

Spis treści

Wstęp (7)

Rozdział 1. Podstawy bezpieczeństwa sieci (9)

- o Firma Cisco (9)
- o Certyfikacja i egzamin (10)
 - Tematyka i materiał CCNA Security (11)
- o Historia bezpieczeństwa sieci (13)
- o Bezpieczeństwo sieci i zarządzanie nim (15)
 - Organizacje związane z bezpieczeństwem (16)
 - Główne rodzaje niebezpieczeństw (21)
 - NFP - ochrona infrastruktury sieciowej (24)
- o Sprzęt potrzebny podczas nauki (28)

Rozdział 2. Lokalne zabezpieczenie urządzeń (31)

- o Zabezpieczanie urządzenia za pomocą lokalnej bazy i CLI (31)
 - Zabezpieczenie routera za pomocą lokalnej bazy haseł (32)
- o Informacje wstępne na temat Cisco Configuration Professional (CCP) (55)
 - Konfiguracja CCP Express na routerze uruchomionym w programie GNS (56)
 - Konfiguracja CCP na stacji roboczej i podłączenie do routera uruchomionego w programie GNS3 (70)
- o Model AAA (76)

Rozdział 3. Działanie i wykorzystanie RADIUS i TACACS+ (79)

- o RADIUS (79)
 - Instalacja RADIUS-a na serwerze Microsoft Server 2008R2 i uwierzytelnienie z routera R1 (80)
- o Podstawowe informacje o TACACS+ (93)
 - Cisco Secure Access Control System (94)
 - Opcja Security Audit w CCP (110)
- o Konfiguracja lokalnych trybów pracy (widoków) (118)

Rozdział 4. Sposoby zabezpieczania warstwy 2. modelu ISO OSI (121)

- o Informacje wstępne o warstwie 2. ISO OSI (121)
- o Urządzenia warstwy 2. - przełączniki (124)
- o Oprogramowanie do przeprowadzania ataków - Kali Linux (126)
- o Przeprowadzanie niektórych ataków i zabezpieczanie urządzeń (127)
 - DHCP snooping (128)
 - Tablica MAC i Port Security (134)
 - Podstawowe informacje o sieciach VLAN (148)
 - Połączenia TRUNK (153)
 - Atak VLAN hooping (157)

Rozdział 5. Listy ACL w sieci IPv4 (193)

- o Informacje wstępne (193)
- o Rodzaje list ACL (194)
- o Konfiguracja standardowych list ACL (195)
- o Konfiguracja rozszerzonych list ACL (207)

Rozdział 6. Listy ACL w sieci IPv6 (221)

- o Podstawowe informacje o IPv6 (221)
 - Konfiguracja interfejsu routera za pomocą adresu IPv6 (223)
 - Rodzaje adresów IPv6 (224)
- o Listy ACL w IPv6 (227)

Rozdział 7. Firewall i jego zastosowanie w oparciu o IOS (233)

- o Podstawy działania firewalla (233)
- o NAT w IPv4 (235)
- o Port Address Translation (PAT) (236)
- o Stateful Packet Inspection (SPI) (239)
- o Context Based Access Control (CBAC) (242)
 - Konfiguracja CBAC (243)
- o Zone Based Firewalls (ZBF) (244)
 - Edycja ZBF (251)
 - Statystyki działania ZBF (260)
 - Przykład ręcznej konfiguracji ZBF (264)

Rozdział 8. Firewall oparty na urządzeniu Cisco ASA (267)

- o Urządzenie Cisco ASA (267)
 - Funkcje urządzenia ASA 5505 (268)
- o Przygotowanie urządzenia do pracy za pomocą CLI (270)
 - Ręczna zmiana podstawowych ustawień na przykładzie urządzenia ASA 5505 (271)
 - Podłączenie urządzenia ASA do sieci zewnętrznej (internet) (277)
- o Konfiguracja urządzenia ASA przez ASDM (287)
 - Instalacja ASDM na lokalnym dysku (289)
 - Menu programu (290)
 - Przywracanie ustawień fabrycznych w ASDM (294)
 - Konfiguracja za pomocą kreatora (295)
 - Narzędzia do testowania komunikacji (301)
 - Zarządzanie hasłami i użytkownikami (304)
 - Konfiguracja interfejsów (307)
 - Ustawienia czasu (310)
 - Routing statyczny (310)
 - Konfiguracja serwera DHCP (311)
 - Konfiguracja PAT w ASDM (312)
 - Aktualizacja oprogramowania z poziomu ASDM (313)
 - Obiekty i grupy obiektów (315)
 - Listy ACL na urządzeniu ASA (318)
 - Konfiguracja dostępu do urządzenia ASA za pomocą serwera TACACS+ (323)

- Dostęp do urządzenia ASA za pomocą serwera TACACS+ ? konfiguracja w ASDM (325)
- Wykorzystanie grup w listach ACL (328)
- Monitorowanie urządzenia ASA z poziomu ASDM (330)
- Urządzenia ASA w GNS3 (331)

Rozdział 9. Systemy IPS (Intrusion Prevention System) (339)

- o Sposób działania systemów IPS (339)
- o Włączenie IPS na routerze z systemem IOS i konfiguracja przez CLI (345)
- o Przykładowy atak na sieć chronioną przez IPS i analiza wyników (353)
- o Ustawienie akcji dla sygnatury w CLI (358)
- o Dezaktywacja sygnatur IPS w CLI (361)
- o Włączenie IPS na routerze z systemem IOS i konfiguracja przez CCP (362)
 - Konfiguracja IPS przy użyciu kreatora (363)
 - Konfiguracja parametrów IPS (368)
 - Przykładowy atak SYN_flood (369)
 - Modyfikacja sygnatur w CCP (372)
 - Monitoring IPS (376)

Rozdział 10. Konfiguracja szyfrowania i sieci VPN (379)

- o Podstawy kryptografii i szyfrowania (379)
 - Zachowanie poufności - szyfrowanie (380)
 - Zachowanie integralności (383)
 - Uwierzytelnienie (386)
- o Sieci VPN (386)
- o Implementacja VPN site-to-site na routerze Cisco za pomocą CLI (389)
- o Implementacja VPN site-to-site na routerze Cisco za pomocą CCP (399)
 - Tunel GRE w site-to-site (408)
- o Implementacja VPN site-to-site na urządzeniu ASA 5505 za pomocą ASDM (416)
- o Implementacja VPN remote access na urządzeniu ASA 5505 za pomocą ASDM (422)
 - Opis działania SSL/TLS (423)
 - Konfiguracja dostępu przez przeglądarkę (425)
 - Konfiguracja dostępu przez klienta VPN (434)

Rozdział 11. Logowanie zdarzeń, raportowanie i zarządzanie bezpieczeństwem sieci za pomocą 802.1x (451)

- o Logowanie zdarzeń i raportowanie (451)
 - Obsługa logów systemowych syslog (452)
 - Wykorzystanie SNMP (456)
 - Network Time Protocol (NTP) (464)
 - Użycie uwierzytelniania 802.1x dla stacji roboczej (465)

Zakończenie (501)

Skorowidz (503)