Adam Józefiok

SECURITY CCNA 210-260

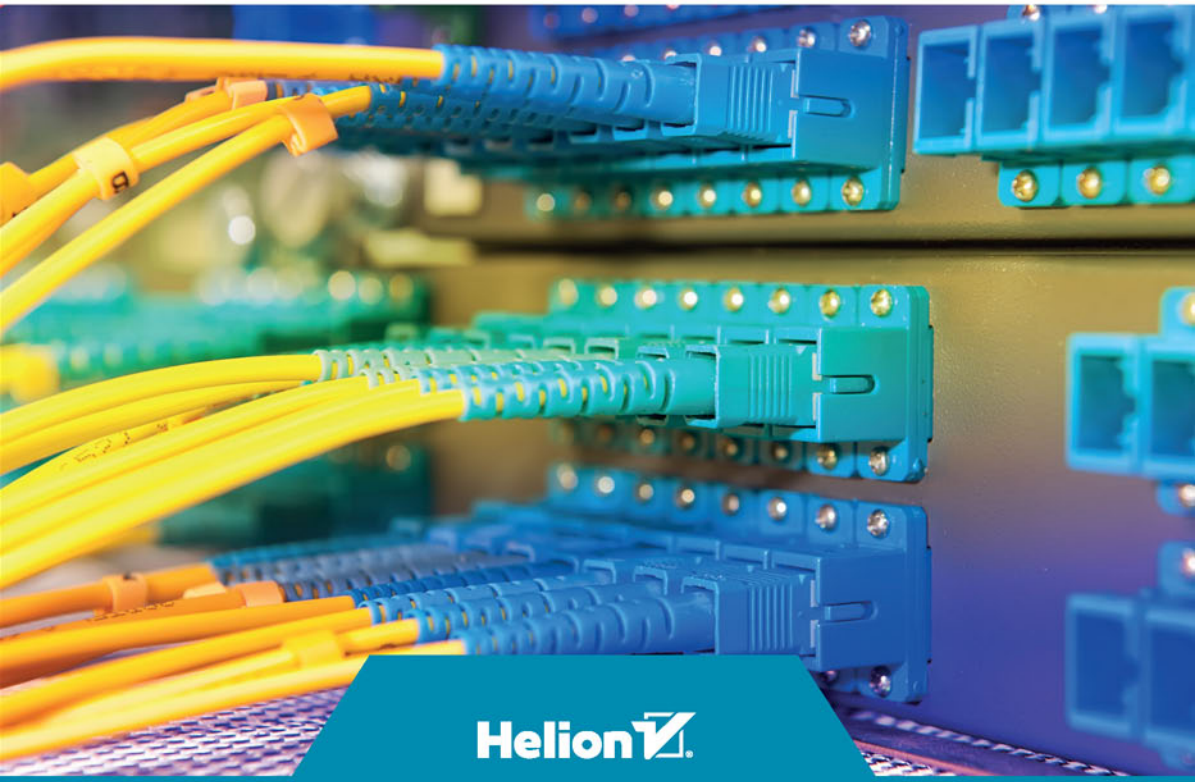
ZOSTAŃ ADMINISTRATOREM SIECI KOMPUTEROWYCH CISCO

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

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

Printed in Poland.

Spis treści

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 nieznajomość byłaby dla Ciebie przeszkodą w opanowaniu zagadnień zawartych w niniejszej książce.

A jeśli już masz opanowaną treść zaleconej 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 sprzęcie 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 Spannig 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 przejrzenie 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 około15 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) dojdziesz 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 czyjejś 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 przepełnianie 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 umożliwiało rozpoczęcie zdalnych ataków. Nastała 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 przesyła 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 Intrusion 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 zapomniałeś 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 przekupki 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*).

Zarządzenie 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. Zacznijmy 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

B

C

D

E

F

G

H

I

K

L

Ł

M

N

O

P

R

S

T

U

V

W

Z

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 opisanej 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, firewalle 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://helion.pl
zamówienia telefoniczne
0 801 339900
0 601 339900
Informatyka w najlepszym wydaniu

Sprawdź najnowsze promocje:
http://helion.pl/promocje
Książki najchętniej czytane:
http://helion.pl/bestsellery
Zamów informacje o nowościach:
http://helion.pl/nowosci

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: helion@helion.pl
http://helion.pl

ISBN 978-83-283-1814-4
9 788328 318144
cena: 89,00 zł