# %

Topic: %AppData%, Book: 1, Page: 39

# /

Topic: /AA, Book: 3, Page: 6

Topic: /Annots, Book: 3, Page: 16

Topic: /DCTDecode, Book: 3, Page: 13

Topic: /ObjStm, Book: 3, Page: 29

Topic: /OpenAction, Book: 3, Page: 8

Topic: /URI, Book: 3, Page: 8

Topic: /XObject, Book: 3, Page: 9

# 1

Topic: 1768.py, Book: 3, Page: 76

# 3

Topic: 32-bit Architecture, Book: 2, Page: 27

Topic: 32-bit malware on 64-bit OS, Book: 2, Page: 148

# 6

Topic: 64-bit vs 32-bit Assembly, Book: 2, Page: 149-155, 159

# A

Topic: AND, Book: 2, Page: 41

Topic: AND Assembly, Book: 2, Page: 124

Topic: API Monitor, Book: 1, Page: 102-103

Topic: Assembly Instructions Format, Book: 2, Page: 23

Topic: Assembly.Load(), Book: 4, Page: 114

Topic: Assembly.LoadFile(), Book: 4, Page: 114

Topic: Assembly.LoadFrom(), Book: 4, Page: 114

Topic: AutoOpen, Book: 3, Page: 45

# B

Topic: BlockInput, Book: 5, Page: 75-76

Topic: Branching, Book: 2, Page: 39-44

Topic: Burp, Book: 3, Page: 20

# C

Topic: CALL, Book: 2, Page: 40

Topic: CFF Explorer, Book: 4, Page: 19-20

Topic: CMP, Book: 2, Page: 41

Topic: CS register, Book: 2, Page: 26

Topic: Code Injection Steps, Book: 4, Page: 150-152

Topic: Code injection, Book: 4, Page: 135

Topic: Code lifecycle overview, Book: 2, Page: 5

Topic: CreateMutexA, Book: 2, Page: 143

Topic: CreateRemoteThread, Book: 4, Page: 136, 141-143

Topic: CreateToolhelp32Snapshot, Book: 5, Page: 84

Topic: CreateToolhelp32Snapshot, Book: 4, Page: 136

Topic: CryptDecrypt, Book: 1, Page: 98-100

Topic: CyberChef, Book: 1, Page: 105-109

# D

Topic: DLL, Book: 2, Page: 137

Topic: DS register, Book: 2, Page: 26

Topic: Data Structures, Book: 2, Page: 34

Topic: Debugger Detection Methods, Book: 5, Page: 6, 12-14

Topic: Debugging packed malware, Book: 4, Page: 46-54

Topic: Detect It Easy, Book: 1, Page: 49

Topic: Direct Memory Access, Book: 2, Page: 31

Topic: Disable ASLR before trying to unpack, Book: 4, Page: 18-19

Topic: DotDumper, Book: 4, Page: 108, 131

Topic: DynamicInvoke(), Book: 4, Page: 114

# E

Topic: EAX, Book: 2, Page: 25

Topic: EBP, Book: 2, Page: 25

Topic: ECX, Book: 2, Page: 25

Topic: EFLAGS, Book: 2, Page: 26

Topic: EIP, Book: 2, Page: 26

Topic: ES register, Book: 2, Page: 26

Topic: ESI/EDI, Book: 2, Page: 25

Topic: ESP, Book: 2, Page: 25

Topic: Embedded Strings, Book: 1, Page: 44-45

Topic: Emulators Overview, Book: 1, Page: 83

Topic: EnumProcesses, Book: 4, Page: 136

Topic: Exeinfo PE, Book: 1, Page: 49

# F

Topic: FS register, Book: 2, Page: 26

Topic: Fiddler, Book: 1, Page: 124, 131

Topic: Fiddler, Book: 3, Page: 20-26

Topic: FindResourceW, Book: 2, Page: 140

Topic: Finding OEP of packed code, Book: 4, Page: 31-35

Topic: Function Calling Convention, Book: 2, Page: 85, 92

Topic: Function Epilogue, Book: 2, Page: 84, 91

Topic: Function Prologue, Book: 2, Page: 83, 90

Topic: Functions, Book: 2, Page: 65-72

# G

Topic: GS register, Book: 2, Page: 26

Topic: GetModuleHandleW, Book: 5, Page: 77

Topic: GetTempFileNameW, Book: 2, Page: 62-64

Topic: GetTempPathW, Book: 2, Page: 121, 128

Topic: Ghidra, Book: 2, Page: 6-18, 44, 104-105

# H

Topic: HTTP/Internet API Calls, Book: 2, Page: 45-57

Topic: Hex Strings, Book: 3, Page: 45

# I

Topic: ILSpy, Book: 4, Page: 108, 127-128

Topic: INetSim, Book: 1, Page: 120-123

Topic: Identify Packers, Book: 4, Page: 9-13

Topic: If-Else Assembly Translation, Book: 2, Page: 100

Topic: If-ElseIf-Else Assembly, Book: 2, Page: 102

Topic: Indicators of Compromise, Book: 1, Page: 45

Topic: Indirect Memory Access, Book: 2, Page: 32-33

Topic: Initial assessment, Book: 1, Page: 43

Topic: Inline Functions, Book: 2, Page: 77-78

Topic: Invoke(), Book: 4, Page: 114

Topic: InvokeMember(), Book: 4, Page: 114

Topic: IpProcessInformation, Book: 2, Page: 94

Topic: IpStartupInfo, Book: 2, Page: 95

Topic: IsDebuggerPresent, Book: 5, Page: 6-10

# J

Topic: JA, Book: 2, Page: 42

Topic: JMP, Book: 2, Page: 40

Topic: JNGE, Book: 2, Page: 42

Topic: JNZ, Book: 2, Page: 42

Topic: JZ, Book: 2, Page: 40, 42

Topic: Jcc, Book: 2, Page: 40, 42

# L

Topic: LOOP, Book: 2, Page: 41

Topic: Lab creation and isolation measures, Book: 1, Page: 25-30

Topic: Living-Off-The-Land Technique, Book: 3, Page: 53

Topic: LockResource, Book: 2, Page: 140

Topic: Loop Assembly, Book: 2, Page: 113-114

Topic: Loops, Book: 2, Page: 108-112

# M

Topic: MOV, Book: 2, Page: 76

Topic: Macros Enabled/Blocked Flowchart, Book: 3, Page: 39

Topic: Malware Defenses Summary, Book: 5, Page: 91

Topic: Malware using HTTPS, Book: 1, Page: 119-125

Topic: Malware using IP instead of DNS, Book: 1, Page: 126-130

# N

Topic: Netcat (nc), Book: 3, Page: 62

Topic: NtAllocateVirtualMemory, Book: 4, Page: 137

Topic: NtCreateThreadEx, Book: 4, Page: 137

Topic: NtOpenProcess, Book: 4, Page: 137

Topic: NtQueryInformationProcess, Book: 5, Page: 40

Topic: NtQuerySystemInformation, Book: 4, Page: 137

Topic: NtUnmapViewOfSection, Book: 5, Page: 59

Topic: NtWriteVirtualMemory, Book: 4, Page: 137

# O

Topic: OLE1, Book: 3, Page: 81

Topic: OLE2 vs OOXML, Book: 3, Page: 40

Topic: OR Assembly, Book: 2, Page: 125

Topic: Obfuscation Techniques, Book: 1, Page: 104

Topic: OllyDumpEx, Book: 4, Page: 36-39

Topic: OpenProcess, Book: 4, Page: 136, 142-143

# P

Topic: PDF Components, Book: 3, Page: 5

Topic: PDF Objects and Streams, Book: 3, Page: 6

Topic: PDF Risky Keywords, Book: 3, Page: 4

Topic: PUSH, Book: 2, Page: 76

Topic: Packer/Creation recognizing tools, Book: 1, Page: 49

Topic: PeStudio, Book: 2, Page: 138, 142

Topic: PeStudio, Book: 1, Page: 46-47

Topic: Pinpoint, Book: 3, Page: 20

Topic: Pointers, Book: 2, Page: 29

Topic: ProcDOT, Book: 1, Page: 53, 64-66

Topic: ProcDOT, Book: 4, Page: 61-64

Topic: Process Hacker, Book: 1, Page: 53-63

Topic: Process Hacker, Book: 4, Page: 21

Topic: Process Hollowing Pattern, Book: 5, Page: 52

Topic: Process Monitor, Book: 1, Page: 53-63

Topic: Process32First, Book: 5, Page: 84

Topic: Process32Next, Book: 5, Page: 84

# R

Topic: RET, Book: 2, Page: 40

Topic: ReadFile, Book: 1, Page: 95-97

Topic: RegOpenKeyExA, Book: 4, Page: 87

Topic: RegOpenKeyExA, Book: 2, Page: 20-23, 36-38

Topic: Registers, Book: 2, Page: 24

Topic: Regshot, Book: 1, Page: 53-63

Topic: Running commands from a remote source, Book: 1, Page: 115-118

# S

Topic: SRP Streams (VBA Macros), Book: 3, Page: 54

Topic: SS register, Book: 2, Page: 26

Topic: SUB, Book: 2, Page: 41

Topic: Scout, Book: 3, Page: 20

Topic: Scylla, Book: 4, Page: 23-24

Topic: Scylla, Book: 4, Page: 41-42

Topic: ScyllaHide, Book: 5, Page: 28-29

Topic: Segment Registers, Book: 5, Page: 127

Topic: SetWindowsHookExA, Book: 5, Page: 68

Topic: SizeofResource, Book: 2, Page: 140

Topic: Stack usage in functions, Book: 2, Page: 69

Topic: Static Properties, Book: 1, Page: 43

Topic: StrReverse, Book: 3, Page: 45

Topic: Structured Exception Handling (SEH), Book: 5, Page: 98-99

Topic: Switch Assembly, Book: 2, Page: 132

# T

Topic: TEST, Book: 2, Page: 41

Topic: Thread Local Storage (TLS), Book: 5, Page: 115

Topic: Thug, Book: 3, Page: 20

# U

Topic: URLDownloadToFileA, Book: 3, Page: 45

Topic: Unpacking by dumping, Book: 4, Page: 26

Topic: Using hardware vs software breakpoint, Book: 4, Page: 52

# V

Topic: VBA Module Overview, Book: 3, Page: 65, 78

Topic: VirtualAlloc, Book: 4, Page: 92

Topic: VirtualAllocEx, Book: 4, Page: 136, 145-147

Topic: Virtualization Detection, Book: 5, Page: 64-65

# W

Topic: Wireshark, Book: 1, Page: 53-63, 67-76, 119, 129-130

Topic: WriteProcessMemory, Book: 4, Page: 136, 144

# A

Topic: accept-all-ips, Book: 1, Page: 127-129

# B

Topic: base64dump.py, Book: 4, Page: 73

Topic: base64dump.py, Book: 3, Page: 69-71, 74

Topic: bbcrack, Book: 5, Page: 19

Topic: brxor.py, Book: 5, Page: 18

# C

Topic: capa, Book: 1, Page: 87-89

Topic: capa, Book: 5, Page: 45-46

Topic: cdecl, Book: 2, Page: 74

Topic: cscript, Book: 3, Page: 110-113

Topic: curl, Book: 3, Page: 20

# D

Topic: de4dot, Book: 4, Page: 108

Topic: dnSpyEx, Book: 4, Page: 108, 117-126

Topic: droppers, Book: 2, Page: 140

# E

Topic: evilclippy, Book: 3, Page: 57

Topic: exiftool, Book: 3, Page: 54

# F

Topic: fakedns , Book: 1, Page: 68-73, 116

Topic: fastcall, Book: 2, Page: 73, 75

Topic: feh (image viewer), Book: 3, Page: 14

Topic: feh (image viewer), Book: 3, Page: 43

Topic: floss, Book: 5, Page: 25-26

Topic: format-bytes.py, Book: 3, Page: 88

Topic: fs:[0], Book: 5, Page: 131

# G

Topic: grep, Book: 3, Page: 51

Topic: gunzip, Book: 3, Page: 71

# H

Topic: httpd, Book: 1, Page: 72-73, 116-117

# I

Topic: iconv, Book: 4, Page: 71

Topic: ilspycmd, Book: 4, Page: 111

Topic: iptables, Book: 1, Page: 127

# J

Topic: js, Book: 3, Page: 106-108, 114, 117

Topic: js, Book: 4, Page: 71

Topic: js-beautify, Book: 3, Page: 104

Topic: js-beautify, Book: 4, Page: 71

# L

Topic: logman, Book: 3, Page: 109-110

# M

Topic: mshta, Book: 4, Page: 60

# N

Topic: nslookup, Book: 1, Page: 68

Topic: numbers-to-string.py, Book: 3, Page: 59

# O

Topic: oledump.py, Book: 3, Page: 47-51, 58-59, 66-70, 85-88

Topic: olevba, Book: 3, Page: 45

# P

Topic: pdf-parser.py, Book: 3, Page: 9-17, 30-35

Topic: pdfid.py, Book: 3, Page: 8, 29

Topic: peframe, Book: 1, Page: 48

Topic: pestr, Book: 1, Page: 44

Topic: powershell\_ise, Book: 4, Page: 77

# R

Topic: rar, Book: 3, Page: 98-99

Topic: re-search.py, Book: 3, Page: 51

Topic: reflective code loading, Book: 4, Page: 114

Topic: reg\_export, Book: 4, Page: 69

Topic: regsvr32, Book: 3, Page: 53

Topic: rootkit, Book: 4, Page: 135

Topic: rtfdump.py , Book: 3, Page: 83-84, 89-91

Topic: runsc32, Book: 4, Page: 82

Topic: runsc32, Book: 3, Page: 97

# S

Topic: scdbg, Book: 4, Page: 80-81

Topic: scdbg, Book: 3, Page: 75, 95-96

Topic: sed, Book: 3, Page: 51, 60

Topic: setdllcharacteristics, Book: 4, Page: 20

Topic: sets.py, Book: 3, Page: 51

Topic: speakeasy, Book: 1, Page: 84-86

Topic: sshd, Book: 4, Page: 70

Topic: stdcall, Book: 2, Page: 74

Topic: strdeob.pl, Book: 5, Page: 24

Topic: strings, Book: 5, Page: 17-19

Topic: strings, Book: 1, Page: 44

# T

Topic: thiscall, Book: 2, Page: 73, 75

Topic: tr, Book: 4, Page: 71

Topic: translate.py, Book: 3, Page: 74

Topic: trid, Book: 3, Page: 41

# U

Topic: upx, Book: 4, Page: 16

# V

Topic: vmonkey, Book: 3, Page: 56

# W

Topic: wget, Book: 3, Page: 20

Topic: wmiprvse, Book: 4, Page: 60

Topic: word, Book: 2, Page: 28

# X

Topic: x32/x64dbg, Book: 1, Page: 90-101

Topic: x32dbg, Book: 4, Page: 83-104

Topic: x64dbg, Book: 4, Page: 30-42

Topic: xorsearch, Book: 5, Page: 17

Topic: xorsearch, Book: 3, Page: 92

Topic: xxd, Book: 4, Page: 71

Topic: xxd (convert hex to ASCII), Book: 1, Page: 76

# Y

Topic: yara-rules, Book: 3, Page: 76

# Z

Topic: zipdump.py, Book: 3, Page: 43, 55