

BRIEF CONTENTS

Acknowledgments	xix
Introduction	xxi

PART I: INTO THE MACHINE: AWAKENING CODE SPELLS

Chapter 1: Spell of the Binary Oracle: When Hardware Whispers in Opcodes	3
Chapter 2: Spell of Essence: Distilling C to Its Primordial ASM	27
Chapter 3: Spell of Rebirth: Transmuting Greetings into Shellcode	73
Chapter 4: Spell of the Overflowing Frame: Mastering Stack Secrets	107
Chapter 5: Spell of the Undead: Writing a REPL to Animate a Botnet.....	157

PART II: ONTO THE NETWORK: UNVEILING MYSTIC GATEWAYS

Chapter 6: Veil of Shadows: Unlocking Hidden Backdoors	205
Chapter 7: Veil of Ash: The Dropper That Leaves No Flame Behind	241

PART III: THROUGH THE NETWORK: CASTING CRAWLERS

Chapter 8: Casting the Twin Serpent: Summoning a Two-Headed Worm	275
Chapter 9: Casting the Lone Strand: Single-Stage Wormcraft	315
Chapter 10: Casting the Lost Hosts: Conjuring Network Scanners	337

APPENDIXES: THE FORGE

Appendix A: The Sorcerer's Forge: Preparing Your Workshop	371
Appendix B: Secrets of the Forge: Arcane Tricks for Low-Level Tools	375
Appendix C: The Sorcerer's Anvil: Full Spellcraft Listings	399
Index	415