
Contents

| | | |
|------------------|--|----|
| Chapter 1 | Check Point Specialist - IPS-1 | 1 |
| | Course Layout | 3 |
| | Prerequisites | 3 |
| | CPCS - IPS-1 | 3 |
| | Recommended Setup for Labs | 5 |
| | Recommended Lab Topology | 6 |
| | IP Addresses | 7 |
| | Lab Terms | 9 |
| | Lab Stations | 10 |
| | | |
| Chapter 2 | Intrusion Prevention Systems | 11 |
| | Today's Security Risks | 13 |
| | Detection vs. Prevention | 14 |
| | Check Point IPS-1 | 18 |
| | Hybrid Detection Engine | 20 |
| | Confidence Indexing | 22 |
| | Customizable Signature Language | 23 |
| | Security Profiles | 23 |
| | Forensic Analysis | 24 |
| | Vulnerability Management | 25 |
| | Reporting | 26 |
| | IPS-1 in Action | 27 |
| | Protocol Anomaly Detection | 28 |
| | Other Types of Detection | 31 |
| | Beyond Intrusion | 31 |
| | Review | 33 |
| | Review Questions | 33 |
| | | |
| Chapter 3 | Check Point IPS-1 | 35 |
| | IPS-1 Components | 37 |
| | IPS-1 Sensor | 37 |
| | IPS-1 Alerts Concentrator | 38 |
| | IPS-1 Server | 40 |
| | IPS-1 Management Dashboard | 41 |
| | Architecture and Placement | 43 |
| | Selecting Placement Points | 43 |
| | IPS-1 Sensor Placement — In Your DMZ | 44 |
| | IPS-1 Sensor Placement — On Network Backbones | 45 |
| | IPS-1 Sensor Placement — On Critical Network Subnets | 46 |
| | Other Possible PS-1 Sensor Locations | 47 |
| | Deployments | 48 |
| | Organizational Deployment | 51 |
| | High Availability | 51 |

| | |
|--|------------|
| IPS-1 Sensor Installation Modes | 53 |
| IPS-1 Sensor Inline-Mode Packet Flow | 55 |
| Review | 57 |
| Review Questions | 57 |
| | |
| Chapter 4 Installing IPS-1 | 59 |
| Installing IPS-1 for the First Time | 60 |
| IPS-1 Alerts Concentrator Requirements | 60 |
| IPS-1 Server Requirements | 60 |
| IPS-1 Management Dashboard | 61 |
| Additional Requirements | 62 |
| Installing IPS-1 Sensors | 64 |
| Installing the IPS-1 Sensor Hardware | 65 |
| Example Installation | 66 |
| Accessing the Sensor Management Menu | 66 |
| Sensor Access — Serial Console | 67 |
| Sensor Access — Keyboard/Monitor | 67 |
| Lab 1: IPS-1 Sensor Configuration | 71 |
| Lab 2: IPS-1 Installation | 81 |
| Lab 3: IPS-1 Management Dashboard | 91 |
| Review | 115 |
| Review Questions | 115 |
| | |
| Chapter 5 Managing Packages and Back-Ends | 117 |
| Understanding Packages, Back-Ends, and Variables | 119 |
| Understanding Policies | 119 |
| Policy Groups | 120 |
| Policy-Group Behavior | 120 |
| Managing Policies | 121 |
| Passing Down and Inheriting Policy Settings | 123 |
| Modify Policy Settings Directly | 125 |
| Policy Subgroups | 127 |
| Policy Inspector | 128 |
| Special Back-Ends and Variables | 130 |
| General Event Recorders | 130 |
| Using the General Recorders | 131 |
| The Attack Package | 132 |
| The Packet Capture Back-End | 133 |
| Implicit Attack Details Back-End | 134 |
| Alert-Flood Suppression Back-End | 134 |
| Alert Tuning | 135 |
| Variables in the Attack/Inhibit Back-End | 136 |
| Initial Basic-Prevention Configuration | 139 |
| Attack/Prevention Back-End | 139 |
| Tuning the Sensor for Your Network | 141 |
| Review | 143 |
| Review Questions | 143 |

| | | |
|-------------------|--|-----|
| Chapter 6 | Monitoring IPS-1 Alerts | 145 |
| | Alert Browser | 147 |
| | Tool Buttons | 149 |
| | Browsing Alerts | 151 |
| | Alert Grouping | 152 |
| | Viewing Alerts by Priority | 156 |
| | Lab 4: Testing IPS-1 | 171 |
| | Lab 5: Using The Timeline | 205 |
| | Review | 225 |
| | Review Questions | 225 |
| | | |
| Chapter 7 | The Vulnerability Browser | 227 |
| | Nessus | 229 |
| | Importing Nessus Data | 230 |
| | Compromise Risk | 232 |
| | Lab 6: IPS-1 Vulnerability Browser | 235 |
| | Review | 245 |
| | Review Questions | 245 |
| | | |
| Chapter 8 | IPS-1 Reports | 247 |
| | Setting Up Reports | 248 |
| | Setting Up Reports | 248 |
| | Generating a Report | 251 |
| | Subreports | 254 |
| | Available Reports | 256 |
| | Review | 259 |
| | Review Questions | 259 |
| | | |
| Appendix A | Review Answers | 261 |
| | Chapter 2: Intrusion Prevention Systems | 261 |
| | Chapter 3: Check Point IPS-1 | 263 |
| | Chapter 4: Installing IPS-1 | 264 |
| | Chapter 5: Managing Packages and Back-Ends | 265 |
| | Chapter 6: Monitoring IPS-1 Alerts | 266 |
| | Chapter 7: The Vulnerability Browser | 267 |
| | Chapter 8: IPS-1 Reports | 268 |

