Windows API Exploitation Recipes for Red – Blue Teams

Vivek Ramachandran

Chief Trainer, Pentester Academy

http://PentesterAcademy.com

Process Listing APIs: WTSEnumerateProcessesEx Part 2

WTSEnumerateProcessesEx()

```
BOOL WINAPI WTSEnumerateProcessesEx(
  _In_    HANDLE hServer,
  _Inout_ DWORD  *pLevel,
  _In_    DWORD  SessionID,
  _Out_   LPTSTR *ppProcessInfo,
  _Out_   DWORD  *pCount
);
```

https://msdn.microsoft.com/en-us/library/windows/desktop/ee621013(v=vs.85).aspx

- Uses the Remote Desktop API to get the list of processes
- Works both for local and remote systems

More info? Love the EX ☺

```
typedef struct _WTS_PROCESS_INFO_EX {
  DWORD          SessionId;
  DWORD          ProcessId;
  LPTSTR         pProcessName;
  PSID           pUserSid;
  DWORD          NumberOfThreads;
  DWORD          HandleCount;
  DWORD          PagefileUsage;
  DWORD          PeakPagefileUsage;
  DWORD          WorkingSetSize;
  DWORD          PeakWorkingSetSize;
  LARGE_INTEGER UserTime;
  LARGE_INTEGER KernelTime;
} WTS_PROCESS_INFO_EX, *PWTS_PROCESS_INFO_EX;
```

What more info can we get?

- Convert SID to string
- Use SID to get account name and domain

ConvertSidToStringSid

```
BOOL ConvertSidToStringSid(
  _In_  PSID   Sid,
  _Out_ LPTSTR *StringSid
);
```

https://msdn.microsoft.com/en-us/library/windows/desktop/aa376399(v=vs.85).aspx

LookupAccountSid

```
BOOL WINAPI LookupAccountSid(
  _In_opt_  LPCTSTR        lpSystemName,
  _In_      PSID           lpSid,
  _Out_opt_ LPTSTR         lpName,
  _Inout_   LPDWORD        cchName,
  _Out_opt_ LPTSTR         lpReferencedDomainName,
  _Inout_   LPDWORD        cchReferencedDomainName,
  _Out_     PSID_NAME_USE peUse
);
```

https://msdn.microsoft.com/en-us/library/windows/desktop/aa379166(v=vs.85).aspx

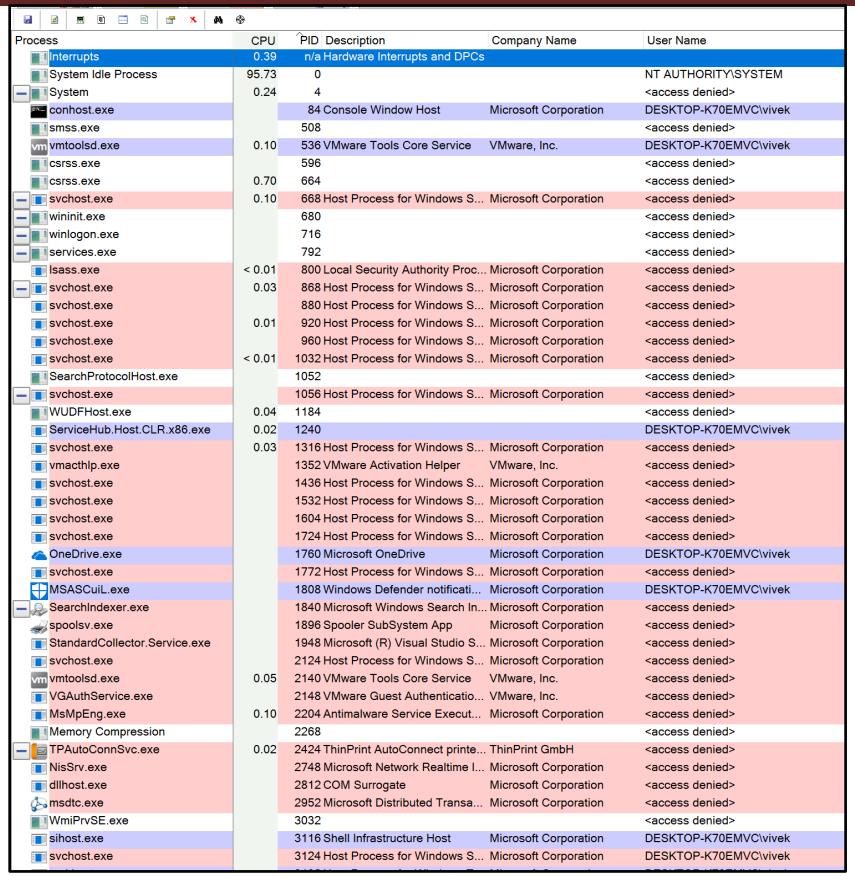
Games II ☺

```
Processes Found: 76

#       PID     Handles Threads Process Name    SID     Account

1       0       0       1               Error: ConvertSidToStringSid failed with error 87: The parameter is incorrect.
 Error: LookupAccountSid failed with error 87: The parameter is incorrect.
2       4       1174    98      System  Error: ConvertSidToStringSid failed with error 87: The parameter is incorrect.
Error: LookupAccountSid failed with error 87: The parameter is incorrect.
3       508     51      3       smss.exe        Error: ConvertSidToStringSid failed with error 87: The parameter is incorrect.
Error: LookupAccountSid failed with error 87: The parameter is incorrect.
4       596     374     11      csrss.exe       Error: ConvertSidToStringSid failed with error 87: The parameter is incorrect.
Error: LookupAccountSid failed with error 87: The parameter is incorrect.
5       664     440     12      csrss.exe       Error: ConvertSidToStringSid failed with error 87: The parameter is incorrect.
Error: LookupAccountSid failed with error 87: The parameter is incorrect.
6       680     89      2       wininit.exe     Error: ConvertSidToStringSid failed with error 87: The parameter is incorrect.
Error: LookupAccountSid failed with error 87: The parameter is incorrect.
7       716     187     3       winlogon.exe    Error: ConvertSidToStringSid failed with error 87: The parameter is incorrect.
Error: LookupAccountSid failed with error 87: The parameter is incorrect.
8       792     277     4       services.exe    Error: ConvertSidToStringSid failed with error 87: The parameter is incorrect.
Error: LookupAccountSid failed with error 87: The parameter is incorrect.
9       800     1017    8       lsass.exe       Error: ConvertSidToStringSid failed with error 87: The parameter is incorrect.
Error: LookupAccountSid failed with error 87: The parameter is incorrect.
10      868     704     16      svchost.exe     Error: ConvertSidToStringSid failed with error 87: The parameter is incorrect.
Error: LookupAccountSid failed with error 87: The parameter is incorrect.
11      920     735     11      svchost.exe     Error: ConvertSidToStringSid failed with error 87: The parameter is incorrect.
Error: LookupAccountSid failed with error 87: The parameter is incorrect.
12      668     3970    73      svchost.exe     Error: ConvertSidToStringSid failed with error 87: The parameter is incorrect.
Error: LookupAccountSid failed with error 87: The parameter is incorrect.
13      880     563     23      svchost.exe     Error: ConvertSidToStringSid failed with error 87: The parameter is incorrect.
Error: LookupAccountSid failed with error 87: The parameter is incorrect.
14      960     666     16      svchost.exe     Error: ConvertSidToStringSid failed with error 87: The parameter is incorrect.
Error: LookupAccountSid failed with error 87: The parameter is incorrect.
15      1032    1226    32      svchost.exe     Error: ConvertSidToStringSid failed with error 87: The parameter is incorrect.
Error: LookupAccountSid failed with error 87: The parameter is incorrect.
16      1056    890     19      svchost.exe     Error: ConvertSidToStringSid failed with error 87: The parameter is incorrect.
Error: LookupAccountSid failed with error 87: The parameter is incorrect.
17      1184    352     7       WUDFHost.exe    Error: ConvertSidToStringSid failed with error 87: The parameter is incorrect.
Error: LookupAccountSid failed with error 87: The parameter is incorrect.
18      1316    496     20      svchost.exe     Error: ConvertSidToStringSid failed with error 87: The parameter is incorrect.
Error: LookupAccountSid failed with error 87: The parameter is incorrect.
19      1352    95      2       vmacthlp.exe    Error: ConvertSidToStringSid failed with error 87: The parameter is incorrect.
Error: LookupAccountSid failed with error 87: The parameter is incorrect.
20      1436    591     19      svchost.exe     Error: ConvertSidToStringSid failed with error 87: The parameter is incorrect.
Error: LookupAccountSid failed with error 87: The parameter is incorrect.
21      1532    212     6       svchost.exe     Error: ConvertSidToStringSid failed with error 87: The parameter is incorrect.
```

What’s wrong? Let’s check Process Explorer



Process	CPU	PID	Description	Company Name	User Name
Interrupts	0.39	n/a	Hardware Interrupts and DPCs		
System Idle Process	95.73	0			NT AUTHORITY\SYSTEM
System	0.24	4			<access denied>
conhost.exe		84	Console Window Host	Microsoft Corporation	DESKTOP-K70EMVC\vivek
smss.exe		508			<access denied>
vmtoolsd.exe	0.10	536	VMware Tools Core Service	VMware, Inc.	DESKTOP-K70EMVC\vivek
csrss.exe		596			<access denied>
csrss.exe	0.70	664			<access denied>
svchost.exe	0.10	668	Host Process for Windows S...	Microsoft Corporation	<access denied>
wininit.exe		680			<access denied>
winlogon.exe		716			<access denied>
services.exe		792			<access denied>
lsass.exe	< 0.01	800	Local Security Authority Proc...	Microsoft Corporation	<access denied>
svchost.exe	0.03	868	Host Process for Windows S...	Microsoft Corporation	<access denied>
svchost.exe		880	Host Process for Windows S...	Microsoft Corporation	<access denied>
svchost.exe	0.01	920	Host Process for Windows S...	Microsoft Corporation	<access denied>
svchost.exe		960	Host Process for Windows S...	Microsoft Corporation	<access denied>
svchost.exe	< 0.01	1032	Host Process for Windows S...	Microsoft Corporation	<access denied>
SearchProtocolHost.exe		1052			<access denied>
svchost.exe		1056	Host Process for Windows S...	Microsoft Corporation	<access denied>
WUDFHost.exe	0.04	1184			<access denied>
ServiceHub.Host.CLR.x86.exe	0.02	1240			DESKTOP-K70EMVC\vivek
svchost.exe	0.03	1316	Host Process for Windows S...	Microsoft Corporation	<access denied>
vmacthlp.exe		1352	VMware Activation Helper	VMware, Inc.	<access denied>
svchost.exe		1436	Host Process for Windows S...	Microsoft Corporation	<access denied>
svchost.exe		1532	Host Process for Windows S...	Microsoft Corporation	<access denied>
svchost.exe		1604	Host Process for Windows S...	Microsoft Corporation	<access denied>
svchost.exe		1724	Host Process for Windows S...	Microsoft Corporation	<access denied>
OneDrive.exe		1760	Microsoft OneDrive	Microsoft Corporation	DESKTOP-K70EMVC\vivek
svchost.exe		1772	Host Process for Windows S...	Microsoft Corporation	<access denied>
MSASCuiL.exe		1808	Windows Defender notificati...	Microsoft Corporation	DESKTOP-K70EMVC\vivek
SearchIndexer.exe		1840	Microsoft Windows Search In...	Microsoft Corporation	<access denied>
spoolsv.exe		1896	Spooler SubSystem App	Microsoft Corporation	<access denied>
StandardCollector.Service.exe		1948	Microsoft (R) Visual Studio S...	Microsoft Corporation	<access denied>
svchost.exe		2124	Host Process for Windows S...	Microsoft Corporation	<access denied>
vmtoolsd.exe	0.05	2140	VMware Tools Core Service	VMware, Inc.	<access denied>
VGAuthService.exe		2148	VMware Guest Authenticatio...	VMware, Inc.	<access denied>
MsMpEng.exe	0.10	2204	Antimalware Service Execut...	Microsoft Corporation	<access denied>
Memory Compression		2268			<access denied>
TPAutoConnSvc.exe	0.02	2424	ThinPrint AutoConnect printe...	ThinPrint GmbH	<access denied>
NisSrv.exe		2748	Microsoft Network Realtime I...	Microsoft Corporation	<access denied>
dllhost.exe		2812	COM Surrogate	Microsoft Corporation	<access denied>
msdtc.exe		2952	Microsoft Distributed Transa...	Microsoft Corporation	<access denied>
WmiPrvSE.exe		3032			<access denied>
sihost.exe		3116	Shell Infrastructure Host	Microsoft Corporation	DESKTOP-K70EMVC\vivek
svchost.exe		3124	Host Process for Windows S...	Microsoft Corporation	DESKTOP-K70EMVC\vivek

Shouldn't ADMIN solve it?

```
Processes Found: 74

#       PID     Handles Threads Process Name    SID     Account

1       0       0       1               Error: ConvertSidToStringSid failed with error 87: The parameter is incorrect.
 Error: LookupAccountSid failed with error 87: The parameter is incorrect.
 2      4       1125    118     System  Error: ConvertSidToStringSid failed with error 87: The parameter is incorrect.
 Error: LookupAccountSid failed with error 87: The parameter is incorrect.
 3      508     51      3       smss.exe        S-1-5-18        NT AUTHORITY\SYSTEM
4       596     383     11      csrss.exe       Error: ConvertSidToStringSid failed with error 87: The parameter is incorrect.
 Error: LookupAccountSid failed with error 87: The parameter is incorrect.
 5      664     426     12      csrss.exe       Error: ConvertSidToStringSid failed with error 87: The parameter is incorrect.
 Error: LookupAccountSid failed with error 87: The parameter is incorrect.
 6      680     89      2       wininit.exe     S-1-5-18        NT AUTHORITY\SYSTEM
7       716     195     5       winlogon.exe    S-1-5-18        NT AUTHORITY\SYSTEM
8       792     270     4       services.exe    S-1-5-18        NT AUTHORITY\SYSTEM
9       800     972     8       lsass.exe       S-1-5-18        NT AUTHORITY\SYSTEM
10      868     661     21      svchost.exe     S-1-5-18        NT AUTHORITY\SYSTEM
11      920     719     11      svchost.exe     S-1-5-20        NT AUTHORITY\NETWORK SERVICE
12      668     3894    74      svchost.exe     S-1-5-18        NT AUTHORITY\SYSTEM
13      880     561     23      svchost.exe     S-1-5-19        NT AUTHORITY\LOCAL SERVICE
14      960     659     16      svchost.exe     S-1-5-19        NT AUTHORITY\LOCAL SERVICE
15      1032    1217    31      svchost.exe     S-1-5-19        NT AUTHORITY\LOCAL SERVICE
16      1056    894     18      svchost.exe     S-1-5-18        NT AUTHORITY\SYSTEM
17      1184    352     7       WUDFHost.exe    Error: ConvertSidToStringSid failed with error 87: The parameter is incorrect.
 Error: LookupAccountSid failed with error 87: The parameter is incorrect.
 18     1316    494     20      svchost.exe     S-1-5-19        NT AUTHORITY\LOCAL SERVICE
19      1352    95      2       vmacthlp.exe    S-1-5-18        NT AUTHORITY\SYSTEM
20      1436    588     20      svchost.exe     S-1-5-20        NT AUTHORITY\NETWORK SERVICE
21      1532    228     8       svchost.exe     S-1-5-19        NT AUTHORITY\LOCAL SERVICE
22      1604    352     13      svchost.exe     S-1-5-19        NT AUTHORITY\LOCAL SERVICE
23      1724    363     7       svchost.exe     S-1-5-18        NT AUTHORITY\SYSTEM
24      1840    650     14      SearchIndexer.exe       S-1-5-18        NT AUTHORITY\SYSTEM
25      1896    507     14      spoolsv.exe     S-1-5-18        NT AUTHORITY\SYSTEM
26      1772    585     13      svchost.exe     S-1-5-18        NT AUTHORITY\SYSTEM
27      2124    234     6       svchost.exe     S-1-5-18        NT AUTHORITY\SYSTEM
28      2140    265     8       vmtoolsd.exe    S-1-5-18        NT AUTHORITY\SYSTEM
29      2148    132     3       VGAuthService.exe       S-1-5-18        NT AUTHORITY\SYSTEM
30      2204    652     29      MsMpEng.exe     S-1-5-18        NT AUTHORITY\SYSTEM
31      2268    0       8       Memory Compression      S-1-5-18        NT AUTHORITY\SYSTEM
32      2424    195     8       TPAutoConnSvc.exe       S-1-5-18        NT AUTHORITY\SYSTEM
33      2748    279     8       NisSrv.exe      S-1-5-19        NT AUTHORITY\LOCAL SERVICE
34      2812    217     12      dllhost.exe     S-1-5-18        NT AUTHORITY\SYSTEM
35      2952    187     10      msdtc.exe       S-1-5-20        NT AUTHORITY\NETWORK SERVICE
36      3032    221     9       WmiPrvSE.exe    Error: ConvertSidToStringSid failed with error 87: The parameter is incorrect.
 Error: LookupAccountSid failed with error 87: The parameter is incorrect.
 37     3116    403     10      sihost.exe      S-1-5-21-3504999536-1538188155-3485737794-1001  DESKTOP-K70EMVC\vivek
38      3124    307     6       svchost.exe     S-1-5-21-3504999536-1538188155-3485737794-1001  DESKTOP-K70EMVC\vivek
39      3192    439     16      taskhostw.exe   S-1-5-21-3504999536-1538188155-3485737794-1001  DESKTOP-K70EMVC\vivek
```

Thank You!