## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>xiii</td>
</tr>
<tr>
<td>Acknowledgments</td>
<td>xvii</td>
</tr>
</tbody>
</table>

### 1 INTRODUCTION

1. Why Attack DNS?
2. Network Disruption
3. DNS as a Backdoor
4. DNS Basic Operation
5. Basic DNS Data Sources and Flows
6. DNS Trust Model
7. DNS Administrator Scope
8. Security Context and Overview
9. Cybersecurity Framework Overview
10. Framework Implementation
11. What’s Next

### 2 INTRODUCTION TO THE DOMAIN NAME SYSTEM (DNS)

1. DNS Overview – Domains and Resolution
2. Domain Hierarchy
3. Name Resolution
4. Zones and Domains
5. Dissemination of Zone Information
6. Additional Zones
7. Resolver Configuration
8. Summary

### 3 DNS PROTOCOL AND MESSAGES

1. DNS Message Format
2. Encoding of Domain Names
vi

CONTENTS

Name Compression 32
Internationalized Domain Names 34
DNS Message Format 35
DNS Update Messages 43
The DNS Resolution Process Revisited 48
  DNS Resolution Privacy Extension 55
Summary 56

4 DNS VULNERABILITIES 57
  Introduction 57
  DNS Data Security 57
  DNS Information Trust Model 59
    DNS Information Sources 60
  DNS Risks 61
  DNS Infrastructure Risks and Attacks 62
    DNS Service Availability 62
    Hardware/OS Attacks 63
    DNS Service Denial 63
    Pseudorandom Subdomain Attacks 67
    Cache Poisoning Style Attacks 67
    Authoritative Poisoning 71
    Resolver Redirection Attacks 73
  Broader Attacks that Leverage DNS 74
    Network Reconnaissance 75
    DNS Rebinding Attack 77
    Reflector Style Attacks 78
    Data Exfiltration 79
    Advanced Persistent Threats 81
Summary 83

5 DNS TRUST SECTORS 85
  Introduction 85
  Cybersecurity Framework Items 87
    Identify 87
    Protect 87
    Detect 88
  DNS Trust Sectors 88
CONTENTS

External DNS Trust Sector 91
   Basic Server Configuration 93
   DNS Hosting of External Zones 97
   External DNS Diversity 97
Extranet DNS Trust Sector 98
Recursive DNS Trust Sector 99
   Tiered Caching Servers 100
   Basic Server Configuration 101
Internal Authoritative DNS Servers 103
   Basic Server Configuration 105
Additional DNS Deployment Variants 108
   Internal Delegation DNS Master/Slave Servers 109
   Multi-Tiered Authoritative Configurations 109
   Hybrid Authoritative/Caching DNS Servers 111
   Stealth Slave DNS Servers 111
   Internal Root Servers 111
   Deploying DNS Servers with Anycast Addresses 113
Other Deployment Considerations 118
   High Availability 118
   Multiple Vendors 118
   Sizing and Scalability 118
   Load Balancers 119
   Lab Deployment 119
Putting It All Together 119

6 SECURITY FOUNDATION 121
   Introduction 121
   Hardware/Asset Related Framework Items 122
      Identify: Asset Management 122
      Identify: Business Environment 123
      Identify: Risk Assessment 124
      Protect: Access Control 126
      Protect: Data Security 127
      Protect: Information Protection 129
      Protect: Maintenance 130
      Detect: Anomalies and Events 131
CONTENTS

Detect: Security Continuous Monitoring 131
Respond: Analysis 132
Respond: Mitigation 132
Recover: Recovery Planning 133
Recover: Improvements 133
DNS Server Hardware Controls 134
DNS Server Hardening 134
Additional DNS Server Controls 136
Summary 137

7 SERVICE DENIAL ATTACKS 139
Introduction 139
Denial of Service Attacks 139
Pseudorandom Subdomain Attacks 141
Reflector Style Attacks 143
Detecting Service Denial Attacks 144
Denial of Service Protection 145
DoS/DDoS Mitigation 145
Bogus Queries Mitigation 147
PRSD Attack Mitigation 148
Reflector Mitigation 148
Summary 151

8 CACHE POISONING DEFENSES 153
Introduction 153
Attack Forms 154
Packet Interception or Spoofing 154
ID Guessing or Query Prediction 155
Name Chaining 155
The Kaminsky DNS Vulnerability 156
Cache Poisoning Detection 159
Cache Poisoning Defense Mechanisms 160
UDP Port Randomization 160
Query Name Case Randomization 161
DNS Security Extensions 161
Last Mile Protection 167
### 9 SECURING AUTHORITATIVE DNS DATA

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>169</td>
</tr>
<tr>
<td>Attack Forms</td>
<td>170</td>
</tr>
<tr>
<td>Resolution Data at Rest</td>
<td>170</td>
</tr>
<tr>
<td>Domain Registries</td>
<td>170</td>
</tr>
<tr>
<td>DNS Hosting Providers</td>
<td>171</td>
</tr>
<tr>
<td>DNS Data in Motion</td>
<td>172</td>
</tr>
<tr>
<td>Attack Detection</td>
<td>172</td>
</tr>
<tr>
<td>Authoritative Data</td>
<td>172</td>
</tr>
<tr>
<td>Domain Registry</td>
<td>173</td>
</tr>
<tr>
<td>Domain Hosting</td>
<td>173</td>
</tr>
<tr>
<td>Falsified Resolution</td>
<td>173</td>
</tr>
<tr>
<td>Defense Mechanisms</td>
<td>174</td>
</tr>
<tr>
<td>Defending DNS Data at Rest</td>
<td>174</td>
</tr>
<tr>
<td>Defending Resolution Data in Motion with DNSSEC</td>
<td>176</td>
</tr>
<tr>
<td>Summary</td>
<td>186</td>
</tr>
</tbody>
</table>

### 10 ATTACKER EXPLOITATION OF DNS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>187</td>
</tr>
<tr>
<td>Network Reconnaissance</td>
<td>187</td>
</tr>
<tr>
<td>Data Exfiltration</td>
<td>188</td>
</tr>
<tr>
<td>Detecting Nefarious use of DNS</td>
<td>189</td>
</tr>
<tr>
<td>Detecting Network Reconnaissance</td>
<td>189</td>
</tr>
<tr>
<td>DNS Tunneling Detection</td>
<td>190</td>
</tr>
<tr>
<td>Mitigation of Illicit DNS Use</td>
<td>193</td>
</tr>
<tr>
<td>Network Reconnaissance Mitigation</td>
<td>193</td>
</tr>
<tr>
<td>Mitigation of DNS Tunneling</td>
<td>193</td>
</tr>
</tbody>
</table>

### 11 MALWARE AND APTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>195</td>
</tr>
<tr>
<td>Malware Proliferation Techniques</td>
<td>196</td>
</tr>
<tr>
<td>Phishing</td>
<td>196</td>
</tr>
<tr>
<td>Spear Phishing</td>
<td>196</td>
</tr>
<tr>
<td>Downloads</td>
<td>196</td>
</tr>
<tr>
<td>File Sharing</td>
<td>197</td>
</tr>
<tr>
<td>Email Attachments</td>
<td>197</td>
</tr>
<tr>
<td>Watering Hole Attack</td>
<td>197</td>
</tr>
</tbody>
</table>
CONTENTS

Replication 197
Implantation 197
Malware Examples 198
Malware Use of DNS 198
  DNS Fluxing 198
  Dynamic Domain Generation 202
Detecting Malware 202
  Detecting Malware Using DNS Data 203
Mitigating Malware Using DNS 206
  Malware Extrication 206
  DNS Firewall 207
Summary 210

12 DNS SECURITY STRATEGY 213
  Major DNS Threats and Mitigation Approaches 214
  Common Controls 214
    Disaster Defense 214
    Defenses Against Human Error 220
  DNS Role-Specific Defenses 220
    Stub Resolvers 220
    Forwarder DNS Servers 221
    Recursive Servers 221
    Authoritative Servers 222
  Broader Security Strategy 222
    Identify Function 223
    Protect Function 224
    Detect Function 225
    Respond Function 226
    Recover Function 227

13 DNS APPLICATIONS TO IMPROVE NETWORK SECURITY 229
  Safer Web Browsing 230
    DNS-Based Authentication of Named Entities (DANE) 230
  Email Security 232
    Email and DNS 233
    DNS Block Listing 237
    Sender Policy Framework (SPF) 238
CONTENTS

Domain Keys Identified Mail (DKIM) 242
Domain-Based Message Authentication, Reporting, and Conformance (DMARC) 245
Securing Automated Information Exchanges 246
Dynamic DNS Update Uniqueness Validation 246
Storing Security-Related Information 247
Other Security Oriented DNS Resource Record Types 247
Summary 251

14 DNS SECURITY EVOLUTION 253

Appendix A: Cybersecurity Framework Core DNS Example 257
Appendix B: DNS Resource Record Types 285
Bibliography 291
Index 299