Windows API Exploitation Recipes for Red – Blue Teams

Vivek Ramachandran

Chief Trainer, Pentester Academy

http://PentesterAcademy.com

Requesting Elevation: ShellExecuteEx()

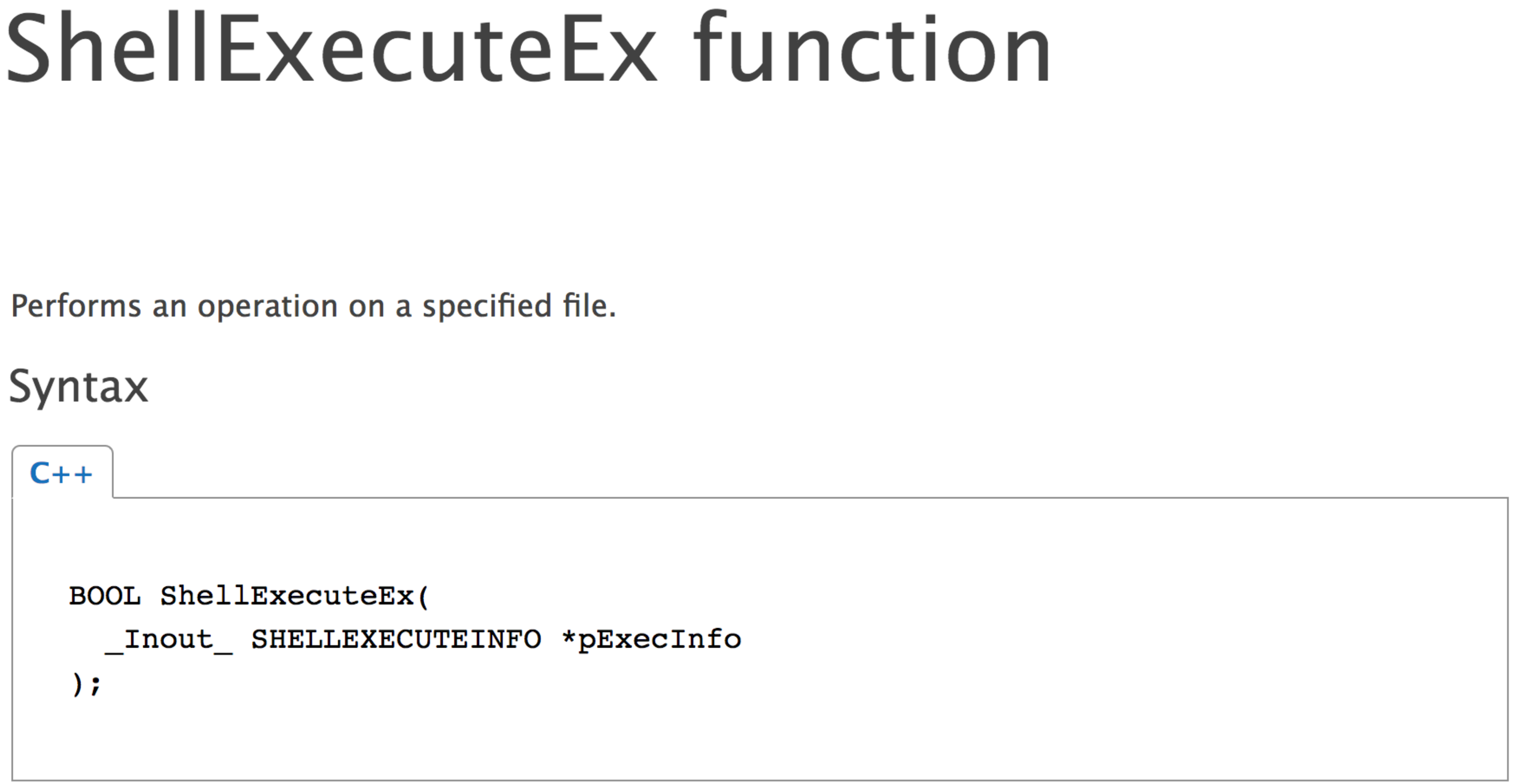
Solving the Problem Permanently!

- Program starts
- Detects if its running privileged
- No? relaunch itself!
- Alternately, have a manifest file which forces this when invoked

Runtime Checking and Re-Launch

- Runtime Checking for Privileges
  - Covered in last videos
- Re-Launch requesting for Privileges
  - ShellExecuteEx

ShellExecuteEx()



ShellExecuteEx function

Performs an operation on a specified file.

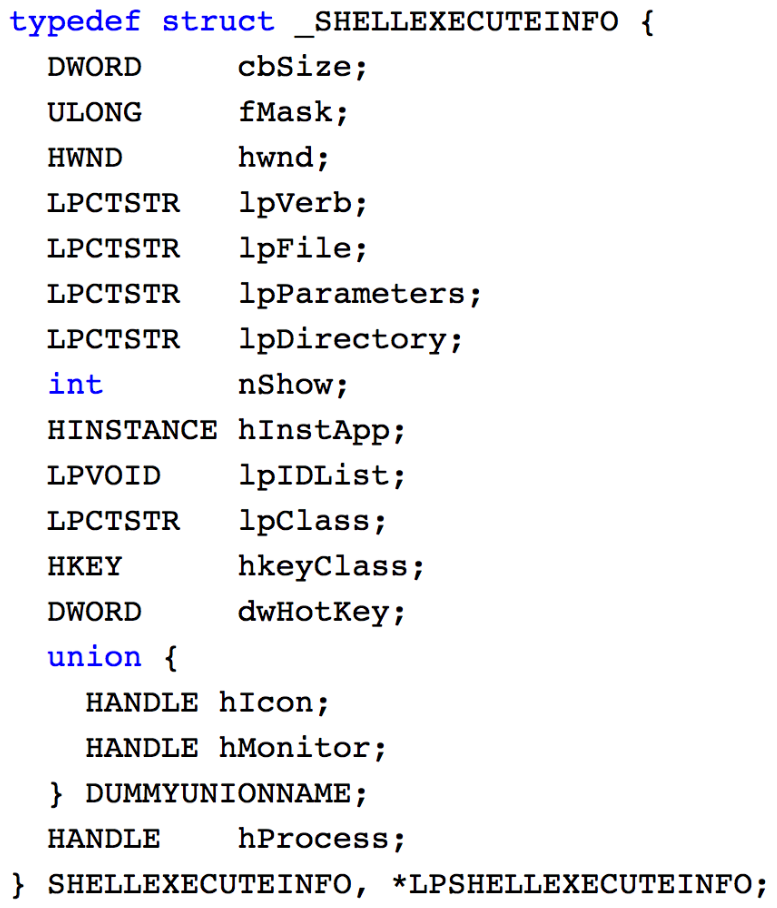
Syntax

C++

```
BOOL ShellExecuteEx(
  _Inout_ SHELLEXECUTEINFO *pExecInfo
);
```

https://msdn.microsoft.com/en-us/library/windows/desktop/bb762154(v=vs.85).aspx

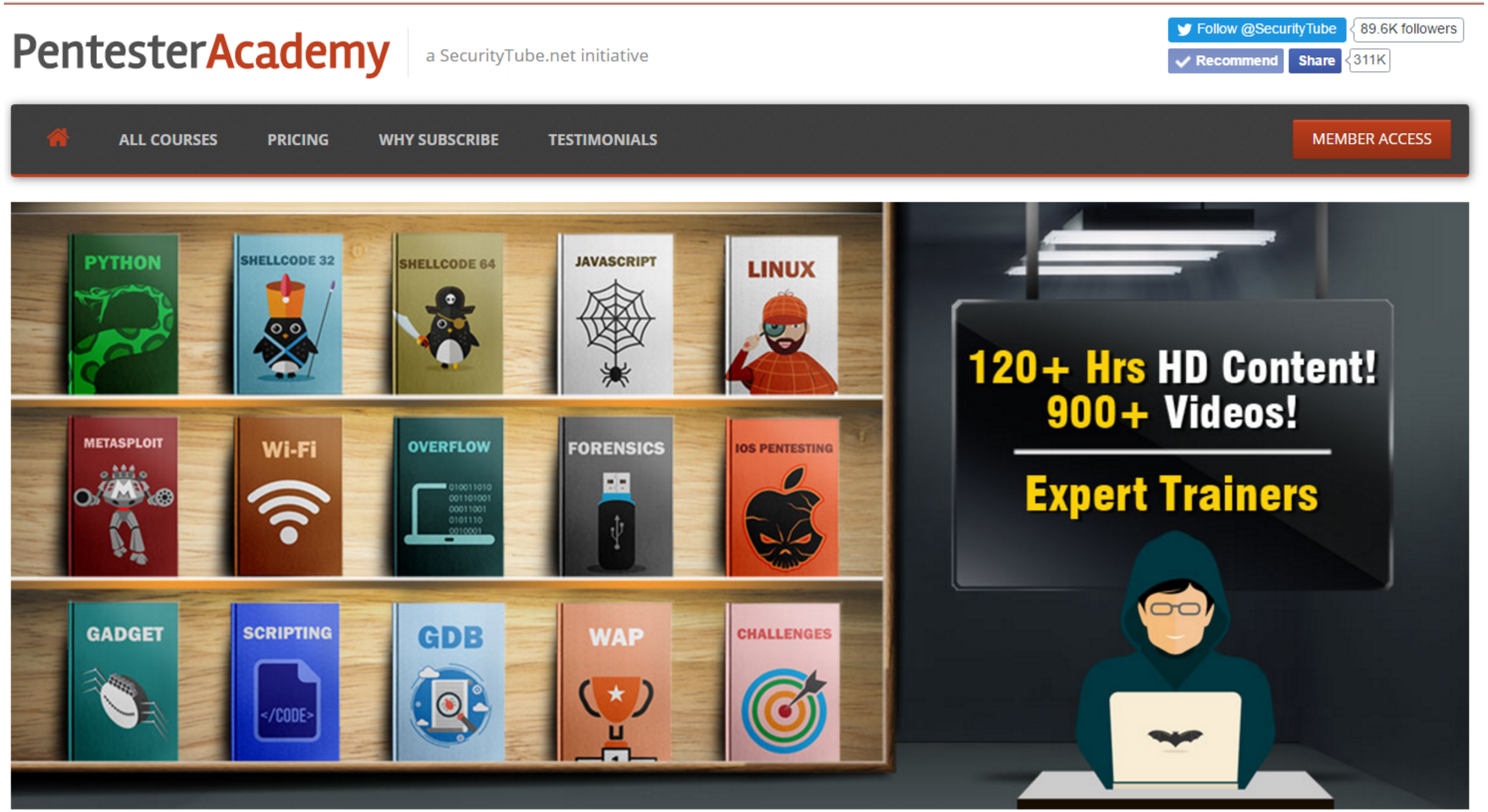
SHELLEXECUTEINFO



```
typedef struct _SHELLEXECUTEINFO {
  DWORD     cbSize;
  ULONG     fMask;
  HWND      hwnd;
  LPCTSTR   lpVerb;
  LPCTSTR   lpFile;
  LPCTSTR   lpParameters;
  LPCTSTR   lpDirectory;
  int       nShow;
  HINSTANCE hInstApp;
  LPVOID    lpIDList;
  LPCTSTR   lpClass;
  HKEY      hkeyClass;
  DWORD     dwHotKey;
  union {
    HANDLE hIcon;
    HANDLE hMonitor;
  } DUMMYUNIONNAME;
  HANDLE    hProcess;
} SHELLEXECUTEINFO, *LPSHELLEXECUTEINFO;
```

https://msdn.microsoft.com/en-us/library/windows/desktop/bb759784(v=vs.85).aspx

Thank You!


PentesterAcademy
a SecurityTube.net initiative
Follow @SecurityTube
89.6K followers
Recommend
Share
311K
ALL COURSES
PRICING
WHY SUBSCRIBE
TESTIMONIALS
MEMBER ACCESS
PYTHON
SHELLCODE 32
SHELLCODE 64
JAVASCRIPT
LINUX
METASPLOIT
Wi-Fi
OVERFLOW
FORENSICS
IOS PENTESTING
GADGET
SCRIPTING
</CODE>
GDB
WAP
CHALLENGES
120+ Hrs HD Content!
900+ Videos!
Expert Trainers