FOR610: GIAC Reverse Engineering Malware

# #

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic** | **Book** | **Page** | **Notes** |
| 1768.py | 3 | 76 | nan |
| 32-bit Architecture | 2 | 27 | nan |
| 32-bit malware on 64-bit OS | 2 | 148 | nan |
| 64-bit vs 32-bit Assembly | 2 | 149-155, 159 | nan |

# A

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic** | **Book** | **Page** | **Notes** |
| /AA | 3 | 6 | nan |
| accept-all-ips | 1 | 127-129 | nan |
| AND | 2 | 41 | nan |
| AND Assembly | 2 | 124 | nan |
| /Annots | 3 | 16 | nan |
| API Monitor | 1 | 102-103 | nan |
| %AppData% | 1 | 39 | nan |
| Assembly Instructions Format | 2 | 23 | nan |
| Assembly.Load() | 4 | 114 | nan |
| Assembly.LoadFile() | 4 | 114 | nan |
| Assembly.LoadFrom() | 4 | 114 | nan |
| AutoOpen | 3 | 45 | nan |

# B

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic** | **Book** | **Page** | **Notes** |
| base64dump.py | 4 | 73 | nan |
| base64dump.py | 3 | 69-71, 74 | nan |
| bbcrack | 5 | 19 | nan |
| BlockInput | 5 | 75-76 | nan |
| Branching | 2 | 39-44 | nan |
| brxor.py | 5 | 18 | nan |
| Burp | 3 | 20 | nan |

# C

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic** | **Book** | **Page** | **Notes** |
| CALL | 2 | 40 | nan |
| capa | 1 | 87-89 | nan |
| capa | 5 | 45-46 | nan |
| cdecl | 2 | 74 | nan |
| CFF Explorer | 4 | 19-20 | nan |
| CMP | 2 | 41 | nan |
| Code injection | 4 | 135 | nan |
| Code Injection Steps | 4 | 150-152 | nan |
| Code lifecycle overview | 2 | 5 | nan |
| CreateMutexA | 2 | 143 | nan |
| CreateRemoteThread | 4 | 136, 141-143 | nan |
| CreateToolhelp32Snapshot | 5 | 84 | nan |
| CreateToolhelp32Snapshot | 4 | 136 | nan |
| CryptDecrypt | 1 | 98-100 | nan |
| cscript | 3 | 110-113 | nan |
| CS register | 2 | 26 | nan |
| curl | 3 | 20 | nan |
| CyberChef | 1 | 105-109 | nan |

# D

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic** | **Book** | **Page** | **Notes** |
| Data Structures | 2 | 34 | nan |
| /DCTDecode | 3 | 13 | nan |
| de4dot | 4 | 108 | .NET Malware |
| Debugger Detection Methods | 5 | 6, 12-14 | nan |
| Debugging packed malware | 4 | 46-54 | nan |
| Detect It Easy | 1 | 49 | nan |
| Direct Memory Access | 2 | 31 | nan |
| Disable ASLR before trying to unpack | 4 | 18-19 | nan |
| DLL | 2 | 137 | nan |
| dnSpyEx | 4 | 108, 117-126 | .NET Malware |
| DotDumper | 4 | 108, 131 | .NET Malware |
| droppers | 2 | 140 | nan |
| DS register | 2 | 26 | nan |
| DynamicInvoke() | 4 | 114 | nan |

# E

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic** | **Book** | **Page** | **Notes** |
| EAX | 2 | 25 | nan |
| EBP | 2 | 25 | nan |
| ECX | 2 | 25 | nan |
| EFLAGS | 2 | 26 | nan |
| EIP | 2 | 26 | nan |
| Embedded Strings | 1 | 44-45 | nan |
| Emulators Overview | 1 | 83 | nan |
| EnumProcesses | 4 | 136 | nan |
| ESI/EDI | 2 | 25 | nan |
| ESP | 2 | 25 | nan |
| ES register | 2 | 26 | nan |
| evilclippy | 3 | 57 | nan |
| Exeinfo PE | 1 | 49 | nan |
| exiftool | 3 | 54 | nan |

# F

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic** | **Book** | **Page** | **Notes** |
| fakedns | 1 | 68-73, 116 | nan |
| fastcall | 2 | 73, 75 | nan |
| feh (image viewer) | 3 | 14 | nan |
| feh (image viewer) | 3 | 43 | nan |
| Fiddler | 1 | 124, 131 | nan |
| Fiddler | 3 | 20-26 | nan |
| Finding OEP of packed code | 4 | 31-35 | nan |
| FindResourceW | 2 | 140 | nan |
| floss | 5 | 25-26 | nan |
| format-bytes.py | 3 | 88 | nan |
| fs:[0] | 5 | 131 | nan |
| FS register | 2 | 26 | nan |
| Function Calling Convention | 2 | 85, 92 | nan |
| Function Epilogue | 2 | 84, 91 | nan |
| Function Prologue | 2 | 83, 90 | nan |
| Functions | 2 | 65-72 | nan |

# G

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic** | **Book** | **Page** | **Notes** |
| GetModuleHandleW | 5 | 77 | nan |
| GetTempFileNameW | 2 | 62-64 | nan |
| GetTempPathW | 2 | 121, 128 | nan |
| Ghidra | 2 | 6-18, 44, 104-105 | nan |
| grep | 3 | 51 | nan |
| GS register | 2 | 26 | nan |
| gunzip | 3 | 71 | nan |

# H

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic** | **Book** | **Page** | **Notes** |
| Hex Strings | 3 | 45 | nan |
| httpd | 1 | 72-73, 116-117 | nan |
| HTTP/Internet API Calls | 2 | 45-57 | nan |

# I

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic** | **Book** | **Page** | **Notes** |
| iconv | 4 | 71 | nan |
| Identify Packers | 4 | 9-13 | nan |
| If-Else Assembly Translation | 2 | 100 | nan |
| If-ElseIf-Else Assembly | 2 | 102 | nan |
| ILSpy | 4 | 108, 127-128 | .NET Malware |
| ilspycmd | 4 | 111 | nan |
| Indicators of Compromise | 1 | 45 | nan |
| Indirect Memory Access | 2 | 32-33 | nan |
| INetSim | 1 | 120-123 | nan |
| Initial assessment | 1 | 43 | nan |
| Inline Functions | 2 | 77-78 | nan |
| Invoke() | 4 | 114 | nan |
| InvokeMember() | 4 | 114 | nan |
| IpProcessInformation | 2 | 94 | nan |
| IpStartupInfo | 2 | 95 | nan |
| iptables | 1 | 127 | nan |
| IsDebuggerPresent | 5 | 6-10 | nan |

# J

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic** | **Book** | **Page** | **Notes** |
| JA | 2 | 42 | nan |
| Jcc | 2 | 40, 42 | nan |
| JMP | 2 | 40 | nan |
| JNGE | 2 | 42 | nan |
| JNZ | 2 | 42 | nan |
| js | 3 | 106-108, 114, 117 | nan |
| js | 4 | 71 | nan |
| js-beautify | 4 | 71 | nan |
| js-beautify | 3 | 104 | nan |
| JZ | 2 | 40, 42 | nan |

# L

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic** | **Book** | **Page** | **Notes** |
| Lab creation and isolation measures | 1 | 25-30 | nan |
| Living-Off-The-Land Technique | 3 | 53 | nan |
| LockResource | 2 | 140 | nan |
| logman | 3 | 109-110 | nan |
| LOOP | 2 | 41 | nan |
| Loop Assembly | 2 | 113-114 | nan |
| Loops | 2 | 108-112 | nan |

# M

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic** | **Book** | **Page** | **Notes** |
| Macros Enabled/Blocked Flowchart | 3 | 39 | nan |
| Malware Defenses Summary | 5 | 91 | nan |
| Malware using HTTPS | 1 | 119-125 | nan |
| Malware using IP instead of DNS | 1 | 126-130 | nan |
| MOV | 2 | 76 | nan |
| mshta | 4 | 60 | nan |

# N

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic** | **Book** | **Page** | **Notes** |
| Netcat (nc) | 3 | 62 | nan |
| nslookup | 1 | 68 | nan |
| NtAllocateVirtualMemory | 4 | 137 | nan |
| NtCreateThreadEx | 4 | 137 | nan |
| NtOpenProcess | 4 | 137 | nan |
| NtQueryInformationProcess | 5 | 40 | nan |
| NtQuerySystemInformation | 4 | 137 | nan |
| NtUnmapViewOfSection | 5 | 59 | nan |
| NtWriteVirtualMemory | 4 | 137 | nan |
| numbers-to-string.py | 3 | 59 | nan |

# O

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic** | **Book** | **Page** | **Notes** |
| Obfuscation Techniques | 1 | 104 | nan |
| /ObjStm | 3 | 29 | nan |
| OLE1 | 3 | 81 | nan |
| OLE2 vs OOXML | 3 | 40 | --VBA Macros-- |
| oledump.py | 3 | 47-51, 58-59, 66-70, 85-88 | nan |
| olevba | 3 | 45 | nan |
| OllyDumpEx | 4 | 36-39 | nan |
| /OpenAction | 3 | 8 | nan |
| OpenProcess | 4 | 136, 142-143 | nan |
| OR Assembly | 2 | 125 | nan |

# P

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic** | **Book** | **Page** | **Notes** |
| Packer/Creation recognizing tools | 1 | 49 | nan |
| PDF Components | 3 | 5 | nan |
| pdfid.py | 3 | 8, 29 | nan |
| PDF Objects and Streams | 3 | 6 | nan |
| pdf-parser.py | 3 | 9-17, 30-35 | nan |
| PDF Risky Keywords | 3 | 4 | nan |
| peframe | 1 | 48 | nan |
| pestr | 1 | 44 | nan |
| PeStudio | 2 | 138, 142 | nan |
| PeStudio | 1 | 46-47 | nan |
| Pinpoint | 3 | 20 | nan |
| Pointers | 2 | 29 | nan |
| powershell\_ise | 4 | 77 | nan |
| ProcDOT | 4 | 61-64 | nan |
| ProcDOT | 1 | 53, 64-66 | nan |
| Process32First | 5 | 84 | nan |
| Process32Next | 5 | 84 | nan |
| Process Hacker | 4 | 21 | nan |
| Process Hacker | 1 | 53-63 | nan |
| Process Hollowing Pattern | 5 | 52 | nan |
| Process Monitor | 1 | 53-63 | nan |
| PUSH | 2 | 76 | nan |

# R

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic** | **Book** | **Page** | **Notes** |
| rar | 3 | 98-99 | nan |
| ReadFile | 1 | 95-97 | nan |
| reflective code loading | 4 | 114 | nan |
| reg\_export | 4 | 69 | nan |
| Registers | 2 | 24 | nan |
| RegOpenKeyExA | 4 | 87 | nan |
| RegOpenKeyExA | 2 | 20-23, 36-38 | nan |
| Regshot | 1 | 53-63 | nan |
| regsvr32 | 3 | 53 | nan |
| re-search.py | 3 | 51 | nan |
| RET | 2 | 40 | nan |
| rootkit | 4 | 135 | nan |
| rtfdump.py | 3 | 83-84, 89-91 | nan |
| Running commands from a remote source | 1 | 115-118 | nan |
| runsc32 | 3 | 97 | nan |
| runsc32 | 4 | 82 | nan |

# S

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic** | **Book** | **Page** | **Notes** |
| scdbg | 4 | 80-81 | nan |
| scdbg | 3 | 75, 95-96 | nan |
| Scout | 3 | 20 | nan |
| Scylla | 4 | 41-42 | nan |
| Scylla | 4 | 23-24 | nan |
| ScyllaHide | 5 | 28-29 | nan |
| sed | 3 | 51, 60 | nan |
| Segment Registers | 5 | 127 | nan |
| setdllcharacteristics | 4 | 20 | nan |
| sets.py | 3 | 51 | nan |
| SetWindowsHookExA | 5 | 68 | nan |
| SizeofResource | 2 | 140 | nan |
| speakeasy | 1 | 84-86 | nan |
| SRP Streams (VBA Macros) | 3 | 54 | nan |
| sshd | 4 | 70 | nan |
| SS register | 2 | 26 | nan |
| Stack usage in functions | 2 | 69 | nan |
| Static Properties | 1 | 43 | nan |
| stdcall | 2 | 74 | nan |
| strdeob.pl | 5 | 24 | nan |
| strings | 5 | 17-19 | nan |
| strings | 1 | 44 | nan |
| StrReverse | 3 | 45 | nan |
| Structured Exception Handling (SEH) | 5 | 98-99 | nan |
| SUB | 2 | 41 | nan |
| Switch Assembly | 2 | 132 | nan |

# T

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic** | **Book** | **Page** | **Notes** |
| TEST | 2 | 41 | nan |
| thiscall | 2 | 73, 75 | nan |
| Thread Local Storage (TLS) | 5 | 115 | nan |
| Thug | 3 | 20 | nan |
| tr | 4 | 71 | nan |
| translate.py | 3 | 74 | nan |
| trid | 3 | 41 | nan |

# U

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic** | **Book** | **Page** | **Notes** |
| Unpacking by dumping | 4 | 26 | nan |
| upx | 4 | 16 | nan |
| /URI | 3 | 8 | nan |
| URLDownloadToFileA | 3 | 45 | nan |
| Using hardware vs software breakpoint | 4 | 52 | nan |

# V

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic** | **Book** | **Page** | **Notes** |
| VBA Module Overview | 3 | 65, 78 | nan |
| VirtualAlloc | 4 | 92 | nan |
| VirtualAllocEx | 4 | 136, 145-147 | nan |
| Virtualization Detection | 5 | 64-65 | nan |
| vmonkey | 3 | 56 | nan |

# W

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic** | **Book** | **Page** | **Notes** |
| wget | 3 | 20 | nan |
| Wireshark | 1 | 53-63, 67-76, 119, 129-130 | nan |
| wmiprvse | 4 | 60 | nan |
| word | 2 | 28 | nan |
| WriteProcessMemory | 4 | 136, 144 | nan |

# X

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic** | **Book** | **Page** | **Notes** |
| x32dbg | 4 | 83-104 | nan |
| x32/x64dbg | 1 | 90-101 | nan |
| x64dbg | 4 | 30-42 | nan |
| /XObject | 3 | 9 | nan |
| xorsearch | 3 | 92 | nan |
| xorsearch | 5 | 17 | nan |
| xxd | 4 | 71 | nan |
| xxd (convert hex to ASCII) | 1 | 76 | nan |

# Y

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic** | **Book** | **Page** | **Notes** |
| yara-rules | 3 | 76 | nan |

# Z

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic** | **Book** | **Page** | **Notes** |
| zipdump.py | 3 | 43, 55 | nan |