

# Spis treści

|                                                                              |           |
|------------------------------------------------------------------------------|-----------|
| <b>O autorze</b>                                                             | <b>15</b> |
| <b>O recenzentach</b>                                                        | <b>16</b> |
| <b>Przedmowa</b>                                                             | <b>17</b> |
| <b>Wstęp</b>                                                                 | <b>19</b> |
| <br>                                                                         |           |
| <b>Część I. Doskonalenie technik obrony.<br/>Podstawy teoretyczne</b>        | <b>23</b> |
| <br>                                                                         |           |
| <b>Rozdział 1. Przypomnienie pojęć związanych z cyberbezpieczeństwem</b>     | <b>25</b> |
| <br>                                                                         |           |
| <b>Wymagania techniczne</b>                                                  | <b>26</b> |
| <b>Nurkujemy w samo sedno cyberbezpieczeństwa</b>                            | <b>26</b> |
| Triada cyberbezpieczeństwa                                                   | 26        |
| Rodzaje ataków                                                               | 28        |
| <b>Zarządzanie legendarnym słabym punktem w cyberbezpieczeństwie — hasła</b> | <b>36</b> |
| Zdekonspirowane hasła                                                        | 36        |
| Ataki inżynierii społecznej z wykorzystaniem wykradzionych haseł             | 38        |
| Ataki siłowe                                                                 | 39        |
| Ataki słownikowe                                                             | 40        |
| Tworzenie bezpiecznego hasła                                                 | 41        |
| Zarządzanie hasłami na poziomie przedsiębiorstwa                             | 43        |
| Dodatek                                                                      | 45        |
| <b>Doskonalenie obrony w głąb</b>                                            | <b>46</b> |
| Czynniki, które należy wziąć pod uwagę przy tworzeniu modeli DiD             | 46        |
| Identyfikacja aktywów                                                        | 48        |
| Obrona dzięki warstwom                                                       | 49        |
| Dodatek                                                                      | 53        |

|                                                                                   |            |
|-----------------------------------------------------------------------------------|------------|
| <b>Drużyny: niebieskich i czerwonych — porównanie</b>                             | <b>53</b>  |
| <b>Podsumowanie</b>                                                               | <b>56</b>  |
| <b>Lektura uzupełniająca</b>                                                      | <b>56</b>  |
| <b>Rozdział 2. Zarządzanie zagrożeniami, podatności i ryzyko</b>                  | <b>57</b>  |
| <b>Wymagania techniczne</b>                                                       | <b>58</b>  |
| <b>Zrozumienie podatności i zagrożeń związanych z cyberbezpieczeństwem</b>        | <b>58</b>  |
| Przeprowadzenie oceny podatności na zagrożenia                                    | 58         |
| Proces oceny zagrożeń                                                             | 59         |
| Kiedy należy wykonać sprawdzenie pod kątem podatności?                            | 61         |
| Rodzaje podatności                                                                | 61         |
| Podatności w zabezpieczeniach USB HID                                             | 66         |
| Rodzaje ataków USB HID                                                            | 67         |
| Fałszywe poczucie bezpieczeństwa                                                  | 72         |
| Ochrona przed atakami USB HID                                                     | 75         |
| <b>Zarządzanie ryzykiem związanym z cyberbezpieczeństwem</b>                      | <b>78</b>  |
| Identyfikacja ryzyka                                                              | 79         |
| Ocena ryzyka                                                                      | 80         |
| Reakcja na ryzyko                                                                 | 82         |
| Monitorowanie ryzyka                                                              | 83         |
| <b>Ramy cyberbezpieczeństwa NIST</b>                                              | <b>84</b>  |
| Identyfikacja                                                                     | 84         |
| Ochrona                                                                           | 84         |
| Wykrywanie                                                                        | 84         |
| Reakcja                                                                           | 85         |
| Przywracanie                                                                      | 85         |
| <b>Tworzenie skutecznego planu ciągłości działania (BCP)</b>                      | <b>86</b>  |
| Tworzenie analizy wpływu na biznes (BIA)                                          | 87         |
| Planowanie ciągłości działania (BCP)                                              | 91         |
| <b>Wdrażanie najlepszego w swojej klasie DRP</b>                                  | <b>95</b>  |
| Tworzenie DRP                                                                     | 95         |
| Wdrażanie DRP                                                                     | 96         |
| <b>Podsumowanie</b>                                                               | <b>98</b>  |
| <b>Lektura uzupełniająca</b>                                                      | <b>98</b>  |
| <b>Rozdział 3. Zasady, procedury, zgodność i audyty</b>                           | <b>100</b> |
| <b>Tworzenie światowej klasy zasad i procedur dotyczących cyberbezpieczeństwa</b> | <b>101</b> |
| Zasady związane z cyberbezpieczeństwem                                            | 101        |
| Procedury związane z cyberbezpieczeństwem                                         | 102        |
| Metoda CUDSE                                                                      | 103        |
| <b>Zrozumienie i osiągnięcie zgodności</b>                                        | <b>108</b> |
| Rodzaje regulacji                                                                 | 108        |
| Osiągnięcie zgodności                                                             | 110        |
| <b>Eksplorowanie, tworzenie audytów i zarządzanie nimi</b>                        | <b>113</b> |
| Wewnętrzne audyty cyberbezpieczeństwa                                             | 114        |
| Zewnętrzne audyty bezpieczeństwa cybernetycznego                                  | 114        |
| Zarządzanie danymi podczas audytów                                                | 115        |
| Rodzaje audytów cyberbezpieczeństwa                                               | 117        |
| Kiedy przeprowadzać audyt?                                                        | 120        |

|                                                                                             |            |
|---------------------------------------------------------------------------------------------|------------|
| <b>Zastosowanie CMM</b>                                                                     | <b>120</b> |
| Cele CMM                                                                                    | 120        |
| Charakterystyka dobrego CMM                                                                 | 120        |
| Struktura dobrego CMM                                                                       | 121        |
| Analizowanie rezultatów                                                                     | 123        |
| Zalety CMM                                                                                  | 124        |
| <b>Podsumowanie</b>                                                                         | <b>125</b> |
| <b>Lektura uzupełniająca</b>                                                                | <b>125</b> |
| <b>Rozdział 4. Łatanie ósmej warstwy</b>                                                    | <b>126</b> |
| <b>Warstwa 8 — zagrożenie wewnętrzne</b>                                                    | <b>127</b> |
| Działanie nieumyślne                                                                        | 127        |
| Szkodliwy użytkownik                                                                        | 128        |
| Jak rozpoznać wewnętrznego szkodnika?                                                       | 129        |
| Ochrona infrastruktury przed wewnętrznymi szkodnikami                                       | 130        |
| <b>Doskonalenie sztuki inżynierii społecznej</b>                                            | <b>136</b> |
| Przebieg ataku w inżynierii społecznej                                                      | 137        |
| Socjotechniki                                                                               | 138        |
| Rodzaje ataków wykorzystujących inżynierię społeczną                                        | 140        |
| <b>Obrona przed atakami socjotechnicznymi (łatanie warstwy 8)</b>                           | <b>152</b> |
| Tworzenie strategii szkoleń                                                                 | 153        |
| Prawa administratora                                                                        | 153        |
| Wdrożenie silnej zasady BYOD                                                                | 154        |
| Przeprowadzanie losowych ataków inżynierii społecznej                                       | 154        |
| <b>Podsumowanie</b>                                                                         | <b>155</b> |
| <b>Lektura uzupełniająca</b>                                                                | <b>155</b> |
| <b>Rozdział 5. Technologie i narzędzia w cyberbezpieczeństwie</b>                           | <b>156</b> |
| <b>Wymagania techniczne</b>                                                                 | <b>157</b> |
| <b>Zaawansowane narzędzia bezprzewodowe dla cyberbezpieczeństwa</b>                         | <b>157</b> |
| Obrona przed atakami bezprzewodowymi                                                        | 157        |
| <b>Narzędzia i metody testów penetracyjnych</b>                                             | <b>163</b> |
| Metasploit                                                                                  | 163        |
| Zestaw narzędzi do inżynierii społecznej                                                    | 164        |
| exe2hex                                                                                     | 168        |
| <b>Stosowanie narzędzi i metod kryminalistycznych</b>                                       | <b>168</b> |
| Postępowanie z dowodami                                                                     | 169        |
| Narzędzia kryminalistyczne                                                                  | 169        |
| Odzyskiwanie skasowanych plików                                                             | 173        |
| <b>Jak sobie radzić z APT?</b>                                                              | <b>174</b> |
| Techniki obrony                                                                             | 175        |
| <b>Systemy inteligentnego wykrywania zagrożeń w podnoszeniu poziomu cyberbezpieczeństwa</b> | <b>176</b> |
| Inteligentne wykrywanie zagrożeń — podstawy                                                 | 176        |
| Wdrażanie systemu inteligentnego wykrywania zagrożeń                                        | 177        |
| <b>Przekształcenie zagrożenia w rozwiązanie</b>                                             | <b>178</b> |
| Problem                                                                                     | 179        |
| Rozwiązanie                                                                                 | 179        |
| <b>Podsumowanie</b>                                                                         | <b>179</b> |
| <b>Lektura uzupełniająca</b>                                                                | <b>180</b> |

## Część II. Obrona w praktyce

181

|                                                                                            |            |
|--------------------------------------------------------------------------------------------|------------|
| <b>Rozdział 6. Zabezpieczanie infrastruktury działającej pod kontrolą systemów Windows</b> | <b>183</b> |
| <b>Wymagania techniczne</b>                                                                | <b>184</b> |
| <b>Utwardzanie systemu Windows w praktyce</b>                                              | <b>184</b> |
| Utwardzanie przez zespół ds. infrastruktury                                                | 184        |
| Tworzenie listy kontrolnej dla procedur utwardzania                                        | 185        |
| <b>Tworzenie strategii instalowania łatek</b>                                              | <b>190</b> |
| Złożoność łatania                                                                          | 190        |
| Rozdzielanie zadań (łatanie ról i przydziałów)                                             | 192        |
| Dystrybucja i wdrażanie poprawek                                                           | 193        |
| Rodzaje łatek                                                                              | 195        |
| <b>Zabezpieczanie AD w praktyce</b>                                                        | <b>198</b> |
| Bezpieczne hosty administracyjne                                                           | 200        |
| Dokumentacja dotycząca bezpieczeństwa systemu Windows Server                               | 201        |
| <b>Zabezpieczanie końcówek — stacji roboczych</b>                                          | <b>201</b> |
| Aktualizacje systemu Windows                                                               | 201        |
| Dlaczego warto przejść na Windows 10?                                                      | 201        |
| Bezpieczeństwo fizyczne                                                                    | 202        |
| Programy antywirusowe                                                                      | 203        |
| Zapora ogniowa Windows Defender                                                            | 203        |
| Kontrola aplikacji                                                                         | 204        |
| Filtrowanie adresów URL                                                                    | 204        |
| Filtrowanie spamu                                                                          | 205        |
| Systemy, do których ma dostęp klient                                                       | 205        |
| Kopie zapasowe                                                                             | 206        |
| Użytkownicy                                                                                | 206        |
| Zabezpieczanie danych                                                                      | 207        |
| <b>Wykorzystanie szyfrowania</b>                                                           | <b>207</b> |
| Konfiguracja programu BitLocker                                                            | 208        |
| <b>Podsumowanie</b>                                                                        | <b>208</b> |
| <b>Rozdział 7. Utwardzanie serwera Unix</b>                                                | <b>209</b> |
| <b>Wymagania techniczne</b>                                                                | <b>210</b> |
| <b>Zabezpieczanie usług uniksowych</b>                                                     | <b>210</b> |
| Określ przeznaczenia serwera                                                               | 210        |
| Skonfiguruj bezpieczny rozruch                                                             | 211        |
| Zarządzanie usługami                                                                       | 211        |
| <b>Uprawnienia do plików w praktyce</b>                                                    | <b>215</b> |
| Zrozumienie pojęcia „właściciel” i uprawnień                                               | 215        |
| Domyślne uprawnienia                                                                       | 218        |
| Uprawnienia w katalogach (folderach)                                                       | 219        |
| Zmiana domyślnych uprawnień za pomocą umask                                                | 220        |
| Hierarchia uprawnień                                                                       | 221        |
| Porównywanie uprawnień do katalogów                                                        | 222        |
| Zmiana uprawnień i własności pojedynczego pliku                                            | 222        |
| Przydatne polecenia do wyszukiwania niechcianych uprawnień                                 | 223        |

|                                                                         |                |
|-------------------------------------------------------------------------|----------------|
| <b>Zwiększenie ochrony serwera poprzez ulepszenie kontroli dostępu</b>  | <b>224</b>     |
| Przeglądanie ACL                                                        | 224            |
| Zarządzanie listami ACL                                                 | 225            |
| Domyślne ACL dla katalogów                                              | 225            |
| Usuwanie list ACL                                                       | 226            |
| Rozszerzona kontrola dostępu                                            | 227            |
| <b>Konfiguracja zapory sieciowej</b>                                    | <b>228</b>     |
| Zrozumieć iptables                                                      | 228            |
| Konfigurowanie iptables                                                 | 229            |
| Ochrona SSH przed atakami siłowymi przy użyciu iptables                 | 232            |
| Ochrona przed skanowaniem portów za pomocą iptables                     | 233            |
| <b>Zaawansowane zarządzanie dziennikami</b>                             | <b>233</b>     |
| Wykorzystanie logów                                                     | 234            |
| <b>Podsumowanie</b>                                                     | <b>235</b>     |
| <b>Lektura uzupełniająca</b>                                            | <b>235</b>     |
| <br><b>Rozdział 8. Zwiększ swoje umiejętności obrony sieci</b>          | <br><b>236</b> |
| <b>Wymagania techniczne</b>                                             | <b>237</b>     |
| <b>Wykorzystanie eksperckiego narzędzia mapowania sieci — Nmap</b>      | <b>237</b>     |
| Fazy cyberataku                                                         | 238            |
| Nmap                                                                    | 239            |
| Skrypty Nmap                                                            | 242            |
| <b>Lepsza ochrona sieci bezprzewodowych</b>                             | <b>246</b>     |
| Podatności w zabezpieczeniach sieci bezprzewodowych                     | 246            |
| Instrukcja bezpieczeństwa użytkownika dla sieci bezprzewodowych         | 250            |
| <b>Wprowadzenie do programu Wireshark</b>                               | <b>255</b>     |
| Namierzanie użytkowników korzystających z niezabezpieczonych protokołów | 258            |
| FTP, HTTP i inny, nieszyfrowany ruch                                    | 263            |
| Wykorzystanie Wiresharka do obrony                                      | 264            |
| <b>Praca z IPS i IDS</b>                                                | <b>265</b>     |
| Co to jest IDS?                                                         | 265            |
| Co to jest IPS?                                                         | 266            |
| Bezpłatny system IDS/IPS                                                | 267            |
| IPS a IDS                                                               | 267            |
| <b>Podsumowanie</b>                                                     | <b>268</b>     |
| <br><b>Rozdział 9. Nurkujemy w zabezpieczenia fizyczne</b>              | <br><b>269</b> |
| <b>Wymagania techniczne</b>                                             | <b>270</b>     |
| <b>Zrozumienie zabezpieczeń fizycznych i związanych z nimi zagrożeń</b> | <b>270</b>     |
| Potężny LAN Turtle                                                      | 270            |
| Podstępny Plunder Bug LAN Tap                                           | 271            |
| Niebezpieczny Packet Squirrel                                           | 272            |
| Przenośny Shark Jack                                                    | 273            |
| Niesamowity Screen Crab                                                 | 273            |
| Zaawansowany Key Croc                                                   | 275            |
| Zagrożenia związane z USB                                               | 276            |
| Kradzież sprzętu                                                        | 277            |
| Zagrożenia środowiskowe                                                 | 278            |
| <b>Fizyczne mechanizmy zabezpieczeń</b>                                 | <b>278</b>     |

|                                                                                              |            |
|----------------------------------------------------------------------------------------------|------------|
| <b>Doskonalenie zabezpieczeń fizycznych</b>                                                  | <b>280</b> |
| Zasada czystego biurka                                                                       | 280        |
| Przeglądy zabezpieczeń fizycznych                                                            | 281        |
| <b>Podsumowanie</b>                                                                          | <b>282</b> |
| <b>Lektura uzupełniająca</b>                                                                 | <b>282</b> |
| <b>Rozdział 10. Zabezpieczenia IoT w praktyce</b>                                            | <b>283</b> |
| <b>Wymagania techniczne</b>                                                                  | <b>284</b> |
| <b>Zrozumieć internet rzeczy</b>                                                             | <b>284</b> |
| Ryzyko                                                                                       | 285        |
| Podatności                                                                                   | 286        |
| <b>Zrozumienie technologii sieciowych w IoT</b>                                              | <b>287</b> |
| LoRaWAN                                                                                      | 287        |
| Zigbee                                                                                       | 288        |
| Sigfox                                                                                       | 289        |
| Bluetooth                                                                                    | 290        |
| Uwagi dotyczące bezpieczeństwa                                                               | 291        |
| <b>Poprawa bezpieczeństwa IoT</b>                                                            | <b>292</b> |
| <b>Tworzenie sprzętu wspomagającego cyberbezpieczeństwo z wykorzystaniem IoT</b>             | <b>295</b> |
| Wykrywanie fałszywych punktów dostępu                                                        | 295        |
| Ściana ogniowa i system wykrywania włamań na Raspberry Pi                                    | 298        |
| Systemy obrony dla przemysłowych systemów sterowania (SCADA)                                 | 299        |
| Bezpieczne kopiowanie z USB na USB                                                           | 299        |
| Tworzenie przynęty za grosze                                                                 | 300        |
| Zaawansowane monitorowanie aplikacji internetowych i sieci                                   | 302        |
| Tworzenie urządzenia blokującego reklamy internetowe                                         | 303        |
| Kontrola dostępu i systemy fizycznych zabezpieczeń                                           | 303        |
| <b>Dodatkowe informacje: niebezpieczeństwo związane z nieautoryzowanymi urządzeniami IoT</b> | <b>304</b> |
| Wykrywanie nieautoryzowanych urządzeń IoT                                                    | 304        |
| Wykrywanie Raspberry Pi                                                                      | 304        |
| Wyłączanie fałszywych urządzeń Raspberry Pi                                                  | 305        |
| <b>Podsumowanie</b>                                                                          | <b>306</b> |
| <b>Lektura uzupełniająca</b>                                                                 | <b>306</b> |
| <b>Rozdział 11. Bezpieczne wytwarzanie i wdrażanie oprogramowania w środowisku chmury</b>    | <b>307</b> |
| <b>Wymagania techniczne</b>                                                                  | <b>308</b> |
| <b>Bezpieczna implementacja i wdrożenie aplikacji w chmurze</b>                              | <b>308</b> |
| Bezpieczeństwo w różnych modelach chmury                                                     | 308        |
| Bezpieczeństwo danych w chmurze                                                              | 310        |
| <b>Zabezpieczanie Kubernetes i API</b>                                                       | <b>313</b> |
| Zabezpieczenia typowe dla chmury                                                             | 313        |
| Kontrola dostępu do interfejsu API Kubernetes                                                | 314        |
| Kontrola dostępu do kubeletu                                                                 | 314        |
| Zapobieganie ładowaniu niepożądanych modułów jądra przez kontenery                           | 314        |
| Ograniczenie dostępu do etcd                                                                 | 315        |
| W systemach produkcyjnych unikaj korzystania z funkcji będących w wersjach alfa lub beta     | 315        |
| Integracje z elementami innych producentów                                                   | 315        |

|                                                                      |                |
|----------------------------------------------------------------------|----------------|
| <b>Zabezpieczanie usług baz danych</b>                               | <b>316</b>     |
| <b>Testowanie bezpieczeństwa chmury</b>                              | <b>317</b>     |
| Centrum zabezpieczeń Azure                                           | 318            |
| Amazon CloudWatch                                                    | 318            |
| AppDynamics                                                          | 319            |
| Nessus — skaner podatności                                           | 320            |
| InsightVM                                                            | 320            |
| Intruder                                                             | 321            |
| <b>Podsumowanie</b>                                                  | <b>322</b>     |
| <b>Lektura uzupełniająca</b>                                         | <b>322</b>     |
| <br><b>Rozdział 12. Bezpieczeństwo aplikacji internetowych</b>       | <br><b>323</b> |
| <b>Wymagania techniczne</b>                                          | <b>324</b>     |
| <b>Zbieranie informacji o Twojej witrynie/aplikacji internetowej</b> | <b>324</b>     |
| Znaczenie gromadzenia publicznie dostępnych danych                   | 325            |
| Wywiad z wykorzystaniem publicznie dostępnych źródeł                 | 325            |
| Informacje o hostingu                                                | 327            |
| Sprawdzanie ekspozycji danych za pomocą Google hacking (dorki)       | 329            |
| <b>Wykorzystanie DVWA</b>                                            | <b>331</b>     |
| Instalacja DVWA na Kali Linux                                        | 332            |
| <b>Przegląd najczęstszych ataków na aplikacje internetowe</b>        | <b>336</b>     |
| Badanie ataków XSS                                                   | 336            |
| <b>Korzystanie z pakietu Burp Suite</b>                              | <b>338</b>     |
| Wersje Burp Suite                                                    | 338            |
| Konfiguracja Burp Suite na Kali                                      | 339            |
| <b>Atak typu wstrzyknięcie SQL na DVWA</b>                           | <b>340</b>     |
| Naprawienie często występującego błędu                               | 346            |
| <b>Atak siłowy na hasła w aplikacjach internetowych</b>              | <b>347</b>     |
| Analiza wyników                                                      | 350            |
| <b>Podsumowanie</b>                                                  | <b>351</b>     |
| <b>Lektura uzupełniająca</b>                                         | <b>352</b>     |
| <br><b>Część III. Wypływamy na szerokie wody obrony</b>              | <br><b>353</b> |

|                                                   |            |
|---------------------------------------------------|------------|
| <b>Rozdział 13. Narzędzia do oceny podatności</b> | <b>355</b> |
| <b>Wymagania techniczne</b>                       | <b>356</b> |
| <b>Radzenie sobie z podatnościami</b>             | <b>356</b> |
| Kto powinien szukać podatności?                   | 356        |
| Programy nagród za znalezione błędy               | 356        |
| Wewnętrzne podatności                             | 357        |
| Narzędzia do badania podatności                   | 358        |
| <b>Użycie skanera podatności (OpenVAS)</b>        | <b>360</b> |
| Testy z uwierzytelnieniem                         | 360        |
| Instalacja OpenVAS                                | 361        |
| Używanie OpenVAS                                  | 363        |
| Aktualizowanie swoich kanałów                     | 366        |

|                                                                            |            |
|----------------------------------------------------------------------------|------------|
| <b>Skaner Nexpose</b>                                                      | <b>367</b> |
| <b>Podsumowanie</b>                                                        | <b>369</b> |
| <b>Lektura uzupełniająca</b>                                               | <b>369</b> |
| <b>Rozdział 14. Analiza złośliwego oprogramowania</b>                      | <b>370</b> |
| <b>Wymagania techniczne</b>                                                | <b>371</b> |
| <b>Dlaczego warto analizować złośliwe oprogramowanie?</b>                  | <b>371</b> |
| Funkcjonalność złośliwego oprogramowania                                   | 371        |
| Cele złośliwego oprogramowania                                             | 371        |
| Z kim i z czym łączy się złośliwe oprogramowanie                           | 372        |
| Zostawianie furtek                                                         | 373        |
| Narażone systemy                                                           | 373        |
| <b>Rodzaje i kategorie analizy złośliwego oprogramowania</b>               | <b>373</b> |
| Statyczna analiza złośliwego oprogramowania                                | 373        |
| Dynamiczna analiza złośliwego oprogramowania                               | 374        |
| Hybrydowa analiza złośliwego oprogramowania                                | 374        |
| Analiza właściwości statycznych                                            | 375        |
| Interaktywna analiza zachowania                                            | 375        |
| Analiza w pełni zautomatyzowana                                            | 375        |
| Inżynieria wsteczna kodu                                                   | 376        |
| <b>Najlepsze narzędzia do analizy złośliwego oprogramowania</b>            | <b>376</b> |
| Process Explorer                                                           | 377        |
| Process Monitor                                                            | 377        |
| ProcDOT                                                                    | 378        |
| Ghidra                                                                     | 379        |
| PeStudio                                                                   | 379        |
| <b>Przeprowadzanie analizy złośliwego oprogramowania</b>                   | <b>379</b> |
| Zasady bezpieczeństwa                                                      | 380        |
| Przeprowadzamy analizę                                                     | 381        |
| <b>Podsumowanie</b>                                                        | <b>384</b> |
| <b>Lektura uzupełniająca</b>                                               | <b>384</b> |
| <b>Rozdział 15. Wykorzystanie testów penetracyjnych w taktykach obrony</b> | <b>385</b> |
| <b>Wymagania techniczne</b>                                                | <b>386</b> |
| <b>Zrozumienie znaczenia dzienników</b>                                    | <b>386</b> |
| Pliki dzienników                                                           | 386        |
| Zarządzanie dziennikami                                                    | 387        |
| Dlaczego zadbanie o dzienniki jest ważne                                   | 388        |
| <b>Poznaj najlepszego przyjaciela swojego przeciwnika — Metasploit</b>     | <b>389</b> |
| Metasploit                                                                 | 390        |
| Wersje frameworka Metasploit                                               | 391        |
| Instalacja Armitage                                                        | 391        |
| Konfiguracja frameworka Metasploit po raz pierwszy                         | 392        |
| Instalacja Armitage (ciąg dalszy)                                          | 393        |
| Eksploracja Armitage                                                       | 394        |
| Rozpoczęcie ataku z Armitage                                               | 396        |
| Uruchamianie frameworka Metasploit                                         | 400        |

|                                                                                  |            |
|----------------------------------------------------------------------------------|------------|
| <b>Inne hakerskie narzędzia do przeprowadzania ataków</b>                        | <b>403</b> |
| Searchsploit                                                                     | 404        |
| sqlmap                                                                           | 405        |
| Weeveily                                                                         | 405        |
| <b>Podsumowanie</b>                                                              | <b>409</b> |
| <b>Lektura uzupełniająca</b>                                                     | <b>410</b> |
| <b>Rozdział 16. Informatyka śledcza w praktyce</b>                               | <b>411</b> |
| <b>Wprowadzenie do kryminalistyki cyfrowej</b>                                   | <b>412</b> |
| Techniki śledcze w odzyskiwaniu usuniętych lub brakujących danych                | 412        |
| <b>Metody i techniki kryminalistyki cyfrowej w zabezpieczaniu infrastruktury</b> | <b>416</b> |
| Kto powinien zajmować się cyfrową kryminalistyką?                                | 416        |
| Proces cyfrowej kryminalistyki                                                   | 417        |
| <b>Platformy kryminalistyczne</b>                                                | <b>418</b> |
| CAINE                                                                            | 418        |
| Stacja robocza SIFT                                                              | 419        |
| PALADIN                                                                          | 420        |
| <b>Znalezienie dowodów</b>                                                       | <b>421</b> |
| Źródła danych                                                                    | 421        |
| <b>Kryminalistyka urządzeń mobilnych</b>                                         | <b>422</b> |
| Dochodzenie bez urządzenia                                                       | 423        |
| Ważne źródła danych na urządzeniach mobilnych                                    | 425        |
| Transportowanie urządzeń mobilnych                                               | 426        |
| <b>Zarządzanie materiałem dowodowym (z perspektywy prawnej)</b>                  | <b>426</b> |
| ISO 27037                                                                        | 427        |
| Podręcznik polityki i procedur dotyczących dowodów cyfrowych                     | 427        |
| Przewodnik po polityce FBI dotyczącej dowodów cyfrowych                          | 427        |
| Regionalne Laboratorium Informatyki Śledczej                                     | 428        |
| Amerykańska Agencja Bezpieczeństwa Cybernetycznego i Infrastruktury              | 428        |
| RFC 3227 — wytyczne dotyczące gromadzenia i archiwizacji dowodów                 | 428        |
| <b>Podsumowanie</b>                                                              | <b>428</b> |
| <b>Lektura uzupełniająca</b>                                                     | <b>429</b> |
| <b>Rozdział 17. Automatyzacja zadań związanych z cyberbezpieczeństwem</b>        | <b>430</b> |
| <b>Po co zawracać sobie głowę automatyzacją?</b>                                 | <b>431</b> |
| Korzyści z automatyzacji                                                         | 431        |
| Ryzyko związane z ignorowaniem automatyzacji                                     | 431        |
| <b>Rodzaje automatycznych ataków</b>                                             | <b>432</b> |
| Gromadzenie kont                                                                 | 432        |
| Tworzenie kont                                                                   | 432        |
| Oszustwo reklamowe                                                               | 432        |
| Porażka CAPTCHA                                                                  | 433        |
| Rozszyfrowywanie kart                                                            | 433        |
| Carding                                                                          | 433        |
| Wypłata gotówki                                                                  | 433        |
| Łamanie danych uwierzytelniających                                               | 434        |
| Faszerowanie danymi uwierzytelniającymi                                          | 434        |
| Odmowa z magazynu                                                                | 434        |

|                                                                                    |            |
|------------------------------------------------------------------------------------|------------|
| DoS                                                                                | 434        |
| Przyspieszanie                                                                     | 435        |
| Zbieranie odcisków palców                                                          | 435        |
| Tropienie                                                                          | 435        |
| Scalping                                                                           | 436        |
| Strzał z ukrycia                                                                   | 436        |
| Zbieranie                                                                          | 436        |
| Wypaczanie                                                                         | 436        |
| Spamowanie                                                                         | 436        |
| Rozgryzanie tokenów                                                                | 437        |
| Skanowanie podatności                                                              | 437        |
| <b>Automatyzacja narzędzi cyberbezpieczeństwa z wykorzystaniem języka Python</b>   | <b>437</b> |
| Lokalne wyszukiwanie plików                                                        | 437        |
| Podstawowe zadania kryminalistyki cyfrowej                                         | 439        |
| Zbieranie danych ze stron internetowych                                            | 441        |
| Automatyzacja zabezpieczania sieci                                                 | 442        |
| <b>Automatyzacja zadań związanych z cyberbezpieczeństwem z Raspberry Pi</b>        | <b>443</b> |
| Automatyzacja systemu inteligentnego zbierania informacji                          |            |
| za pomocą przynęty Fail2ban na Raspberry Pi                                        | 444        |
| Zautomatyzowany system monitorowania internetu za pomocą Raspberry Pi              | 445        |
| <b>Podsumowanie</b>                                                                | <b>447</b> |
| <b>Lektura uzupełniająca</b>                                                       | <b>447</b> |
| <b>Rozdział 18. Kompilacja narzędzi eksperta. Przydatne zasoby</b>                 | <b>448</b> |
| <b>Darmowe szablony dotyczące cyberbezpieczeństwa</b>                              | <b>449</b> |
| Szablony planu ciągłości działania i planu odzyskiwania po awarii                  | 449        |
| Zarządzanie ryzykiem                                                               | 449        |
| Projektowanie i zarządzanie zasadami i procedurami dotyczącymi cyberbezpieczeństwa | 450        |
| <b>Niezbędne zasoby internetowe</b>                                                | <b>450</b> |
| Mapy zagrożeń cybernetycznych lub ataków cyfrowych                                 | 451        |
| Certyfikaty w dziedzinie cyberbezpieczeństwa                                       | 452        |
| Wiadomości i blogi dotyczące cyberbezpieczeństwa                                   | 453        |
| Narzędzia w cyberbezpieczeństwie                                                   | 453        |
| Narzędzia związane z hasłami                                                       | 454        |
| <b>Wiodące najlepsze praktyki branżowe</b>                                         | <b>454</b> |
| Przepisy i normy                                                                   | 454        |
| Ramy, standardy i inne elementy bezpieczeństwa cybernetycznego                     | 455        |
| <b>Podsumowanie</b>                                                                | <b>456</b> |
| <b>Lektura uzupełniająca</b>                                                       | <b>456</b> |
| <b>Skorowidz</b>                                                                   | <b>457</b> |