

Adam Józefiok

S E C U R I T Y
CCNA
210-260

ZOSTAŃ ADMINISTRATOREM SIECI KOMPUTEROWYCH CISCO

Nie pozwól, by sieć wymknęła Ci się z rąk!

- Uwierzytelnianie i hasła, czyli jak wstępnie zabezpieczyć sieć i urządzenia –
- Systemy IPS i szyfrowanie danych, czyli jak wytoczyć cięższe działa –
- Zapory ogniowe i listy ACL, czyli jak bezwzględnie walczyć z intruzami –



Helion 

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz Wydawnictwo HELION dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz Wydawnictwo HELION nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

Opieka redakcyjna: Ewelina Burska

Projekt okładki: ULABUKA

Materiały graficzne na okładce zostały wykorzystane za zgodą Shutterstock.

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: helion@helion.pl
WWW: <http://helion.pl> (księgarnia internetowa, katalog książek)

Drogi Czytelniku!

Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres

<http://helion.pl/user/opinie/seccna>

Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-283-1814-4

Copyright © Helion 2016

Printed in Poland.

- [Kup książkę](#)
- [Poleć książkę](#)
- [Oceń książkę](#)

- [Księgarnia internetowa](#)
- [Lubię to! » Nasza społeczność](#)

Spis treści

Wstęp	7
Rozdział 1. Podstawy bezpieczeństwa sieci	9
Firma Cisco	9
Certyfikacja i egzamin	10
Tematyka i materiał CCNA Security	11
Historia bezpieczeństwa sieci	13
Bezpieczeństwo sieci i zarządzanie nim	15
Organizacje związane z bezpieczeństwem	16
Główne rodzaje niebezpieczeństw	21
NFP — ochrona infrastruktury sieciowej	24
Sprzęt potrzebny podczas nauki	28
Rozdział 2. Lokalne zabezpieczenie urządzeń	31
Zabezpieczanie urządzenia za pomocą lokalnej bazy i CLI	31
Zabezpieczenie routera za pomocą lokalnej bazy haseł	32
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
Model AAA	76
Rozdział 3. Działanie i wykorzystanie RADIUS i TACACS+	79
RADIUS	79
Instalacja RADIUS-a na serwerze Microsoft Server 2008R2 i uwierzytelnienie z routera R1	80
Podstawowe informacje o TACACS+	93
Cisco Secure Access Control System	94
Opcja Security Audit w CCP	110
Konfiguracja lokalnych trybów pracy (widoków)	118
Rozdział 4. Sposoby zabezpieczania warstwy 2. modelu ISO OSI	121
Informacje wstępne o warstwie 2. ISO OSI	121
Urządzenia warstwy 2. — przełączniki	124
Oprogramowanie do przeprowadzania ataków — Kali Linux	126

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
Informacje wstępne	193
Rodzaje list ACL	194
Konfiguracja standardowych list ACL	195
Konfiguracja rozszerzonych list ACL	207
Rozdział 6. Listy ACL w sieci IPv6	221
Podstawowe informacje o IPv6	221
Konfiguracja interfejsu routera za pomocą adresu IPv6	223
Rodzaje adresów IPv6	224
Listy ACL w IPv6	227
Rozdział 7. Firewall i jego zastosowanie w oparciu o IOS	233
Podstawy działania firewalla	233
NAT w IPv4	235
Port Address Translation (PAT)	236
Stateful Packet Inspection (SPI)	239
Context Based Access Control (CBAC)	242
Konfiguracja CBAC	243
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
Urządzenie Cisco ASA	267
Funkcje urządzenia ASA 5505	268
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
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
Sposób działania systemów IPS	339
Włączenie IPS na routerze z systemem IOS i konfiguracja przez CLI	345
Przykładowy atak na sieć chronioną przez IPS i analiza wyników	353
Ustawienie akcji dla sygnatury w CLI	358
Dezaktywacja sygnatur IPS w CLI	361
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
Podstawy kryptografii i szyfrowania	379
Zachowanie poufności — szyfrowanie	380
Zachowanie integralności	383
Uwierzytelnienie	386
Sieci VPN	386
Implementacja VPN site-to-site na routerze Cisco za pomocą CLI	389
Implementacja VPN site-to-site na routerze Cisco za pomocą CCP	399
Tunel GRE w site-to-site	408
Implementacja VPN site-to-site na urządzeniu ASA 5505 za pomocą ASDM	416
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
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

Rozdział 1.

Podstawy bezpieczeństwa sieci

CCNA Security to kolejna ścieżka certyfikacji, jaką oferuje firma Cisco w ramach swojego programu nauki. Napisałem „kolejna ścieżka” celowo, gdyż nie zalecam zaczynania właśnie od niej swojej przygody z certyfikatami i nauką Cisco.

Zanim przejdziesz do ścieżki związanej z zabezpieczeniem sieci komputerowych, trzeba zapoznać się z podstawowym działaniem urządzeń sieciowych i nauczyć się ich podstawowej konfiguracji, a to gwarantuje ścieżka CCNA Routing and Switching. Tak więc, jak już wspomniałem, jeśli chcesz zajmować się bezpieczeństwem sieci, wpierw zapoznaj się z materiałem tej certyfikacji. Pomocą może być książka *CCNA 200-120. Zostań administratorem sieci komputerowych Cisco*, ponieważ dzięki niej poznasz materiał, którego nieznanomość byłaby dla Ciebie przeszkodą w opanowaniu zagadnień zawartych w niniejszej książce.

A jeśli już masz opanowaną treść zalecanej lektury lub mimo wszystko chcesz spróbować bez tego, zapraszam na pokład, witam Cię i zaczynamy przygodę z bezpieczeństwem sieci na poziomie CCNA.

Firma Cisco

Zanim przejdziemy do tematów związanych z bezpieczeństwem i przygotowaniem Cię do roli administratora i do zdania egzaminu, napiszę kilka słów o firmie, która jest autorem opisywanej tutaj ścieżki certyfikującej. Również na spręcie tej firmy będziemy wspólnie praktykować opisywane tematy.

Firma została założona w 1984 roku przez pracowników Uniwersytetu Stanforda. Nazwa „Cisco” pochodzi od nazwy jednego z amerykańskich miast, mianowicie San Francisco, a logo przedstawiające dziewięć pionowych linii symbolizuje znajdujący się tam most

Golden Gate. Obecnie szefem Cisco jest Chuck Robbins. Firma zajmuje się nie tylko produkcją routerów, lecz także ogromu innych urządzeń zapewniających i rozwijających dostęp do sieci internetowej, ale również mających nieco mniejsze możliwości.

Obecnie Cisco posiada w swojej ofercie między innymi routery, przełączniki, punkty dostępowe, serwery, sprzęt do telekonferencji oraz telefonii IP i przekazu wideo. Ponadto z roku na rok stara się wkraczać również w inne dziedziny sieciowego życia, takie jak wirtualizacja, serwerownie i urządzenia końcowe. Sztandarowym produktem Cisco, bez którego urządzenia byłyby bezużyteczne, są ich systemy operacyjne, które w zależności od modelu urządzenia i jego przeznaczenia mogą występować w różnych wersjach.

Ze względu na tak ogromną ofertę firma stara się od samego początku dbać o swoich przyszłych specjalistów i systematycznie wdraża swój program nauki do szkół średnich i uczelni wyższych.

Certyfikacja i egzamin

Certyfikacja w firmie Cisco składa się z kilku poziomów (CCENT, CCNA, CCNP, CCIE oraz CCAr). Zawsze punktem wyjściowym jest certyfikat CCNA (*Cisco Certified Network Associate*).

Wyróżniamy poziom początkujący, w którym możesz zdobyć między innymi certyfikat CCENT (*Cisco Certified Entry Networking Technician*) lub CCT (*Cisco Certified Technician*). Certyfikat CCENT otrzymasz po zdaniu egzaminu *ICND1 100-101*.

Certyfikaty początkowe nie uprawniają Cię do podążania dalej ścieżką certyfikacyjną. Tak jak wspomniałem wcześniej, umożliwi to dopiero uzyskanie certyfikatu CCNA.

Obecnie certyfikat CCNA możesz zdobyć w kilku dziedzinach. W tej książce skupiamy się na materiale z zakresu bezpieczeństwa. Jeśli chcesz zdobyć certyfikat z tej dziedziny, musisz opanować wiedzę z tego zakresu i zdać egzamin oznaczony jako *210-260 IINS Implementing Cisco Network Security* (IINS). Szczegółowe informacje dotyczące tego egzaminu znajdziesz na stronie www.cisco.com/certifications.

Jeśli chodzi o sam egzamin, to przygotować się do niego możesz na wiele sposobów. Pierwszym z nich jest wiedza teoretyczna. Niniejsza książka ma na celu gruntowne przedstawienie wszystkich pojawiających się na egzaminie tematów, tak aby ułatwić Ci optymalne przygotowanie się do niego. Nie znajdziesz tu jednak gotowych odpowiedzi do zadań egzaminacyjnych. Podobnie jak w każdym innym egzaminie Cisco, ważne jest posiadanie wiedzy praktycznej, która pomoże Ci lepiej zrozumieć wszystkie tematy teoretyczne. W tej książce staram się większy nacisk położyć na praktyczne podejście, ze względu na to, że administrator sieci raczej powinien cechować się wiedzą praktyczną. Niestety na egzaminie certyfikującym CCNA wiedza teoretyczna stanowi większość.

Jeśli chodzi o źródło wiedzy, to ta książka, uzupełniona o materiały z oficjalnej strony Cisco i połączona z praktyką, powinna wystarczyć. Niemniej jednak każdy z nas uczy się w inny sposób, poza tym jedni przyswajają wiedzę szybciej, inni wolniej, dlatego samodzielnie musisz zdecydować, czy nastał odpowiedni moment, by podejść do egzaminu.

Jeżeli podejmiesz decyzję, aby spróbować zdać egzamin certyfikujący, to po zakończonej nauce konieczna będzie wizyta na stronie www.pearsonvue.com. Jeśli jeszcze nie posiadasz tam konta, należy je założyć, a jeśli je posiadasz, to zapewne już wiesz, jak odszukać właściwy egzamin i go opłacić.

Egzamin *210-260 IINS Implementing Cisco Network Security* (IINS) kosztuje około 310 dolarów z VAT. Podobnie jak pozostałe certyfikaty Cisco, również certyfikat CCNA Security ważny jest przez trzy lata; wyjątek stanowią certyfikaty CCIE, których ważność wynosi dwa lata. Każdy kolejny zdany egzamin certyfikujący przedłuża ważność certyfikatów tego samego poziomu lub niższych.

Tematyka i materiał CCNA Security

CCNA Security to duża porcja materiału z zakresu podstaw bezpieczeństwa sieciowego. Z punktu widzenia egzaminu teoria jest istotna i stanowi fundament konieczny do zrozumienia praktyki. Tematy wchodzące w zakres CCNA Security to między innymi:

- ♦ ogólne informacje dotyczące bezpieczeństwa;
- ♦ opis najczęściej przeprowadzanych ataków;
- ♦ informacje dotyczące bezpieczeństwa urządzeń Cisco;
- ♦ konfiguracja ustawień bezpieczeństwa w Cisco Configuration Professional (CCP);
- ♦ podstawy NFP;
- ♦ konfiguracja zabezpieczeń w oparciu o IPv6;
- ♦ implementacja AAA;
- ♦ konfiguracja TACACS+ i RADIUS;
- ♦ listy ACL oparte na IPv4 i IPv6;
- ♦ filtrowanie ruchu;
- ♦ omówienie protokołów SSH, SNMP, NTP, SCP i SLL;
- ♦ bezpieczeństwo warstwy 2 ISO OSI;
- ♦ konfiguracja VLAN i implementacja Spanning Tree;
- ♦ technologie związane z pojęciem firewall;
- ♦ konfiguracja NAT;
- ♦ konfiguracja Zone Based Firewall;
- ♦ konfiguracja wstępna urządzeń Cisco ASA;

- ◆ rozwiązania IPS i ich konfiguracja w CCP;
- ◆ technologia VPN;
- ◆ szyfrowanie symetryczne i asymetryczne;
- ◆ certyfikaty i podpis cyfrowy;
- ◆ konfiguracja VPN w CCP i CLI;
- ◆ omówienie programu Cisco Any Connect i konfiguracja VPN.

Tak więc tematów, które będę się starał Ci przybliżyć w tej publikacji, jest wiele. Dzięki temu, mam nadzieję, rozpoczniesz swoją przygodę z bezpieczeństwem sieci, a dodatkowo przygotujesz się do egzaminu certyfikującego.

Rodzaj pytań egzaminacyjnych i opis egzaminu

Jeśli już masz za sobą egzamin certyfikujący, możesz pominąć ten podrozdział. Jeśli zaś CCNA Security będzie Twoim pierwszym egzaminem, możesz przeczytać poniżej o jego przebiegu.

Podczas egzaminu w przygotowanej przez Cisco aplikacji w prawym górnym rogu znajduje się zegar odliczający czas. Staraj się nie zatrzymywać zbyt długo na jednym zagadnieniu. Jeśli naprawdę nie znasz odpowiedzi na pytanie, nie zostawiaj pustego pola, lecz postaraj się odrzucić w pierwszej kolejności prawdopodobne błędne odpowiedzi. Jeżeli zostanie kilka Twoim zdaniem prawidłowych, a dalej nie będziesz wiedzieć, która jest właściwa, po prostu strzel.

Niestety na egzaminie nie można wracać do wcześniejszych pytań. Nie jest możliwe również przejście pytań, a następnie powrót do początku. Pamiętaj, że po kliknięciu przycisku *Next* przechodzisz do następnego pytania i nie ma możliwości powrotu. Na egzaminie lepiej poświęcić więcej czasu na pytania symulacyjne, które są wyżej punktowane niż pytania jednokrotnego wyboru, choć te również są ważne. Pamiętaj, że punkty liczone są przy użyciu średniej ważonej i określonych przez Cisco algorytmów. Nawet jeśli na niektóre pytania odpowiesz źle, jest szansa, że zdasz egzamin.

Przed rozpoczęciem jest około 15 minut na zapoznanie się z wprowadzeniem do egzaminu. Będzie to kilka przykładowych pytań i jedna symulacja, tak aby można było się zapoznać ze specyfiką testu. Jeśli uznasz, że nie potrzebujesz wstępu, możesz w każdej chwili go zakończyć i rozpocząć właściwy egzamin.

Oto rodzaj i zakres pytań, z jakimi się spotkasz:

- ◆ pytania wielokrotnego wyboru (ang. *multiple choice*);
- ◆ pytania z jedną poprawną odpowiedzią (ang. *single choice*);
- ◆ pytania typu „przeciągnij i upuść” (ang. *drag and drop*);
- ◆ wypełnianie luk (ang. *filling gaps*);
- ◆ symulacje (ang. *simulations*).

Pytania wielokrotnego wyboru charakteryzują się tym, że wśród zaproponowanych odpowiedzi musisz wybrać kilka prawidłowych. W nawiasie podana jest liczba poprawnych odpowiedzi; jeśli zaznaczysz mniej lub więcej, system poinformuje Cię o tym.

Pytania jednokrotnego wyboru zawierają tylko jedną poprawną odpowiedź i nie ma w nich możliwości zaznaczenia kilku odpowiedzi.

W pytaniach typu „przeciągnij i upuść” musisz przeciągnąć odpowiedzi w odpowiednie miejsca.

Wypełnianie luk to rodzaj pytania, w którym odpowiedź musisz wpisać w określone pole, na przykład: „W białe pole wpisz wynik dodawania 2 + 3”. Wtedy w wolnym polu wpisujesz prawidłową odpowiedź, w tym przypadku 5.

Z całego egzaminu najbardziej rozbudowanymi pytaniami są symulacje. Jest ich kilka rodzajów. W innych pytaniach będziesz mieć możliwość zalogowania się do routera i na podstawie dostępnych poleceń będziesz uzupełniać rysunek lub wykonywać czynności zabezpieczające.

Pytania oparte na symulacji nie są trudne, wymagają jednak szybkich odpowiedzi ze względu na czas i liczbę czynności do wykonania. Po kilku wykonanych w domu ćwiczeniach i scenariuszach (które możesz sobie dowolnie wymyślać) dojdiesz do takiej wprawy, że nie będziesz się zastanawiać nad wykonaniem ćwiczenia, tylko po prostu odpowiedzi same będą przychodziły. Praktyka czyni mistrza — to powiedzenie przecież znasz.

Po udzieleniu odpowiedzi na wszystkie pytania i kliknięciu przycisku *END* musisz odczekać około 30 sekund na podliczenie i wyświetlenie na ekranie monitora wyniku egzaminu. Będzie to najdłuższe 30 sekund w Twoim życiu. No i tylko dwie możliwości: *ZDANE* (ang. *PASSED*) albo *NIEZDANE* (ang. *FAILED*).

Historia bezpieczeństwa sieci

Bezpieczeństwo sieci komputerowych to bardzo złożony temat. Przede wszystkim jest to umiejętność. Umiejętność spoglądania w przyszłość i myślenia jak potencjalny włamywacz. Często żeby dobrze zabezpieczyć stację roboczą, warto samemu spróbować się do niej włamać. Pomyśleć, co się stanie, jeśli ktoś ją teraz ukradnie, czy dane są bezpieczne, jak je zabezpieczyć.

Obecnie bezpieczeństwo sieci komputerowych stanowi jeden z najważniejszych problemów i wyzwań, przed jakimi stoi administrator.

Kiedyś bezpieczeństwo danych wyglądało zupełnie inaczej i opierało się na zapewnieniu bezpieczeństwa głównie fizycznego. Większość danych znajdowała się bowiem na papierze i chowana była w szafie. Obecnie odwróciło się to o 180 stopni.

Mamy do czynienia z coraz większą cyfryzacją różnego rodzaju danych. Stają się więc one podatne na przechwycenie lub skasowanie. Zapewne za kilkanaście lat wykasowanie czyjejs tożsamości z systemu stanie się bardziej realne. Czyli to, co teraz możemy oglądać jedynie w filmach science fiction, zamieni się w rzeczywistość.

Praktycznie od momentu powstania komputerów mamy do czynienia również z wirusami komputerowymi, czyli realnym niebezpieczeństwem dla danych na nich umieszczonych. W latach siedemdziesiątych ubiegłego wieku powstały bowiem pierwsze programy, które potrafiły samodzielnie się kopiować. Nie były to jeszcze wirusy, ale ich zapowiedź. Kilka lat później na komputerach Apple'a pojawił się wirus o nazwie Elk Cloner, powodujący wyświetlenie komunikatu. Późniejsze lata to pierwszy wirus, którego celem były komputery IBM: Brain infekował dyskietki i również wyświetlał komunikat. Potem było już tylko gorzej...

Pierwszy wirus został nazwany Melissa i powstał w 1999 roku. Napisał go programista ze Stanów Zjednoczonych David Smith. Wirus został rozpropagowany jako załącznik do wiadomości e-mail i powodował przepelnianie pamięci serwerów pocztowych. Działał na tej zasadzie, że wybierał 50 pierwszych odbiorców z książki adresowej programu Outlook i rozsyłał się dalej, powodując przeciążenia systemów pocztowych.

Warto również wspomnieć o wirusie ILOVEYOU, który zainfekował kilkaset tysięcy komputerów, a szacowane straty to kilkanaście milionów dolarów. Istotą jego działania było replikowanie się do wszystkich użytkowników książki adresowej i rozsyłanie się dalej. Nazwa wirusa widniała w temacie każdej przesyłanej wiadomości. Wirusem, który również zapisał się niechlubnie w historii, był MyDoom, działający podobnie jak ILOVEYOU. Umieszczony w załączniku wiadomości, powodował swoje dalsze rozsyłanie i w konsekwencji spowalnianie działania internetu.

Oczywiście w miarę upływu czasu i pojawiania się nowych technologii, takich jak Java, ActiveX czy SQL, powstawało coraz więcej wirusów, robaków i koni trojańskich. Powstawały również firmy zajmujące się ochroną przed złośliwym oprogramowaniem.

Wirusy to jednak nie jedyny temat związany z bezpieczeństwem sieci. W miarę rozwoju sieci komputerowych i sieci internet możliwości ataków się poszerzały. Sieci komputerowe zaczęły się łączyć, a to umożliwiło rozpoczęcie zdalnych ataków. Nastąpiła więc nowa era i pojawiły się nowe możliwości — włamań do sieci komputerowych.

Włamania te miały różne konsekwencje, a najpoważniejsze w skutkach były między innymi ataki z 2005 roku na instytucje obsługujące płatności elektroniczne. Hakerzy włamali się wtedy do baz danych za pomocą kodu SQL i wyciekły dane kilku milionów użytkowników kart kredytowych. Natomiast w 2009 roku miał miejsce atak chińskich hakerów polegający na włamaniach do firm takich jak Google, Yahoo i Microsoft w 2009 roku w celu dokonania kradzieży danych osobowych.

Wielki problem stanowił również brak mechanizmów obrony sieci firmowej od wewnątrz i ochrona danych przed nieuczciwymi pracownikami. W dziedzinie ochrony danych wewnątrz firmy znaczący wpływ miało wprowadzenie systemu zwanego Intrusion Detection System (IDS), który umożliwiał wykrywanie określonych rodzajów ruchu, które zostały zdefiniowane we wzorcach.

Zatem w pierwszej kolejności należało opracować sygnatury ruchu, który jest uważany za poprawny. Podczas działania systemu IDS można wyróżnić trzy główne komponenty: sensory, moduł zarządzający i konsola.

Sensor to rodzaj aplikacji monitorującej ruch i występującej w różnych częściach sieci. Każdy sensor przysyła swoje dane do modułu zarządzającego, który ma zainstalowane sygnatury określonego (poprawnego) działania. Sensory odpowiedzialne są więc za monitorowanie ruchu i sprawdzane go z istniejącymi sygnaturami. Jeśli rodzaj przesyłanego ruchu nie pasuje do sygnatur, wówczas włącza się alarm.

Trzeba pamiętać, że działanie systemów IDS było oparte głównie na analizie zdarzeń *post factum*, co oznacza, że nie blokowały one ruchu przed atakiem, ale podnosiły alarm po ataku.

Trzeci komponent systemów IDS, czyli konsola, służy do konfiguracji sensorów.

To właśnie ograniczenie spowodowane brakiem ochrony w czasie rzeczywistym było powodem opracowania rozbudowanej wersji systemu ochrony sieci. Mowa tutaj o In-trusion Prevention System (IPS). Jest to system wykrywania i blokowania zagrożeń. Do IPS jeszcze wrócimy w dalszej części książki.

Pamiętaj na tym etapie o tym, że jeśli sieć ma być w stu procentach bezpieczna, to trzeba ją po prostu wyłączyć. Może wydawać Ci się to dziwne, ale tak naprawdę wszelkie zabiegi mające na celu zabezpieczenie sieci nigdy nie będą w stu procentach skuteczne. Zawsze istnieje bowiem ryzyko, że o czymś zapomnieliś lub ktoś użył nowej techniki do włamania. Wszystkie czynności opisane w tej książce obniżają jedynie ryzyko włamania, nigdy jednak nie są w stanie zupełnie go wyeliminować.

Bezpieczeństwo sieci i zarządzanie nim

Zarządzanie bezpieczeństwem to wiele czynności i celów. Przede wszystkim należy zapewnić poufność przesyłanych danych (ang. *confidentiality*). Zapewnienie poufności przesyłanych danych to podjęcie takich kroków, które uniemożliwią innym osobom uzyskanie dostępu do tych danych i poznanie ich zawartości. Typowym przykładem jest zastosowanie szyfrowania.

Kolejnym celem jest zachowanie integralności danych (ang. *integrity*). Jest to pewność, że dane od miejsca wysłania do miejsca docelowego nie zostaną przez kogoś zmienione. Wyobraź sobie sytuację, w której piszesz do kogoś wiadomość i nagle się okazuje, że odbiorca otrzymuje sfabrykowanego maila. Oczywiście skutki mogłyby być opłakane.

Trzecim ważnym celem jest dostępność (ang. *availability*), nie mniej ważna niż integralność i poufność. Bo co to za sieć, jeśli nie można z niej skorzystać? Co to za administrator, jeśli na to pozwala? Sieć musi być dostępna i nieważne, czy jest atakowana, czy nie, musi działać.

Oczywiście powyższe cele to jedynie wstęp do dość rozbudowanej teorii bezpieczeństwa sieci. Twoim wrogiem w ich realizacji będą wszelkiego rodzaju zagrożenia i niebezpieczeństwa, które również można dla ułatwienia zrozumienia ich działania podzielić.

I tak zagrożenia sieci można podzielić na *external threat*, czyli spoza sieci, i *internal threat*, czyli zagrożenia pochodzące z sieci wewnętrznej.

Trzeba przyznać, że zagrożenia z sieci są znacznie bardziej niebezpieczne. W tym przypadku potencjalny włamywacz lub złodziej jest już bowiem w Twojej sieci i ma do niej dostęp. Natomiast osoby próbujące przełamać zabezpieczenia sieci określa się mianem hakerów.

Oczywiście tak jak złodziei można podzielić na takich, którzy kradną jabłka od przepkupi na targu, i na takich, którzy napadają na banki, tak i wśród hakerów są tacy, którzy tylko amatorsko korzystają z gotowych programów, nie zacierając za sobą śladów, i jedynie próbują używać ogólnodostępnych technologii, i tacy specjaliści, którzy znają systemy komputerowe bardzo dogłębnie i wykorzystują różnego rodzaju znalezione w nich luki, aby przejąć nad nimi kontrolę. Sam sposób włamania zależy jednak od wielu czynników. Może to być podejrzenie hasła dostępu przez ramię, a może to być bardzo skomplikowany atak programistyczny.

Warto w tym miejscu wspomnieć, że tak szeroki temat, jakim jest bezpieczeństwo sieci, wymaga rozległej wiedzy i sporych umiejętności. Ta rozbudowana tematyka coraz częściej powoduje wyodrębnianie specjalizacji w zakresie bezpieczeństwa sieciowego. To właśnie dzięki temu możesz zaobserwować na rynku pracy oferty przeznaczone dla takich specjalistów jak network security engineer (inżynier bezpieczeństwa sieci), information security analyst (analityk systemów bezpieczeństwa), network security specialist (specjalista bezpieczeństwa sieci), network security administrator (administrator bezpieczeństwa sieci) czy network security architect (architekt bezpieczeństwa sieci).

Wszystkie te specjalizacje nastawione są na tematykę związaną z bezpieczeństwem sieci, a wyodrębnienie specjalizacji powoduje, że specjalista powinien znać się na wszystkich, ale specjalizować się w jednej konkretnej. Dzięki temu przy ogromie informacji i zachodzących w błyskawicznym tempie zmianach będzie mógł skupić się na swojej tematyce i być na bieżąco ze wszystkimi trendami.

Organizacje związane z bezpieczeństwem

Wiedzę z zakresu bezpieczeństwa sieci możesz czerpać z książek takich jak ta lub zainteresować się różnego rodzaju materiałami publikowanymi na stronach organizacji na co dzień zajmujących się bezpieczeństwem teleinformatycznym.

Jedną z organizacji zajmujących się bezpieczeństwem sieci jest SANS. Zajmuje się ona organizowaniem badań i prowadzeniem szeroko pojętej edukacji obecnych i przyszłych specjalistów w dziedzinie bezpieczeństwa informatycznego. Organizacja nie skupia się jedynie na bezpieczeństwie sieci, ale na znacznie szerszym pojęciu, jakim jest bezpieczeństwo informatyczne.

SANS powstał w 1989 roku i wyszkolił setki audytorów i specjalistów w zakresie bezpieczeństwa. Organizacja oferuje program studiów, egzaminy certyfikujące i różnego rodzaju kursy. Prowadzi również badania nad bezpieczeństwem informacji i publikuje rozmaite artykuły związane z bezpieczeństwem. Strona organizacji znajduje się pod adresem www.sans.org.

Najbardziej znaną organizacją tego typu jest powołany w 1988 roku CERT (*Computer Emergency Response Team*). Głównym celem jego powstania było stałe nadzorowanie ruchu internetowego i przeciwdziałanie różnego rodzaju zmasowanym atakom w razie ich wystąpienia. Organizacja ta zajmuje się opracowywaniem metod i technologii zapobiegających zagrożeniom cybernetycznym, przeprowadza wiele badań w zakresie bezpieczeństwa sieci internetowej, rejestruje i obsługuje zdarzenia bezpieczeństwa sieci oraz nieustannie rozwija narzędzia do wykrywania i analizy zagrożeń. Strona organizacji znajduje się pod adresem www.cert.org.

Ogromny wkład w bezpieczeństwo sieci ma także ISO (*International Organization for Standardization*), czyli Międzynarodowa Organizacja Normalizacyjna, która powstała w 1946 roku w Londynie. Organizacja ta 17 września 2007 roku opublikowała normę ISO/IEC27002, w której znalazło się kilka dziedzin związanych z zapewnieniem bezpieczeństwa teleinformatycznego sieci komputerowych. Więcej na temat tej normy możesz przeczytać na stronie <http://www.iso27001security.com/html/27002.html>. W niniejszej książce chciałbym się skupić jedynie na dwóch dziedzinach z tej normy, moim zdaniem najważniejszych, a mianowicie na zarządzaniu ryzykiem (ang. *risk assessment*) i polityce bezpieczeństwa (ang. *security policy*).

Zarządzanie ryzykiem i analiza ryzyka

Jeśli chodzi o aspekt teoretyczny zagadnień związanych z zarządzaniem ryzykiem czy analizą ryzyka, istnieje wiele opracowań, które zawierają ogrom teoretycznych opisów i schematów. Chciałbym je pominąć i skupić się na praktycznym podejściu do tego tematu. Zaczniemy od tego, że ryzyko występuje zawsze i wszędzie — to tak jak strach.

Strach towarzyszy nam w ciągu całego naszego życia. Jest to naturalne, a nawet dobre. Nienaturalne jest natomiast uleganie mu lub pozwolenie na to, aby nas paraliżował. Oczywiście strachu nie można lekceważyć, ponieważ jest strach, który chroni nasze życie.

Podobnie jest z ryzykiem. Podłączając urządzenie do sieci publicznej, musisz liczyć się z tym, że Twoje dane trafią w niepowołane ręce i zostaną skradzione lub zniszczone. Można stąd wyciągnąć wniosek, że skoro podłączenie komputera do sieci niesie ze sobą ryzyko utraty danych, to nie należy go podłączać. Słusznie, zawsze możesz tak zrobić, ale taki sposób myślenia spowodowałby, że internet przestałby istnieć. Tak więc podłączasz komputer do sieci, bo chcesz z niej korzystać. Wiesz o ryzyku związanym z tym działaniem, świadomie jednak na nie się decydujesz.

Co jeszcze robisz? Minimalizujesz ryzyko, zabezpieczając komputer programem antywirusowym, firewallem oraz innym oprogramowaniem, które ma zabezpieczyć Twoją sieć. Sam zatem narażasz się na niebezpieczeństwo, a potem tylko minimalizujesz ryzyko. W tych kilku liniach tekstu zawarta jest teoria tego, co nazywamy analizą ryzyka i zarządzaniem ryzykiem.

Skorowidz

A

AAA, authentication, authorization, accounting, 76

ACL, Access Control List, 193

- konfiguracja list rozszerzonych, 207

- konfiguracja list standardowych, 195

- przypisanie do interfejsu, 203

- przypisywanie do linii wirtualnych, 206

- wstawianie komentarzy, 199

- wykorzystanie grup, 328

ACS, Access Control System, 94

- Common Tasks, 102

- dodawanie urządzeń, 99

- instalacja, 94, 95

- konfiguracja, 96

- tworzenie użytkownika, 100

- uwierzytelnienie TACACS+, 99

ActiveX, 447

adres

- global, 224

- IPv4, 128

- IPv6, 223

- link-local, 224

- loopback, 224

- MAC, 124

- MAC multicast, 123

- multicast, 224

- unspecified, 224

agenty SNMP, 457

AIM, Advanced Integration Modules, 387

akcja dla sygnatury, 358, 374

alarmy, 357

- falszywe, 343

- prawdziwe, 344

algorytm

- AES, 391

- drzewa rozpinającego, 164

alias, 38

analiza

- ruchu, 342

- anomaly-based, 343

- honeypot detection, 343

- policy-based, 343

- signature-based, 343

- ryzyka, 17

aplet Użytkownicy, 483

ARP, Address Resolution Protocol, 123

ARP spoofing, 178

ASA, Adaptive Security Appliance, 267

- aktualizacja oprogramowania, 313

- dostęp do urządzenia, 323, 325

- funkcje, 268

- grupy obiektów, 315

- implementacja VPN remote access, 422

- implementacja VPN site-to-site, 416

- konfiguracja dostępu, 323

- konfiguracja przez CLI, 270

- konfiguracja urządzenia, 287

- konsola, 336

- listy ACL, 318

- monitorowanie urządzenia, 330

- obiekty, 315

- podłączenie do sieci, 277

- projekt sieci, 335

- reset hasła, 286

- reset ustawień, 286

- serwer DHCP, 280

- wgranie oprogramowania, 284, 285

- zaawansowane ustawienia, 334

- zmiana ustawień, 271

ASDM, 287

- aktualizacja oprogramowania ASA, 313

- implementacja VPN remote access, 422

- implementacja VPN site-to-site, 416

- instalacja, 289

ASDM

- konfiguracja interfejsów, 307
- konfiguracja PAT, 312
- konfigurowanie reguł ACL, 320
- kreator konfiguracji, 295
- logowanie, 325
- menu Configuration, 292
- menu górne, 293
- menu programu, 290
- monitorowanie urządzenia ASA, 330
- ustawienia czasu, 310
- ustawienia fabryczne, 294
- zarządzanie hasłami, 304
- zarządzanie użytkownikami, 304

atak

- ARP spoofing, 178
- Buffer overflow attack, 23
- Claiming Root Role, 176
- DTP, 158
- man-in-the-middle, 23, 385
- na root bridge, 175
- na sieć chronioną przez IPS, 353
- na STP, 174
- Passwords attack, 22
- Smurf attack, 23
- SYN_flood, 369
- Trust exploitation attack, 23
- typu rekonesans, 22
- VLAN hooping, 157

audyt bezpieczeństwa urządzenia, 113

authenticator, 81

autokonfiguracja zabezpieczeń, 26

automatyczna konfiguracja sieci przewodowej, 496

autoryzacja, authorization, 76, 108

B

baner informujący, 44

banner motd, 36

bezpieczeństwo sieci, 9, 13, 15

blokowanie, blocking, 172

BPDU, Bridge Protocol Data Units, 164

BPDU guard, 176

broadcast storm, 163

burza ogłoszeniowa, 163

C

C3PL, 263

CBAC, Context Based Access Control, 242

CCNA Security, 11

CCP, Cisco Configuration Professional, 29, 55

- funkcja one-step lockdown, 116

- funkcja perform security audit, 113

implementacja VPN site-to-site, 399

instalacja, 71

konfiguracja firewalla, 246, 251

konfiguracja IPS, 362

konfiguracja syslog, 455, 456

konfiguracja zabezpieczeń, 74

modyfikacja sygnatur, 372

monitorowanie urządzenia, 74

okno główne, 71, 73

opcja Security Audit, 110

pierwsze uruchomienie, 71

standardowe listy, 199

CCP Express, 56, 68

cele ataku, 182

certyfikacja, 10

certyfikat, 424

- serwera, 437

character mode, 76

Cisco

- AnyConnect, 445

- ASA, 267

- ASA 5505, 268

- ASDM, 287

- Secure ACS, 94

- Switched Port Analyzer, 187

class map, 26, 27

CLI, 31, 270

- dezaktywacja sygnatur, 361

- implementacja VPN site-to-site, 389

- konfiguracja IPS, 345

- konfiguracja SNMPv3, 458

- konfiguracja urządzenia ASA, 270

- ustawienie akcji, 358

CoPP, Control Plane Policing, 26

D

DAD, Duplicate Address Detection, 225

Data Plane, 26

detekcja ruchu, 343

dezaktywacja sygnatur IPS, 361

DHCP, 67

- Discover, 128, 133

- Offer, 128

- Request, 128

- snooping, 128, 132, 191

dodawanie

- przystawki, 477

- reguły, 200, 254

- roli, 467

- ról, 468

- urządzenia, 461

- użytkownika do grupy, 486

dostęp

- do ASA, 275, 323, 325
- do logowania, 88
- do routera, 110
- do sieci VPN, 387
- do trybu uprzywilejowanego, 52
- przez klienta VPN, 434
- przez przeglądarkę, 425

działanie

- firewalla, 233
- SSL/TLS, 423
- STP, 164
- systemów IPS, 339
- tunelu VPN, 407
- ZBF, 260

dziennik zdarzeń, 499

E

Edge router, 31

edycja

- par stref, 259
- reguły, 253
- stref, 257
- ZBF, 251
- zone pairs, 258

egzamin, 10, 12

ekran powitalny ASDM, 274

eksport certyfikatu, 479

F

filtrowanie pakietów, 244

firewall, 233, 267

- sprzętowy, 32

firma

- Cisco, 9
- QNAP, 80

format eksportu certyfikatu, 481

forwarding, 172

funkcja

- autouruchamiania interfejsu, 147
- Dynamic ARP Inspection, 184
- one-step lockdown, 116
- perform security audit, 113
- RiskRating, 375
- Storm Control, 186

funkcje urządzenia ASA, 268

funkcjonalność BPDU Guard, 162

G

generowanie

- certyfikatu, 438
- klucza, 49

GNS3

- dodawanie urządzenia, 63
- łączenie wirtualnych stacji, 60
- obszar roboczy, 68
- projekt sieci, 66
- uruchomienie maszyny wirtualnej, 60
- urządzenia ASA, 331
- ustawienia, 56
- wykorzystanie VirtualBox, 59
- zmiana ustawień, 63

graficzny interfejs użytkownika, GUI, 55

GRE, Generic Routing Encapsulation, 408

grupa

- administratorów, 329
- obiektów, 315
- użytkowników, 330

GUI, graphical user interface, 55

H

hasło

- trybu uprzywilejowanego, 36
- użytkownika, 485

historia bezpieczeństwa sieci, 13

HMAC, Hashed Message Authentication Code, 385

I

Idle PC, 65

IKE, 419

implementacja

- VPN remote access, 422
- VPN site-to-site, 389, 399, 416

implementowanie listy, 202

import certyfikatu, 446

informacje o IPv6, 221

instalacja

- ACS, 95
- ASDM, 289
- ról serwera, 476

instalator

- AnyConnect, 440
- Cisco AnyConnect, 447

integralność danych, 383

IOS, 62, 233, 345, 362

IPS, Intrusion Prevention System, 339

- konfiguracja parametrów, 368
- konfiguracja przez CCP, 362
- konfiguracja przez CLI, 345

IPS, Intrusion Prevention System
 kreator konfiguracji, 363
 monitoring, 376
 IPv6, 221
 istotność alarmu, 357

K

Kali Linux, 126
 kierunek stref, 258
 klawisze skrótu Ctrl+Break, 54
 klient
 RADIUS, 490, 492
 VPN, 434
 klucz, 365
 prywatny, 386
 publiczny, 48, 386
 tajny, 387
 komenda, *Patrz* polecenie
 komunikat Bad secrets, 52
 konfiguracja
 802.1x, 467
 ACS, 96
 bazy danych certyfikatów, 475
 CBAC, 243
 CCP, 70
 CCP Express, 56
 dostępu przez klienta VPN, 434
 dostępu przez przeglądarkę, 425
 elementów kontroli ruchu w sieci, 491
 firewalla, 251
 IKE Phase 1, 390, 393
 interfejsów, 307
 interfejsu, 401
 interfejsu routera, 223
 interfejsu zewnętrznego, 278
 IPS, 345, 348, 362
 klucza prywatnego, 472
 kryptografii, 473
 linku, 431
 lokalnych trybów pracy, 118
 metod uwierzytelniania, 88, 490
 NAT, 249
 NAT dynamicznego, 284
 NAT statycznego, 283
 nazwy urzędu certyfikacji, 473
 parametrów IPS, 368
 PAT, 282, 312
 połączenia 802.1X, 488
 Port Security, 136, 137
 profilu połączenia, 444
 programu GNS3, 56
 PRTG, 460
 przełącznika, 494

przystawki certyfikatów, 478
 reguł ACL, 320
 routera, 89, 103
 routera do pracy z TACACS+, 103, 105
 rozszerzonych list ACL, 207
 serwera DHCP, 311
 sieci przewodowej, 496
 SNMP, 462
 SNMPv3, 458
 SSH, 49
 stacji roboczej, 495
 sygnatur, 373
 syslog, 456
 tunelu GRE, 409
 uwierzytelniania, 401
 VPN, 396
 ZBF, 264
 konsola MMC, 476
 konto użytkownika, 40
 koń trojański, trojan horse, 22
 koszty tras, 169
 kreator
 dodawania ról, 81
 konfiguracji GRE, 409
 konfiguracji IPS, 363
 połączenia VPN, 426
 kryptografia, 379

L

learning, 172
 linia
 aux, line aux, 33
 konsolowa, 110
 konsolowa, line console, 33
 wirtualna, line vty, 33
 lista
 dostępu, 43
 hostów, 182
 linków, 431
 sesji, 262
 zakładek, 430
 listening, 172
 listy
 ACL, 318
 ACL w sieci IPv4, 193
 ACL w sieci IPv6, 221, 227
 rozszerzone ACL, 207
 standardowe ACL, 195
 logi, 91
 systemowe, 452
 logowanie
 do ACS, 97
 do routera, 45

- do sieci, 498
- do sieci VPN, 433
- z wykorzystaniem grupy VPN, 446
- zdarzeń, 451

lokalna

- baza, 31
- baza haseł, 32, 45

lokalne

- tryby pracy, 118
- zabezpieczenie urządzeń, 31

Ł

ładowanie sygnatur, 351

M

mechanizm CSMA/CD, 121

metoda

- asymetryczna, 382
- HMAC, 385
- symetryczna, 381

metody ochrony, 189

MIB, Management Information Base, 457

Microsoft Server 2008R2, 80

model

- AAA, 76
- ISO OSI, 121

modyfikacja

- listy ACL, 368
- sygnatur, 372
- ramki, 161

monitoring IPS, 376

monitorowanie

- urządzenia, 74
- urządzenia ASA, 330
- zdarzeń, 344

N

NAC, Network Admission Control, 189

naprawa problemów, 115

narzędzie

- Nmap, 354
- Packet Tracer, 303
- Ping, 301
- Traceroute, 302

NAS, Network Attached Storage, 80

nasłuchiwanie, 172

NAT, Network Address Translation, 235, 442

NAT w IPv4, 235

nazwa zasady, 86

ND, Neighbour discovery, 224

negocjacja ustawień, 388

NFP, Network Foundation Protection, 24

niezaufane połączenie, 50

niezaufany certyfikat wydawcy, 447

NTP, Network Time Protocol, 464

O

obiekty, 315

obsługa

- logów systemowych, 452
- sygnatur, 366

obszar roboczy GNS3, 58

ochrona infrastruktury sieciowej, NFP, 24

okno

- Add a Rule, 255, 256

- Add AAA Server, 107

- Add Network Object, 317

- Add Target Value Rating, 375

- Add Traffic, 255

- Additional Tasks, 257

- Administrative Access, 300

- AnyConnect Client Deployment, 443

- Attacks list, 130

- Authentication, 411

- Basic Configuration, 296

- Choose attack, 130

- Client Images, 440

- Deliver Configuration to Device, 75, 107, 115, 202, 250, 367, 403, 414

- dodawania przystawki, 477

- Edit VTY Lines, 109

- edycji policy maps, 263

- edycji reguły, 253

- Eksportowanie klucza prywatnego, 480

- File Management, 313

- Follow TCP Stream, 46, 47, 50

- główne CCP, 71

- główne PRTG, 460

- GRE Tunnel Information, 410

- Grupy użytkowników, 86

- informacyjne Cisco CP Warning, 117

- Information, 327

- Interface IP Address Configuration, 298

- Introduction, 417

- Java Control Panel, 445

- konfiguracji linku, 431

- konfiguracji NAT i PAT, 313

- konfiguracji sygnatur, 373

- konfiguracji VPN, 400

- Konfigurator urządzenia, 64

- Konfigurowanie bazy danych certyfikatów, 475

- Konfigurowanie klucza prywatnego, 472

- Konfigurowanie kryptografii, 473

okno

- Konfigurowanie nazwy urzędu certyfikacji, 473
- Kreator dodawania ról, 81
- logowania, 433
- logowania do routera, 68
- logowania do sieci, 498
- Manage Identity Certificates, 437
- Menedżer serwera, 81, 82
- NAT, 238
- NAT Exempt, 420
- New IOS router template, 63
- Określanie grup użytkowników, 491
- Określanie przełączników 802.1X, 489
- Określanie typu instalacji, 471
- Określanie typu urzędu certyfikacji, 472
- podsumowania konfiguracji, 414
- Potwierdzanie opcji instalacji, 475
- powitalne kreatora eksportu, 480
- przeglądania raportów, 104
- PuTTY Security Alert, 49
- Select Bookmark Type, 430
- Select Routing Protocol, 413
- Serwer zasad sieciowych, 487
- Sessions, 449
- Signature Compilation Status, 374
- Signature File and Public Key, 364
- Site-to-Site VPN, 400
- Summary, 366
- Summary of the Configuration, 403
- Targets, 183
- Test AAA Server, 327
- testowania tunelu VPN, 406
- Traffic to protect, 403, 418
- Transform Set, 403, 412
- Ustawianie okresu ważności, 474
- ustawień globalnych, 369
- Właściwości zdarzenia, 500
- Wybieranie komputera, 478
- Wybieranie usług ról, 470
- wyboru ataku, 175
- wyboru interfejsów, 247, 364
- wyboru interfejsu, 181
- wyboru peera, 418
- wyboru poziomu zabezpieczeń, 248
- Wybrane przystawki, 478
- wydajności routera, 70
- zarządzania grupą urządzeń, 72
- Zasady żądań połączeń, 493

opcja

- Scan for Hosts, 181
- Security Audit, 110

organizacja

- ISO, 17
- CERT, 17
- SANS, 16

P

- packet mode, 77
- PAT, Port Address Translation, 236, 282
- PCP, Payload Compression Protocol, 228
- pętla, 163
- podgląd
 - przechwyconej zawartości, 51
 - uwierzytelnienia, 92
- podłączenie do sieci, 495
- podpis elektroniczny, 386
- podsumowanie konfiguracji, 404, 414, 420, 432
- polecenie
 - aaa authentication login, 103, 119
 - aaa new-model, 103, 118
 - apt-get install isc-dhcp-server, 134
 - authentication, 391
 - auto secure, 110
 - banner motd, 37, 44
 - block-for, 42
 - category, 349
 - category all, 349
 - clock set, 464
 - configure terminal, 33
 - confreg 0x2142, 52
 - copy, 351
 - copy startup-cunfig running-config, 53
 - crypto isakmp policy, 391
 - crypto map, 393
 - debug aaa authentication, 91
 - disable, 37
 - enable secret ?, 37
 - enable view, 119
 - encryption, 391
 - exec-timeout, 40
 - exit, 34, 349
 - hash, 391
 - hostname, 48
 - idconf, 351
 - ip access-group, 240
 - ip dhcp snooping, 132
 - ip dhcp snooping trust, 132
 - ip http secure-server, 74
 - ip ips, 350
 - ip ips config location, 346
 - ip ips name, 347
 - ip ips notify log, 347
 - ip ips notify sdee, 347
 - ip sdee subscriptions 2, 347
 - ip ssh version 2, 49
 - line console, 33
 - logging, 347
 - logging host, 454
 - logging on, 454

- logging source-interface, 454
- logging trap, 454
- login, 34
- login delay, 42
- login local, 40
- login quiet-mode access-class, 44
- name, 151
- nmap, 354
- no service password-recovery, 54
- ping, 38
- qemu-img create, 332
- remark, 43
- retired false, 350
- security password min-length, 40
- service password-encryption, 35
- show crypto ipsec sa, 397
- show crypto isakmp peers, 395, 398
- show crypto isakmp sa, 394, 397
- show crypto map, 394
- show ip, 118
- show ip dhcp binding, 129, 131, 185
- show ip ips signature count, 352
- show ip route, 38
- show ips signatures count, 350
- show login failures, 43
- show monitor session, 188
- show parser view, 119
- show port-security, 143, 144
- show privilege, 38
- show processes cpu utilization, 175
- show running-config, 34, 120
- show secure bootset, 54
- show snmp, 459
- show spanning-tree, 164, 165, 167
- show spanning-tree summary, 165
- show vlan, 151
- shutdown, 133
- switchport mode access, 152
- switchport trunk allowed vlan, 156
- transport input ssh, 49
- username, 39
- username test password test, 41
- vlan, 151
- who, 40
- policy map, 26, 27
- polityka bezpieczeństwa, 19
- połączenia TRUNK, 153
- połączenie
 - 802.1X, 488
 - do routera, 51
 - VPN site-to-site, 392, 422
 - z serwerem RADIUS, 499
 - z VPN przez Cisco AnyConnect, 445
- port główny, 168
- Port Security, 134, 147
- PortFast, 172
- POST, Power On Self Test, 270
- potwierdzanie opcji instalacji, 475
- proces EUI-64 i DAD, 225
- program
 - 3CDAemon, 453
 - ASDM, 287
 - CCP, 29
 - CCP Express, 69
 - ettercap, 181
 - GNS, 56
 - GNS3, 28, 56, 331
 - Kali Linux, 126
 - KALI LINUX, 29
 - PRTG, 460
 - PuTTY, 45
 - VirtualBox, 59, 29
 - VMware, 29
 - Wireshark, 45, 92, 160
 - Yersinia, 133
- projekt sieci, 66
- protokoły
 - hashujące, 380
 - IPsec, 380
 - negocjacyjne, 380
 - ochrony procesu wymiany kluczy, 380
 - szyfrowania, 380
- protokół
 - AHP, 227
 - ARP, 123
 - EAP, 497
 - ESP, 227
 - ICMP, 27, 228, 241
 - IP, 228
 - IKE, 388
 - NTP, 464
 - OSPF, 310
 - PCP, 228
 - RADIUS, 79
 - SDEE, 343
 - SHA, 387
 - SNMP, 456
 - STP, 162
 - TACACS+, 93
- przechwycona komunikacja, 189
- sesja logowania, 425
- przechwycone ramki, 399
- przechwycony atak, 184
- przechwytywanie pakietów, 45
- przeglądanie
 - logów, 91
 - raportów, 104

przełęczarka, 425
 przekazywanie informacji, 172, 451
 przełącznik, 124, 494
 Cisco, 29
 przycisk
 Crack Password, 35
 Launch attack, 130
 przypisanie akcji do sygnatury, 374
 PSK, preshared key, 387
 PVST, Per-VLAN Spanning Tree, 165
 pytania egzaminacyjne, 12

R

RADIUS, 79, 466
 instalacja, 80
 konfiguracja routera, 89
 konfigurowanie metod uwierzytelniania, 88
 tworzenie klienta, 82
 tworzenie użytkownika, 89
 tworzenie zasady, 86
 tworzenie zasady połączeń, 83
 uwierzytelnianie, 81
 wybieranie atrybutu, 85
 ramka
 BPDU, 164, 174
 DTP, 159
 ethernetowa, 122
 ramki dotyczące uwierzytelnienia, 92
 raportowanie, accounting, 76, 77, 451
 rejestracja serwera zasad sieciowych, 487
 rekonesans, 22
 Nmap, 356
 rekonfiguracja listy, 368
 robak, worm, 21
 rodzaje
 adresów IPv6, 224
 ataków, 22
 list ACL, 194
 niebezpieczeństw, 21
 pytań, 12
 rola
 Usługi certyfikatów, 468
 Usługi zasad i dostępu sieciowego, 468
 root bridge, 167
 root port, 168
 router, 65
 brzegowy, 31
 routing statyczny, 310
 rozszerzona lista dostępu, 27
 ruch VOIP, 248
 ryzyko, 17

S

SDEE, Security Device Event Exchange, 343
 sensor IPS, 342, 345
 service policy, 27
 serwer
 ACS, 97
 DHCP, 67, 280, 311
 Microsoft Server 2008R2, 80
 NAS, 434
 NTP, 464
 RADIUS, 80
 syslog, 453, 454, 455
 TACACS+, 323
 TFTP, 285
 VPN, 387
 zasad sieciowych, 81, 487, 488
 sieć
 IPv4, 193
 LAN, 188
 VLAN, 148
 VPN, 386
 z IPS, 345
 SLAAC, 226
 SNMP, 456, 457
 specyfikacja RFC4250-RFC4254, 47
 SPI, Stateful Packet Inspection, 239
 sprawdzanie bezpieczeństwa SSH, 50
 SSH, secure shell, 45, 51, 275
 SSL, Secure Socket Layer, 423
 SSL handshake, 424
 stan
 blocking, 172
 forwarding, 172
 learning, 172
 listening, 172
 standard IEEE 802.1Q, 148
 status połączenia VPN, 448
 statusy STP, 172
 statystyki działania ZBF, 260
 STP, Spanning Tree Protocol, 162
 strefa, 244
 DMZ, 247
 supplicant, 81
 sygnatura
 enabled, 348
 retired false, 348
 sygnatury
 atomic, 344
 composite, 344
 funkcja RiskRating, 375
 ustawienie akcji, 358
 systemy IPS, 339
 szacowanie ryzyka, 357

szyfrowanie, 379, 380
 metoda asymetryczna, 382
 metoda symetryczna, 381

T

tablica
 ARP, 123
 MAC, 125, 134
 translacji, 235
TACACS+, 93, 323
 konfiguracja routera, 103
Telnet, 275
testowanie
 komunikacji, 301
 tunelu VPN, 406
translacja, 442
trunk, 154
tryb
 interactive, 110
 rommon, 53, 54
 uprzywilejowany, 37
 uwierzytelniania, 497
 znakowy, 76
tunel
 GRE, 408
 VPN SSL, 423
tworzenie
 aliasu, 38
 banera informującego, 44
 crypto map, 393
 grupy, 100, 484
 grupy użytkowników VPN, 429
 klienta RADIUS, 83
 listy dostępu, 43
 listy rozszerzonej, 208
 menu strony, 429
 metody autoryzacji, 108
 metody uwierzytelniania, 108
 nazwy dla urządzenia, 333
 obiektu, 483
 profilu VPN, 435
 puli adresów IP, 442
 trasy statycznej, 413
 urządzenia, 333
 użytkownika, 39, 89, 100, 306, 441, 484
 użytkownika VPN, 428
 zasady, 86
 zasady połączeń, 83
 zasady sieciowej, 87
typy list ACL, 319

U

uaktualnienia NTP, 465
uczenie się, 172
ujawnienie konfiguracji, 52
uprawnienia dla grupy, 101
uruchamianie
 ActiveX, 447
 alarmu, 357
 konsoli MMC, 476
 maszyny wirtualnej, 60
 serwera RADIUS, 81
 tunelu GRE, 408
urządzenia
 NAC, 189
 warstwy 2., 124
urządzenie
 ASA, 268
 ASA 5505, 268, 416, 422
 Cisco ASA, 267
 IPS, 344
usługa
 Active Directory, 80, 468
 RADIUS, 492
 syslog, 452
ustawienia
 algorytmu szyfrowania, 402
 banerów informacyjnych, 305
 Cisco AnyConnect, 448
 crypto map, 394
 czasu, 310
 globalne IPS, 369
 IKE, 412
 NAT, 443
 TCP/IP, 450
ustawienie
 akcji dla sygnatury, 358
 okresu ważności, 474
 zdarzeń, 455
uwierzytelnienie, authentication, 76, 108, 386, 498
 802.1x, 465
 informacji, 26
 oparte na serwerze, 77
 RADIUS, 81
 TACACS+, 99
 użytkownika lub komputera, 497
użytkownik, 39

V

VirtualBox, 59
VLAN, Virtual LAN, 148
VLAN site-to-site, 389

VOIP, 248
 VPN, Virtual Private Network, 77, 386
 VPN remote access, 422
 VPN site-to-site, 389

W

warstwa 2. modelu ISO OSI, 121
 wartość Idle PC, 65
 weryfikacja
 adresu, 489
 nazwy, 489
 widoki, 118
 wirtualizacja, 59
 wirtualna karta pamięci, 66
 wirus, 21
 właściwości
 chronionego protokołu EAP, 497
 klienta RADIUS, 492
 zdarzenia, 500
 włączenie IPS, 345, 362
 wstawianie komentarzy, 199
 wybór
 adresów, 404
 akcji, 358
 algorytmu szyfrowania, 420
 formatu eksportu certyfikatu, 481
 interfejsów, 113
 interfejsu połączeniowego, 435
 metody ataku, 183
 metody uwierzytelnienia, 441
 protokołu, 436
 roota, 175
 ról serwera, 81, 468
 usług ról, 469
 wersji IKE, 419
 wymiana kluczy, 48
 wyszukiwanie hostów, 181

Z

zabezpieczenie
 konfiguracji, 52, 54
 konta użytkownika, 40
 linii, 33
 routera, 32
 trybu uprzywilejowanego, 37
 urządzenia, 31, 127
 warstwy 2., 190
 zabezpieczenie BPDU guard, 176
 zakładka
 AnyConnect Connection Profiles, 444
 Authentication Methods, 419
 Common Tasks, 102
 Edit IPS, 367
 IKE Policy, 419
 IPS Alert Statistics, 377
 IPSSignature Statistics, 376
 Syslog Server, 453
 zakończenie eksportu, 482
 zapisywanie konfiguracji, 405
 zapytanie ARP, 180
 zarządzanie
 bezpieczeństwem, 15
 hasłami, 304
 listami ACL, 321
 ryzykiem, 17
 użytkownikami, 304
 zasady
 lokalnego konta, 93
 zadań połączeń, 493
 ZBF, Zone Based Firewalls, 244
 zdarzenia logowania, 104
 zmiana hasła, 52

PROGRAM PARTNERSKI

GRUPY WYDAWNICZEJ HELION



- 1. ZAREJESTRUJ SIĘ**
- 2. PREZENTUJ KSIĄŻKI**
- 3. ZBIERAJ PROWIZJĘ**

Zmień swoją stronę WWW
w działający bankomat!

Dowiedz się więcej i dołącz już dzisiaj!

<http://program-partnerski.helion.pl>

Bezpieczeństwo sieci komputerowych to temat, którego nie da się zgłębić do końca. Systemy informatyczne bezustannie ewoluują, a utalentowany haker złamie najbardziej wyrafinowane zabezpieczenia. Jednak nie ma co załamywać rąk. Ta książka powstała po to, by pomóc Ci zabezpieczyć Twoją sieć tak dokładnie, jak to możliwe. Na tym etapie powinieneś wiedzieć, jak działają podstawowe technologie wykorzystywane w sieciach. Jeśli jeszcze tego nie wiesz, najpierw zapoznaj się z pozycją *CCNA 200-120. Zostań administratorem sieci komputerowych Cisco*.

W opisaney tu historii odegrasz kolejno rolę obserwatora, włamywacza i administratora bezpieczeństwa. Poznasz teorię, potem zastosujesz ją, by włamać się do sieci, a na końcu zabezpieczysz tę sieć. Dowiesz się stąd, jak ochronić całą sieć wraz z urządzeniami peryferyjnymi. Zobaczysz, jak wykorzystać różne protokoły uwierzytelniania, listy kontroli dostępu, firewalles systemowe i zewnętrzne oraz systemy IPS. Odkryjesz, na czym polega dobre szyfrowanie i jak zabezpieczyć komunikację przez skonfigurowanie sieci VPN. Zapoznasz się także bliżej z kwestią rejestrowania i raportowania niepożądanych zdarzeń. Wiedza zawarta w tej książce pozwoli Ci zdać egzamin na certyfikat Cisco CCNA Security, ale przede wszystkim zabezpieczyć Twoją sieć na mistrzowskim poziomie!

ADMINISTROWANIE PRZEZ ZABEZPIECZANIE!

- Podstawy bezpieczeństwa sieci
- Lokalne zabezpieczanie urządzeń
- Działanie i wykorzystanie RADIUS i TACACS+
- Sposoby zabezpieczania warstwy 2 modelu ISO OSI
- Listy ACL IPv4
- ACL w sieci IPv6
- Zapora i jej zastosowanie na bazie IOS
- Zapora ogniowa oparta na urządzeniu Cisco ASA
- Systemy IPS (Intrusion Prevention System)
- Konfiguracja szyfrowania i sieci VPN
- Logowanie zdarzeń, raportowanie i zarządzanie bezpieczeństwem sieci za pomocą 802.1x
- Administrowanie przez zabezpieczanie!

Helion	
41714	numer katalogowy
księgarnia internetowa	
http://hellon.pl	
zamówienia telefoniczne	
	0 801 339900
	0 601 339900

Sprawdź najnowsze promocje:
● <http://hellon.pl/promocje>
Książki najchętniej czytane:
● <http://hellon.pl/bestsellery>
Zamów informacje o nowościach:
● <http://hellon.pl/nowości>

Helion SA
ul. Kościuski 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: hellon@hellon.pl
<http://hellon.pl>



ISBN 978-83-283-1814-4



Informatyka w najlepszym wydaniu

cena: 89,00 zł