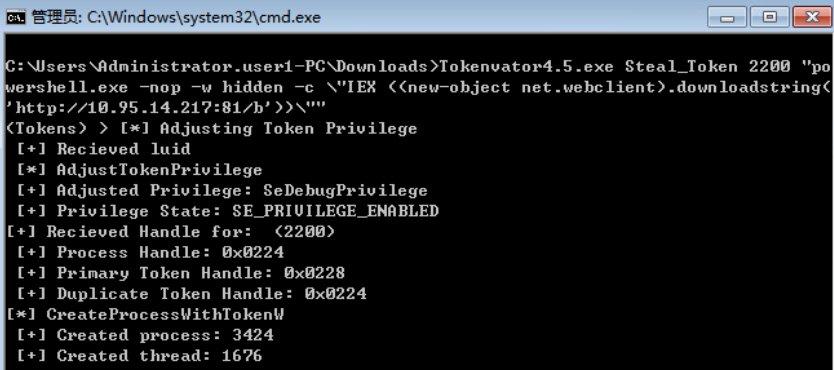


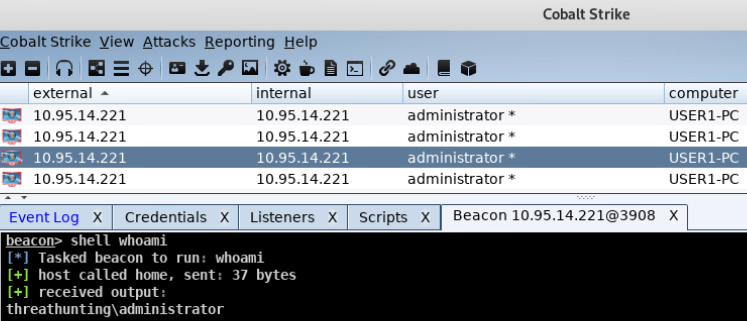


**使用 Tokenvator.exe 来伪造指定用户的访问令牌执行任payload:**

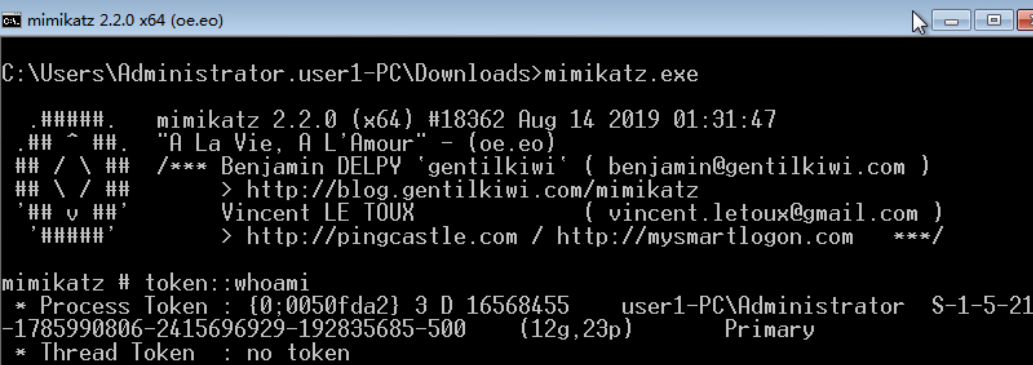


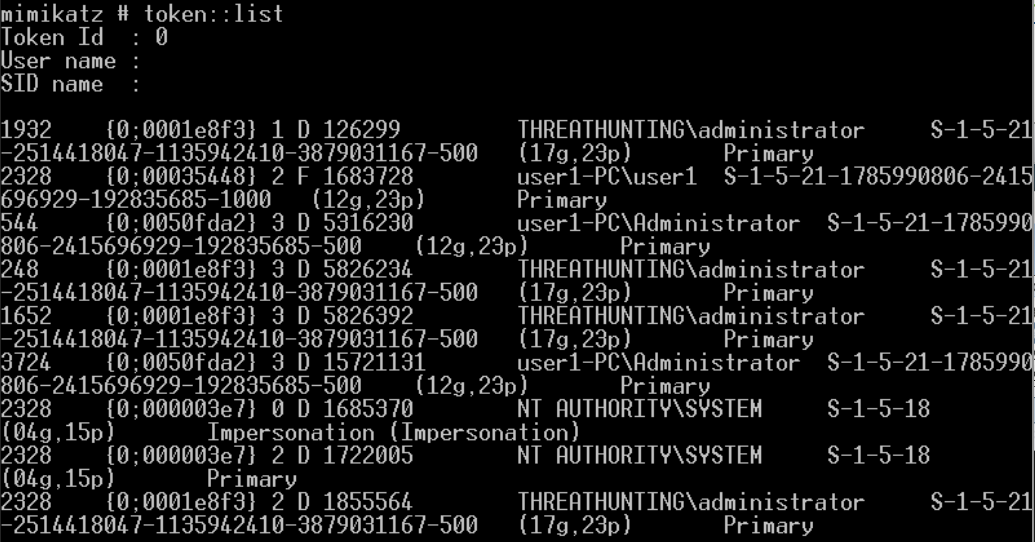


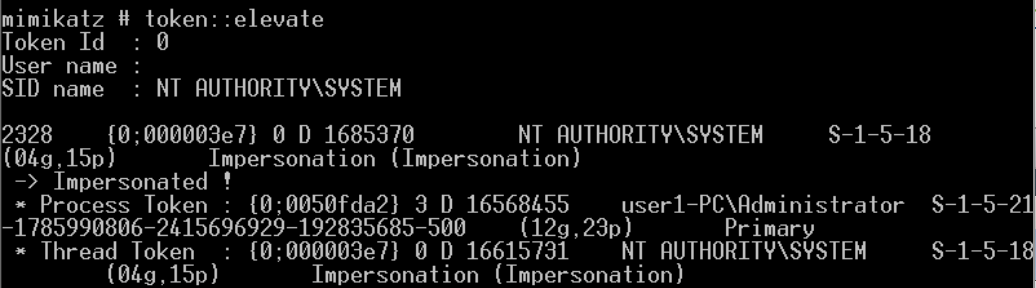




**使用Mimikatz 伪造指定用户的访问令牌:**

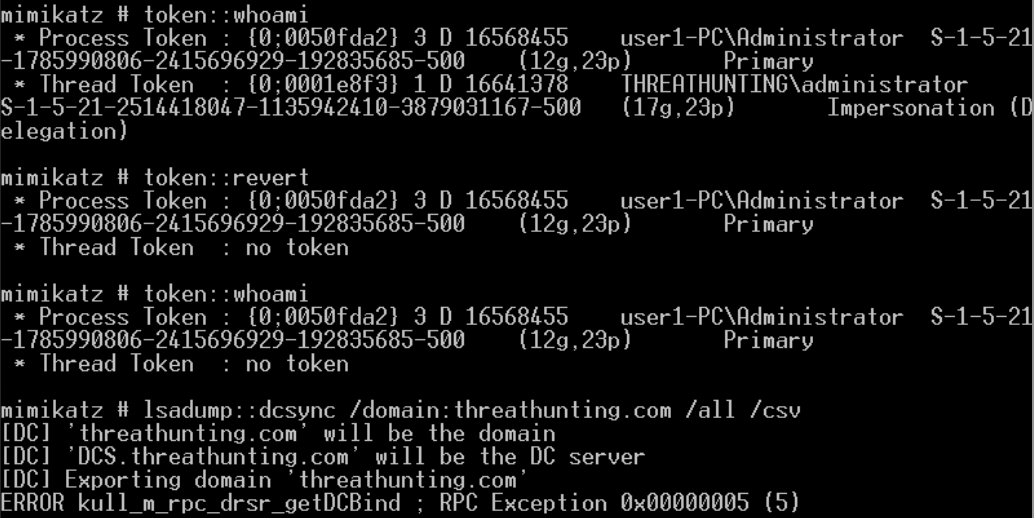










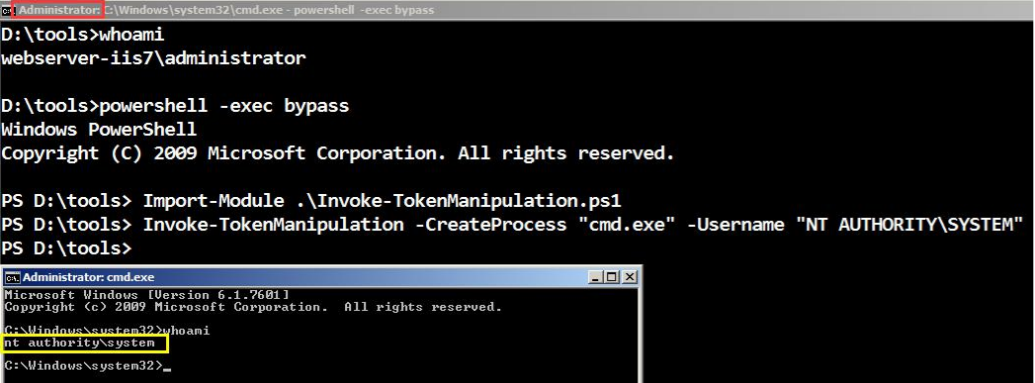


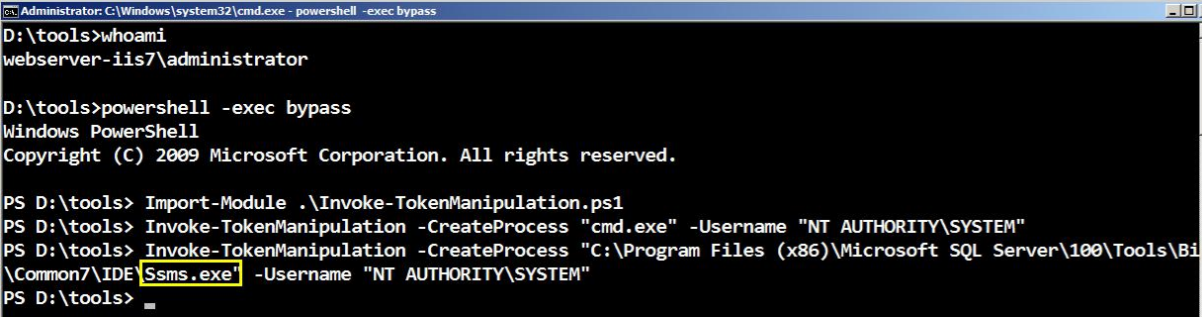
**使用Invoke-TokenManipulation.ps1 伪造 system 访问令牌实现 mssql 本地免密码登录:**

mssql 本地免密码登录的核心其实就在于 mssql 支持以 windows 本地登录验证,默认情况下,用于安装 mssql 的 administrator 用户[一般在 windows 服务器也都是这个用户]

和 system 用户[其实也并非完全是这样,这还要看你在安装 mssql 时指明用的那个用户来跑服务的]直接在本地以 windows 验证方式登录是不需要密码直接连接即可登录的,也正是由于此,我们才可以通过窃取 system 的 token 的方式,直接在目标机器本地实现免密码登录 mssql

一般都是什么情况才会导致必须要这么干呢? 比如,你现在已经通过其它的方式拿下了当前这台数据库服务器的最高权限[比如,system 权限],但比较蛋疼的是,你抓不到当前系统管理员的明文账号密码,管理员密码 hash 虽然是抓过来了,但死活跑不出来,数据库的任何账号密码都没有,但是我还想要当前机器中的数据库中的数据,怎么办呢,可以这样,等你确认那边管理员不在的时候,你可以先在这台机器创建个管理用户,然后rdp 登过去,登上去以后,当你试着直接打开SQL Server Management Studio 以windows认证方式执行本地连接时却连不上[连不上的原因可能是因为你当前这个用户并不是安装mssql的用户,所以,认证通不过,不能达到免密码的效果],这怎么搞呢,其实也非常简单,先在目标桌面里面起个 system 权限的 cmd,而后直接用这个权限的 cmd 去启动 SQL Server Management Studio 就可以了,或者可以更直接点,就像我们下面这样直接用 powershell 一键搞,此时,同样是以 windows 认证直接无需密码即可登录,具体如下

找到 SQL Server Management Studio 的客户端的绝对路径直接以 system 权限去启动



之后会正常弹出 mssql 的登录界面,此时你只需要在 Server name 中输入'.[表示本地,当前机器]',而后点击 connect 即可直接连进去,过程中不再需要输入任何密码,如下是实际的连接效果,至此,关于 Invoke-TokenManipulation.ps1 脚本的利用,也就算顺带着说完了,对了,脚本中一样也提供了 RevToSelf 选项,当你用完某个用户令牌后,记得再把它恢复回来,话说回来,如果目标机器环境确实允许你这么干,对于 windows 来讲,个人肯定推荐首选 powershell,当然啦,有时候碰到内网断网机直接 IEX 外网加载就不大现实了,其实也并不是完全不能用,你可以试着把这些 ps 脚本都统一放到目标边界的一台已控的 web 机器的指定站点目录下,放的隐蔽点就行,而后再去内网的其它机器上 IEX 这台边界机器就行,这也只是其中的一种办法,并不是绝对,唯一的缺点就是 powershell 不能适用于一些老系统上,不过也没多大关系,用 incognito.exe 或者后面的 Tokenvator.exe 去搞也都是一样的