



# Windows API Exploitation Recipes for Red – Blue Teams

Vivek Ramachandran

Chief Trainer, Pentester Academy

<http://PentesterAcademy.com>

©Pentester Academy

# Process Listing APIs: WTSEnumerateProcessesEx Part 1

# 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](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

# What information is available?

```
typedef struct _WTS_PROCESS_INFO {  
    DWORD SessionId;  
    DWORD ProcessId;  
    LPTSTR pProcessName;  
    PSID pUserSid;  
} WTS_PROCESS_INFO, *PWTS_PROCESS_INFO;
```

# 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;
```

# Let the Games begin!

```
C:\Users\vivek\Desktop\Course\Process Listing Remote Desktop API\Basics\64\Debug
Processes Found: 62
#      PID      Handles Threads Process Name
1       0         0         1      System
2       4       1119      95     System
3      508        51         3     smss.exe
4      596       374        11     csrss.exe
5      664       374        12     csrss.exe
6      680        89         2     wininit.exe
7      716       187         3     winlogon.exe
8      792       271         4     services.exe
9      800       952         8     lsass.exe
10     868       701        19     svchost.exe
11     920       690        10     svchost.exe
12     668     3854        67     svchost.exe
13     880       559        22     svchost.exe
14     960       657        15     svchost.exe
15    1032     1193        32     svchost.exe
16    1056     842         20     svchost.exe
17    1184     349         6     WUDFHost.exe
18    1316     494         20     svchost.exe
19    1352     95          2     vmacthlp.exe
20    1436     583         20     svchost.exe
21    1532     212         5     svchost.exe
22    1604     352         13     svchost.exe
23    1724     365         7     svchost.exe
24    1840     653         15     SearchIndexer.exe
25    1896     509         15     spoolsv.exe
26    1772     578         12     svchost.exe
27    2124     232         6     svchost.exe
28    2140     267         8     vmtoolsd.exe
29    2148     132         3     VGAuthService.exe
30    2204     519         24     MsMpEng.exe
31    2268     0          16     Memory Compression
32    2424     198         8     TPAutoConnSvc.exe
33    2748     281         9     NisSrv.exe
34    2812     217         12     dllhost.exe
35    2952     187         10     msdtc.exe
36    3032     221         9     WmiPrvSE.exe
37    3116     417         8     sihost.exe
38    3124     307         6     svchost.exe
39    3192     440         15     taskhostw.exe
```

# Verification

- Sysinternals Toolsuite

<https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx>

- Process Explorer

# Thank You!

PentesterAcademy

a SecurityTube.net initiative

Follow @SecurityTube 89.6K followers

Recommend Share 311K



ALL COURSES

PRICING

WHY SUBSCRIBE

TESTIMONIALS

MEMBER ACCESS

**120+ Hrs HD Content!**  
**900+ Videos!**  
**Expert Trainers**

©Pentester Academy