Windows API Exploitation Recipes for Red – Blue Teams

Vivek Ramachandran

Chief Trainer, Pentester Academy

http://PentesterAcademy.com

Process Memory: Read Basics with ReadProcessMemory

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.

ReadProcessMemory

ReadProcessMemory function

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

Syntax

C++

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

Thank You!