

Spis treści

O autorze (9)

Podziękowania (10)

Słowo wstępne (11)

Przedmowa (13)

Rozdział 1. Ogólne pojęcia dotyczące bezpieczeństwa (21)

Część 1. Podstawy zabezpieczeń (21)

Podstawowe zasady bezpieczeństwa (22)

Podstawy bezpieczeństwa haseł (25)

Część 2. Metody zabezpieczeń przed doświadczonymi napastnikami (31)

Najlepsze praktyki dotyczące zabezpieczeń (31)

Techniki łamania haseł (34)

Utrudnianie łamania haseł (38)

Część 3. Metody ochrony przed zaawansowanymi napastnikami (42)

Zaawansowane techniki łamania haseł (42)

Środki zaradcze przeciwko zaawansowanym technikom łamania haseł (44)

Podsumowanie (46)

Rozdział 2. Bezpieczeństwo stacji roboczych (47)

Część 1. Podstawy zabezpieczeń (48)

Podstawy bezpieczeństwa stacji roboczych (48)

Podstawy bezpieczeństwa sieci (50)

Wprowadzenie do dystrybucji Tails (52)

Pobieranie, weryfikowanie i instalowanie dystrybucji Tails (52)

Posługiwanie się dystrybucją Tails (54)

Część 2. Dodatkowe hartowanie stacji roboczej (56)

Szyfrowanie dysków stacji roboczych (56)

Hasła BIOS (57)

Utrwalanie i szyfrowanie w Tails (57)

Część 3. Qubes (61)

Wprowadzenie do Qubes (61)

Pobieranie Qubes i instalacja (66)

Pulpit Qubes (68)

Przykład kompartmentalizacji maszyn appVM (72)

Split GPG (75)

USB VM (76)

Podsumowanie (78)

Rozdział 3. Bezpieczeństwo serwerów (79)

Część 1. Podstawy bezpieczeństwa serwerów (79)

Podstawowe praktyki w zakresie zabezpieczania serwerów (79)

Konfiguracja SSH (81)

Sudo (82)

Część 2. Średnio zaawansowane techniki hartowania serwerów (85)

Uwierzytelnianie za pomocą klucza SSH (86)

AppArmor (90)

Zdalne logi (94)

Część 3. Zaawansowane techniki hartowania serwerów (96)

Szyfrowanie dysku serwera (97)

Bezpieczne alternatywy serwera NTP (99)

Uwierzytelnianie dwuskładnikowe za pomocą SSH (100)

Podsumowanie (103)

Rozdział 4. Sieć (105)

Część 1. Podstawowe hartowanie sieci (106)

Podstawy bezpieczeństwa sieci (106)

Ataki man-in-the-middle (108)

Ustawienia firewall serwera (110)

Część 2. Sieci szyfrowane (118)

Konfiguracja OpenVPN (118)

Tunele SSH (125)

Równoważenie obciążenia z wykorzystaniem protokołu SSL/TLS (127)

Część 3. Sieci anonimowe (132)

Konfiguracja sieci Tor (133)

Ukryte usługi Tor (138)

Podsumowanie (140)

Rozdział 5. Serwery WWW (141)

Część 1. Podstawy bezpieczeństwa serwerów WWW (141)

Uprawnienia (141)

Podstawowe uwierzytelnianie HTTP (142)

Część 2. HTTPS (145)

Włączanie HTTPS (146)

Przekierowanie HTTP na HTTPS (148)

Odwrócone proxy HTTPS (149)

Uwierzytelnianie klienta za pomocą protokołu HTTPS (150)

Część 3. Zaawansowana konfiguracja HTTPS (151)

HSTS (151)

Utajnienie przekazywania HTTPS (152)

Zapory WAF (154)

Podsumowanie (164)

Rozdział 6. E-mail (167)

Część 1. Podstawowe hartowanie serwerów e-mail (168)

Podstawy bezpieczeństwa poczty e-mail (168)

Podstawowe hartowanie serwerów e-mail (170)

Część 2. Uwierzytelnianie i szyfrowanie (172)

Uwierzytelnianie SMTP (173)

SMTPS (175)

Część 3. Hartowanie zaawansowane (176)

SPF (177)

DKIM (182)

DMARC (189)

Podsumowanie (193)

Rozdział 7. DNS (195)

Część 1. Podstawy bezpieczeństwa DNS (196)

Hartowanie autorytatywnych serwerów DNS (197)

Hartowanie rekursywnych serwerów DNS (199)

Część 2. Ataki DNS Amplification i mechanizm Rate Limiting (200)

Rejestrowanie zapytań DNS (201)

Dynamiczne uwierzytelnianie DNS (201)

Część 3. DNSSEC (205)

Jak działa DNS? (205)

Bezpieczeństwo DNS (206)

Jak działa DNSSEC? (207)

Terminologia DNSSEC (210)

Dodawanie obsługi DNSSEC dla strefy (212)

Podsumowanie (215)

Rozdział 8. Baza danych (217)

Część 1. Podstawy bezpieczeństwa baz danych (218)

Podstawowe zabezpieczenia bazy danych (218)

Lokalne administrowanie bazą danych (220)

Uprawnienia użytkowników baz danych (223)

Część 2. Wzmacnianie zabezpieczeń bazy danych (226)

Sieciowe mechanizmy kontroli dostępu do baz danych (227)

Włączanie SSL/TLS (230)

Część 3. Szyfrowanie bazy danych (233)

Szyfrowanie całego dysku (233)

Szyfrowanie po stronie aplikacji (234)

Szyfrowanie po stronie klienta (237)

Podsumowanie (237)

Rozdział 9. Reagowanie na incydenty (239)

Część 1. Podstawy reagowania na incydenty (239)

Kto zajmuje się reagowaniem na incydenty? (239)

Czy będziesz ścigać cyberprzestępcę? (240)

Wyciągnij wtyczkę (240)

Wykonaj obraz serwera (241)

Przywróć serwer do pracy (241)

Śledztwo (242)

Część 2. Bezpieczne techniki tworzenia obrazu dysku (243)

Wybór systemu do tworzenia obrazu (244)

Utworzenie obrazu (244)

Wprowadzenie w tematykę narzędzi Sleuth Kit i Autopsy (244)

Część 3. Przykładowe śledztwo (252)

Reagowanie na incydenty w chmurze (256)

Podsumowanie (258)

Dodatek A. Tor (259)

Czym jest Tor? (259)

Dlaczego warto korzystać z usługi Tor? (260)

Jak działa Tor? (260)

Zagrożenia dla bezpieczeństwa (262)

Przestarzałe oprogramowanie usługi Tor (263)

Wycieki tożsamości (263)

Dodatek B. SSL/TLS (265)

Czym jest TLS? (265)

Dlaczego warto korzystać z TLS? (266)

Jak działa TLS? (266)

Odszyfrowanie nazw szyfrów (268)

Polecenia przydatne do rozwiązywania problemów z TLS (268)

Przeglądanie zawartości certyfikatu (268)

Przeglądanie zawartości żądania CSR (269)

Rozwiązywanie problemów w komunikacji z TLS (269)

Zagrożenia dla bezpieczeństwa (269)

Ataki man-in-the-middle (269)

Ataki degradacji protokołu (270)

Utajnianie przekazywania (271)

Skorowidz (273)