

Table of Contents

| | |
|---|-----------|
| List of Figures | xii |
| Preface | xvii |
| Chapter 1 — Introduction | 1 |
| Overview | 1 |
| Professional utility of information security knowledge | 1 |
| Brief history | 5 |
| Definition of information security | 11 |
| Summary | 14 |
| Example case – Wikileaks, Cablegate, and free reign over classified networks | 14 |
| Chapter review questions | 15 |
| Example case questions | 16 |
| Hands-on activity – Software Inspector, Steganography | 16 |
| Critical thinking exercise: identifying CIA area(s) affected by sample real-life hacking incidents | 21 |
| Design case | 21 |
| Chapter 2 — System Administration (Part 1) | 26 |
| Overview | 26 |
| Introduction | 26 |
| What is system administration? | 27 |
| System administration and information security | 28 |
| Common system administration tasks | 29 |
| System administration utilities | 33 |
| Summary | 37 |
| Example case – T. J. Maxx | 37 |
| Chapter review questions | 39 |

| | |
|--|-----------|
| Example case questions..... | 40 |
| Hands-on Activity – Linux system installation | 40 |
| Critical thinking exercise – Google executives sentenced to prison over video | 48 |
| Design case..... | 49 |
| Chapter 3 — System Administration (Part 2) | 51 |
| Overview | 51 |
| Operating system structure..... | 51 |
| The command-line interface..... | 53 |
| Files and directories..... | 53 |
| Moving around the filesystem – pwd, cd | 54 |
| Listing files and directories | 55 |
| Shell expansions | 56 |
| File management | 57 |
| Viewing files..... | 59 |
| Searching for files..... | 60 |
| Access control and user management | 61 |
| Access control lists | 64 |
| File ownership | 65 |
| Editing files..... | 66 |
| Software installation and updates..... | 67 |
| Account management | 72 |
| Command-line user administration | 75 |
| Example case – Northwest Florida State College | 77 |
| Summary | 78 |
| Chapter review questions..... | 78 |
| Example case questions..... | 79 |
| Hands-on activity – basic Linux system administration..... | 79 |
| Critical thinking exercise – offensive cyber effects operations (OCEO)..... | 80 |
| Design Case | 80 |

| | |
|--|------------|
| Chapter 4 — The Basic Information Security Model | 82 |
| Overview | 82 |
| Introduction | 82 |
| Components of the basic information security model..... | 82 |
| Common vulnerabilities, threats, and controls..... | 90 |
| Example case – ILOVEYOU virus..... | 99 |
| Summary | 100 |
| Chapter review questions..... | 100 |
| Example case questions..... | 101 |
| Hands-on activity – web server security | 101 |
| Critical thinking exercise – the internet, “American values,” and security | 102 |
| Design case..... | 103 |
| Chapter 5 — Asset Identification and Characterization | 104 |
| Overview | 104 |
| Assets overview..... | 104 |
| Determining assets that are important to the organization | 105 |
| Asset types..... | 109 |
| Asset characterization..... | 114 |
| IT asset life cycle and asset identification | 119 |
| System profiling | 124 |
| Asset ownership and operational responsibilities..... | 127 |
| Example case – Stuxnet..... | 130 |
| Summary | 130 |
| Chapter review questions..... | 131 |
| Example case questions..... | 131 |
| Hands-on activity – course asset identification | 132 |
| Critical thinking exercise – uses of a hacked PC | 132 |
| Design case..... | 133 |
| Chapter 6 — Threats and Vulnerabilities | 135 |
| Overview | 135 |
| Introduction | 135 |

| | | |
|-----|--|------------|
| 58 | Threat models..... | 136 |
| 58 | Threat agent..... | 137 |
| 58 | Threat action..... | 149 |
| 58 | Vulnerabilities..... | 162 |
| 99 | Example case – Gozi..... | 167 |
| 99 | Summary..... | 168 |
| 100 | Chapter review questions..... | 168 |
| 100 | Example case questions..... | 168 |
| 101 | Hands-on activity – Vulnerability scanning..... | 169 |
| 101 | Critical thinking exercise – Iraq cyberwar plans in 2003..... | 174 |
| 101 | Design case..... | 174 |
| | Chapter 7 — Encryption Controls | 176 |
| 104 | Overview..... | 176 |
| 104 | Introduction..... | 176 |
| 104 | Encryption basics..... | 177 |
| 104 | Encryption types overview..... | 181 |
| 104 | Encryption types details..... | 187 |
| 111 | Encryption in use..... | 194 |
| 111 | Example case – Nation technologies..... | 197 |
| 124 | Summary..... | 198 |
| 127 | Chapter review questions..... | 198 |
| 130 | Example case questions..... | 199 |
| 130 | Hands-on activity – encryption..... | 199 |
| 131 | Critical thinking exercise – encryption keys embed business models..... | 205 |
| 131 | Design case..... | 206 |
| | Chapter 8 — Identity and Access Management | 207 |
| 137 | Overview..... | 207 |
| 137 | Identity management..... | 207 |
| 137 | Access management..... | 212 |
| 137 | Authentication..... | 213 |

| | |
|---|------------|
| Single sign-on..... | 221 |
| Federation..... | 228 |
| Example case – Markus Hess..... | 237 |
| Summary..... | 239 |
| Chapter review questions..... | 239 |
| Example case questions..... | 240 |
| Hands-on activity – identity match and merge..... | 240 |
| Critical thinking exercise – feudalism the security solution for the internet? | 244 |
| Design case..... | 245 |
| Chapter 9 — Hardware and Software Controls | 247 |
| Overview..... | 247 |
| Password management..... | 247 |
| Access control..... | 251 |
| Firewalls..... | 252 |
| Intrusion detection/prevention systems..... | 256 |
| Patch management for operating systems and applications..... | 261 |
| End-point protection..... | 264 |
| Example case – AirTight networks..... | 266 |
| Chapter review questions..... | 270 |
| Example case questions..... | 270 |
| Hands-on activity – host-based IDS (OSSEC)..... | 271 |
| Critical thinking exercise – extra-human security controls..... | 275 |
| Design case..... | 275 |
| Chapter 10 — Shell Scripting | 277 |
| Overview..... | 277 |
| Introduction..... | 277 |
| Output redirection..... | 279 |
| Text manipulation..... | 280 |
| Variables..... | 283 |
| Conditionals..... | 287 |

| | |
|---|------------|
| User input | 290 |
| Loops | 292 |
| Putting it all together | 299 |
| Example case – Max Butler..... | 301 |
| Summary | 302 |
| Chapter review questions..... | 303 |
| Example case questions..... | 303 |
| Hands-on activity – basic scripting | 303 |
| Critical thinking exercise – script security | 304 |
| Design case..... | 305 |
| Chapter 11 — Incident Handling | 306 |
| Introduction | 306 |
| Incidents overview..... | 306 |
| Incident handling..... | 307 |
| The disaster..... | 327 |
| Example case – on-campus piracy | 328 |
| Summary | 330 |
| Chapter review questions..... | 330 |
| Example case questions..... | 331 |
| Hands-on activity – incident timeline using OSSEC | 331 |
| Critical thinking exercise – destruction at the EDA | 331 |
| Design case..... | 332 |
| Chapter 12 — Incident Analysis | 333 |
| Introduction | 333 |
| Log analysis..... | 333 |
| Event criticality | 337 |
| General log configuration and maintenance..... | 345 |
| Live incident response..... | 347 |
| Timelines | 350 |
| Other forensics topics..... | 352 |
| Example case – backup server compromise..... | 353 |

| | |
|---|------------|
| Chapter review questions..... | 355 |
| Example case questions..... | 356 |
| Hands-on activity – server log analysis..... | 356 |
| Critical thinking exercise – destruction at the EDA..... | 358 |
| Design case..... | 358 |
| Chapter 13 — Policies, Standards, and Guidelines | 360 |
| Introduction..... | 360 |
| Guiding principles..... | 360 |
| Writing a policy..... | 367 |
| Impact assessment and vetting..... | 371 |
| Policy review..... | 373 |
| Compliance..... | 374 |
| Key policy issues..... | 377 |
| Example case – HB Gary..... | 378 |
| Summary..... | 379 |
| Reference..... | 379 |
| Chapter review questions..... | 379 |
| Example case questions..... | 380 |
| Hands-on activity – create an AUP..... | 380 |
| Critical thinking exercise – Aaron Swartz..... | 380 |
| Design case..... | 381 |
| Chapter 14 — IT Risk Analysis and Risk Management | 382 |
| Overview..... | 382 |
| Introduction..... | 382 |
| Risk management as a component of organizational management..... | 383 |
| Risk-management framework..... | 384 |
| The NIST 800-39 framework..... | 385 |
| Risk assessment..... | 387 |
| Other risk-management frameworks..... | 389 |
| IT general controls for Sarbanes–Oxley compliance..... | 391 |

| | |
|---|------------|
| Compliance versus risk management | 398 |
| Selling security | 399 |
| Example case – online marketplace purchases..... | 399 |
| Summary | 400 |
| Chapter review questions..... | 400 |
| Hands-on activity – risk assessment using LSOF..... | 401 |
| Critical thinking exercise – risk estimation biases | 403 |
| Design case..... | 403 |
| Appendix A — Password List for the Linux Virtual Machine | 404 |
| Glossary | 405 |
| Index | 413 |