

SPIS TREŚCI

1	WSTĘP	11
2	PODSTAWOWE DEFINICJE I ZAGROŻENIA	15
2.1.1	<i>Podstawowa klasyfikacja zagrożeń.....</i>	16
2.1.2	<i>Zagrożenia wg przyczyn</i>	16
2.1.3	<i>Zagrożenia wg miejsca powstawania</i>	17
2.1.4	<i>Zagrożenia wg czynników socjologicznych (tzw. oszustwa internetowe).....</i>	17
2.1.5	<i>Zagrożenia fizyczne</i>	17
2.1.6	<i>Zagrożenia wirusami, robakami oraz typowe ataki sieciowe.....</i>	18
2.2	ZAGROŻENIA ZWIĄZANE Z DZIAŁANIEM WIRUSÓW I ROBAKÓW	18
2.3	RODZAJE TYPOWYCH ATAKÓW SIECIOWYCH	19
2.3.1	<i>Ataki pasywne i aktywne.....</i>	19
2.3.1.1	<i>Pasywne.....</i>	19
2.3.1.2	<i>Aktywne.....</i>	19
2.3.2	<i>Pozostałe typy ataków</i>	20
2.3.2.1	<i>Ataki typu Rekonesans/Rozpoznanie (ang. Reconnaissance).....</i>	20
2.3.2.2	<i>Ataki typu skanowanie za pomocą ping (ang. ping sweep)</i>	20
2.3.2.3	<i>Ataki typu skanowanie portów (ang. port scanning)</i>	21
2.3.2.4	<i>Ataki dostępowe (ang. access attacks)</i>	21
2.3.2.5	<i>Ataki typu DoS (ang. Denial of Service)</i>	22
2.3.2.6	<i>Ataki typu DDoS (ang. Distributed Denial of Service)</i>	22
2.4	OGÓLNE ZASADY OBRONY SIECI PRZED ATAKAMI	24
2.5	POLITYKA BEZPIECZEŃSTWA WG CISCO SYSTEMS	25
2.6	TECHNIKI TESTOWANIA BEZPIECZEŃSTWA	25
2.6.1	<i>Bezpieczeństwo operacyjne.....</i>	25
2.6.2	<i>Testowanie i ocena bezpieczeństwa sieci.....</i>	26
2.6.3	<i>Typy testów sieciowych</i>	26
2.6.4	<i>Wykorzystanie wyników testu bezpieczeństwa sieci.....</i>	27
2.6.5	<i>Narzędzia do testowania sieci.....</i>	28
2.6.5.1	<i>Nmap</i>	28
2.6.5.2	<i>Zenmap.....</i>	29
2.6.5.3	<i>SIEM.....</i>	29
2.6.6	<i>Podsumowanie</i>	30
2.7	CYKL PROJEKTOWANIA BEZPIECZEŃSTWA SIECI	31
2.8	PROJEKTOWANIE ZASAD POLITYKI BEZPIECZEŃSTWA	32
2.8.1	<i>Odbiorcy polityki bezpieczeństwa</i>	33
2.8.2	<i>Polityka zabezpieczeń na poziomie kadry zarządzającej.....</i>	33
2.8.3	<i>Polityka zabezpieczeń na poziomie kadry technicznej.....</i>	34

Spis treści

2.8.4	<i>Polityka zabezpieczeń na poziomie użytkownika końcowego</i>	34
2.8.5	<i>Dokumenty dotyczące polityki zabezpieczeń</i>	35
2.8.6	<i>Dokumenty dotyczące procedur</i>	35
2.8.7	<i>Kadra zarządzająca polityką zabezpieczeń wg CISCO</i>	35
2.8.8	<i>Szkolenia uświadamiające zagrożenia</i>	36
2.8.9	<i>Szkolenia dotyczące bezpieczeństwa</i>	36
2.8.10	<i>Proces zbierania danych</i>	38
2.8.11	<i>RODO - Rozporządzenie o ochronie danych osobowych</i>	38
2.8.11.1	RODO – Zakres rozporządzenia	39
2.8.11.2	RODO – Obowiązki przedsiębiorstw (organizacji)	39
2.8.11.3	RODO – Procedura oceny oddziaływania na ochronę danych osobowych	40
2.8.11.4	RODO – Wpływ na procesy pozyskiwania danych od klientów	40
2.8.11.5	RODO – Zgoda na przetwarzanie danych	41
2.8.11.6	RODO – Obowiązek powiadamiania i kary	41
3	MINIMALNE ZABEZPIECZENIA DOSTĘPU DO ROUTERÓW	45
3.1	PODSTAWOWE ZABEZPIECZENIA ROUTERÓW CISCO	45
3.2	PODŁĄCZENIE KABLA KONSOLOWEGO	45
3.3	TWORZENIE BANERÓW OSTRZEGAJĄCYCH I INFORMUJĄCYCH	52
3.4	HASŁO DO PORTU KONSOLOWEGO	55
3.5	HASŁO DOSTĘPU DO TRYBU UPRIWILEJOWANEGO	61
3.6	WYŁĄCZENIE USŁUGI TELNET I SSH	65
4	ZABEZPIECZENIA ROUTERÓW CISCO	71
4.1	WŁĄCZENIE I KONFIGUROWANIE USŁUGI SSH	71
4.2	POZIOMY UPRAWNIENI DLA UŻYTKOWNIKÓW	74
4.3	MECHANIZM RBAC	75
4.4	KONFIGUROWANIE RBAC	84
4.4.1	<i>Definicje</i>	84
4.4.2	<i>Wymagania</i>	84
4.4.3	<i>Przykładowa konfiguracja krok po kroku</i>	85
4.5	ZABEZPIECZANIE OBRAZU SYSTEMU IOS I PLIKÓW KONFIGURACYJNYCH	91
4.5.1	<i>Archiwizowanie systemu IOS oraz konfiguracji za pomocą TFTP</i>	91
4.5.2	<i>Procedura przywracania IOS i konfiguracji z serwera TFTP</i>	95
4.6	PROTOKOŁY NTP, SYSLOG	99
4.6.1	<i>Wprowadzenie i definicje</i>	99
4.6.2	<i>Protokół NTP</i>	100
4.6.3	<i>Polecenia konfiguracyjne NTP i SYSLOG</i>	100
4.7	USŁUGI AAA ORAZ PROTOKOŁY RADIUS I TACACS+	108
4.7.1	<i>Wstęp do protokołów i zabezpieczeń</i>	108

4.7.2	Protokół RADIUS.....	108
4.7.3	Protokół TACACS+.....	109
4.7.4	Różnice pomiędzy protokołami RADIUS i TACACS+.....	109
4.7.5	Usługi AAA.....	110
4.7.6	Konfigurowanie lokalnego uwierzytelniania AAA.....	111
4.7.7	Konfigurowanie zdalnego uwierzytelniania AAA za pomocą serwerów.....	115
4.8	STANDARDOWE I ROZSZERZONE LISTY KONTROLI DOSTĘPU.....	121
4.8.1	Standardowe ACL.....	121
4.8.2	Rozszerzone ACL.....	122
4.8.3	Przyporządkowanie list ACL do interfejsu.....	122
4.8.4	Nazywane ACL.....	123
4.8.5	Rejestrowanie operacji na ACL (logi systemowe).....	124
4.9	KONFIGUROWANIE STANDARDOWYCH I ROZSZERZONYCH ACL.....	125
4.9.1	Przykład konfiguracji listy standardowej.....	125
4.9.2	Przykład konfiguracji listy rozszerzonej.....	126
4.9.3	Przetwarzanie listy ACL – algorytm dla ruchu wejściowego.....	127
4.9.4	Przetwarzanie listy ACL – algorytm dla ruchu wyjściowego.....	127
4.10	KONTEKSTOWA KONTROLA DOSTĘPU CBAC.....	129
4.10.1	Wstęp do kontekstowej kontroli dostępu.....	129
4.10.2	Polecenia monitorujące (inspekcyjne).....	129
4.10.3	Przykładowe konfigurowanie kontekstowej kontroli dostępu.....	130
5	ZABEZPIECZENIA W WARSTWIE 2.....	145
5.1	GŁÓWNE ZAGROŻENIA WYSTĘPUJĄCE W WARSTWIE 2.....	145
5.1.1	Przypomnienie zasady działania przełącznika warstwy 2.....	145
5.1.2	Atak typu MAC Address Table Overflow.....	146
5.1.3	Atak typu MAC Address Spoofing.....	146
5.1.4	Atak typu Storm.....	147
5.1.5	Atak STP Manipulation.....	148
5.2	KONFIGUROWANIE ZABEZPIECZEŃ W WARSTWIE 2.....	149
5.2.1	Konfiguracja VTP oraz sieci VLAN.....	149
5.2.2	Tryb PortFast oraz Storm Control na aktywnych portach.....	154
5.2.3	Zabezpieczanie portów przełącznika dostępowego.....	159
6	TUNELOWANIE.....	169
6.1	TUNELOWANIE OPARTE NA PROTOKOLE GRE.....	170
6.1.1	Protokół GRE.....	170
6.1.2	Konfigurowanie sieci Site-to-Site za pomocą GRE.....	170
6.2	TUNELOWANIE ZA POMOCĄ PROTOKOŁU IPSEC.....	175
6.2.1	Protokół IPsec.....	175

Spis treści

6.2.2	Konfigurowanie sieci VPN Site-to-Site za pomocą IPsec.....	175
7	ZAPORY SIECIOWE	187
7.1	PROSTA ZAPORA SIECIOWA NA SERWERZE I ROUTERZE	187
7.1.1	Konfiguracja zapory sieciowej na serwerze.....	187
7.1.2	Konfiguracja zapory sieciowej na routerze.....	198
7.2	ADAPTACYJNE URZĄDZENIE ZABEZPIECZAJĄCE ASA 5505.....	203
7.2.1	Ogólny opis urządzenia ASA 5505	203
7.2.2	Konfigurowanie ASA 5505.....	207
7.2.3	Filtrowanie ruchu ICMP.....	214
7.2.4	Filtrowanie ruchu WWW.....	218
7.2.5	Strefa DMZ oraz listy ACL filtrujące ruch.....	226
8	SYSTEMY IDS ORAZ IPS.....	239
8.1	OGÓLNA KLASYFIKACJA ORAZ CECHY SYSTEMÓW IDS/IPS	239
8.2	SYSTEMY OCHRONY PRZED WŁAMANIAMI IPS	239
8.2.1	Typy technologii systemów IPS.....	240
8.2.2	Zalety i wady Host-Based IPS	240
8.2.3	Zalety i wady Network-Based IPS.....	240
8.3	KONFIGURACJA IDS/IPS	241
8.3.1	Konfiguracja IDS w systemie IOS (monitorowanie)	242
8.3.2	Konfiguracja IPS w systemie IOS (blokowanie).....	251
9	ĆWICZENIA	257
9.1	ZABEZPIECZENIA ROUTERÓW CISCO	257
9.1.1	Ćwiczenie 9-1-1 (banery, hasła, timeout).....	257
9.1.2	Ćwiczenie 9-1-2 (konfigurowanie ssh).....	264
9.1.3	Ćwiczenie 9-1-3 (kontrola adresów MAC)	269
9.1.4	Ćwiczenie 9-1-4 (poziomy uprawnień oraz RBAC).....	275
9.1.5	Ćwiczenie 9-1-5 (przywracanie obrazu IOS)	285
9.1.6	Ćwiczenie 9-1-6 (konfigurowanie NTP i SYSLOG)	289
9.2	KONFIGUROWANIE UWIERZYTELNIANIA RADIUS, TACACS+	297
9.2.1	Ćwiczenie 9-2-1 (protokół RADIUS)	297
9.2.2	Ćwiczenie 9-2-2 (protokół TACACS+)	302
9.3	KONFIGUROWANIE STANDARDOWYCH LIST KONTROLI DOSTĘPU	306
9.3.1	Ćwiczenie 9-3-1 (standardowa ACL blokująca ruch do podsieci).....	306
9.3.2	Ćwiczenie 9-3-2 (standardowa ACL blokująca ruch z podsieci).....	309
9.3.3	Ćwiczenie 9-3-3 (standardowa ACL blokująca ruch telnetu).....	312
9.4	KONFIGUROWANIE ROZSZERZONYCH LIST KONTROLI DOSTĘPU	316
9.4.1	Ćwiczenie 9-4-1 (rozszerzona ACL blokująca usługę FTP).....	316

9.4.2	Ćwiczenie 9-4-2 (rozszerzona ACL blokująca usługę WWW).....	322
9.4.3	Ćwiczenie 9-4-3 (rozszerzona ACL blokująca usługę e-mail)	327
9.4.4	Ćwiczenie 9-4-4 (rozszerzona ACL blokująca protokół icmp).....	331
9.4.5	Ćwiczenie 9-4-5 (rozszerzona ACL blokująca protokół telnet).....	335
9.4.6	Ćwiczenie 9-4-6 (rozszerzona ACL blokująca protokół dns).....	338
9.4.7	Ćwiczenie 9-4-7 (rozszerzone nazywane ACL).....	342
9.5	KONFIGUROWANIE ZABEZPIECZEŃ W WARSTWIE 2	350
9.5.1	Ćwiczenie 9-5-1 (konfigurowanie VTP oraz routera na patyku).....	350
9.5.2	Ćwiczenie 9-5-2 (konfigurowanie trybu PortFast).....	357
9.5.3	Ćwiczenie 9-5-3 (konfigurowanie blokady portu przełącznika).....	362
9.5.4	Ćwiczenie 9-5-4 (konfigurowanie blokad portów przełącznika).....	367
9.6	KONFIGUROWANIE TUNELOWANIA	374
9.6.1	Ćwiczenie 9-6-1 (konfigurowanie tunelu z trasami statycznymi).....	374
9.6.2	Ćwiczenie 9-6-2 (konfigurowanie tunelu za pomocą protokołu GRE) ...	376
9.6.3	Ćwiczenie 9-6-3 (konfigurowanie tunelu za pomocą protokołu IPsec)..	382
9.6.4	Ćwiczenie 9-6-4 (sieć VPN IPsec Site-to-Site-zabezpieczenia routerów)	390
9.7	KONFIGUROWANIE URZĄDZENIA ZABEZPIEZAJĄCEGO ASA	401
9.7.1	Ćwiczenie 9-7-1 (konfiguracja podstawowa)	401
9.7.2	Ćwiczenie 9-7-2 (odblokowanie ruchu http).....	408