

# Contents

|          |   |           |
|----------|---|-----------|
| <b>1</b> | <b>Security Principles</b>                | <b>1</b>  |
| 1.1      | Objectives                                | 1         |
| 1.2      | Problem Context                           | 1         |
| 1.3      | The Principles                            | 2         |
| 1.3.1    | Simplicity                                | 3         |
| 1.3.2    | Open Design                               | 3         |
| 1.3.3    | Compartmentalization                      | 4         |
| 1.3.4    | Minimum Exposure                          | 5         |
| 1.3.5    | Least Privilege                           | 6         |
| 1.3.6    | Minimum Trust and Maximum Trustworthiness | 7         |
| 1.3.7    | Secure, Fail-Safe Defaults                | 9         |
| 1.3.8    | Complete Mediation                        | 10        |
| 1.3.9    | No Single Point of Failure                | 11        |
| 1.3.10   | Traceability                              | 12        |
| 1.3.11   | Generating Secrets                        | 13        |
| 1.3.12   | Usability                                 | 13        |
| 1.4      | Discussion                                | 14        |
| 1.5      | Assignment                                | 14        |
| 1.6      | Exercises                                 | 14        |
| <b>2</b> | <b>The Virtual Environment</b>            | <b>17</b> |
| 2.1      | Objectives                                | 17        |
| 2.2      | VirtualBox                                | 18        |
| 2.2.1    | Setting up a New Virtual Machine          | 18        |
| 2.2.2    | The Network                               | 19        |
| 2.3      | The Lab Environment                       | 21        |
| 2.3.1    | The Hosts                                 | 22        |
| 2.4      | Installing the Virtual Machines           | 24        |
| 2.4.1    | Installing host <b>alice</b>              | 24        |
| 2.4.2    | Installing host <b>bob</b>                | 25        |
| 2.4.3    | Installing host <b>mallet</b>             | 26        |

|          |  |    |
|----------|--|----|
| <b>3</b> | <b>Network Services</b>                  | 27 |
| 3.1      | Objectives                               | 27 |
| 3.2      | Networking Background                    | 28 |
| 3.2.1    | Internet Layer                           | 29 |
| 3.2.2    | Transport Layer                          | 29 |
| 3.3      | The Adversary's Point of View            | 31 |
| 3.3.1    | Information Gathering                    | 31 |
| 3.3.2    | Finding Potential Vulnerabilities        | 33 |
| 3.3.3    | Exploiting Vulnerabilities               | 35 |
| 3.3.4    | Vulnerable Configurations                | 36 |
| 3.4      | The Administrator's Point of View        | 38 |
| 3.5      | Actions to Be Taken                      | 39 |
| 3.5.1    | Deactivating Services                    | 39 |
| 3.5.2    | Restricting Services                     | 42 |
| 3.6      | Exercises                                | 45 |
| <b>4</b> | <b>Authentication and Access Control</b> | 47 |
| 4.1      | Objectives                               | 47 |
| 4.2      | Authentication                           | 47 |
| 4.2.1    | Telnet and Remote Shell                  | 48 |
| 4.2.2    | Secure Shell                             | 49 |
| 4.3      | User IDs and Permissions                 | 52 |
| 4.3.1    | File Access Permissions                  | 52 |
| 4.3.2    | Setuid and Setgid                        | 55 |
| 4.4      | Shell Script Security                    | 57 |
| 4.4.1    | Symbolic Links                           | 58 |
| 4.4.2    | Temporary Files                          | 59 |
| 4.4.3    | Environment                              | 60 |
| 4.4.4    | Data Validation                          | 61 |
| 4.5      | Quotas                                   | 62 |
| 4.6      | Change Root                              | 63 |
| 4.7      | Exercises                                | 66 |
| <b>5</b> | <b>Logging and Log Analysis</b>          | 69 |
| 5.1      | Objectives                               | 69 |
| 5.2      | Logging Mechanisms and Log Files         | 70 |
| 5.2.1    | Remote Logging                           | 72 |
| 5.3      | Problems with Logging                    | 72 |
| 5.3.1    | Tampering and Authenticity               | 72 |
| 5.3.2    | Tamper-Proof Logging                     | 73 |
| 5.3.3    | Input Validation                         | 73 |
| 5.3.4    | Rotation                                 | 74 |
| 5.4      | Intrusion Detection                      | 74 |
| 5.4.1    | Log Analysis                             | 75 |
| 5.4.2    | Suspicious Files and Rootkits            | 76 |

|          |   |            |
|----------|---|------------|
| 5.4.3    | Integrity Checks .....                                | 77         |
| 5.5      | Exercises .....                                       | 79         |
| <b>6</b> | <b>Web Application Security .....</b>                 | <b>81</b>  |
| 6.1      | Objectives .....                                      | 81         |
| 6.2      | Preparatory Work .....                                | 82         |
| 6.3      | Black-Box Audit .....                                 | 82         |
| 6.4      | Attacking Web Applications .....                      | 84         |
| 6.4.1    | Remote File Upload Vulnerability in Joomla! .....     | 84         |
| 6.4.2    | Remote Command Execution .....                        | 85         |
| 6.4.3    | SQL Injections .....                                  | 86         |
| 6.4.4    | Privilege Escalation .....                            | 88         |
| 6.5      | User Authentication and Session Management .....      | 89         |
| 6.5.1    | A PHP-Based Authentication Mechanism .....            | 89         |
| 6.5.2    | HTTP Basic Authentication .....                       | 90         |
| 6.5.3    | Cookie-Based Session Management .....                 | 92         |
| 6.6      | Cross-Site Scripting (XSS) .....                      | 94         |
| 6.6.1    | Persistent XSS Attacks .....                          | 94         |
| 6.6.2    | Reflected XSS Attacks .....                           | 95         |
| 6.6.3    | DOM-Based XSS Attacks .....                           | 96         |
| 6.7      | SQL Injections Revisited .....                        | 97         |
| 6.8      | Secure Socket Layer .....                             | 98         |
| 6.9      | Further Reading .....                                 | 100        |
| 6.10     | Exercises .....                                       | 100        |
| <b>7</b> | <b>Certificates and Public Key Cryptography .....</b> | <b>103</b> |
| 7.1      | Objectives .....                                      | 103        |
| 7.2      | Fundamentals of Public Key Cryptography .....         | 103        |
| 7.3      | Distribution of Public Keys and Certificates .....    | 105        |
| 7.4      | Creating Keys and Certificates .....                  | 107        |
| 7.5      | Running a Certificate Authority .....                 | 108        |
| 7.6      | Certificate-Based Client Authentication .....         | 111        |
| 7.7      | Exercises .....                                       | 112        |
| <b>8</b> | <b>Risk Management .....</b>                          | <b>117</b> |
| 8.1      | Objectives .....                                      | 117        |
| 8.2      | Risk and Risk Management .....                        | 117        |
| 8.3      | The Core Elements of Risk Analysis .....              | 120        |
| 8.4      | Risk Analysis: An Implementation .....                | 129        |
| 8.4.1    | System Description .....                              | 130        |
| 8.4.2    | Stakeholders .....                                    | 132        |
| 8.4.3    | Assets and Vulnerabilities .....                      | 132        |
| 8.4.4    | Vulnerabilities .....                                 | 137        |
| 8.4.5    | Threat Sources .....                                  | 138        |
| 8.4.6    | Risks and Countermeasures .....                       | 139        |

|          |  |            |
|----------|--|------------|
| 8.4.7    | Summary .....                                | 144        |
| <b>A</b> | <b>Using This Book in a Lab Course .....</b> | <b>147</b> |
| A.1      | Course Structure .....                       | 147        |
| A.2      | Project.....                                 | 148        |
| <b>B</b> | <b>Report Template .....</b>                 | <b>155</b> |
| B.1      | System Characterization .....                | 155        |
| B.1.1    | System Overview .....                        | 155        |
| B.1.2    | System Functionality .....                   | 155        |
| B.1.3    | Components and Subsystems .....              | 156        |
| B.1.4    | Interfaces .....                             | 156        |
| B.1.5    | Backdoors .....                              | 156        |
| B.1.6    | Additional Material .....                    | 156        |
| B.2      | Risk Analysis and Security Measures .....    | 156        |
| B.2.1    | Information Assets .....                     | 156        |
| B.2.2    | Threat Sources .....                         | 156        |
| B.2.3    | Risks and Countermeasures.....               | 157        |
| B.3      | Review of the External System .....          | 158        |
| B.3.1    | Background .....                             | 158        |
| B.3.2    | Completeness in Terms of Functionality ..... | 158        |
| B.3.3    | Architecture and Security Concepts .....     | 158        |
| B.3.4    | Implementation.....                          | 158        |
| B.3.5    | Backdoors .....                              | 159        |
| B.3.6    | Comparison .....                             | 159        |
| <b>C</b> | <b>Linux Basics and Tools .....</b>          | <b>161</b> |
| C.1      | System Documentation.....                    | 161        |
| C.2      | Tools .....                                  | 163        |
| C.2.1    | Variables .....                              | 163        |
| C.2.2    | Quoting and Wildcards .....                  | 164        |
| C.2.3    | Pipelining and Backquotes .....              | 164        |
| C.2.4    | ls, find and locate.....                     | 165        |
| C.2.5    | wc, sort, uniq, head and tail .....          | 165        |
| C.2.6    | ps, pgrep, kill and killall .....            | 165        |
| C.2.7    | grep .....                                   | 166        |
| C.2.8    | awk and sed .....                            | 167        |
| C.2.9    | Tcpdump .....                                | 168        |
| <b>D</b> | <b>Answers to Questions .....</b>            | <b>169</b> |
|          | <b>References .....</b>                      | <b>197</b> |
|          | <b>Index .....</b>                           | <b>199</b> |



<http://www.springer.com/978-3-642-24473-5>

Applied Information Security

A Hands-on Approach

Basin, D.; Schaller, P.; Schläpfer, M.

2011, XIV, 202 p., Hardcover

ISBN: 978-3-642-24473-5