

Table of Contents

Table of Contents.....	2
Kernel Array Management.....	4
Dynamic Array Allocation.....	5
Using a Static Array.....	7
Reallocating an Array.....	8
Kernel File Management.....	10
Creating and Writing to a File.....	10
Reading from a File.....	12
Deleting a File.....	13
Checking if a File Exists.....	14
Kernel Mapped Files Management.....	18
Create and Write in a Mapped File.....	19
Read content of a Mapped File.....	22
Delete Mapped File.....	24
Check if exists mapped file.....	26
Kernel Registry Management.....	33
Create Registry Key.....	33
Delete Registry Key.....	34
Write Registry Value.....	36
Modify Registry Value.....	37
Delete Registry Value.....	38
Query Registry Value.....	39
Register Windows Object Callbacks.....	47
- OB_OPERATION_HANDLE_CREATE.....	49
- OB_OPERATION_HANDLE_DUPLICATE.....	49
Hiding Payload in ADS.....	51
Key Functions and Workflow.....	53
Step-by-Step Code Explanation.....	54
Exercise.....	55
Passing a Kernel HANDLE to Userland via Shared Memory.....	55
Conclusions.....	56