



Windows API Exploitation Recipes for Red – Blue Teams

Vivek Ramachandran
Chief Trainer, Pentester Academy
<http://PentesterAcademy.com>

©Pentester Academy

Process Memory: Write Basics with WriteProcessMemory

Writing Process Memory

- Requires Debug privileges
- Write Process Memory
 - Change runtime data
 - Overlay part/whole process (malware)

WriteProcessMemory

WriteProcessMemory function

Writes data to an area of memory in a specified process. The entire area to be written to must be accessible or the operation fails.

Syntax

C++

```
BOOL WINAPI WriteProcessMemory(  
    _In_ HANDLE hProcess,  
    _In_ LPVOID lpBaseAddress,  
    _In_ LPCVOID lpBuffer,  
    _In_ SIZE_T nSize,  
    _Out_ SIZE_T *lpNumberOfBytesWritten  
);
```

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 blue hoodie sitting at a desk with a laptop. Above the person, a large white box contains the text: '120+ Hrs HD Content!', '900+ Videos!', and 'Expert Trainers'.

©Pentester Academy