

Spis treści

Przedmowa 9

Notacja 21

O autorach 23

Rozdział 1. Przegląd 25

1.1. Koncepcje bezpieczeństwa komputerowego 26

1.2. Zagrożenia, ataki i aktywa 35

1.3. Funkcjonalne wymagania bezpieczeństwa 42

1.4. Podstawowe zasady projektowania bezpieczeństwa 44

1.5. Powierzchnie ataków i drzewa ataków 49

1.6. Strategia bezpieczeństwa komputerowego 53

1.7. Standardy 56

1.8. Podstawowe pojęcia, pytania sprawdzające i zadania 57

CZĘŚĆ I. TECHNIKI I ZASADY BEZPIECZEŃSTWA KOMPUTEROWEGO

Rozdział 2. Narzędzia kryptograficzne 61

2.1. Osiąganie poufności za pomocą szyfrowania symetrycznego 62

2.2. Uwierzytelnianie komunikatów i funkcje haszowania 69

2.3. Szyfrowanie z kluczem publicznym 79

2.4. Podpisy cyfrowe i zarządzanie kluczami 85

2.5. Liczby losowe i pseudolosowe 90

2.6. Zastosowanie praktyczne: szyfrowanie przechowywanych danych 93

2.7. Podstawowe pojęcia, pytania sprawdzające i zadania 95

Rozdział 3. Uwierzytelnianie użytkownika 101

3.1. Zasady cyfrowego uwierzytelniania użytkownika 103

3.2. Uwierzytelnianie oparte na hasłach 109

3.3. Uwierzytelnianie oparte na żetonach 124

3.4. Uwierzytelnianie biometryczne 129

3.5. Zdalne uwierzytelnianie użytkownika 135

3.6. Zagadnienia bezpieczeństwa uwierzytelniania użytkownika 140

3.7. Zastosowanie praktyczne: tęczówkowy system biometryczny 142

3.8. Przykład konkretny: problemy bezpieczeństwa w systemach bankomatowych 144

3.9. Podstawowe pojęcia, pytania sprawdzające i zadania 147

Rozdział 4. Kontrolowanie dostępu 151

4.1. Zasady kontrolowania dostępu 154

4.2. Podmioty, obiekty i prawa dostępu 156

4.3. Uznaniowe kontrolowanie dostępu 158

4.4. Przykład: kontrolowanie dostępu w uniksowym systemie plików 165

4.5. Kontrolowanie dostępu według ról 169

4.6. Kontrolowanie dostępu według atrybutów 176

4.7. Tożsamość, poświadczenia i zarządzanie dostępem 183

4.8. Ramy zaufania 187

4.9. Przykład konkretny: kontrolowanie ról w systemie bankowym 192

4.10. Podstawowe pojęcia, pytania sprawdzające i zadania 195

Rozdział 5. Bezpieczeństwo baz i centrów danych 201

- 5.1. Zapotrzebowanie na bezpieczeństwo baz danych 202
- 5.2. Systemy zarządzania bazami danych 204
- 5.3. Relacyjne bazy danych 206
- 5.4. Ataki wstrzykiwania w sql 210
- 5.5. Kontrolowanie dostępu do bazy danych 217
- 5.6. Wnioskowanie 223
- 5.7. Szyfrowanie baz danych 226
- 5.8. Bezpieczeństwo centrum danych 231
- 5.9. Podstawowe pojęcia, pytania sprawdzające i zadania 237

Rozdział 6. Malware - szkodliwe oprogramowanie 243

- 6.1. Rodzaje szkodliwego oprogramowania 245
- 6.2. Zaawansowane trwałe zagrożenie 249
- 6.3. Rozsiewanie - zainfekowana treść - wirusy 250
- 6.4. Rozsiewanie - wykorzystanie wrażliwych punktów - robaki 257
- 6.5. Rozsiewanie - socjotechnika - spam pocztowy, konie trojańskie 269
- 6.6. Ładunek - psucie systemu 272
- 6.7. Ładunek - agent ataku - zombie, boty 275
- 6.8. Ładunek - kradzież informacji - keylogery, phishing, spyware 277
- 6.9. Ładunek - działania ukradkowe - boczne drzwi, rootkity 280
- 6.10. Przeciwdziałania 285
- 6.11. Podstawowe pojęcia, pytania sprawdzające i zadania 293

Rozdział 7. Ataki polegające na odmowie świadczenia usług 297

- 7.1. Odmowa usług jako rodzaj ataku 298
- 7.2. Ataki zatapiające 307
- 7.3. Rozproszone ataki blokowania usług 310

- 7.4. Ataki na przepływność oparte na aplikacjach 312
- 7.5. Ataki odbijające i ataki ze wzmocnieniem 315
- 7.6. Obrona przed odmową świadczenia usług 321
- 7.7. Reagowanie na atak typu odmowa świadczenia usług 325
- 7.8. Podstawowe pojęcia, pytania sprawdzające i zadania 327

Rozdział 8. Wykrywanie włamań 331

- 8.1. Intruzi 332
- 8.2. Wykrywanie włamań 336
- 8.3. Podejścia analityczne 341
- 8.4. Wykrywanie włamań oparte na hoście 344
- 8.5. Wykrywanie włamań oparte na sieci 351
- 8.6. Rozproszone lub hybrydowe wykrywanie włamań 358
- 8.7. Format wymiany wykrywania włamań 361
- 8.8. Miodownice (honeypoty) 364
- 8.9. Przykład systemu: snort 367
- 8.10. Podstawowe pojęcia, pytania sprawdzające i zadania 371

Rozdział 9. Zapory sieciowe i systemy zapobiegania włamaniom 377

- 9.1. Zapotrzebowanie na zapory sieciowe 378
- 9.2. Charakterystyka zapór sieciowych i polityka dostępu 379
- 9.3. Rodzaje zapór sieciowych 381
- 9.4. Posadowienie zapór sieciowych 389
- 9.5. Umiejscowienie i konfiguracja zapór sieciowych 392
- 9.6. Systemy zapobiegania włamaniom 398
- 9.7. Przykład: ujednolicone środki opanowywania zagrożeń 404
- 9.8. Podstawowe pojęcia, pytania sprawdzające i zadania 409

CZĘŚĆ II. BEZPIECZEŃSTWO OPROGRAMOWANIA I SYSTEMÓW

Rozdział 10. Przepiętnienie bufora 415

- 10.1. Przepiętnienia stosu 417
- 10.2. Obrona przed przepiętnieniami bufora 442
- 10.3. Inne formy ataków przepiętniających 450
- 10.4. Podstawowe pojęcia, pytania sprawdzające i zadania 457

Rozdział 11. Bezpieczeństwo oprogramowania 461

- 11.1. Zagadnienia bezpieczeństwa oprogramowania 463
- 11.2. Obsługa wejścia programu 468
- 11.3. Pisanie bezpiecznego kodu 482
- 11.4. Współpraca z systemem operacyjnym i innymi programami 488
- 11.5. Obsługa wyjścia programu 504
- 11.6. Podstawowe pojęcia, pytania sprawdzające i zadania 507

Rozdział 12. Bezpieczeństwo systemów operacyjnych 511

- 12.1. Wprowadzenie do bezpieczeństwa systemów operacyjnych 514
- 12.2. Planowanie bezpieczeństwa systemu operacyjnego 514
- 12.3. Hartowanie systemów operacyjnych 515
- 12.4. Bezpieczeństwo aplikacji 521
- 12.5. Dbalność o bezpieczeństwo 522
- 12.6. Bezpieczeństwo w systemach Linux i UNIX 524
- 12.7. Bezpieczeństwo w systemie Windows 529
- 12.8. Bezpieczeństwo wirtualizacji 532
- 12.9. Podstawowe pojęcia, pytania sprawdzające i zadania 542

Rozdział 13. Bezpieczeństwo chmur i internetu rzeczy 545

13.1. Obliczenia w chmurze 546

13.2. Koncepcje bezpieczeństwa chmury 556

13.3. Podejścia do bezpieczeństwa chmury 561

13.4. Internet rzeczy (ir) 570

13.5. Bezpieczeństwo internetu rzeczy 576

13.6. Podstawowe pojęcia i pytania sprawdzające 587

Spis treści tomu 2. 589

Słowniczek 595

Akronimy 605

Literatura 607

Skorowidz 621