CONTENTS IN DETAIL

INTRODUCTION **XVI**
About This Book xvii
A Note on the Castle Theory Thought Exercises xix
For Future Use xx
A Ninja Primer xx
The Historical Ninja xx
The Ninja Scrolls xxi
Ninja Philosophy xxii
Ninja Techniques xxiii

1
MAPPING NETWORKS **1**

With these maps, the general can consider how to defend and attack a castle.

Understanding Network Maps 2
Collecting Intelligence Undetected 6
Creating Your Map 9
Recommended Security Controls and Mitigations 13
Debrief 13

2
GUARDING WITH SPECIAL CARE **15**

Even castles with strong fortifications should be guarded, paying particular attention to the recessed corners.

Understanding Attack Vectors 16
The Concept of Guarding 17
Guarding Within a Cybersecurity Framework 17
Threat Modeling 18
Using Threat Modeling to Find Potential Attack Vectors 20
Recommended Security Controls and Mitigations 23
Debrief 24

3 XENOPHOBIC SECURITY 25

If you accept strangers without much thought, the enemy shinobi may come in disguised as a stranger and seek information from the inside.

Understanding Anti-Privilege . . . 26
The Problem with Interoperability and Universal Standards . . . 27
Developing Unique Characteristics for Your Environment . . . 29
Do it yourself or seek commercial products . . . 29
Recommended Security Controls and Mitigations . . . 30
Debrief . . . 31

4 IDENTIFICATION CHALLENGE 33

Though there are ancient ways for identifying marks, passwords, and certificates, unless you invent new ones and rotate them, the enemy will manage to infiltrate by having similar fake ones.

Understanding Authentication . . . 35
Developing Matched-Pair Authenticators . . . 37
Recommended Security Controls and Mitigations . . . 38
Debrief . . . 39

5 DOUBLE-SEALED PASSWORD 41

Sometimes, a set of signs such as pinching the nose or holding the ear should be used with these passwords.

A Concealed 2-Step Authentication . . . 43
Developing Double-Sealed Passwords . . . 44
Recommended Security Controls and Mitigations . . . 46
Debrief . . . 47

6 HOURS OF INFILTRATION 49

After waiting until the hour of Ox, the ninja realized that the guard had fallen asleep; everything was dead quiet, and the fire was out leaving all in darkness.

Understanding Time and Opportunities . . . 50
Developing Time-Based Security Controls and Anomaly Detectors . . . 51
Recommended Security Controls and Mitigations . . . 54
Debrief . . . 55

7 ACCESS TO TIME 57

You should start your attack with no delay and not prematurely but perfectly on time.

The Importance of Time . . . 58

Keeping Time Confidential 60
Determine Your Baseline 60
Assess Technical Capability 60
Establish Policy 60
Recommended Security Controls and Mitigations 61
Debrief 62

8
TOOLS 63

Remember, if you use a ninja tool, be sure to use it when the wind is whistling so as to hide any sound and always retrieve it.

Living Off the Land 65
Securing Tools 66
Recommended Security Controls and Mitigations 68
Debrief 69

9
SENSORS 71

Whether day or night, scouts for a far-distance observation should be sent out.

Identifying and Detecting Threats with Sensors 72
Better Sensors 73
Recommended Security Controls and Mitigations 76
Debrief 77

10
BRIDGES AND LADDERS 79

There will be no wall or moat that you cannot pass, no matter how high or steep it is, particularly if you use a ninja ladder.

Network Boundary Bridging 80
Countering Bridges 82
Recommended Security Controls and Mitigations 83
Debrief 83

11
LOCKS 85

There is no padlock that you cannot open. However, this all depends on how skilled you are; therefore, you should always get hands-on practice.

Physical Security 87
Improving Locks 88
Recommended Security Controls and Mitigations 89
Debrief 89

12
MOON ON THE WATER 91

After making an agreement with your lord, you should lure the enemy out with bait to infiltrate their defenses.

Social Engineering 92
Defenses Against Social Engineering 94
Recommended Security Controls and Mitigations 96
Debrief 97

13
WORM AGENT 99

Make a minomushi*, or worm agent (aka insider threat), out of an enemy.*

Insider Threats 101
A New Approach to Insider Threats 102
Recommended Security Controls and Mitigations 105
Debrief 106

14
GHOST ON THE MOON 107

According to Japanese legend, if you knew how to seek the ghost who tends trees on the moon, he could invite you to the moon to eat the leaves of his tree, making you invisible.

Implants 108
Protections from Implants 109
Recommended Security Controls and Mitigations 111
Debrief 112

15
THE ART OF THE FIREFLIES 113

The art of fireflies should be performed only after you know everything about the enemy in great detail so that you can construct your deception in accordance with the target's mindset.

Attribution 114
Approaches to Handling Attribution 116
Recommended Security Controls and Mitigations 118
Debrief 119

16
LIVE CAPTURE 121

Use good judgment to determine whether the target is actually inattentive or whether they are employing a ruse to lure ninjas and capture them.

Live Analysis 124
Confronting Live Threats 125

Recommended Security Controls and Mitigations 127
Debrief 129

17
FIRE ATTACK 131

First, it is easy to set fires; second, it is not easy for the enemy to put out the fire; and third, if your allies are coming to attack the castle at the same time, the enemy will lose any advantage as the fortifications will be understaffed.

Destructive Cyber Attacks 133
Safeguards from (Cyber) Fire Attacks 134
Recommended Security Controls and Mitigations 137
Debrief 138

18
COVERT COMMUNICATION 139

When a shinobi is going to communicate with the general after he has gotten into the enemy's castle, the shinobi needs to let his allies know where he is. It is essential to arrange for the time and place to do this.

Command and Control Communication 141
Controlling Coms 143
Recommended Security Controls and Mitigations 144
Debrief 146

19
CALL SIGNS 147

When you steal in, the first thing you should do is mark the route, showing allies the exit and how to escape.

Operator Tradecraft 148
Detecting the Presence of Call Signs 149
Recommended Security Controls and Mitigations 150
Debrief 151

20
LIGHT, NOISE, AND LITTER DISCIPLINE 153

The traditions of the ancient shinobi say you should lock the doors before you have a look at the enemy with fire.

Cyber Light, Noise, and Litter 155
Detection Discipline 156
Recommended Security Controls and Mitigations 158
Debrief 158

21
CIRCUMSTANCES OF INFILTRATION 159

You should infiltrate at the exact moment that the enemy moves and not try when they do not move—this is a way of principled people.

Adversarial Opportunity 161
Adversarial Adversity 162
Recommended Security Controls and Mitigations 163
Debrief 163

22
ZERO-DAYS 165

A secret will work if it is kept; you will lose if words are given away.

Zero-Day 168
Zero-Day Defense 169
Recommended Security Controls and Mitigations 172
Debrief 174

23
HIRING SHINOBI 175

In order to defend against enemy plans or shinobi, or should an emergency arise, you may think it more desirable to have a large number of people. However, you should not hire more people into your army without careful consideration.

Cybersecurity Talent 177
Talent Management 179
Recommended Security Controls and Mitigations 181
Debrief 182

24
GUARDHOUSE BEHAVIOR 185

Do not let your guard down, even if you are not confronting the enemy.

Security Operations Center Issues and Expectations 187
Influencing Behavior 188
Recommended Security Controls and Mitigations 191
Debrief 192

25
ZERO-TRUST THREAT MANAGEMENT 195

If you enter a room from the rear and if there is someone in the room who is not asleep, then they will not suspect you as an intruder. It is because those who come from the rear are not considered possible thieves or assailants.

Threat Opportunity 196
Blocking the Suspicious 198
Recommended Security Controls and Mitigations 200
Debrief 200

26
SHINOBI TRADECRAFT 201

Secret techniques to infiltrate without fail are deceptive, and they are varied and flexible and are done according to opportunity. Thus, as a basis, you should embrace the old ways of the shinobi who served under ancient great generals, but remember not only to keep to these ways but to adapt them, each dependent on the situation and the moment.

Techniques, Tactics, and Procedures 204
    Pyramid of Pain 205
    ATT&CK Framework 206
    Threat Intelligence 206
Cyber Threat Intelligence 208
Recommended Security Controls and Mitigations 210
Debrief 211

NOTES 213

INDEX 223