

Podziękowania (9)

Współpracownicy (10)

Przedmowa (13)

Rozdział 1. Metodologia włamań (15)

- Wprowadzenie (15)
 - Podstawowe terminy (16)
- Krótka historia hackingu (17)
 - Hacking sieci telefonicznych (17)
 - Hacking komputerowy (18)
- Co motywuje hakera? (20)
 - Hacking etyczny a hacking złośliwy (20)
 - Współpraca ze specjalistami ds. bezpieczeństwa (21)
- Współczesne rodzaje ataków (22)
 - DoS (DDoS) (22)
 - Hacking wirusowy (24)
 - Kradzież (29)
- Zagrożenia bezpieczeństwa aplikacji WWW (32)
 - Ukryta manipulacja (32)
 - Zamiana parametrów (33)
 - Zewnętrzne skrypty (33)
 - Przepelnienie buforów (33)
 - Zatrute cookies (34)
- Zapobieganie włamaniom poprzez przyjęcie postawy hakera (34)
- Podsumowanie (36)
- Skrót rozwiązań (37)
- Pytania i odpowiedzi (39)

Rozdział 2. Jak nie zostać "maszynką do kodu"? (41)

- Wprowadzenie (41)
- Kim jest "maszynka do kodu"? (42)
 - Postępując zgodnie z zasadami (45)
- Twórcze kodowanie (46)
 - Zastanawiać się (48)
- Bezpieczeństwo z punktu widzenia "maszynki do kodu" (50)
 - Programowanie w próżni (51)
- Tworzenie sprawnych i bezpiecznych aplikacji sieciowych (52)
 - Przecież mój kod działa! (56)
- Podsumowanie (61)
- Skrót rozwiązań (62)
- Pytania i odpowiedzi (63)

Rozdział 3. Ryzyko związane z kodem przenośnym (65)

- Wprowadzenie (65)
- Działanie ataków wykorzystujących kod przenośny (66)
 - Ataki z wykorzystaniem przeglądarek (66)
 - Ataki z wykorzystaniem programów pocztowych (67)
 - Złośliwe skrypty lub makra (68)

- Identyfikacja popularnych form kodu przenośnego (68)
 - o Języki makropoleczeń: Visual Basic for Applications (VBA) (69)
 - o JavaScript (74)
 - o VBScript (77)
 - o Aplety w Javie (79)
 - o Kontrolki ActiveX (82)
 - o Załączniki listów elektronicznych i pobrane pliki wykonywalne (86)
- Ochrona systemu przez atakami wykorzystującymi kod przenośny (89)
 - o Aplikacje bezpieczeństwa (90)
 - o Narzędzia na stronach WWW (93)
- Podsumowanie (93)
- Skrót rozwiązań (95)
- Pytania i odpowiedzi (95)

Rozdział 4. Wrażliwe skrypty CGI (97)

- Wprowadzenie (97)
- Czym jest i co robi skrypt CGI? (98)
 - o Typowe zastosowania skryptów CGI (99)
 - o Kiedy powinno się stosować CGI? (103)
 - o Zagrożenia związane z instalacją skryptów CGI (104)
- Włamania umożliwiające przez słabe skrypty CGI (105)
 - o Jak pisać bardziej szczelne skrypty CGI? (106)
 - o Polecenia katalogów (108)
 - o Opakowania skryptów CGI (109)
- Języki wykorzystywane do tworzenia skryptów CGI (112)
 - o Powłoka systemu Unix (113)
 - o Perl (113)
 - o C (C++) (114)
 - o Visual Basic (114)
- Korzyści ze stosowania skryptów CGI (115)
- Zasady tworzenia bezpiecznych skryptów CGI (115)
 - o Składowanie skryptów CGI (118)
- Podsumowanie (120)
- Skrót rozwiązań (120)
- Pytania i odpowiedzi (123)

Rozdział 5. Techniki i narzędzia włamań (125)

- Wprowadzenie (125)
- Cele hakera (126)
 - o Omijanie alarmów (127)
 - o Zdobywanie dostępu (128)
 - o Zniszczenia, zniszczenia, zniszczenia (130)
 - o Jak być lepszym od hakera (131)
- Pięć etapów włamania (132)
 - o Tworzenie planu ataku (132)
 - o Tworzenie planu przebiegu włamania (134)
 - o Wybranie punktu wejścia (135)
 - o Stały i szeroki dostęp (136)

- o Atak (137)
- Socjotechnika (138)
 - o Informacje poufne (138)
- Celowo pozostawione tylne wejścia (143)
 - o Wprowadzenie do kodu ukrytego hasła (143)
- Wykorzystanie słabych stron właściwych kodowi lub środowisku programowania (145)
- Narzędzia wykorzystywane przez hakera (145)
 - o Edytory szesnastkowe (145)
 - o Programy uruchomieniowe (147)
 - o Deasemblerzy (148)
- Podsumowanie (150)
- Skrót rozwiązań (150)
- Pytania i odpowiedzi (153)

Rozdział 6. Kontrola kodu i odwrotna analiza (155)

- Wprowadzenie (155)
- Jak efektywnie śledzić działanie programu (156)
- Monitorowanie i kontrola w wybranych językach programowania (158)
 - o Java (158)
 - o Java Server Pages (159)
 - o Active Server Pages (159)
 - o Server Side Includes (159)
 - o Python (159)
 - o Tool Command Language (160)
 - o Practical Extraction and Reporting Language (160)
 - o PHP: Hypertext Preprocessor (160)
 - o C (C++) (160)
 - o ColdFusion (161)
- Lokalizacja słabych punktów (161)
 - o Pobieranie danych od użytkownika (161)
 - o Lokalizacja potencjalnych błędów przepełnienia buforów (162)
 - o Weryfikacja wyświetlanych informacji (165)
 - o Kontrola operacji na systemie plików (168)
 - o Uruchamianie zewnętrznego kodu i programów (170)
 - o Zapytania do baz danych SQL (172)
 - o Sieci i strumienie komunikacyjne (174)
- Praktyka (175)
- Podsumowanie (176)
- Skrót rozwiązań (176)
- Pytania i odpowiedzi (177)

Rozdział 7. Bezpieczeństwo w języku Java (179)

- Wprowadzenie (179)
- Architektura bezpieczeństwa Javy (180)
 - o Model bezpieczeństwa w języku Java (181)
 - o Piaskownica (183)
- Podejście do problemów bezpieczeństwa w Javie (187)

- o Programy ładujące klasy (187)
 - o Weryfikator bajt-kodu (190)
 - o Chronione domeny Javy (194)
- Potencjalne luki bezpieczeństwa w Javie (201)
 - o Ataki DoS (degradacji usług) (202)
 - o Konie trojańskie (204)
- Programowanie funkcjonalnych, ale bezpiecznych apletów w Javie (205)
 - o Skróty wiadomości (206)
 - o Podpisy cyfrowe (208)
 - o Uwierzytelnianie (214)
 - o Ochrona zabezpieczeń za pomocą podpisywania plików JAR (220)
 - o Szyfrowanie (223)
 - o Zalecenia Sun Microsystems odnośnie bezpieczeństwa w Javie (227)
- Podsumowanie (230)
- Skrót rozwiązań (231)
- Pytania i odpowiedzi (232)

Rozdział 8. Bezpieczeństwo w języku XML (235)

- Wprowadzenie (235)
- Definicja języka XML (236)
 - o Struktura logiczna (237)
 - o Elementy (237)
 - o Dokumenty XML, XSL i DTD (240)
 - o Zastosowanie szablonów w języku XSL (240)
 - o Zastosowanie wzorów w języku XSL (241)
 - o DTD (243)
- Wykorzystanie języka XML do tworzenia aplikacji WWW (245)
- Ryzyko związane z językiem XML (247)
 - o Problemy tajności (248)
- Bezpieczeństwo w języku XML (249)
 - o Specyfikacja XML Encryption (250)
 - o Specyfikacja XML Digital Signatures (254)
- Podsumowanie (256)
- Skrót rozwiązań (257)
- Pytania i odpowiedzi (258)

Rozdział 9. Tworzenie bezpiecznych sieciowych kontrolerek ActiveX (259)

- Wprowadzenie (259)
- Zagrożenia związane z technologią ActiveX (260)
 - o Unikanie typowych luk bezpieczeństwa w kontrolkach ActiveX (262)
 - o Usuwanie skutków luk w technologii ActiveX (264)
- Metodologia tworzenia bezpiecznych kontrolerek ActiveX (267)
 - o Parametry bezpieczeństwa obiektu (267)
- Bezpieczne kontrolki ActiveX (268)
 - o Podpisywanie kontrolerek (268)
 - o Znakowanie kontrolerek (271)
- Podsumowanie (276)
- Skrót rozwiązań (276)

- Pytania i odpowiedzi (278)

Rozdział 10. Bezpieczeństwo w ColdFusion (281)

- Wprowadzenie (281)
- Jak działa ColdFusion? (282)
 - o Zalety szybkiego projektowania (283)
 - o Zarys znacznikowego języka ColdFusion (284)
- Zachowanie bezpieczeństwa w technologii ColdFusion (286)
 - o Projektowanie z uwzględnieniem bezpieczeństwa (288)
 - o Bezpieczne rozpowszechnianie (297)
- Przetwarzanie w aplikacjach ColdFusion (297)
 - o Sprawdzanie istnienia danych (298)
 - o Kontrola typów danych (299)
 - o Szacowanie danych (301)
- Ryzyko związane z technologią ColdFusion (302)
 - o Zastosowanie programów obsługi błędów (304)
- Stosowanie śledzenia sesji (308)
- Podsumowanie (309)
- Skrót rozwiązań (310)
- Pytania i odpowiedzi (311)

Rozdział 11. Projektowanie aplikacji spełniających wymogi bezpieczeństwa (313)

- Wprowadzenie (313)
- Zalety stosowania aplikacji spełniających wymogi bezpieczeństwa (314)
- Rodzaje zabezpieczeń stosowanych w aplikacjach (315)
 - o Podpisy elektroniczne (316)
 - o Pretty Good Privacy (317)
 - o Protokół S/MIME (319)
 - o Secure Sockets Layer (319)
 - o Certyfikaty cyfrowe (323)
- Podstawowe informacje na temat PKI (325)
 - o Usługi certyfikujące (327)
- Zastosowanie PKI do zabezpieczania aplikacji WWW (328)
- Implementacja PKI w infrastrukturze WWW (329)
 - o Microsoft Certificate Services (330)
 - o Netscape Certificate Server (333)
 - o PKI dla Serwera Apache (339)
 - o PKI i Secure Software Toolkits (341)
- Testowanie zabezpieczeń (341)
- Podsumowanie (343)
- Skrót rozwiązań (345)
- Pytania i odpowiedzi (347)

Rozdział 12. Od początku do końca - praca z planem bezpieczeństwa (349)

- Wprowadzenie (349)
- Analiza kodu (350)
 - o Sprawdzanie kodu (351)

- o Perspektywa współpracownika (352)
- Świadomość słabych punktów kodu (354)
 - o Testy, testy, testy (355)
- Rozsądek podczas kodowania (357)
 - o Planowanie (357)
 - o Standardy kodowania (358)
 - o Narzędzia (359)
- Tworzenie planu bezpieczeństwa (362)
 - o Planowanie bezpieczeństwa na poziomie sieci (364)
 - o Planowanie bezpieczeństwa na poziomie aplikacji (364)
 - o Planowanie bezpieczeństwa na poziomie biura (365)
 - o Proces bezpieczeństwa aplikacji WWW (365)
- Podsumowanie (367)
- Skróty rozwiązań (368)
- Pytania i odpowiedzi (369)

Dodatek A Skróty zagadnień omawianych w książce (371)
Skorowidz (389)