

# CONTENTS IN DETAIL

## 1

### INTRODUCTION

#### 1

## 2

### PROGRAMMING

0x210	What Is Programming?	8
0x220	Program Exploitation	11
0x230	Generalized Exploit Techniques	14
0x240	Multi-User File Permissions	15
0x250	Memory	16
0x251	Memory Declaration	17
0x252	Null Byte Termination	18
0x253	Program Memory Segmentation	18
0x260	Buffer Overflows	22
0x270	Stack-Based Overflows	23
0x271	Exploiting Without Exploit Code	27
0x272	Using the Environment	31
0x280	Heap- and bss-Based Overflows	41
0x281	A Basic Heap-Based Overflow	41
0x282	Overflowing Function Pointers	46
0x290	Format Strings	54
0x291	Format Strings and printf()	54
0x292	The Format-String Vulnerability	59
0x293	Reading from Arbitrary Memory Addresses	61
0x294	Writing to Arbitrary Memory Addresses	62
0x295	Direct Parameter Access	71
0x296	Detours with dtors	74
0x297	Overwriting the Global Offset Table	80
0x2a0	Writing Shellcode	84
0x2a1	Common Assembly Instructions	84
0x2a2	Linux System Calls	85
0x2a3	Hello, World!	87
0x2a4	Shell-Spawning Code	90
0x2a5	Avoiding Using Other Segments	92
0x2a6	Removing Null Bytes	94
0x2a7	Even Smaller Shellcode Using the Stack	98
0x2a8	Printable ASCII Instructions	101
0x2a9	Polymorphic Shellcode	102
0x2aa	ASCII Printable Polymorphic Shellcode	103

	0x2ab	Dissembler .....	118
0x2b0		Returning into libc .....	129
	0x2b1	Returning into system() .....	130
	0x2b2	Chaining Return into libc Calls .....	132
	0x2b3	Using a Wrapper .....	133
	0x2b4	Writing Nulls with Return into libc .....	134
	0x2b5	Writing Multiple Words with a Single Call .....	136

### 3

## NETWORKING

0x310		What Is Networking? .....	139
	0x311	OSI Model .....	140
0x320		Interesting Layers in Detail .....	142
	0x321	Network Layer .....	142
	0x322	Transport Layer .....	143
	0x323	Data-Link Layer .....	145
0x330		Network Sniffing .....	146
	0x331	Active Sniffing .....	149
0x340		TCP/IP Hijacking .....	156
	0x341	RST Hijacking .....	157
0x350		Denial of Service .....	160
	0x351	The Ping of Death .....	160
	0x352	Teardrop .....	161
	0x353	Ping Flooding .....	161
	0x354	Amplification Attacks .....	161
	0x355	Distributed DoS Flooding .....	162
	0x356	SYN Flooding .....	162
0x360		Port Scanning .....	162
	0x361	Stealth SYN Scan .....	163
	0x362	FIN, X-mas, and Null Scans .....	163
	0x363	Spoofing Decoys .....	163
	0x364	Idle Scanning .....	163
	0x365	Proactive Defense (Shroud) .....	165

### 4

## CRYPTOLOGY

0x410		Information Theory .....	174
	0x411	Unconditional Security .....	174
	0x412	One-Time Pads .....	175
	0x413	Quantum Key Distribution .....	175
	0x414	Computational Security .....	176
0x420		Algorithmic Runtime .....	177
	0x421	Asymptotic Notation .....	178

0x430	Symmetric Encryption .....	178
0x431	Lov Grover's Quantum Search Algorithm .....	179
0x440	Asymmetric Encryption .....	180
0x441	RSA .....	180
0x442	Peter Shor's Quantum Factoring Algorithm .....	184
0x450	Hybrid Ciphers .....	185
0x451	Man-in-the-Middle Attacks .....	186
0x452	Differing SSH Protocol Host Fingerprints .....	189
0x453	Fuzzy Fingerprints .....	192
0x460	Password Cracking .....	196
0x461	Dictionary Attacks .....	197
0x462	Exhaustive Brute-Force Attacks .....	199
0x463	Hash Lookup Table .....	200
0x464	Password Probability Matrix .....	201
0x470	Wireless 802.11b Encryption .....	211
0x471	Wired Equivalent Privacy (WEP) .....	212
0x472	RC4 Stream Cipher .....	213
0x480	WEP Attacks .....	214
0x481	Offline Brute-Force Attacks .....	214
0x482	Keystream Reuse .....	215
0x483	IV-Based Decryption Dictionary Tables .....	216
0x484	IP Redirection .....	216
0x485	Fluhrer, Mantin, and Shamir (FMS) Attack .....	217

## 5

### CONCLUSION

References .....	230
------------------	-----

### INDEX