Windows API Exploitation Recipes for Red – Blue Teams

Vivek Ramachandran

Chief Trainer, Pentester Academy

http://PentesterAcademy.com

Process Listing APIs: WTSEnumerateProcessesEx Part 3

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

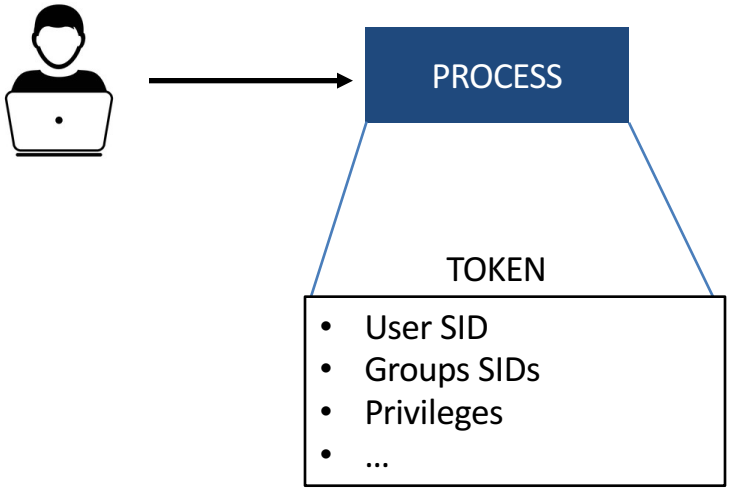
Shouldn't ADMIN solve it?

```
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
```

Process Tokens



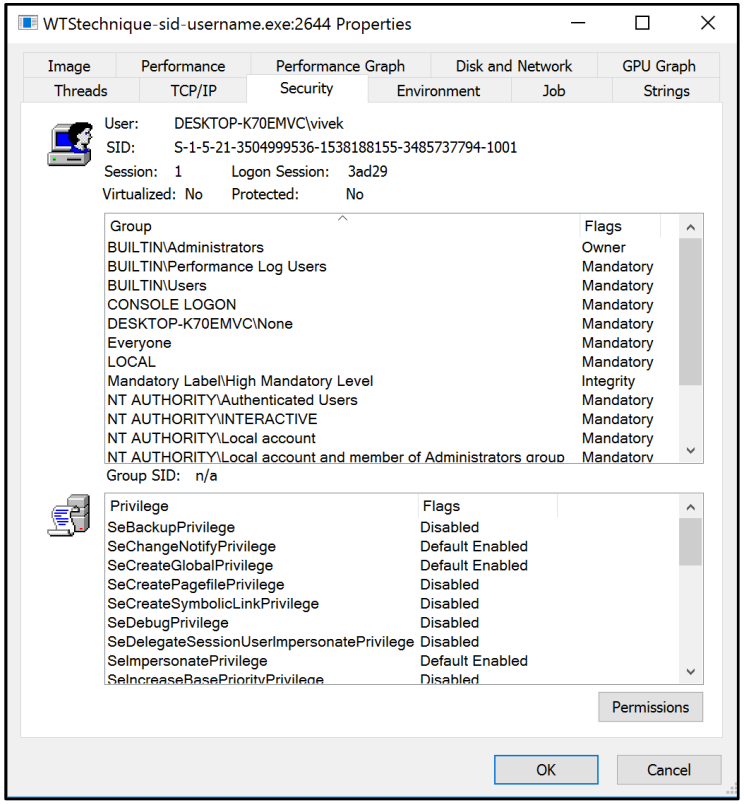
SID: https://msdn.microsoft.com/en-us/library/windows/desktop/aa379571(v=vs.85).aspx

Privileges: https://msdn.microsoft.com/en-us/library/windows/desktop/bb530716(v=vs.85).aspx

SID and Privileges

- SID:
  - Trustee identification
  - Unique for every user account across domain
  - Format:
    https://msdn.microsoft.com/en-us/library/windows/desktop/aa379597(v=vs.85).aspx
- Privileges
  - Right to perform system operations
  - E.g. Shutdown, Debugging other processes

Privileges



- Not all privileges will be enabled by default
- A process can enable/disable available privileges

Adjusting Privileges

- LookupPrivilegeValue()
  https://msdn.microsoft.com/en-us/library/windows/desktop/aa379180(v=vs.85).aspx

- OpenProcessToken()
  https://msdn.microsoft.com/en-us/library/windows/desktop/aa379295(v=vs.85).aspx

- AdjustTokenPrivileges()
  https://msdn.microsoft.com/en-us/library/windows/desktop/aa375202(v=vs.85).aspx

Thank You!