Windows API Exploitation Recipes for Red – Blue Teams

Vivek Ramachandran

Chief Trainer, Pentester Academy

http://PentesterAcademy.com

Process Listing APIs:
Process Status API: EnumProcess

PSAPI: EnumProcess()

EnumProcesses function

Retrieves the process identifier for each process object in the system.

Syntax

C++

```
BOOL WINAPI EnumProcesses(
  _Out_ DWORD *pProcessIds,
  _In_  DWORD cb,
  _Out_ DWORD *pBytesReturned
);
```

https://msdn.microsoft.com/en-us/library/windows/desktop/ms682629(v=vs.85).aspx

Let’s Roll!

```
67      3924    \Device\HarddiskVolume2\Program Files (x86)\Microsoft Visual Studio\2017\Professional\Common7\IDE\VC\vcpackages\vcpkgsrv.exe
68      3452    \Device\HarddiskVolume2\Program Files (x86)\Microsoft Visual Studio\2017\Professional\Common7\ServiceHub\Hosts\ServiceHub.Host.CLR.AnyCPU\ServiceHu
69      6068    Error: OpenProcess() failed with error 5: Access is denied.

70      492     Error: OpenProcess() failed with error 5: Access is denied.

71      4924    \Device\HarddiskVolume2\Windows\System32\audiodg.exe
72      6752    Error: OpenProcess() failed with error 5: Access is denied.

73      5188    \Device\HarddiskVolume2\Program Files (x86)\Microsoft Visual Studio\2017\Professional\Common7\IDE\PrivateAssemblies\ScriptedSandbox64.exe
74      1644    \Device\HarddiskVolume2\Program Files (x86)\Microsoft Visual Studio\2017\Professional\MSBuild\15.0\Bin\MSBuild.exe
75      3500    \Device\HarddiskVolume2\Windows\System32\conhost.exe
76      4524    \Device\HarddiskVolume2\Program Files (x86)\Microsoft Visual Studio\2017\Professional\VC\Tools\MSVC\14.10.25017\bin\HostX86\x86\mspdbsrv.exe
77      5628    \Device\HarddiskVolume2\Windows\System32\smartscreen.exe
78      6228    Error: OpenProcess() failed with error 5: Access is denied.

79      4184    Error: OpenProcess() failed with error 5: Access is denied.

80      2128    Error: OpenProcess() failed with error 5: Access is denied.

81      4844    \Device\HarddiskVolume2\Windows\System32\cmd.exe
82      6792    \Device\HarddiskVolume2\Windows\System32\conhost.exe
83      896     \Device\HarddiskVolume2\Windows\System32\backgroundTaskHost.exe
84      2224    \Device\HarddiskVolume2\Users\vivek\Documents\Visual Studio 2017\Projects\ListProcesses\x64\Debug\ListProcesses.exe
```

Do we need PRIVS?

Value	Meaning
PROCESS_ALL_ACCESS	All possible access rights for a process object. **Windows Server 2003 and Windows XP:** The size of the **PROCESS_ALL_ACCESS** flag increased on Windows Server 2008 and Windows Vista. If an application compiled for Windows Server 2008 and Windows Vista is run on Windows Server 2003 or Windows XP, the **PROCESS_ALL_ACCESS** flag is too large and the function specifying this flag fails with **ERROR_ACCESS_DENIED**. To avoid this problem, specify the minimum set of access rights required for the operation. If **PROCESS_ALL_ACCESS** must be used, set _WIN32_WINNT to the minimum operating system targeted by your application (for example, `#define _WIN32_WINNT _WIN32_WINNT_WINXP`). For more information, see Using the Windows Headers.
PROCESS_CREATE_PROCESS (0x0080)	Required to create a process.
PROCESS_CREATE_THREAD (0x0002)	Required to create a thread.
PROCESS_DUP_HANDLE (0x0040)	Required to duplicate a handle using **DuplicateHandle**.
PROCESS_QUERY_INFORMATION (0x0400)	Required to retrieve certain information about a process, such as its token, exit code, and priority class (see **OpenProcessToken**).
PROCESS_QUERY_LIMITED_INFORMATION (0x1000)	Required to retrieve certain information about a process (see **GetExitCodeProcess**, **GetPriorityClass**, **IsProcessInJob**, **QueryFullProcessImageName**). A handle that has the **PROCESS_QUERY_INFORMATION** access right is automatically granted **PROCESS_QUERY_LIMITED_INFORMATION**. **Windows Server 2003 and Windows XP:** This access right is not supported.

https://msdn.microsoft.com/en-us/library/windows/desktop/ms684880(v=vs.85).aspx

Let’s Roll with Privs!

```
33      2052    \Device\HarddiskVolume2\Program Files\Windows Defender\MsMpEng.exe
34      2756    \Device\HarddiskVolume2\Windows\System32\svchost.exe
35      2776    \Device\HarddiskVolume2\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe
36      2908    \Device\HarddiskVolume2\Windows\System32\wbem\WmiPrvSE.exe
37      3008    \Device\HarddiskVolume2\Windows\System32\dllhost.exe
38      2580    \Device\HarddiskVolume2\Windows\System32\msdtc.exe
39      3312    \Device\HarddiskVolume2\Program Files\Windows Defender\NisSrv.exe
40      3804    \Device\HarddiskVolume2\Windows\System32\SearchIndexer.exe
41      3792    \Device\HarddiskVolume2\Windows\System32\sihost.exe
42      2576    \Device\HarddiskVolume2\Windows\System32\svchost.exe
43      2624    \Device\HarddiskVolume2\Windows\System32\taskhostw.exe
44      3256    \Device\HarddiskVolume2\Program Files\VMware\VMware Tools\TPAutoConnect.exe
45      4084    \Device\HarddiskVolume2\Windows\System32\conhost.exe
46      1612    \Device\HarddiskVolume2\Windows\System32\RuntimeBroker.exe
47      992     \Device\HarddiskVolume2\Windows\explorer.exe
48      3484    \Device\HarddiskVolume2\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe
49      3832    \Device\HarddiskVolume2\Program Files\Windows Defender\MSASCuiL.exe
50      2088    \Device\HarddiskVolume2\Program Files\VMware\VMware Tools\vmtoolsd.exe
51      2408    \Device\HarddiskVolume2\Users\vivek\AppData\Local\Microsoft\OneDrive\OneDrive.exe
52      4060    \Device\HarddiskVolume2\Program Files (x86)\Xoreax\IncrediBuild\xgTrayIcon.exe
53      6620    \Device\HarddiskVolume2\Windows\System32\ApplicationFrameHost.exe
54      3948    \Device\HarddiskVolume2\Windows\ImmersiveControlPanel\SystemSettings.exe
55      6584    \Device\HarddiskVolume2\Windows\System32\dllhost.exe
56      7120    \Device\HarddiskVolume2\Windows\System32\taskhostw.exe
57      5164    \Device\HarddiskVolume2\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe
58      3188    \Device\HarddiskVolume2\Program Files\WindowsApps\Microsoft.SkypeApp_11.12.112.0_x64__kzf8qxf38zg5c\SkypeHost.exe
59      5112    \Device\HarddiskVolume2\Program Files (x86)\Microsoft Visual Studio\2017\Professional\Common7\IDE\devenv.exe
60      2044    \Device\HarddiskVolume2\Program Files (x86)\Microsoft Visual Studio\2017\Professional\Common7\IDE\PerfWatson2.exe
61      4016    \Device\HarddiskVolume2\Program Files (x86)\Microsoft Visual Studio\2017\Professional\Common7\ServiceHub\Hosts\ServiceHub.Host.N
```

Conclusion?

- Noisy compared to CreateToolhelp32Snapshot
- Requires calls to OpenProcess()
  - We might need to obfuscate this in binary
  - API call obfuscation techniques to be discussed later

Thank You!