Windows API Exploitation Recipes for Red – Blue Teams

Vivek Ramachandran

Chief Trainer, Pentester Academy

http://PentesterAcademy.com

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

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

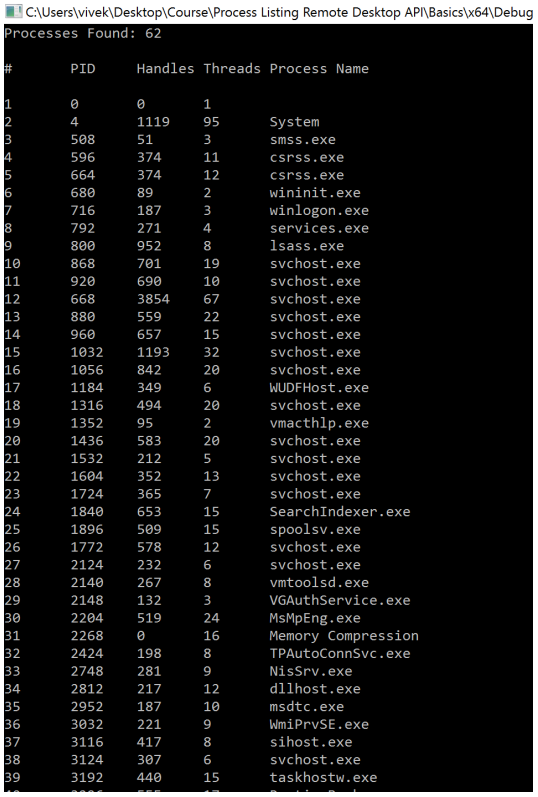
What information is available?

```
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!



Verification

- Sysinternals Toolsuite

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

- Process Explorer

Thank You!