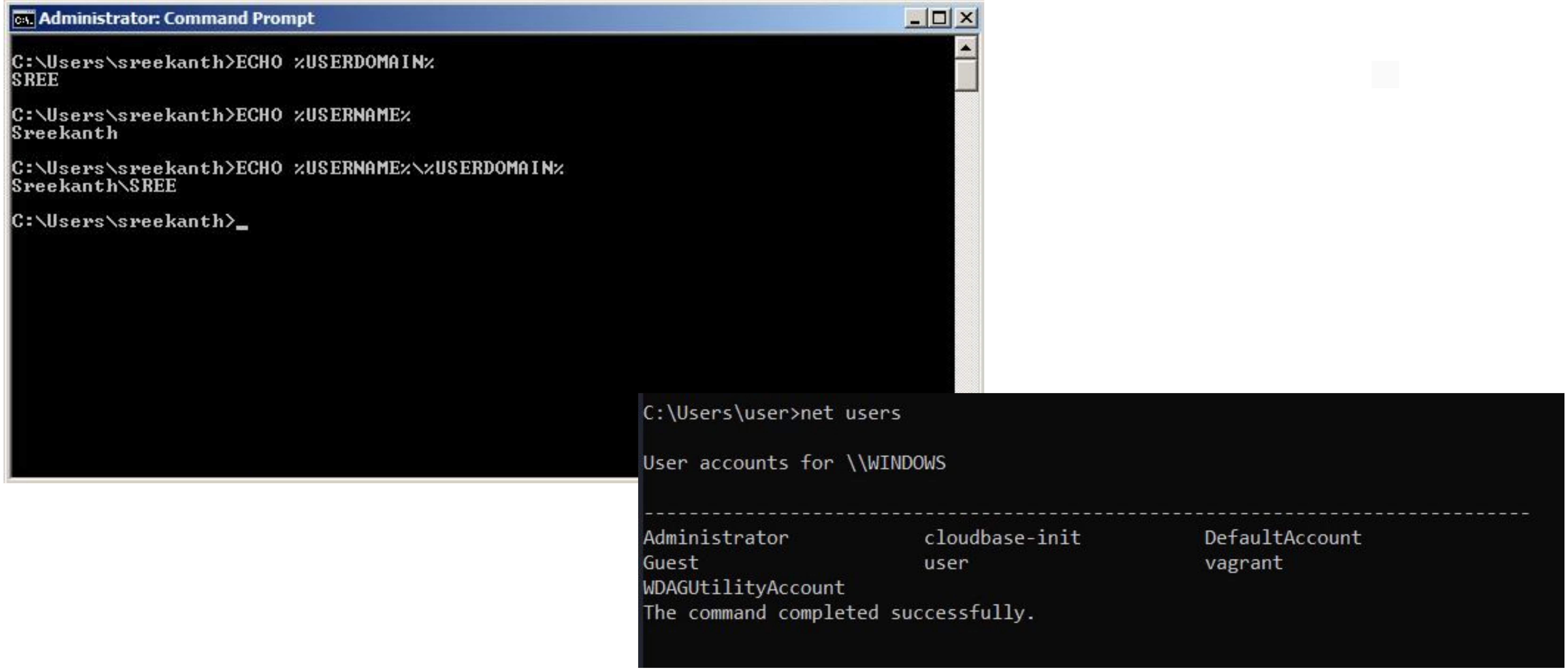
THE BRIDGE

CYBER SECURITY

Escalada de Privilegios Windows I

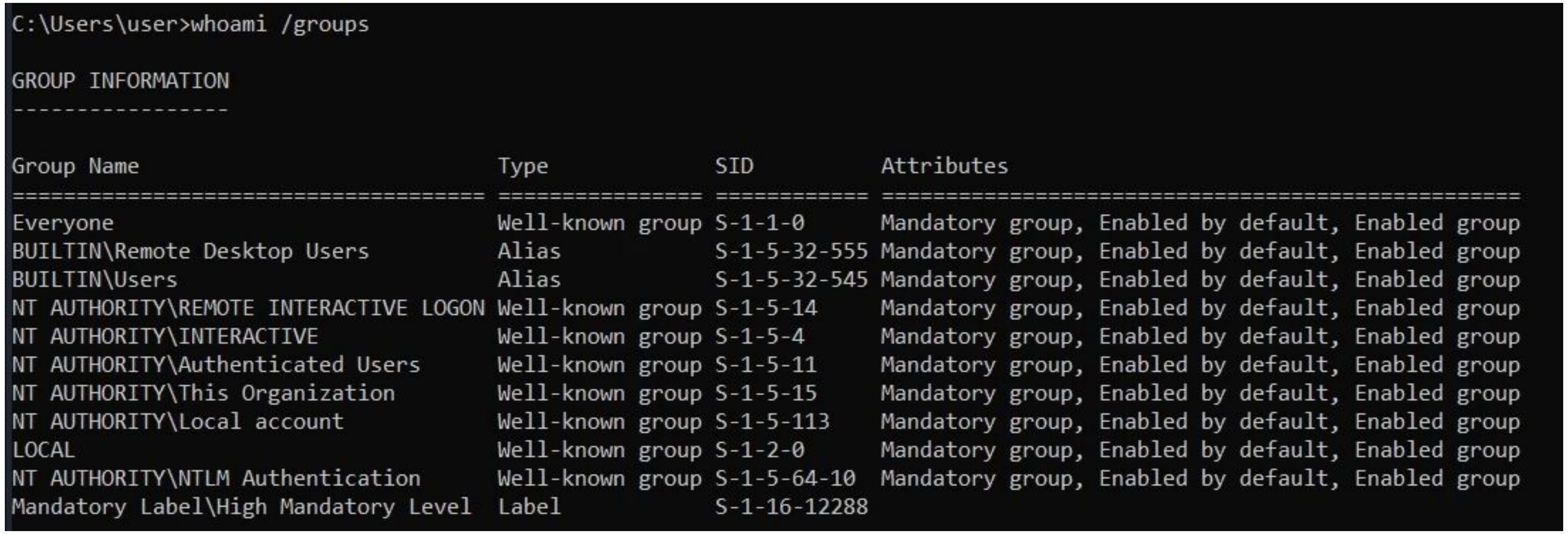
User Enumeration: user



```
C:\Users\sreekanth>ECHO %USERDOMAIN%
SREE

C:\Users\sreekanth>ECHO %USERNAME%
Sreekanth

C:\Users\sreekanth>ECHO %USERNAME%\%USERDOMAIN%
Sreekanth\SREE

C:\Users\sreekanth>_
```

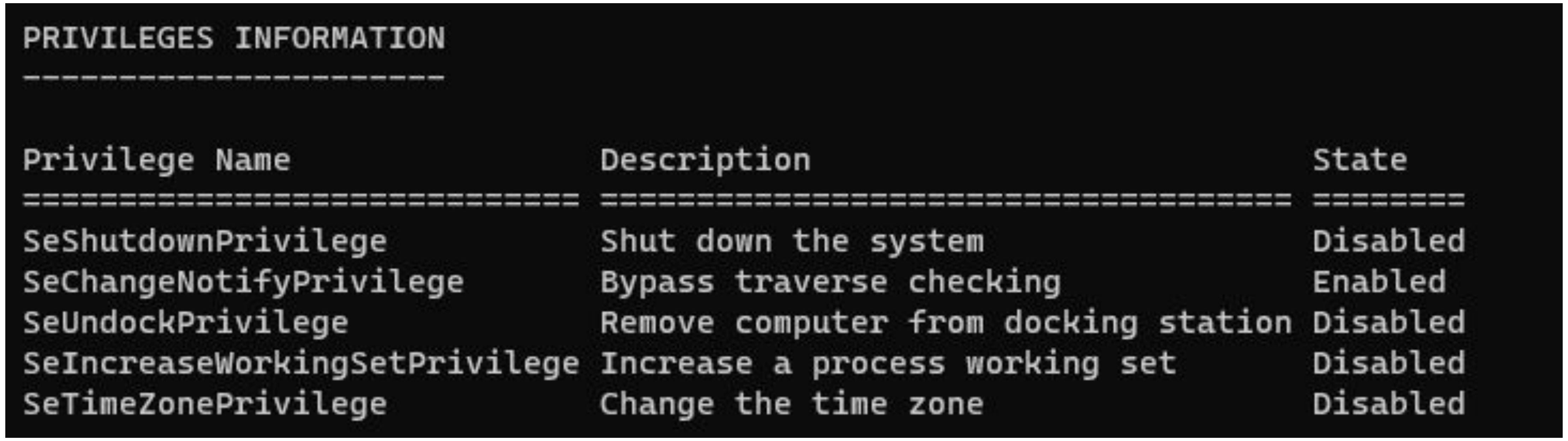
```
C:\Users\user>net users

User accounts for \\WINDOWS

-------------------------------------------------------------------------------
Administrator            cloudbase-init           DefaultAccount
Guest                    user                     vagrant
WDAGUtilityAccount
The command completed successfully.
```

User Enumeration: groups



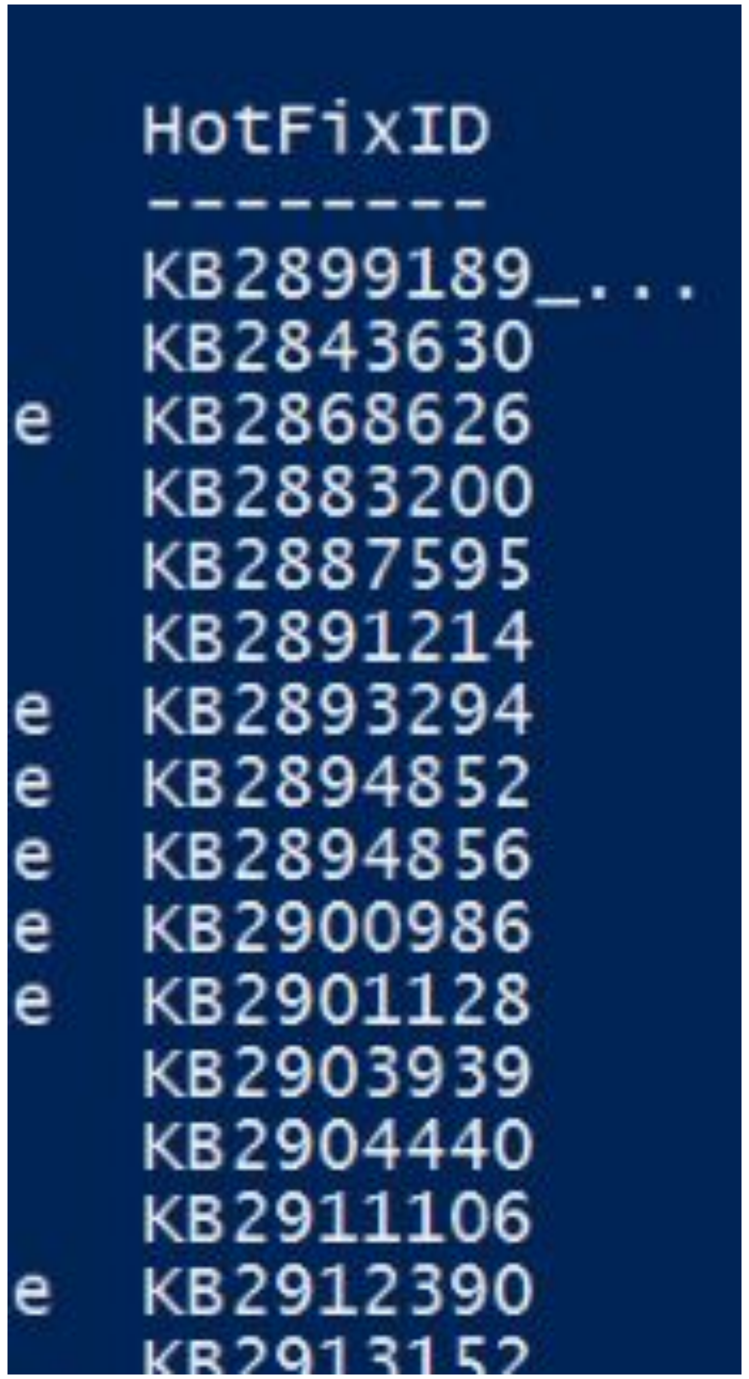
```
C:\Users\user>whoami /groups

GROUP INFORMATION
-----------------

Group Name                            Type             SID          Attributes
===================================== ================ ============ ==================================================
Everyone                              Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Desktop Users          Alias            S-1-5-32-555 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                         Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\REMOTE INTERACTIVE LOGON Well-known group S-1-5-14     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE              Well-known group S-1-5-4      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users      Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization        Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account            Well-known group S-1-5-113    Mandatory group, Enabled by default, Enabled group
LOCAL                                 Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication      Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level  Label            S-1-16-12288
```

User Enumeration: Privilege

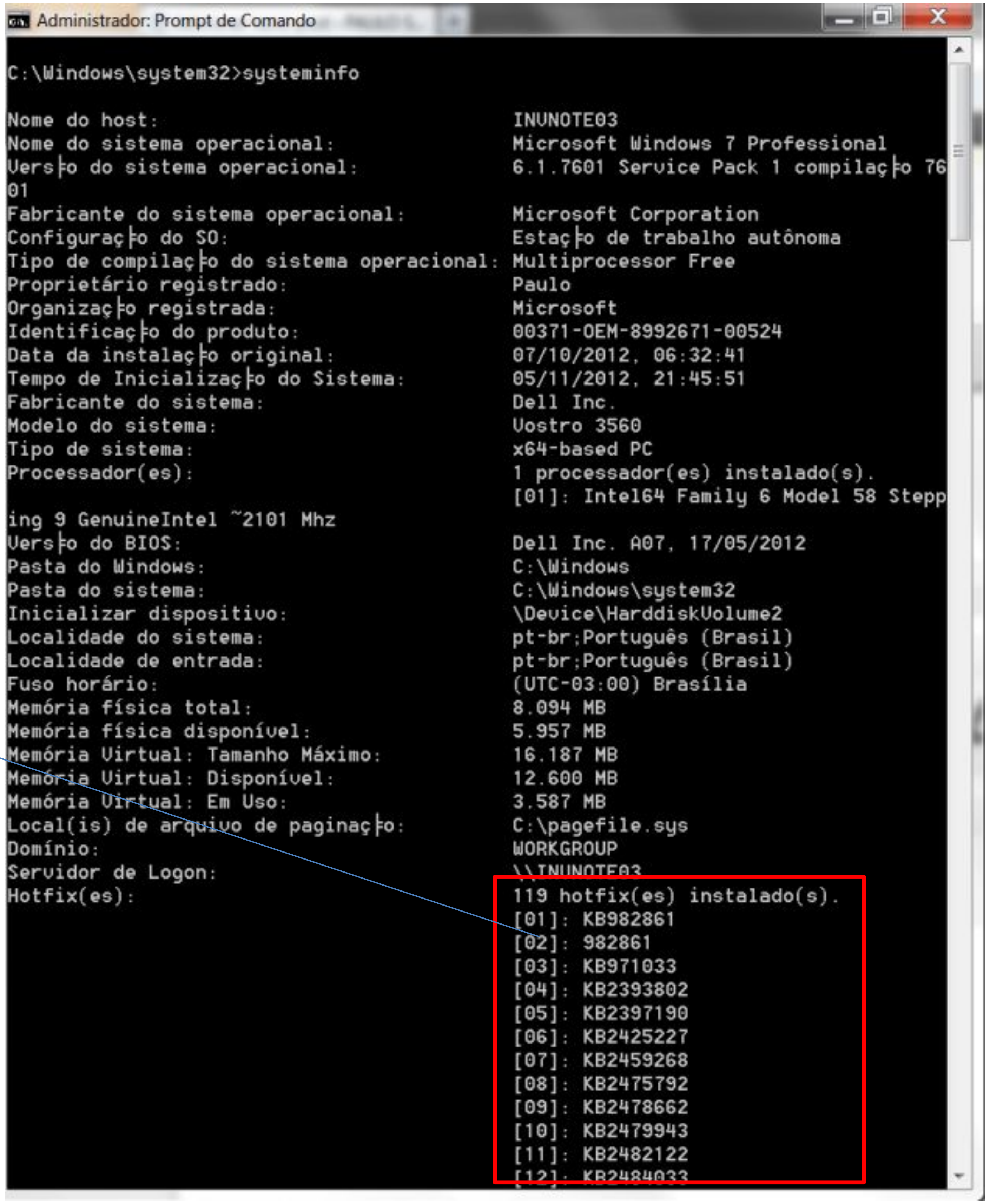


```
PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled
```

System Enumeration

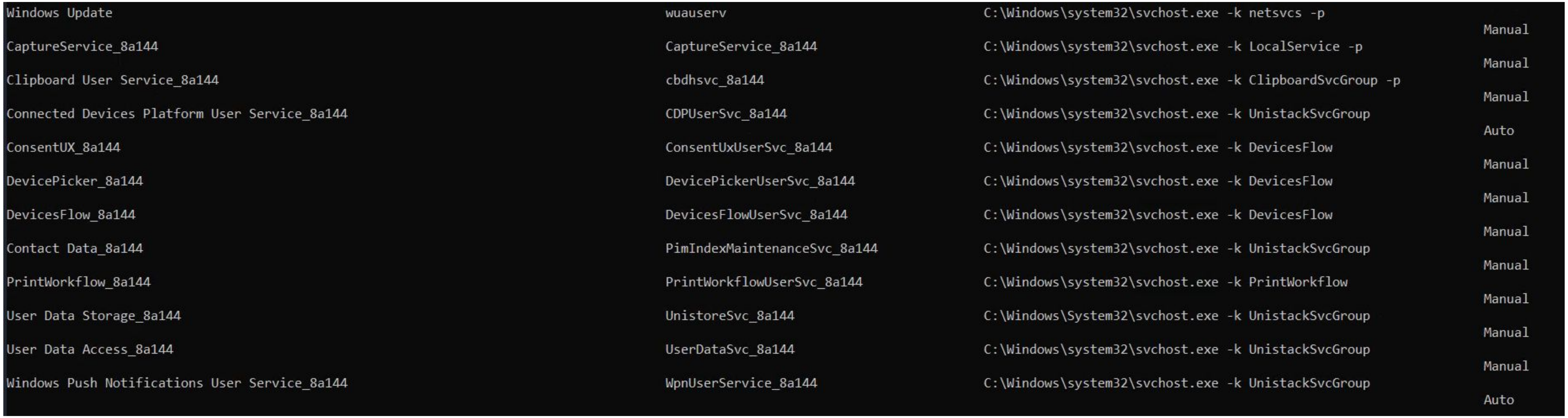


```
    HotFixID
    ---------
    KB2899189_...
    KB2843630
e   KB2868626
    KB2883200
    KB2887595
    KB2891214
e   KB2893294
e   KB2894852
e   KB2894856
e   KB2900986
e   KB2901128
    KB2903939
    KB2904440
    KB2911106
e   KB2912390
    KB2913152
```



```
C:\Windows\system32>systeminfo

Nome do host:                                  INUNOTE03
Nome do sistema operacional:                   Microsoft Windows 7 Professional
Vers╞o do sistema operacional:                 6.1.7601 Service Pack 1 compilaç╞o 76
01
Fabricante do sistema operacional:             Microsoft Corporation
Configuraç╞o do SO:                            Estaç╞o de trabalho autônoma
Tipo de compilaç╞o do sistema operacional:     Multiprocessor Free
Proprietário registrado:                       Paulo
Organizaç╞o registrada:                        Microsoft
Identificaç╞o do produto:                      00371-OEM-8992671-00524
Data da instalaç╞o original:                   07/10/2012, 06:32:41
Tempo de Inicializaç╞o do Sistema:             05/11/2012, 21:45:51
Fabricante do sistema:                         Dell Inc.
Modelo do sistema:                             Vostro 3560
Tipo de sistema:                               x64-based PC
Processador(es):                               1 processador(es) instalado(s).
                                               [01]: Intel64 Family 6 Model 58 Stepp
ing 9 GenuineIntel ~2101 Mhz
Vers╞o do BIOS:                                Dell Inc. A07, 17/05/2012
Pasta do Windows:                              C:\Windows
Pasta do sistema:                              C:\Windows\system32
Inicializar dispositivo:                       \Device\HarddiskVolume2
Localidade do sistema:                         pt-br;Português (Brasil)
Localidade de entrada:                         pt-br;Português (Brasil)
Fuso horário:                                  (UTC-03:00) Brasília
Memória física total:                          8.094 MB
Memória física disponível:                     5.957 MB
Memória Virtual: Tamanho Máximo:               16.187 MB
Memória Virtual: Disponível:                   12.600 MB
Memória Virtual: Em Uso:                       3.587 MB
Local(is) de arquivo de paginaç╞o:             C:\pagefile.sys
Domínio:                                       WORKGROUP
Servidor de Logon:                             \\INUNOTE03
Hotfix(es):                                    119 hotfix(es) instalado(s).
                                               [01]: KB982861
                                               [02]: 982861
                                               [03]: KB971033
                                               [04]: KB2393802
                                               [05]: KB2397190
                                               [06]: KB2425227
                                               [07]: KB2459268
                                               [08]: KB2475792
                                               [09]: KB2478662
                                               [10]: KB2479943
                                               [11]: KB2482122
                                               [12]: KB2484033
```

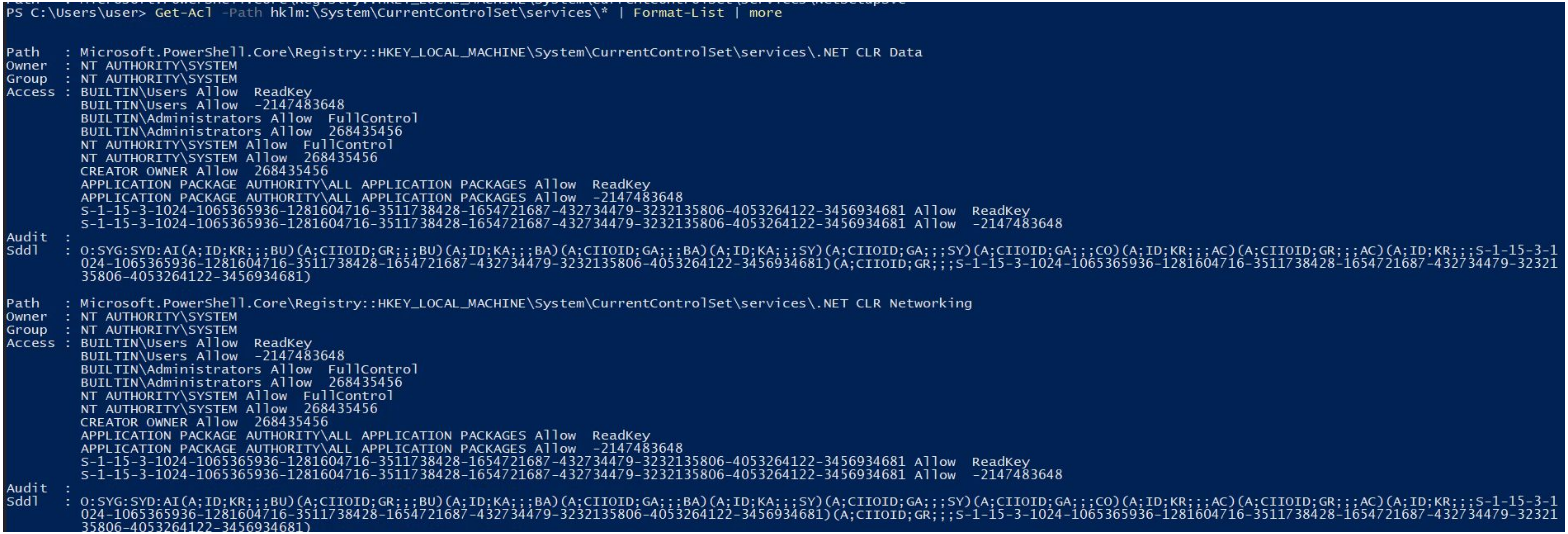
Services Enumeration



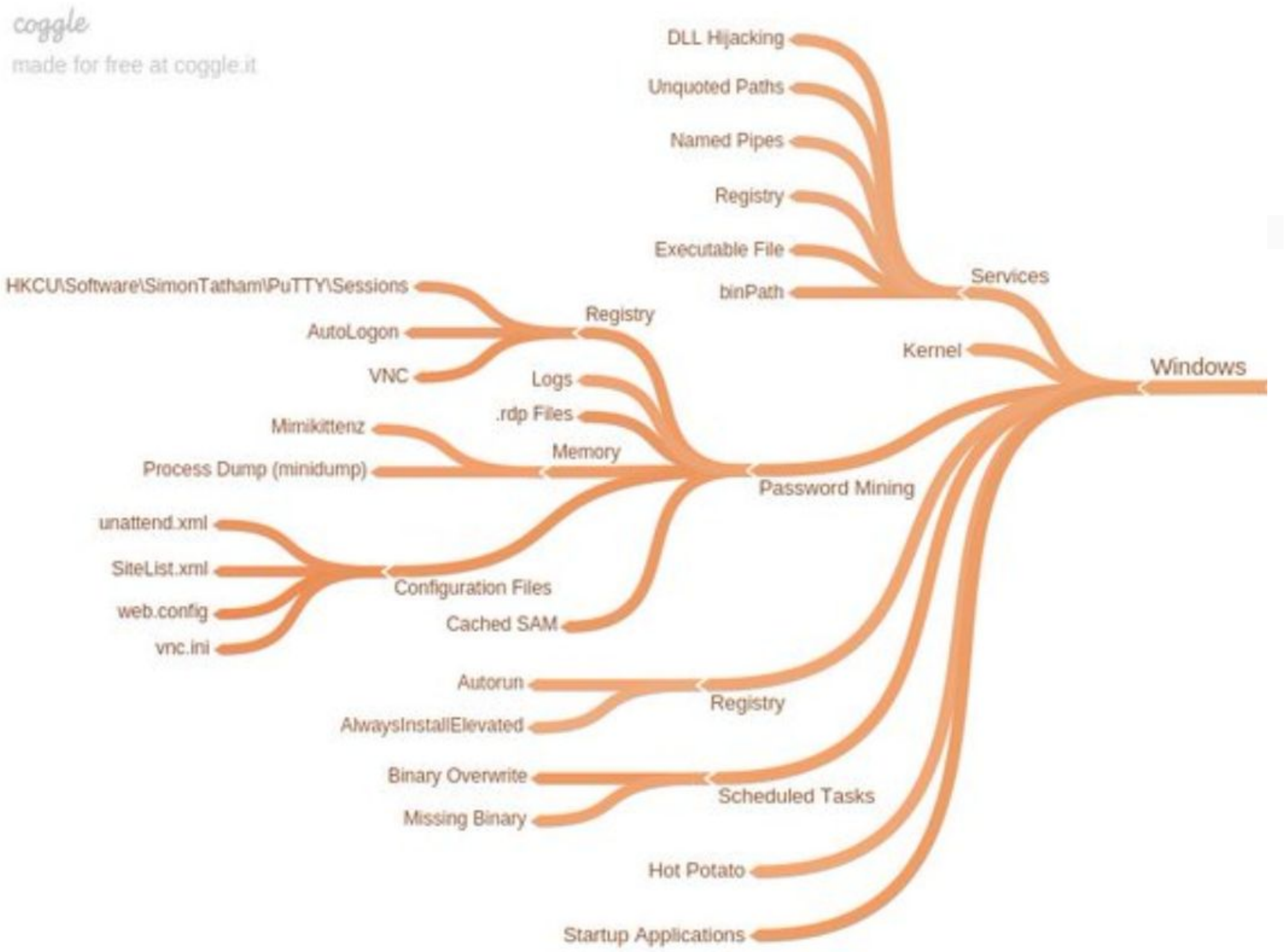
```
Windows Update                                      wuauserv                    C:\Windows\system32\svchost.exe -k netsvcs -p
                                                                                                                                     Manual
CaptureService_8a144                                CaptureService_8a144        C:\Windows\system32\svchost.exe -k LocalService -p
                                                                                                                                     Manual
Clipboard User Service_8a144                        cbdhsvc_8a144               C:\Windows\system32\svchost.exe -k ClipboardSvcGroup -p
                                                                                                                                     Manual
Connected Devices Platform User Service_8a144       CDPUserSvc_8a144            C:\Windows\system32\svchost.exe -k UnistackSvcGroup
                                                                                                                                     Auto
ConsentUX_8a144                                     ConsentUxUserSvc_8a144      C:\Windows\system32\svchost.exe -k DevicesFlow
                                                                                                                                     Manual
DevicePicker_8a144                                  DevicePickerUserSvc_8a144   C:\Windows\system32\svchost.exe -k DevicesFlow
                                                                                                                                     Manual
DevicesFlow_8a144                                   DevicesFlowUserSvc_8a144    C:\Windows\system32\svchost.exe -k DevicesFlow
                                                                                                                                     Manual
Contact Data_8a144                                  PimIndexMaintenanceSvc_8a144 C:\Windows\system32\svchost.exe -k UnistackSvcGroup
                                                                                                                                     Manual
PrintWorkflow_8a144                                 PrintWorkflowUserSvc_8a144  C:\Windows\system32\svchost.exe -k PrintWorkflow
                                                                                                                                     Manual
User Data Storage_8a144                             UnistoreSvc_8a144           C:\Windows\System32\svchost.exe -k UnistackSvcGroup
                                                                                                                                     Manual
User Data Access_8a144                              UserDataSvc_8a144           C:\Windows\system32\svchost.exe -k UnistackSvcGroup
                                                                                                                                     Manual
Windows Push Notifications User Service_8a144       WpnUserService_8a144        C:\Windows\system32\svchost.exe -k UnistackSvcGroup
                                                                                                                                     Auto
```

DLL Hijacking
Weak Service File permissions
Insecure Service Permissions
Unquote Service Path

Enumerating Registry Keys



```
PS C:\Users\user> Get-Acl -Path hklm:\System\CurrentControlSet\services\* | Format-List | more


Path   : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\.NET CLR Data
Owner  : NT AUTHORITY\SYSTEM
Group  : NT AUTHORITY\SYSTEM
Access : BUILTIN\Users Allow  ReadKey
         BUILTIN\Users Allow  -2147483648
         BUILTIN\Administrators Allow  FullControl
         BUILTIN\Administrators Allow  268435456
         NT AUTHORITY\SYSTEM Allow  FullControl
         NT AUTHORITY\SYSTEM Allow  268435456
         CREATOR OWNER Allow  268435456
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadKey
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  -2147483648
         S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681 Allow  ReadKey
         S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681 Allow  -2147483648
Audit  :
Sddl   : O:SYG:SYD:AI(A;ID;KR;;;BU)(A;CIIOID;GR;;;BU)(A;ID;KA;;;BA)(A;CIIOID;GA;;;BA)(A;ID;KA;;;SY)(A;CIIOID;GA;;;SY)(A;CIIOID;GA;;;CO)(A;ID;KR;;;AC)(A;CIIOID;GR;;;AC)(A;ID;KR;;;S-1-15-3-1
         024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681)(A;CIIOID;GR;;;S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-32321
         35806-4053264122-3456934681)

Path   : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\.NET CLR Networking
Owner  : NT AUTHORITY\SYSTEM
Group  : NT AUTHORITY\SYSTEM
Access : BUILTIN\Users Allow  ReadKey
         BUILTIN\Users Allow  -2147483648
         BUILTIN\Administrators Allow  FullControl
         BUILTIN\Administrators Allow  268435456
         NT AUTHORITY\SYSTEM Allow  FullControl
         NT AUTHORITY\SYSTEM Allow  268435456
         CREATOR OWNER Allow  268435456
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadKey
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  -2147483648
         S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681 Allow  ReadKey
         S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681 Allow  -2147483648
Audit  :
Sddl   : O:SYG:SYD:AI(A;ID;KR;;;BU)(A;CIIOID;GR;;;BU)(A;ID;KA;;;BA)(A;CIIOID;GA;;;BA)(A;ID;KA;;;SY)(A;CIIOID;GA;;;SY)(A;CIIOID;GA;;;CO)(A;ID;KR;;;AC)(A;CIIOID;GR;;;AC)(A;ID;KR;;;S-1-15-3-1
         024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681)(A;CIIOID;GR;;;S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-32321
         35806-4053264122-3456934681)
```


coggle
made for free at coggle.it
Windows
Services
DLL Hijacking
Unquoted Paths
Named Pipes
Registry
Executable File
binPath
Kernel
Password Mining
Registry
HKCU\Software\SimonTatham\PuTTY\Sessions
AutoLogon
VNC
Logs
.rdp Files
Memory
Mimikittenz
Process Dump (minidump)
Configuration Files
unattend.xml
SiteList.xml
web.config
vnc.ini
Cached SAM
Registry
Autorun
AlwaysInstallElevated
Scheduled Tasks
Binary Overwrite
Missing Binary
Hot Potato
Startup Applications

THE BRIDGE