Windows API Exploitation Recipes for Red – Blue Teams

Vivek Ramachandran

Chief Trainer, Pentester Academy

http://PentesterAcademy.com

©Pentester Academy

Process Memory:Read Basics with Toolhelp32ReadProcessMemory

©Pentester Academy

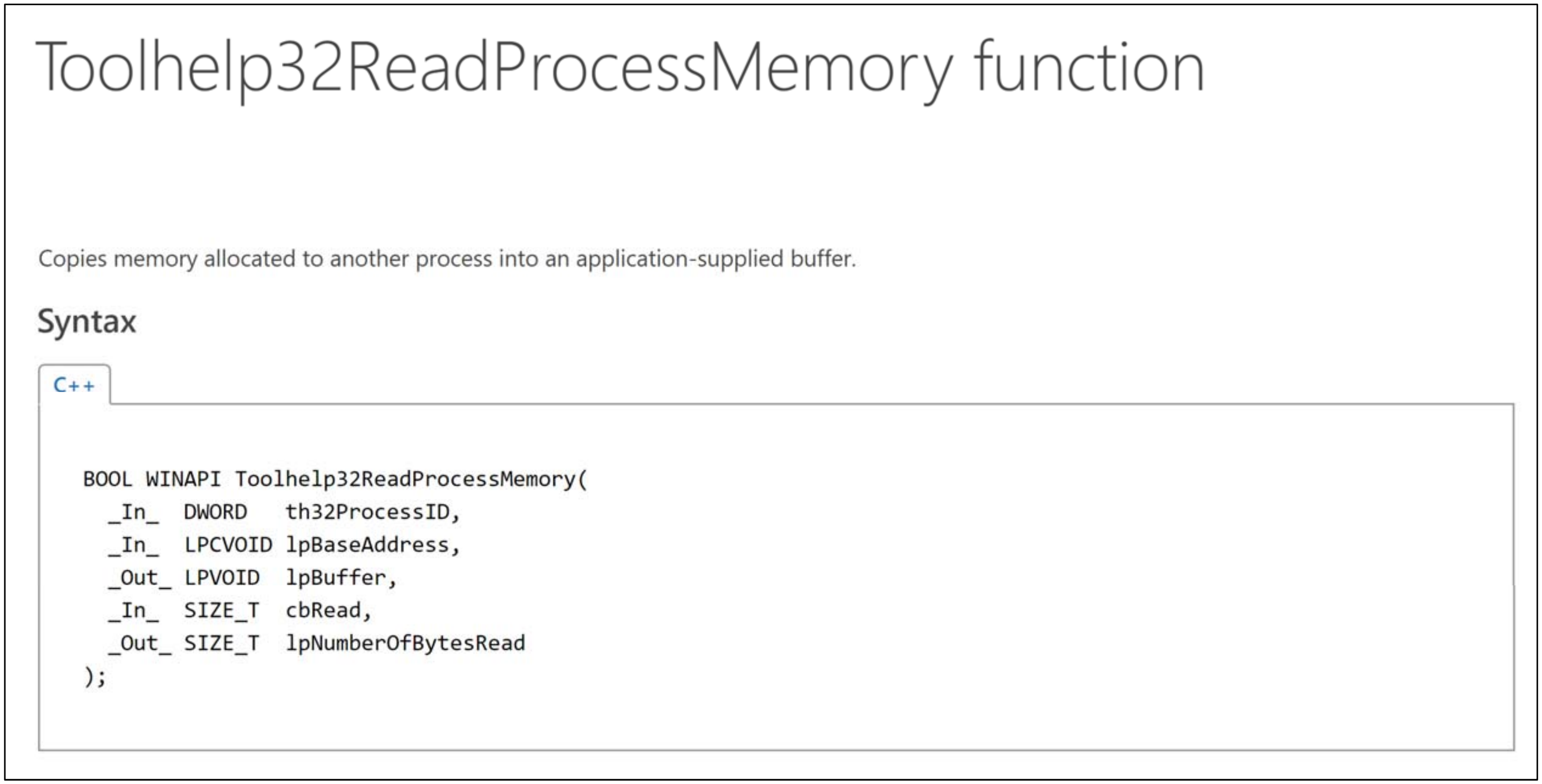
Reading Process memory

- Process Debug privileges

- What can we read?
  - Anything in memory
  - Might have to search to find interesting information
  - Could recover sensitive information e.g. passwords, hashes, tokens etc.

©Pentester Academy

Toolhelp32ReadProcessMemory



Toolhelp32ReadProcessMemory function

Copies memory allocated to another process into an application-supplied buffer.

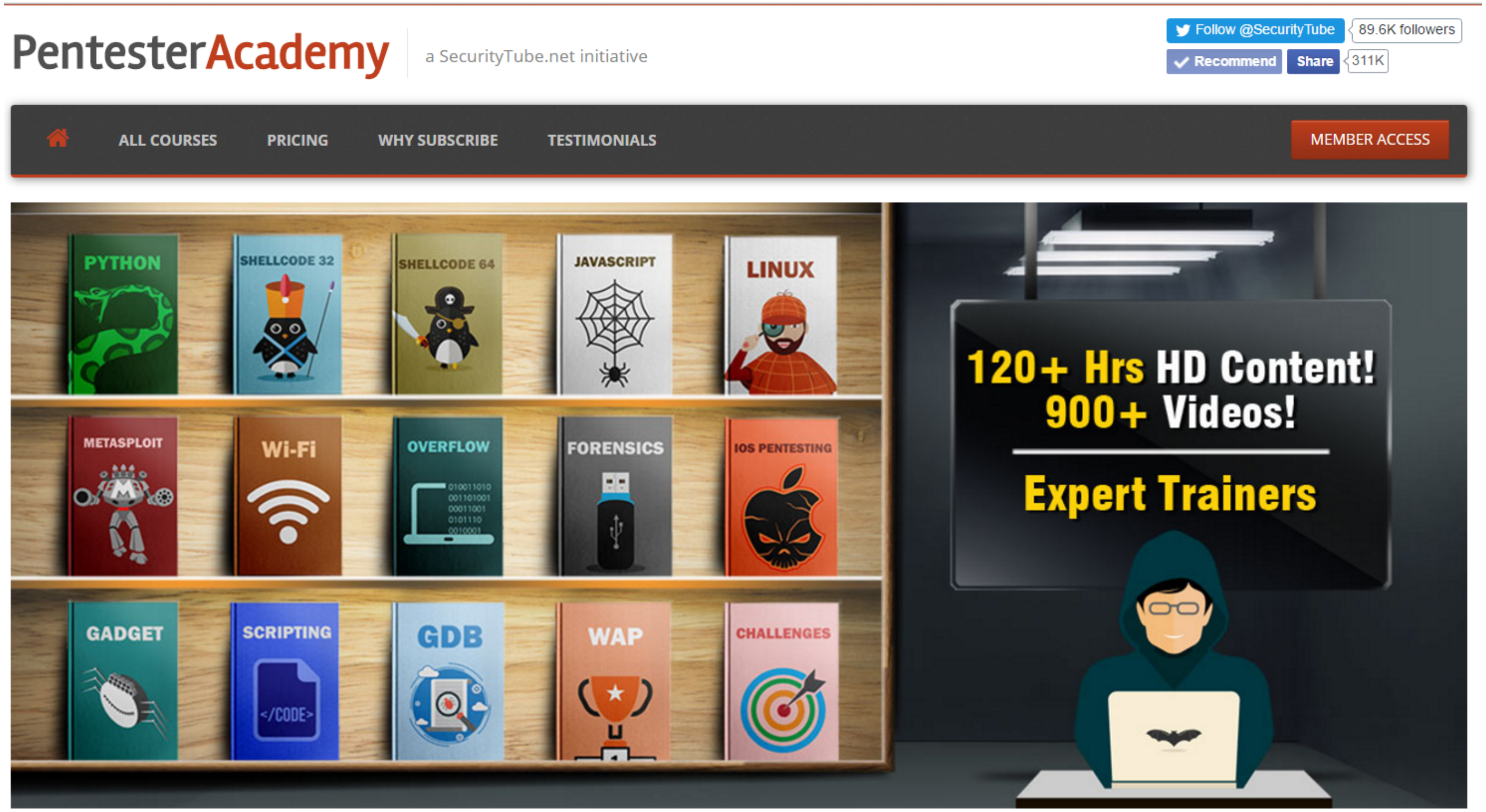
Syntax

```
BOOL WINAPI Toolhelp32ReadProcessMemory(
  _In_  DWORD   th32ProcessID,
  _In_  LPCVOID lpBaseAddress,
  _Out_ LPVOID  lpBuffer,
  _In_  SIZE_T  cbRead,
  _Out_ SIZE_T  lpNumberOfBytesRead
);
```

https://msdn.microsoft.com/en-us/library/windows/desktop/ms686826(v=vs.85).aspx

©Pentester Academy

Thank You!



©Pentester Academy