

Wstęp (13)

Część I Podstawy (15)

Rozdział 1. Zagrożenia (17)

- Zagrożenia wewnętrzne a zagrożenia zewnętrzne (18)
 - o Zagrożenia wewnętrzne (18)
 - o Zagrożenia zewnętrzne (21)
- Środki bezpieczeństwa wewnętrznego i zewnętrznego (26)
 - o Środki bezpieczeństwa zewnętrznego (27)
 - o Środki bezpieczeństwa wewnętrznego (27)
- Typy ataków (28)
 - o Wandalizm w sieci WWW (29)
 - o Szpiegostwo i kradzież danych (30)
 - o Ataki typu Denial of Service (32)
- Podsumowanie (34)

Rozdział 2. Zabezpieczenia sieci i systemu - przegląd (35)

- Charakterystyka bezpiecznej sieci (36)
 - o Wielopoziomowa struktura zabezpieczeń (37)
 - o Punkty wejścia i wyjścia (43)
 - o Zabezpieczenia systemów komputerowych (45)
 - o Zabezpieczenia aplikacji (47)
- Metody naruszania ochrony danych (49)
 - o Przecieki informacji (50)
 - o Ataki na zasadzie pełnego przeglądu (51)
 - o Przepelnienie bufora (52)
 - o Podstawienie ciągu formatującego (54)
 - o Zmiana katalogu bieżącego (54)
 - o Fałszywy pośrednik (55)
 - o Socjotechnika (55)
- Root kity i konie trojańskie (57)
 - o Wykrywanie root kitów (57)
 - o Usuwanie szkodliwych programów (58)
- Podsumowanie (58)

Rozdział 3. Planowanie architektury zabezpieczeń (61)

- Projektowanie bezpiecznej architektury serwera (62)
 - o Minimalizacja (63)
 - o Wyłączanie zbędnych usług (64)
 - o Uaktualnianie systemu (66)
 - o Dokumentowanie nowej instalacji (69)
 - o Architektura sieci (69)
- Tworzenie planu czynności konserwacyjnych zabezpieczeń (71)
 - o Codzienne czynności administracyjne (71)
 - o Uaktualnienia zabezpieczeń (72)
- Kontrolowanie zmian (73)
- Plan awaryjny (75)
 - o Środki doraźne (75)

- o Gromadzenie dowodów (75)
 - o Przywracanie stanu systemu (77)
- Honeypot (garnek miodu) (77)
- Podsumowanie (78)

Rozdział 4. Inspekcja zabezpieczeń (79)

- Planowanie inspekcji komputerów (79)
- Inspekcja zabezpieczeń w systemie Windows (80)
 - o Ogólny przegląd zabezpieczeń (80)
 - o Przechwytywanie pakietów (sniffing) (82)
- Inspekcja zabezpieczeń w systemie UNIX (88)
 - o Ogólny przegląd zabezpieczeń (88)
 - o Skanowanie portów (95)
 - o Przechwytywanie pakietów w systemie UNIX (96)
- Podsumowanie (101)

Rozdział 5. Mechanizmy zabezpieczeń w systemie Windows Server 2003 (103)

- Architektura systemu Windows Server (103)
- Funkcje zabezpieczeń systemu Windows Server (105)
 - o Co nowego? (105)
 - o Starsze mechanizmy zabezpieczeń systemu Windows (107)
- Active Directory (112)
 - o Architektura Active Directory (113)
 - o Zabezpieczenia w Active Directory (114)
- Microsoft CryptoAPI (114)
- IPSec (115)
- Serwer ISA (116)
 - o Jaka jest rola usług serwera ISA? (116)
 - o Na czym polegają zabezpieczenia serwera ISA? (116)
- Podsumowanie (117)

Część II Zabezpieczenia systemu (119)

Rozdział 6. Zabezpieczanie systemu Windows Server 2003 (121)

- Zabezpieczenia sprzętowe (122)
- Zabezpieczanie systemu operacyjnego (125)
 - o Ograniczanie instalacji (126)
 - o Uprawnienia dostępu do plików (132)
 - o Inspekcja (137)
- Zasady grup (139)
 - o Tworzenie i usuwanie obiektów GPO (140)
 - o Modyfikowanie obiektów GPO (142)
 - o Zabezpieczenia obiektu GPO (144)
- Internet Connection Firewall (ICF) (146)
- Podsumowanie (151)

Rozdział 7. Zabezpieczanie aplikacji (153)

- Zabezpieczanie serwerów WWW i FTP (153)
 - o Zabezpieczanie serwerów WWW (154)
 - o Zabezpieczanie serwerów FTP (165)
- Zabezpieczanie serwerów pocztowych (166)
 - o Zabezpieczenia serwera (166)
 - o Zabezpieczanie przed spamem (167)
- Zabezpieczanie serwerów DNS (168)
- Zabezpieczanie innych aplikacji (169)
 - o Zabezpieczanie aplikacji różnego typu (170)
 - o Zabezpieczanie aplikacji wielowarstwowych (170)
- Podsumowanie (171)

Część III Uwierzytelnianie i szyfrowanie (173)

Rozdział 8. Szyfrowanie danych (175)

- Wprowadzenie do kryptografii (175)
 - o Szyfry z kluczem jednorazowym (177)
 - o Szyfry z kluczem symetrycznym (178)
 - o Szyfry z kluczem publicznym (178)
 - o Kryptografia kontrolowana (179)
 - o Kryptograficzny podpis (180)
 - o Steganografia (181)
- Encrypting File System (EFS) (181)
 - o Czym jest system EFS? (182)
 - o Korzystanie z szyfrowania EFS (182)
- Oprogramowanie kryptograficzne innych firm (196)
- Podsumowanie (202)

Rozdział 9. Zabezpieczanie stron WWW i poczty elektronicznej - protokoły SSL i TLS (203)

- SSL i TLS - wprowadzenie (205)
- Wydajność mechanizmów SSL (207)
- Protokół SSL a bezpieczna komunikacja HTTP (208)
- Szyfrowanie transmisji pocztowych (209)
- Słabe strony SSL (210)
- Protokół SSL w oprogramowaniu serwera Microsoft IIS (211)
- Szyfrowanie komunikacji SMTP w systemie Windows Server (217)
- Podsumowanie (219)

Rozdział 10. Uwierzytelnianie w systemie Windows Server 2003 (221)

- Proces uwierzytelniania (221)
- Uwierzytelnianie podstawowe (223)
- Kerberos (224)
- Uwierzytelnianie zewnętrzne (225)
 - o Metody biometryczne (226)
 - o Systemy żetonowe (226)
 - o Karty inteligentne (226)
 - o Uwierzytelnianie w systemie Windows przy użyciu kart inteligentnych (227)

- Podsumowanie (234)

Rozdział 11. System Kerberos (235)

- Wprowadzenie (236)
 - o Prostý system Kerberos (236)
 - o Rozproszony system Kerberos (236)
 - o Uwierzytelnianie Kerberos w układzie wieloobszarowym (237)
 - o Zaawansowane techniki obsługi biletów Kerberos (239)
- Projektowanie architektury Kerberos (241)
 - o Architektura (241)
 - o Znaczenie synchronizacji czasu (243)
- Kerberos a Windows Server 2003 (243)
 - o Konfigurowanie zasad grup (244)
 - o Współdziałanie z innymi środowiskami (245)
- Podsumowanie (249)

Rozdział 12. Infrastruktura klucza publicznego (PKI) (251)

- Więcej o PKI (253)
 - o Infrastruktura PKI w ujęciu teoretycznym (253)
 - o PKI w praktyce (254)
- Projektowanie infrastruktury PKI (256)
- Podsumowanie (258)

Rozdział 13. Instalowanie i konfigurowanie usług certyfikatów (259)

- Planowanie wdrożenia usług certyfikatów (259)
- Instalowanie usług certyfikatów (260)
- Konfigurowanie urzędu CA (265)
 - o Tworzenie szablonów certyfikatów (274)
 - o Uaktywnianie szablonów certyfikatów (280)
- Zgłaszanie żądań certyfikatów (281)
- Podsumowanie (289)

Rozdział 14. Wirtualne sieci prywatne L2TP i PPTP (291)

- Sieci VPN typu LAN-LAN (292)
 - o Wprowadzenie (292)
 - o Konfigurowanie połączenia VPN typu router-router opartego na protokole PPTP (293)
 - o Konfigurowanie połączenia VPN typu router-router opartego na protokole L2TP (303)
- Połączenia VPN zdalnego dostępu (315)
 - o Konfigurowanie połączenia VPN zdalnego dostępu opartego na protokole PPTP (316)
 - o Konfigurowanie połączenia VPN zdalnego dostępu opartego na protokole L2TP (320)
- Podsumowanie (324)

Rozdział 15. Zabezpieczenia IPSec (325)

- Czym jest protokół IPSec? (325)
- Konfigurowanie zabezpieczeń IPSec (326)
- Wyposażenie sprzętowe (343)
- Podsumowanie (344)

Część IV Microsoft Internet Security and Acceleration Server (345)

Rozdział 16. ISA Server - podstawy (347)

- Zapory firewall (348)
 - o Inspekcja stanowa i bezstanowa (350)
 - o Skalowalność zapory (351)
 - o Systemy wykrywania włamań (IDS) (352)
- Systemy buforowania treści (353)
 - o Buforowanie treści - oprogramowanie (355)
 - o Buforowanie treści - urządzenia (355)
 - o Skalowanie serwera buforującego (356)
 - o Metody i protokoły buforowania (356)
- Serwer ISA - przegląd (357)
 - o Integracja z systemem Windows Server (357)
 - o Wymagania (358)
 - o Zapora - przegląd funkcji (358)
 - o Usługa akceleracji - przegląd (363)
- Podsumowanie (368)

Rozdział 17. Instalowanie i konfigurowanie zapory firewall (369)

- Instalowanie serwera ISA (369)
 - o Instalowanie aktualizacji schematu Active Directory (369)
 - o Instalowanie serwera ISA (372)
- Konfigurowanie zapory firewall (378)
 - o Kreator konfiguracji (Getting Started Wizard) (378)
 - o Filtry (391)
 - o Reguły (399)
 - o Kontrola ruchu sieciowego (408)
 - o Filtry aplikacji (410)
- Podsumowanie (413)

Rozdział 18. Konfigurowanie usługi buforowania (415)

- Konfigurowanie buforowania (415)
 - o Zasady buforowania i rozmiar bufora (416)
 - o Buforowanie proste (424)
 - o Buforowanie odwrotne (428)
 - o Mostkowanie SSL (430)
- Analizowanie ruchu sieciowego i raporty (432)
 - o Mechanizmy raportowania i monitorowania serwera ISA (432)
 - o Liczniki wydajności buforowania (436)
 - o Rozwiązywanie problemów i optymalizowanie pracy bufora (437)

- Podsumowanie (438)

Dodatki (439)

Dodatek A Narzędzia administratora zabezpieczeń (441)

Dodatek B Źródła informacji o zabezpieczeniach (447)

Dodatek C Standardowe przypisania portów TCP/IP (451)

Skorowidz (515)