# Contents

Acknowledgments xix
Introduction xxı

Chapter 1: Finding, Interviewing for, and Getting the Job 1

- Qualifications 1
- Pursuing a Degree 2
- The Perfect Job 2
  - The Intangible Benefits 3
  - The Tangible Benefits 5
- Job Search 7
  - The Résumé 7
  - Company Recruiters 8
  - Professional Networking 8
  - Headhunters 9
  - Tools 9
- Interviewing 10
  - What Employers Want 10
  - Phone Interviews 10
  - On-Site Interviews 12
- Money Talks 13
  - Cost of Living 14
  - Relocating 16
- Accepting or Rejecting the Offer 16
- Summary 18
- Nontechnical Interview Questions 18

Chapter 2: Knowing Networks: Fundamentals 21

- Introduction 21
- Questions 22
  - What Is the OSI Model? 23
  - What Is the TCP/IP Model and How Does It Relate to the OSI Model? 25
  - Tell Me about Cisco’s “Standard” Architecture 26
  - How Does the Concept of Defense-in-Depth Security Work with the OSI Model? 28
  - Why Do We Think of Networking in Terms of Layers? 28
Contents

How Does the Spanning Tree Protocol Work, What Is Its Purpose, and What Are Some of the Types? 29
What Is the Difference between a Broadcast Domain and a Collision Domain? 30
Explain How Port Security Works on a Switch 30
Explain the TCP Three-Way Handshake and Relate It to the TCP State Diagram 31
Briefly Describe the TCP and UDP Packet Headers 32
What Well-Known Port Numbers Are You Familiar With? 34
What Is the Difference between Classful and Classless Routing? 34
Describe Variable-Length Subnet Masking (VLSM) 34
What Is the Difference between a Routed Protocol and a Routing Protocol? 34
Draw the Diagram of a Typical OSPF Network and Explain Generally How It Works: DR, BDR, Election, ASBR, ABR, Route Redistribution, and Summarization 35
Explain BGP, the Differences between BGP and OSPF, What Prefixes Are, and What Attributes and Types Are Used in BGP 36
Describe Routing Filters and What They Accomplish 39

Recommended Reading 39

Chapter 3: Knowing Security: Fundamentals 41

Adjust Your Thinking 41
Core Values 42
Access Control 42
Dealing with the CIA 43
Additional Core Values 43
Basic Concepts 44
Defense in Depth 44
Layered Defense 45
Managing Risk 47
Threat 48
Impact 48
Vulnerabilities 48
Limiting Risk 48
Data Classification and Labeling 49
Data Classification 49
Data Labeling 50
Ethics in Information Security 50
The Hack Back 50
Reacting to an Incident 51
Communication and Knowledge Transfer 51
Managers 51
Users 52
Training 52
Documentation 53
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daily Security Responsibilities</td>
<td>54</td>
</tr>
<tr>
<td>- Patches and Hot Fixes</td>
<td>54</td>
</tr>
<tr>
<td>- Backup and Restore</td>
<td>54</td>
</tr>
<tr>
<td>- Virus Protection</td>
<td>55</td>
</tr>
<tr>
<td>- Perimeter Security</td>
<td>55</td>
</tr>
<tr>
<td><strong>Summary</strong></td>
<td>55</td>
</tr>
<tr>
<td><strong>Interview Q&amp;A</strong></td>
<td>56</td>
</tr>
<tr>
<td><strong>Recommended Reading</strong></td>
<td>57</td>
</tr>
<tr>
<td><strong>Chapter 4: Understanding Regulations, Legislation, and Guidance</strong></td>
<td>59</td>
</tr>
<tr>
<td>Regulations, Legislation, and Guidance Defined</td>
<td>60</td>
</tr>
<tr>
<td>Why Does an Employer Care?</td>
<td>60</td>
</tr>
<tr>
<td>- They Have to Care</td>
<td>61</td>
</tr>
<tr>
<td>- They Want to Care</td>
<td>61</td>
</tr>
<tr>
<td>Why Should You Care?</td>
<td>61</td>
</tr>
<tr>
<td>Government- and DoD-Specific Information</td>
<td>62</td>
</tr>
<tr>
<td>- United States Government Information Security</td>
<td>62</td>
</tr>
<tr>
<td>- Department of Defense and National Security Systems</td>
<td>68</td>
</tr>
<tr>
<td><strong>Commercial Information Security</strong></td>
<td>72</td>
</tr>
<tr>
<td>- State-Specific Cyber Security Laws</td>
<td>72</td>
</tr>
<tr>
<td>- National Infrastructure Protection</td>
<td>73</td>
</tr>
<tr>
<td>- International Standards</td>
<td>77</td>
</tr>
<tr>
<td>- Public Companies</td>
<td>79</td>
</tr>
<tr>
<td><strong>Using This Information in the Interview</strong></td>
<td>80</td>
</tr>
<tr>
<td><strong>Summary</strong></td>
<td>80</td>
</tr>
<tr>
<td><strong>Interview Q&amp;A</strong></td>
<td>80</td>
</tr>
<tr>
<td><strong>Recommended Reading</strong></td>
<td>82</td>
</tr>
<tr>
<td><strong>Chapter 5: Knowing Firewalls: Fundamentals</strong></td>
<td>83</td>
</tr>
<tr>
<td>Firewall Technologies</td>
<td>84</td>
</tr>
<tr>
<td>- Packet Filter</td>
<td>84</td>
</tr>
<tr>
<td>- Stateful Firewall</td>
<td>86</td>
</tr>
<tr>
<td>- Application Proxy</td>
<td>88</td>
</tr>
<tr>
<td>- Unified Threat Management</td>
<td>89</td>
</tr>
<tr>
<td>- Intrusion Protection System</td>
<td>90</td>
</tr>
<tr>
<td>- Network Address Translation</td>
<td>90</td>
</tr>
<tr>
<td>- Virtual Private Networks</td>
<td>90</td>
</tr>
<tr>
<td><strong>Major Vendors</strong></td>
<td>91</td>
</tr>
<tr>
<td>- Cisco</td>
<td>91</td>
</tr>
<tr>
<td>- Juniper Networks</td>
<td>92</td>
</tr>
</tbody>
</table>
# Contents

- **Check Point** 93
- **Other Vendors** 94

## Device Types
- Appliance 95
- Secure Router 96
- Server Based 96

## Management
- Configuration Components 97
- Stand-Alone 97
- Distributed 98
- Global Management 98

## Deployment Strategies
- Basic Deployment 99
- DMZ 101
- High Availability 103

## Summary
- Interview Q&A 105
- Recommended Reading 106

## Chapter 6: Knowing Virtual Private Networks

### Goals and Assumptions

### The Cryptography of VPNs
- Symmetric Key Cryptography 108
- Asymmetric Cryptography 110
- Hash Functions 112
- Message Authentication Codes 112

### IP Security Review
- Security Protocols and Modes 113
- Key Management with IKE 119
- Shoring Up the Tunnel 124
- Best Practice 125
- Complexity Trap 125

### Implementing IPsec
- Design Considerations 127
- Design Scenarios 129

### Alternatives to IPsec
- Transport Layer Security (TLS/SSL) 131
- Internet Protocol V6 131

## Summary
- Interview Q&A 132
- Recommended Reading 133
Chapter 7: Knowing IDS/IPS/IDP

Introduction
Questions

Explain the Types of IDS and IDP Systems and Provide Some Examples of Each.
What Is Deep Inspection and What Is the Benefit?
What Are the Different Modes That a Sensor Can Operate In?
What Are the Layers of the OSI Reference Model and Where Do IDP Systems Operate?
How Does an IDS/IDP System Detect Attacks?
What Are Some of the Problems with an IDP System?
What Is a False Positive? What Is a False Negative?
What Are Some of the Challenges You Have Faced When Looking into IDP Systems?
What Can You Tell Me About Different Attack Categories?
When Would a TCP Host Sweep Be Considered an Attack?
What Is the Difference between a Worm and a Trojan Horse?
What Can You Tell Me about the Back Orifice Trojan Horse Exploit?
What Can You Tell Me about Bot Exploits?
What Can You Tell Me about Buffer Overflow Exploits?
Explain Event Correlation.
Demonstrate How Well You Know the Wireshark (a.k.a. Ethereal) Analyzer and Use It to Decompose an Attack.
What Intrusion Detection and Prevention Products Do You Have Experience With?
Where Is the Proper Place to Deploy an IPS?
Mention the Pros and Cons of Your Choice(s).
How Well Do You Know Snort Rules?
How Well Do You Know Snort Configurations?

What Questions Do You Want to Ask Me?

Recommended Reading

Chapter 8: Everything You Ever Wanted to Know about Wireless but Were Afraid They’d Ask

The Fundamentals

What Do All These Letters Mean?
IEEE and the WiFi Alliance
A Brief History of Wireless Security

Wireless Cards and Chipsets

Prism (2, 2.5, and 3)
Hermes
Atheros
Broadcom
Aironet
Intel
## Contents

**Wireless Drivers for Linux**
- Hermes 154
- MADWIFI 154
- IPW Variants 154
- Wlan-ng 155
- HostAP 155

**WLAN Detection (WarDriving)**
- WarDriving Tools 155
- Access Points Versus Clients 157
- Using WarDrive Data to Compromise Networks 159

**Wireless Security**
- Wired Equivalent Privacy (WEP) 160
- WiFi Protected Access (WPA) 161

**Rogue Wireless Devices**
- What Is a Rogue Access Point? 162
- What Is a Rogue Client? 163
- How Do You Detect a Rogue Wireless Device? 164
- How Can You Become a Rogue Access Point? 164

**Summary**

**Interview Q&A**

**Recommended Reading**

---

**Chapter 9: Finding Your Posture** 167

**History of Information Security** 167

**Modern Information Security** 168

**Security Objectives** 170

**Determining the Security Posture** 172
- Risk Assessments 172
- Vulnerability Assessments 176
- Threat Assessments 176
- Audits 177
- Self-Assessments 178

**Prioritizing the Vulnerabilities** 178
- Developing a Mitigation Roadmap 180
- Resource Allocation for the Roadmap 180

**Vulnerability Management** 181
- Patch Management Is a Start 181
- Tracking Progress 182
- Cost Avoidance versus Return on Investment 182
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>183</td>
</tr>
<tr>
<td>Interview Q&amp;A</td>
<td>184</td>
</tr>
<tr>
<td>Recommended Reading</td>
<td>185</td>
</tr>
</tbody>
</table>

### Chapter 10: Tools

#### Enumeration, Port Scanning, and Banner Grabbing
- SuperScan                                                                 | 188  |
- Nmap                                                                   | 188  |
- SNMP Scanning                                                          | 189  |
- SNScan                                                                 | 189  |
- Net-SNMP                                                               | 189  |
- SolarWinds                                                             | 190  |

#### Wireless Enumeration
- Kismet                                                                 | 191  |
- KisMAC                                                                 | 191  |
- AirMagnet                                                              | 191  |

#### Vulnerability Scanning
- Nessus                                                                 | 192  |
- Saint                                                                  | 192  |
- IBM Internet Scanner Software (ISS)                                   | 193  |
- eEye Retina Network Security Scanner                                  | 193  |
- Host Evaluation                                                        | 193  |
- CIS Scripts                                                            | 193  |
- Bastille                                                               | 194  |
- MBSA                                                                   | 194  |

#### Password Compliance Testing
- John the Ripper                                                        | 195  |
- Cain & Able                                                            | 195  |
- NGSSQL Crack                                                           | 195  |
- Application Scanning                                                  | 195  |
- WebInspect                                                            | 196  |
- Wikto                                                                  | 196  |
- Suru                                                                   | 196  |
- AppDetectivePro                                                       | 196  |
- NGSSquirrel                                                                         | 197  |
- OraScan                                                                | 197  |

#### Network Sniffing
- Tcpdump                                                                | 198  |
- Snoop                                                                   | 198  |
Contents

WinDump 198
Wireshark 199
**Penetration Testing** 199
Ettercap 199
BiDIBLAH 200
Metasploit 200
Core Impact 200
Canvas 201
**Learning** 201
VMWare 202
Parallels 202
Virtual PC 202
Cygwin 203
**Summary** 203
**Interview Q&A** 203
**Recommended Reading** 205
**Additional Resources** 205
Index 207