



# 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

# 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.

# Toolhelp32ReadProcessMemory

## Toolhelp32ReadProcessMemory function

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

### Syntax

C++

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

# Thank You!

PentesterAcademy

a SecurityTube.net initiative

Follow @SecurityTube 89.6K followers

Recommend Share 311K

The screenshot displays the PentesterAcademy website interface. At the top, there is a navigation bar with a home icon, links for 'ALL COURSES', 'PRICING', 'WHY SUBSCRIBE', and 'TESTIMONIALS', and a 'MEMBER ACCESS' button. Below the navigation bar is a grid of course covers. The first row includes 'PYTHON', 'SHELLCODE 32', 'SHELLCODE 64', 'JAVASCRIPT', and 'LINUX'. The second row includes 'METASPLOIT', 'WI-FI', 'OVERFLOW', 'FORENSICS', and 'IOS PENTESTING'. The third row includes 'GADGET', 'SCRIPTING', 'GDB', 'WAP', and 'CHALLENGES'. To the right of the course grid is a large promotional banner with a dark background. The banner features a person in a hoodie sitting at a desk with a laptop. The text on the banner reads: '120+ Hrs HD Content!', '900+ Videos!', and 'Expert Trainers'.

©Pentester Academy