Contents

Introduction xvii

Chapter 1 Computer Network Exploitation 1
Operations 4
Operational Objectives 5
 Strategic Collection 6
 Directed Collection 7
 Non-Kinetic Computer Network Attack (CNA) 7
 Strategic Access 9
 Positional Access 9
 CNE Revisited 11
 A Framework for Computer Network Exploitation 11
 First Principles 12
 Principles 12
 Themes 14
 Summary 15

Chapter 2 The Attacker 17
 Principle of Humanity 17
 Life Cycle of an Operation 18
 Stage 1: Targeting 19
 Stage 2: Initial Access 22
 Stage 3: Persistence 24
 Stage 4: Expansion 25
 Stage 5: Exfiltration 26
 Stage 6: Detection 26
 Principle of Access 27
 Inbound Access 27
 Outbound Access 29
 Bidirectional Access 35
Contents

No Outside Access 35
Access Summary 36
Principle of Economy 37
  Time 37
  Targeting Capabilities 37
  Exploitation Expertise 38
  Networking Expertise 38
  Software Development Expertise 39
  Operational Expertise 40
  Operational Analysis Expertise 40
  Technical Resources 41
Economy Summary 41
Attacker Structure 41
Summary 43

Chapter 3 The Defender 45
  Principle of Humanity 45
    Humanity and Network Layout 46
    Humanity and Security Policy 47
  Principle of Access 48
  The Defensive Life Cycle 49
  Principle of Economy 51
  The Helpful Defender 53
  Summary 54

Chapter 4 Asymmetries 55
  False Asymmetries 56
  Advantage Attacker 59
    Motivation 60
    Initiative 61
    Focus 62
    Effect of Failure 62
    Knowledge of Technology 64
    Analysis of Opponent 64
    Tailored Software 65
    Rate of Change 66
  Advantage Defender 67
    Network Awareness 68
    Network Posture 68
  Advantage Indeterminate 69
    Time 69
    Efficiency 70
  Summary 71

Chapter 5 Attacker Frictions 73
  Mistakes 74
  Complexity 74
  Flawed Attack Tools 75
Contents

Chapter 6 Defender Frictions 83
Mistakes 83
Flawed Software 84
Inertia 86
The Security Community 87
Complexity 89
Users 91
Bad Luck 92
Summary 92

Chapter 7 Offensive Strategy 93
Principle 1: Knowledge 95
Measuring Knowledge 96
Principle 2: Awareness 97
Measuring Awareness 98
Principle 3: Innovation 98
Measuring Innovation 99
Defensive Innovation 100
Principle 4: Precaution 101
Measuring Precaution 103
Principle 5: Operational Security 105
Minimizing Exposure 106
Minimizing Recognition 107
Controlling Reaction 108
Measuring Operational Security 109
Principle 6: Program Security 110
Attacker Liabilities 110
Program Security Costs 112
Measuring Program Security 120
Crafting an Offensive Strategy 121
Modular Frameworks 124
A Note on Tactical Decisions 126
Summary 127

Chapter 8 Defensive Strategy 129
Failed Tactics 130
Antivirus and Signature-Based Detection 130
Password Policies 132
User Training 134
Crafting a Defensive Strategy 135
Cloud-Based Security 143
Summary 145