PRZEGLĄD KONCEPCJI TCP/IP

Prawie wszystko, co robisz jako analityk bezpieczeństwa sieci lub tester bezpieczeństwa, zależy od zrozumienia koncepcji sieciowych i wiedzy na temat protokołu Transmission Control Protocol/Internet Protocol (TCP/IP). Zakłada się, że rozumiesz już koncepcje sieciowe i TCP/IP oraz posiadasz certyfikat CompTIA Network lub równoważną wiedzę. Ten moduł służy jednak jako przegląd tego, w jaki sposób te tematy odnoszą się do bezpieczeństwa IT i testerów bezpieczeństwa. W ramach zajęć i projektów przypadków stosujesz swoją wiedzę na temat TCP/IP i koncepcji sieciowych do technik testowania bezpieczeństwa. Większość narzędzi, z których korzystają zarówno cyberprzestępcy, jak i testerzy bezpieczeństwa, działa w oparciu o protokół IP, który jest standardowym protokołem sieciowym. Jednak protokół IP w wersji 4 (IPv4), nadal najszerzej stosowana wersja, został opracowany bez uwzględnienia funkcji bezpieczeństwa, więc profesjonaliści potrzebują wiedzy i umiejętności, aby uszczelnić luki w zabezpieczeniach wynikające z użycia protokołu IP. W tym module badasz stos protokołów TCP/IP i adresowanie IP. Przeanalizujesz również binarne, ósemkowe i szesnastkowe systemy numeracji oraz porty powiązane z usługami działającymi w protokole TCP/IP.

PRZEGLĄD TCP/IP

Aby komputery mogły się ze sobą komunikować przez Internet lub w biurze, muszą mówić tym samym językiem. Język ten nazywany jest protokołem, a najczęściej używanym jest Transmission Control Protocol/Internet Protocol (TCP/IP). Niezależnie od tego, jakie medium łączy stacje robocze w sieci — przewody miedziane, światłowody lub sieć bezprzewodowa — ten sam protokół musi działać na wszystkich komputerach, aby komunikacja działała prawidłowo. Prawdopodobnie już zapoznałeś się z protokołem TCP/IP, ale przegląd jest pomocny, aby upewnić się, że masz dogłębne zrozumienie. TCP/IP to coś więcej niż tylko połączenie dwóch protokołów (TCP i IP). Zwykle nazywa się go stosem TCP/IP, który zawiera cztery odrębne warstwy (patrz Rysunek 2-1). Warstwa sieciowa zajmuje się fizycznym przenoszeniem bitów przez medium (niezależnie od tego, czy medium jest drut miedziany, światłowody czy sieć bezprzewodowa), a warstwa internetowa odpowiada za kierowanie pakietami przy użyciu adresów IP. Warstwa transportowa zajmuje się kontrolowaniem przepływu danych, sekwencjonowaniem pakietów w celu ponownego złożenia i kapsułkowaniem segmentu za pomocą nagłówka TCP lub User Datagram Protocol (UDP). Warstwa aplikacji to miejsce, w którym działają aplikacje i protokoły, takie jak HTTPS i SSH. W tym module omówiono tylko warstwy aplikacji, transportu i Internetu, omówione w kolejnych sekcjach, ponieważ testowanie bezpieczeństwa zwykle nie obejmuje schodzenia do poziomu sprzętowego warstwy sieciowej. Jednak niektóre ataki komputerowe wykorzystują fizyczny sprzęt, taki jak keylogger.

Warstwa aplikacji

Protokoły warstwy aplikacji są front-endem protokołów niższej warstwy w stosie TCP/IP. Innymi słowy, ta warstwa to to, co można zobaczyć i dotknąć. Tabela 2-1 zawiera listę niektórych głównych aplikacji i protokołów działających na tej warstwie.

Zastosowanie: Opis

Hypertext Transfer Protocol Secure (HTTPS): Podstawowy protokół używany do komunikacji przez sieć

File Transfer Protocol (FTP): Umożliwia różnym systemom operacyjnym (OS) przesyłanie plików między sobą

Simple Mail Transfer Protocol (SMTP): Główny protokół do przesyłania wiadomości e-mail przez Internet

Simple Network Management Protocol (SNMP): Używany głównie do monitorowania urządzeń w sieci, np. zdalnego monitorowania stanu routera

Secure Shell (SSH): Umożliwia użytkownikom bezpieczne logowanie się do zdalnego serwera i interaktywne wydawanie poleceń

Internet Relay Chat (IRC): Umożliwia wielu użytkownikom komunikację przez Internet na forach dyskusyjnych

Telnet: Umożliwia użytkownikom niezabezpieczone logowanie się do zdalnego serwera i interaktywne wydawanie poleceń

Warstwa transportowa

W warstwie transportowej dane są kapsułkowane w segmenty. Segment może używać protokołu TCP lub UDP jako metody łączenia się i przekazywania danych do hosta docelowego (lub węzła). TCP to protokół zorientowany na połączenie, co oznacza, że nadawca nie wysyła żadnych danych do węzła docelowego, dopóki węzeł docelowy nie potwierdzi, że słucha nadawcy. Innymi słowy, połączenie jest nawiązywane przed wysłaniem danych. Na przykład, jeśli komputer A chce wysłać dane do komputera B, najpierw wysyła komputerowi B pakiet SYN. Pakiet SYN (skrót od synchronize) to zapytanie do odbiorcy, podobne do pytania „Witaj, komputerze B. Czy jesteś tam?". Komputer B odsyła potwierdzenie zwane pakietem SYN-ACK, co jest jak odpowiedź „Tak, jestem tutaj. Kontynuuj i wyślij". Na koniec komputer A wysyła pakiet ACK (skrót od acknowledgment) do komputera B w odpowiedzi na pakiet SYN-ACK. Proces ten, nazywany trzyetapowym uzgadnianiem, obejmuje następujące kroki:

1. Host A wysyła pakiet TCP z ustawioną flagą SYN (tj. pakiet SYN) do Hosta B.

2. Po otrzymaniu pakietu Host B wysyła Hostowi A własny pakiet SYN z ustawioną flagą ACK (pakiet SYN-ACK).

3. W odpowiedzi na pakiet SYN-ACK od Hosta B, Host A wysyła Hostowi B pakiet TCP z ustawioną flagą ACK (pakiet ACK).

Nagłówki segmentów TCP

Jako specjalista ds. bezpieczeństwa powinieneś znać krytyczne komponenty nagłówka TCP: flagi TCP, początkowy numer sekwencyjny oraz numery portów źródłowych i docelowych. Rysunek przedstawia diagram nagłówka TCP.

16-bit							32-bit
Source Port							Destination Port
Sequence Number							
Acknowledgment Number (ACK)							
Offset	Reserved	U	A	P	R	S	F	Window
Checksum							Urgent Pointer
Options and Padding							

Atakujący wykorzystują wiedzę o składnikach nagłówka TCP. Musisz zrozumieć te składniki, zanim dowiesz się, jak można je wykorzystać. Dopiero wtedy możesz sprawdzić, czy Twoja sieć ma luki w tych obszarach. Pamiętaj, aby chronić sieć, musisz znać podstawowe metody włamywania się do sieci.

Flagi TCP

Każda flaga TCP zajmuje 1 bit segmentu TCP i może być ustawiona na 0 (wyłączona) lub 1 (włączona). Oto sześć flag segmentu TCP:

• Flaga SYN — flaga synchronizacji oznacza początek sesji.

• Flaga ACK — flaga potwierdzenia potwierdza połączenie i jest wysyłana przez hosta po otrzymaniu pakietu SYNACK.

• Flaga PSH — flaga push służy do dostarczania danych bezpośrednio do aplikacji. Dane nie są buforowane; są wysyłane natychmiast.

• Flaga URG — ta flaga służy do oznaczania pilnych danych.

• Flaga RST — flaga resetowania resetuje lub rozłącza połączenie. • Flaga FIN — flaga zakończenia oznacza, że połączenie zostało zakończone.

Początkowy numer sekwencyjny

Początkowy numer sekwencyjny (ISN) to 32-bitowy numer, który śledzi pakiety odebrane przez węzeł i umożliwia ponowne złożenie dużych pakietów, które zostały podzielone na mniejsze pakiety. Kroki 1 i 2 trzyetapowego uzgadniania wysyłają ISN. Oznacza to, że ISN z węzła wysyłającego jest wysyłany z pakietem SYN, a ISN z węzła odbierającego jest wysyłany z powrotem do węzła wysyłającego z pakietem SYN-ACK. ISN może być dość dużą liczbą, ponieważ 232 pozwala na zakres liczb od zera do ponad czterech miliardów.

BAJTY BEZPIECZEŃSTWA

ISN nagłówka TCP może nie wydawać się ważny dla specjalistów ds. bezpieczeństwa sieci, którzy nie są zaznajomieni z testami penetracyjnymi ani technikami hakerskimi. W rzeczywistości większość ludzi ignoruje wiele z tych podstawowych koncepcji. Jednak liczne ataki sieciowe wykorzystywały przechwytywanie sesji sieciowej, atak polegający na zgadywaniu ISN pakietów TCP. Jednym z najsłynniejszych jest atak Kevina Mitnicka na japońską korporację — określany jako „atak predykcji sekwencji TCP". Zrozumienie flag TCP i podstawowych elementów pakietu TCP może w dużym stopniu pomóc w zrozumieniu, jak myśli atakujący — i jak Ty powinieneś myśleć. Aby stać się lepszym specjalistą ds. bezpieczeństwa, staraj się odkrywać luki lub słabości podczas nauki podstaw. Zbyt wielu specjalistów ds. bezpieczeństwa sieci czeka, aż atakujący odkryją luki w zabezpieczeniach sieci, zamiast pokonać ich w ich własnej grze.

Aktywność 2-1: Przeglądanie RFC-793

Czas trwania: 30 minut

Cel: Zbadanie szczegółów komponentów segmentu TCP i zapoznanie się ze sposobem korzystania z dokumentów Request for Comments (RFC).

Opis: Ilość informacji dostępnych dla specjalisty ds. bezpieczeństwa IT może być przytłaczająca. Aby chronić zasoby organizacji (lub „aktywa", jak są one powszechnie nazywane), oczekuje się od Ciebie umiejętności w wielu obszarach. Aby zdobyć niezbędne umiejętności, powinieneś wiedzieć, gdzie szukać informacji technicznych, które pomogą Ci lepiej zrozumieć daną technologię. Chcesz wiedzieć,

jak działa system nazw domen (DNS)? Chcesz lepiej zrozumieć protokół dynamicznej konfiguracji hosta (DHCP)? Zapoznanie się z dokumentami RFC na te tematy może odpowiedzieć na wszelkie Twoje pytania. W tej aktywności zbadasz szczegóły segmentu TCP i uzyskasz przegląd niektórych komponentów nagłówka TCP. Nie musisz zapamiętywać swoich ustaleń.

Ta aktywność jest jedynie wprowadzeniem do wspaniałego świata RFC.

1. Uruchom przeglądarkę internetową i przejdź do www.ietf.org.

2. Na stronie głównej Internet Engineering Task Force wybierz RFC z menu INTERNET STANDARDS. (Jeśli czas na to pozwoli, możesz przejść do innych opcji, aby uzyskać informacje na temat przydatnych tematów.)

3. Przeczytaj instrukcje na stronie RFC, kliknij łącze RFC Search Page, wpisz 793 w polu tekstowym RFC, a następnie kliknij Search. Kliknij ASCII lub PDF w obszarze Files, aby wyświetlić RFC. Zwróć uwagę na stronę tytułową tego RFC.

4. Przewiń dokument w dół i przeczytaj spis treści, aby uzyskać przegląd informacji w tym dokumencie. Przeczytaj sekcje 2.6, 2.7 i 2.8, aby lepiej zrozumieć, jak działa TCP. (Należy pamiętać, że sekcja 2.6 omawia niezawodną komunikację.)

5. Przewiń w dół do sekcji 3.1, „Format nagłówka”. Diagram może nie być tym, co zwykle widzisz w dokumentacji komputerowej, ale jest typowy dla tego, co można znaleźć w RFC. Liczby u góry ułatwiają zobaczenie pozycji każdego bitu. Na przykład górne 0, 1, 2 i 3 pokazują, że w tym segmencie jest łącznie 32 bity (od 0 do 31). Zwróć uwagę, że pola portu źródłowego i portu docelowego mają długość 16 bitów, a zarówno ISN, jak i numer potwierdzenia mają długość 32 bitów.

6. Przeczytaj sekcję 3.1 i zwróć uwagę na użycie systemu numeracji binarnej. Informacje te powinny pomóc Ci utrwalić wiedzę na temat numeracji binarnej i szesnastkowej.

7. Przewiń w dół do sekcji 3.4, „Nawiązywanie połączenia”, i przejrzyj opis trzyetapowego uzgadniania. Autor wyjaśnia proces i dodaje trochę humoru na temat tego, dlaczego ACK nie zajmuje miejsca na numer sekwencyjny. Wielu autorów RFC ma talent do wyjaśniania złożonych materiałów w sposób łatwy do zrozumienia.

8. Przewiń resztę dokumentu, aby uzyskać przegląd tego, co jest omówione. Możesz przeczytać cały dokument później, jeśli chcesz. Po zakończeniu zamknij przeglądarkę internetową

Porty TCP

Pakiet TCP ma dwa 16-bitowe pola zawierające numery portu źródłowego i docelowego. Port jest logicznym, a nie fizycznym składnikiem połączenia TCP i może być przypisany do procesu, który wymaga połączenia sieciowego. Na przykład usługa HTTPS domyślnie używa portu 443. Zrozumienie portów jest ważne, aby wiedzieć, jak zatrzymać lub wyłączyć usługi, które nie są używane w sieci. Im więcej usług masz uruchomionych na serwerze, tym więcej portów jest otwartych na potencjalny atak. Innymi słowy, zabezpieczenie domu z 1000 otwartych drzwi jest trudniejsze niż zabezpieczenie domu z tylko 10 otwartymi drzwiami.

BAJTY BEZPIECZEŃSTWA

Najtrudniejszą częścią pracy specjalisty ds. bezpieczeństwa sieci jest zrównoważenie bezpieczeństwa systemu z łatwością użytkowania i dostępnością dla użytkowników. Zamknięcie wszystkich portów i zatrzymanie wszystkich usług z pewnością zwiększyłoby bezpieczeństwo sieci, ale użytkownicy nie mogliby łączyć się z Internetem, wysyłać ani odbierać wiadomości e-mail ani uzyskiwać dostępu do

zasobów sieciowych. Twoim zadaniem jest zatem umożliwienie użytkownikom pracy w bezpiecznym środowisku sieciowym bez uniemożliwiania im korzystania z usług, takich jak poczta e-mail i przeglądanie stron internetowych. To zadanie nie jest łatwe, jak dowiesz się w trakcie tego kursu. Dostępnych jest 65 535 numerów portów TCP i UDP, ale dobrą wiadomością jest to, że tylko 1023 z nich uważa się za dobrze znane porty. Aby zobaczyć listę dobrze znanych portów, odwiedź Internet Assigned Numbers Authority (IANA) pod adresem www.iana.org. Witryna prawdopodobnie zawiera więcej informacji, niż potrzebujesz, ale poruszanie się po niej pozwala nabrać wprawy w wyszukiwaniu informacji. Dobry specjalista ds. bezpieczeństwa wie, jak wytrwale szukać odpowiedzi, korzystając ze strukturalnej metodologii.

WSKAZÓWKA Możesz uzyskać dostęp do strony o znanych portach, wpisując www.iana.org/assignments/port-numbers jako adres URL, ale ominiesz stronę główną IANA, która zawiera więcej informacji i dostęp do usługi IANA Whois. Możesz przejrzeć tę usługę, przeglądając stronę IANA.

Nie musisz zapamiętywać 1023 znanych portów. Powinieneś jednak zapamiętać następujące porty TCP i usługi, które one reprezentują. Wiele z tego, co robisz jako specjalista ds. bezpieczeństwa i tester penetracyjny, opiera się w dużej mierze na zrozumieniu tych informacji.

• Porty 20 i 21 (File Transfer Protocol) — FTP istnieje tak długo, jak Internet. Był standardem przenoszenia i kopiowania dużych plików i jest nadal używany, choć w mniejszym stopniu ze względu na popularność HTTP. FTP używa portu 20 do przesyłania danych, a portu 21 do kontroli. FTP wymaga podania nazwy logowania i hasła i jest bezpieczniejszy niż Trivial File Transfer Protocol (TFTP; omówiony później na tej liście). FTP nie używa szyfrowania, więc dane w tranzycie mogą zostać przechwycone i zrozumiane. Secure File Transfer Protocol (SFTP) używa Secure Shell (SSH; omówiony później na tej liście), aby zapewnić bezpieczeństwo FTP poprzez zapewnienie szyfrowania i uwierzytelniania.

• Port 22 (Secure Shell) — Secure Shell (SSH) używa szyfrowania i uwierzytelniania, aby utworzyć bezpieczny kanał w niezabezpieczonej sieci. SSH jest używany do zabezpieczania logowania, przesyłania plików i przekierowywania portów. FTP jest niezabezpieczony, ale można go zabezpieczyć, używając kanału SSH. FTP używający SSH jest znany jako SFTP.

• Port 25 (Simple Mail Transfer Protocol) — Serwery poczty e-mail nasłuchują na tym porcie. Jeśli próbujesz wysłać wiadomość e-mail do zdalnego użytkownika, Twoja stacja robocza łączy się z portem 25 na serwerze pocztowym.

• Port 53 (Domain Name System) — Jeśli serwer w Twojej sieci używa DNS, używa portu 53. Większość sieci wymaga serwera DNS, aby użytkownicy mogli łączyć się ze stronami internetowymi za pomocą adresów URL, a nie adresów IP. Gdy użytkownik wprowadzi adres URL, taki jak www.google.com, serwer DNS rozwiązuje nazwę na adres IP. Serwer DNS może być wewnętrzny dla firmy lub każdy komputer może być skonfigurowany tak, aby wskazywał na adres IP serwera DNS obsługiwanego przez dostawcę usług internetowych firmy.

• Port 69 (Trivial File Transfer Protocol) — wielu inżynierów sieciowych używa usługi TFTP do przesyłania konfiguracji routera i tworzenia kopii zapasowych.

• Port 80 (Hypertext Transfer Protocol) — większość egzaminów certyfikacyjnych zawiera pytanie o port 80 używany do protokołu HTTP. Port 80 jest używany podczas łączenia się z serwerem internetowym. Protokół HTTP nie jest bezpieczny, więc większość serwerów internetowych używa protokołu HTTPS (port 443).

• Port 143 (IMAP) — klienci poczty e-mail używają tego portu do pobierania wiadomości e-mail z serwera pocztowego za pośrednictwem połączenia TCP/IP.

• Port 443 (Secure Hypertext Transfer Protocol) — port 443, podobnie jak port 80, jest używany podczas łączenia się z serwerem WWW. Jednak port 443 jest zazwyczaj zarezerwowany dla bezpiecznych połączeń.

• Port 993 (IMAPS) — IMAP przez SSL/TLS używa portu 993. Połączenia korzystające z tego portu są zabezpieczone, więc jest on preferowany w stosunku do niezabezpieczonej wersji IMAP, która używa portu 143.

BAJTY BEZPIECZEŃSTWA

Często personel techniczny, który nie jest zaznajomiony z technikami bezpieczeństwa, myśli, że ograniczenie dostępu do portów na routerze lub zaporze może chronić sieć przed atakiem. Łatwiej powiedzieć niż zrobić. W końcu, jeśli zapora uniemożliwia jakikolwiek ruch wchodzący lub wychodzący z sieci na portach 80 i 443, rzeczywiście zamknąłeś podatne porty dla dostępu hakerów. Jednak zamknąłeś również drzwi dostępu do Internetu dla swoich użytkowników, co prawdopodobnie nie jest akceptowalne w Twojej organizacji. Trudna (i prawie niemożliwa) część dla personelu ds. bezpieczeństwa polega na próbie powstrzymania atakujących, przy jednoczesnym umożliwieniu autoryzowanym użytkownikom pracy i korzystania z Internetu. W miarę postępów w tym kursie zobaczysz, że dopóki użytkownicy mogą połączyć się z Internetem przez otwarty port, atakujący mogą się dostać. To takie proste. Jeśli użytkownik może wyjść, atakujący może wejść.

• Port 110 (Post Office Protocol 3) — aby pobrać pocztę z serwera pocztowego, jedną z opcji jest dostęp do portu 110 za pomocą Post Office Protocol 3 (POP3). Dostępny jest również ulepszony protokół pobierania poczty e-mail, IMAP4, który jest omówiony dalej na tej liście. POP3 nadal istnieje i jest jednym z najpopularniejszych systemów pobierania poczty e-mail.

• Port 119 (Network News Transfer Protocol) — Ten port jest używany do łączenia się z serwerem wiadomości w celu korzystania z grup dyskusyjnych.

• Port 135 (Remote Procedure Call) — Ten port, używany przez Microsoft RPC, jest krytyczny dla działania Microsoft Exchange Server i Active Directory, dostępnych w systemie Windows 2000 Server i nowszych.

• Port 139 (NetBIOS) — Ten port jest używany przez Microsoft NetBIOS Session Service do udostępniania zasobów.

• Port 143 (Internet Message Access Protocol 4) — IMAP4 używa tego portu do pobierania poczty e-mail.

Aktywność 2-2: Tworzenie serwera poczty za pomocą VirtualBox

Czas trwania: 45 minut

Cel: Utwórz serwer poczty w VirtualBox do wykorzystania w Aktywnościach 2-3 i 2-4.

Opis: Aktywności 2-3 i 2-4 wymagają użycia polecenia telnet w celu uzyskania dostępu do różnych portów serwera poczty. W tej aktywności utworzysz maszynę wirtualną serwera poczty za pomocą Oracle VirtualBox, bezpłatnego produktu do wirtualizacji, który może działać na wielu systemach operacyjnych.

Instalowanie VirtualBox i serwera poczty

1. Użyj przeglądarki internetowej, aby przejść do www.virtualbox.org/wiki/Downloads, aby pobrać i zainstalować VirtualBox

2. Kliknij łącze pobierania dla swojego systemu operacyjnego, takiego jak Windows hosts dla systemów Windows. Uruchom pobrany plik wykonywalny i wykonaj kroki, aby zainstalować VirtualBox. Jeśli potrzebujesz więcej wskazówek, poszukaj łącza do dokumentacji instalacji w lewym panelu strony pobierania.

UWAGA

Potrzebujesz pamięci masowej dla tworzonych maszyn wirtualnych, więc jeśli domyślna lokalizacja instalacji jest prawie pełna, zmień lokalizację na dysk z większą ilością miejsca.

3. Po pomyślnej instalacji otworzy się okno VirtualBox Manager

4. Przejdź do www.axigen.com/mail-server/download, przewiń w dół do sekcji Virtual Appliances, a następnie kliknij przycisk DOWNLOAD dla Axigen 10.3.3 VMWare/VirtualBox Image. Pobranie pliku Axigen może potrwać chwilę. Najnowszy numer wersji obrazu Axigen VMWare/VirtualBox mógł ulec zmianie. Wybierz najnowszą wersję.

5. Wypakuj urządzenie wirtualne (plik z rozszerzeniem .ova) z pobranego pliku zip.

6. W VirtualBox kliknij Plik na pasku menu, a następnie kliknij Importuj urządzenie. Przejdź do folderu zawierającego wyodrębniony plik .ova, kliknij plik .ova, a następnie kliknij przycisk Otwórz, aby zaimportować Axigen do VirtualBox. Wykonaj wszystkie dodatkowe czynności zalecane przez VirtualBox.

Konfigurowanie serwera poczty

1. W lewym panelu okna VirtualBox Manager kliknij urządzenie Axigen, takie jak axigen-centos-vM, kliknij Start na pasku narzędzi, a następnie kliknij Normalny start.

2. Po uruchomieniu urządzenia Axigen otworzy się okno przypominające . Zwróć uwagę na wyświetlany adres URL umożliwiający dostęp do interfejsu WebAdmin.

3. Postępuj zgodnie z instrukcjami, aby otworzyć przeglądarkę internetową, przejdź do adresu URL ebAdmin zanotowanego w kroku 2, zaakceptuj umowę licencyjną, a następnie ustaw hasło administratora. Użyj bezpiecznego i łatwego do zapamiętania hasła.

4. Na stronie Twoja licencja wybierz bezpłatną licencję, a następnie kliknij KONTYNUUJ, aby uruchomić wszystkie wymienione usługi.

5. Utwórz domenę e-mail o nazwie cyber.com, a następnie kliknij KONTYNUUJ, aby wyświetlić panel WebAdmin

6. W lewym panelu okna Dashboard kliknij Acceptance & Routing. Przewiń w dół i kliknij, aby odznaczyć pole wyboru Activate Greylisting, aby wyłączyć Greylisting. Kliknij przycisk Save conFiguration, aby zapisać tę zmianę.

UWAGA Jeśli Greylisting nie jest wyłączony, serwer Axigen odrzuci nieuwierzytelnione wiadomości e-mail, a Activity 2-3 nie będzie działać.

7. W lewym panelu okna Pulpitu kliknij Zarządzanie usługami, aby wyświetlić listę uruchomionych usług. Kliknij przycisk strzałki, aby uruchomić każdą usługę z wyjątkiem Proxy komunikatora internetowego i raportowania

8. W lewym panelu okna Zarządzanie usługami kliknij Odbieranie SMTP, aby upewnić się, że odbiorniki odbierające SMTP są włączone

UWAGA Włącz wszystkie odbiorniki; w przeciwnym razie działanie 2-3 nie zadziała.

9. W lewym panelu okna Odbieranie SMTP kliknij DOMENY I KONTA, a następnie kliknij Zarządzaj kontami, aby dodać konta do serwera Axigen, dzięki czemu będziesz mieć adresy e-mail do wykorzystania w Działaniach 2-3 i 2-4. Kliknij przycisk DODAJ KONTO, uzupełnij żądane informacje, a następnie kliknij SZYBKIE DODAWANIE.

Aktywność 2-3: Łączenie się z portem 25 (SMTP)

Czas trwania: 30 minut

Cel: Użyj polecenia telnet, aby uzyskać dostęp do portu 25 na serwerze pocztowym, zaloguj się i wyślij wiadomość e-mail do odbiorcy. Twoim serwerem pocztowym jest serwer Axigen skonfigurowany w Aktywności 2-2. Możesz spróbować użyć polecenia telnet na innym serwerze pocztowym (takim jak serwer w Twojej klasie lub serwer pocztowy Twojego dostawcy usług internetowych), jeśli reguły zapory uniemożliwiają Ci połączenie. Opis: Jako specjalista ds. bezpieczeństwa IT powinieneś znać porty używane w infrastrukturze sieciowej. Dobrym sposobem na sprawdzenie, czy usługa działa na serwerze, jest użycie polecenia telnet w celu uzyskania dostępu do portu za pomocą tej usługi. Na przykład usługa SMTP używa portu 25. W tej aktywności używasz usługi Telnet, aby uzyskać dostęp do serwera pocztowego Axigen z komputera z systemem Windows.

Aktywność 2-3: Łączenie się z portem 25 (SMTP)

Czas trwania: 30 minut

Cel: Użyj polecenia telnet, aby uzyskać dostęp do portu 25 na serwerze pocztowym, zaloguj się i wyślij wiadomość e-mail do odbiorcy. Twoim serwerem pocztowym jest serwer Axigen skonfigurowany w Aktywności 2-2. Możesz spróbować użyć polecenia telnet na innym serwerze pocztowym (takim jak serwer w Twojej klasie lub serwer pocztowy Twojego dostawcy usług internetowych), jeśli reguły zapory uniemożliwiają Ci połączenie. Opis: Jako specjalista ds. bezpieczeństwa IT powinieneś znać porty używane w infrastrukturze sieciowej. Dobrym sposobem na sprawdzenie, czy usługa działa na serwerze, jest użycie polecenia telnet w celu uzyskania dostępu do portu za pomocą tej usługi. Na przykład usługa SMTP używa portu 25. W tej aktywności używasz usługi Telnet, aby uzyskać dostęp do serwera pocztowego Axigen z komputera z systemem Windows.

UWAGA

Jeśli nie możesz połączyć się z serwerem pocztowym za pomocą poleceń w Działaniach 2-3 i 2-4, powinieneś mimo wszystko przeczytać kroki i przeanalizować rysunki, aby uzyskać wyobrażenie o tym, jak wygląda udane połączenie Telnet

UWAGA

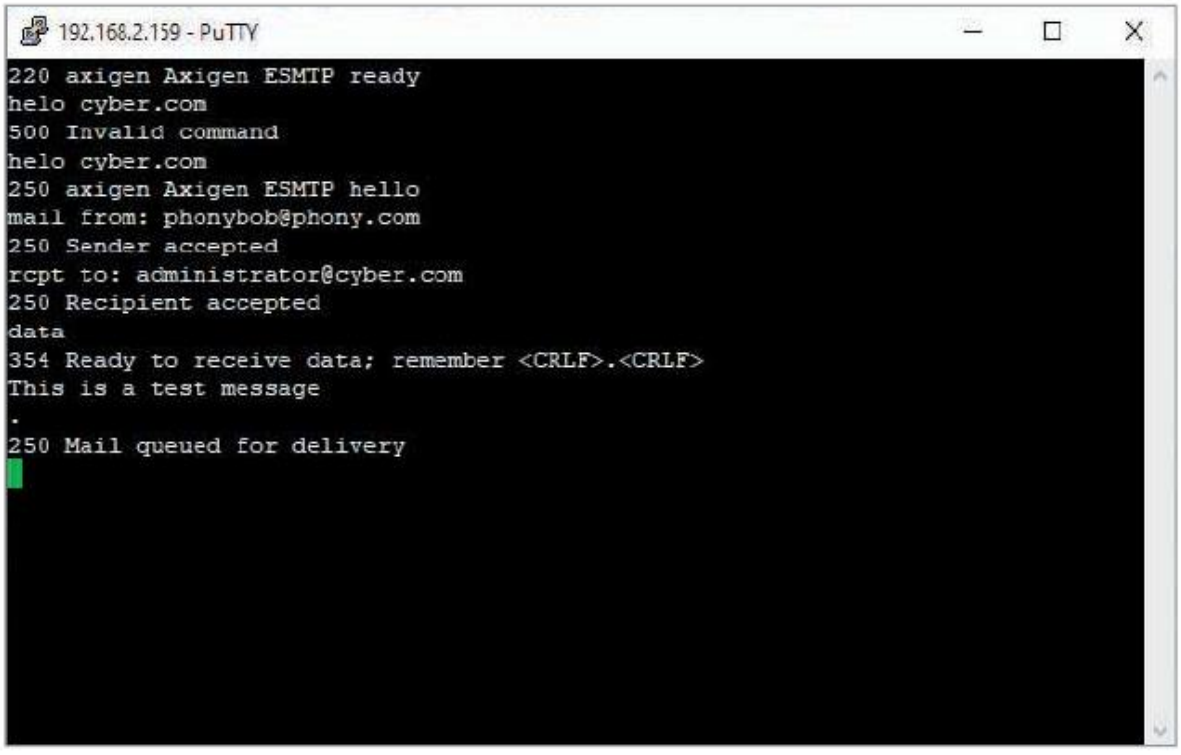
Poniższe kroki obejmują ogólny tekst zastępczy, taki jak LocalDomainName. Podczas wykonywania kroku zamień symbole zastępcze na konkretny tekst, taki jak rzeczywista nazwa domeny.

1. Telnet jest domyślnie wyłączony w większości instalacji systemu Windows, więc najprawdopodobniej będziesz musiał go włączyć. Otwórz Panel sterowania i kliknij Programy. W sekcji Programy i funkcje kliknij Włącz lub wyłącz funkcje systemu Windows. W oknie dialogowym Funkcje systemu Windows przewiń w dół i kliknij pole wyboru Klient Telnet . Możesz również wybrać inne usługi, które chcesz włączyć w tym momencie. Po zakończeniu kliknij OK, a następnie zamknij okno dialogowe Funkcje systemu Windows i Panel sterowania.

2. Aby otworzyć okno wiersza polecenia w systemie Windows 10, kliknij prawym przyciskiem myszy przycisk Start, a następnie kliknij Wiersz polecenia.

3. Wpisz telnet RemoteMailServer 25 (zastępując RemoteMailServer adresem IP serwera poczty e-mail Axigen skonfigurowanym w Ćwiczeniu 2-2). Naciśnij Enter. Musisz wprowadzić numer portu usługi, z którą próbujesz się połączyć. W tym przypadku używasz portu 25 dla SMTP. W wierszu poleceń wpisz helo LocalDomainName i naciśnij Enter. Zastąp LocalDomainName prawdziwą nazwą domeny. Serwer pocztowy akceptuje prawie wszystko, co wpiszesz po poleceniu helo, jako prawidłowe, ale powinieneś użyć domeny cyber.com utworzonej podczas konfigurowania Axigen.

4. Wpisz mail from: YourMailAccount i naciśnij Enter. Zastąp YourMailAccount swoim adresem e-mail, który jest wyświetlany w polu Od odbiorcy. Rysunek 2-11 przedstawia fałszywy adres e-mail, w jaki ktoś może podszyć się pod e-mail. Powinieneś otrzymać komunikat „250 OK”.



5. Wpisz rcpt to: RecipientMailAccount i naciśnij Enter. Zastąp RecipientMailAccount prawidłowym adresem e-mail, takim jak Twój własny adres, aby wysłać wiadomość do siebie w następnej czynności. Wiadomość e-mail nie zostanie faktycznie wysłana, jeśli RecipientMailAccount nie będzie prawidłowy. Powinieneś otrzymać komunikat „Recipient OK”.

6. Wpisz data i naciśnij Enter. Wpisz swoją wiadomość, naciśnij Enter, a następnie wpisz . (pojedyncza kropka) i naciśnij Enter, aby zakończyć wiadomość. Powinieneś otrzymać wiadomość informującą, że Twoja wiadomość e-mail została umieszczona w kolejce.

7. Wpisz quit i naciśnij Enter, aby zakończyć sesję Telnet. Możesz pozostawić okno wiersza poleceń otwarte do następnej czynności.

WSKAZÓWKA Jeśli popełnisz literówkę, musisz ponownie wprowadzić polecenia. Naciśnięcie Backspace lub użycie klawiszy strzałek nie edytuje poleceń.

Aktywność 2-4: Łączenie się z portem 110 (POP3)

Czas trwania: 30 minut

Cel: Użyj polecenia telnet, aby uzyskać dostęp do portu 110 na serwerze pocztowym, zaloguj się i pobierz wiadomość e-mail wysłaną na Twoje konto e-mail.

Opis: Usługa POP3 używa portu 110. W tej aktywności użyjesz polecenia telnet, aby uzyskać dostęp do serwera pocztowego z komputera z systemem Windows i pobrać wiadomość e-mail wysłaną do Twojej skrzynki pocztowej.

1. Otwórz okno wiersza polecenia, jeśli to konieczne.

2. Wpisz telnet RemoteMailServer 110 (zastępując RemoteMailServer adresem IP serwera pocztowego Axigen) i naciśnij Enter. Otrzymasz komunikat 1OK, wskazujący, że możesz się zalogować.

UWAGA Jeśli nie możesz połączyć się ze zdalnym serwerem pocztowym przez port 110 w kroku 2, zapora może blokować połączenie. Jeśli używasz serwera poczty Axigen, możesz zalogować się do serwera Axigen w VirtualBox i wykonać kroki 2–11 w tej czynności na serwerze Axigen z poziomu wiersza poleceń.

3. Wpisz user YourMailAccount (zastępując YourMailAccount prawidłową nazwą konta pocztowego) i naciśnij Enter, aby wprowadzić polecenie użytkownika w celu zalogowania się do konta

4. Wpisz pass YourPassword (zastępując YourPassword prawidłowym hasłem) i naciśnij Enter, aby wprowadzić swoje hasło.

5. Wpisz list i naciśnij Enter, aby wyświetlić listę wszystkich wiadomości w skrzynce pocztowej, w tym liczbę wiadomości

6. Wpisz retr 4 i naciśnij Enter, aby pobrać wiadomość numer 4

7. Wpisz quit i naciśnij Enter. To polecenie usuwa wszystkie wiadomości oznaczone do usunięcia, wylogowuje Cię z serwera pocztowego i kończy sesję Telnet.

8. Otwórz kolejne okno wiersza polecenia, wpisz netstat i naciśnij Enter, aby wyświetlić otwarte porty na komputerze z systemem Windows. 9. Jeśli wyniki nie pokazują żadnych otwartych aktywnych portów, spróbuj wpisać netstat -a i nacisnąć Enter. To polecenie wyświetla wszystkie połączenia i porty nasłuchujące w systemie. Zwróć uwagę na wiele wymienionych portów TCP i UDP.

10. Zminimalizuj okno wiersza polecenia i otwórz przeglądarkę internetową.

11. Połącz się z google.com. Zmaksymalizuj okno wiersza polecenia, wpisz ponownie netstat i naciśnij Enter. Zwróć uwagę na nowy wpis wskazujący, że port 443 (HTTPS) ma połączenie.

12. Zamknij okno wiersza polecenia i wszystkie inne otwarte okna.

Protokół User Datagram Protocol

Protokół User Datagram Protocol (UDP) to szybki, ale zawodny protokół dostarczania, który działa na warstwie transportowej. Wyobraź sobie, że próbujesz konkurować w branży kurierskiej i reklamujesz, że Twoja usługa jest szybka, ale zawodna. Prawdopodobnie trudno byłoby ją sprzedać. Jednak UDP jest szeroko stosowanym protokołem w Internecie ze względu na swoją szybkość. Nie musi weryfikować, czy odbiorca słucha lub jest gotowy do zaakceptowania pakietów. Nadawca nie przejmuje się tym — po prostu wysyła, nawet jeśli odbiorca nie jest gotowy do zaakceptowania pakietu. Widzisz, dlaczego jest szybszy? Niektóre aplikacje korzystające z UDP mają wbudowane narzędzia do ostrzegania odbiorców o niedostarczonych wiadomościach, ale UDP tego nie robi. Innymi słowy, polega na wyższych warstwach stosu TCP/IP, aby poradzić sobie z tymi problemami. Wyobraź sobie UDP jako kogoś ogłaszającego przez głośnik, że szkoła będzie zamknięta tego popołudnia. Niektórzy szczęśliwi uczniowie usłyszą wiadomość, a niektórzy nie. Ten typ protokołu dostarczania jest określany jako bezpołączeniowy.

Warstwa internetowa

Warstwa internetowa stosu TCP/IP odpowiada za kierowanie pakietów do adresu docelowego. Kierowanie odbywa się przy użyciu logicznego adresu, zwanego adresem IP. Podobnie jak UDP, dostarczanie pakietów z adresowaniem IP jest bezpołączeniowe.

Protokół ICMP (Internet Control Message Protocol)

Protokół ICMP (Internet Control Message Protocol) jest używany do wysyłania wiadomości związanych z operacjami sieciowymi. Na przykład, jeśli pakiet nie może dotrzeć do miejsca docelowego, możesz zobaczyć błąd „Destination Unreachable”. ICMP umożliwia specjalistom sieciowym rozwiązywanie problemów z łącznością sieciową (za pomocą polecenia ping) i śledzenie trasy, jaką pokonuje pakiet ze źródłowego adresu IP do docelowego adresu IP (za pomocą polecenia traceroute). Specjaliści ds. bezpieczeństwa mogą używać kodów typu ICMP (patrz Tabela 2-2), aby blokować pakiety ICMP przed wejściem do sieci lub wyjściem z niej.

Kod typu ICMP: Opis

0: Odpowiedź echa

3: Miejsce docelowe nieosiągalne

4: Wygaszenie źródła

5: Przekierowanie

6: Alternatywny adres hosta

8: Echo

9: Reklama routera

10: Żądanie routera

11: Przekroczony czas

12: Problem z parametrem

13: Znak czasu

14: Odpowiedź znacznika czasu

15: Żądanie informacji

16: Odpowiedź informacji

17: Żądanie maski adresu

18: Odpowiedź maski adresu

19: Zarezerwowane (dla bezpieczeństwa)

20–29: Zarezerwowane (dla eksperymentu odporności)

30: Traceroute

31: Błąd konwersji datagramu

32: Przekierowanie hosta mobilnego

33: Gdzie jesteś IPv6

34: Jestem tutaj IPv6

35: Żądanie rejestracji mobilnej

36 : Odpowiedź na rejestrację mobilną

37 : Żądanie nazwy domeny

38 : Odpowiedź na nazwę domeny

39 : Pomiń

40 : Photuris

41–255 : Zarezerwowane

Na przykład router można skonfigurować tak, aby nie zezwalał na wejście do sieci pakietowi ICMP z kodem typu 8. Spróbuj pingować www.microsoft.com i zobacz, co się stanie. Firma Microsoft nie zezwala na pingowanie swojego adresu IP, którego kod to 8 (Echo).

WSKAZÓWKA Bardziej szczegółowy opis protokołu ICMP można znaleźć w dokumencie RFC 792.

ADRESOWANIE IP

Adres IPv4 składa się z 4 bajtów podzielonych na dwa komponenty: adres sieciowy i adres hosta. Na podstawie początkowej liczby dziesiętnej pierwszego bajtu można klasyfikować adresy IP jako klasę A, klasę B lub klasę C, jak pokazano w tabeli .

Klasa adresu: Zakres: Bajty adresu: Liczba sieci: Bajty hosta: Liczba hostów

Klasa A: 1–126: 1: 126: 3: 16 777 214

Klasa B: 128–191: 2: 16 128: 2: 65 534

Klasa C: 192–223: 3: 2 097 152: 1: 254

BAJTY BEZPIECZEŃSTWA

Adres 127, którego brakuje w Tabeli , jest używany do pętli zwrotnej i testowania. Nie jest to prawidłowy adres IP, który można przypisać do urządzenia sieciowego. Adresy klasy D i klasy E są zarezerwowane do adresowania multicast i eksperymentalnego i nie są objęte tym modułem.

Korzystając z Tabeli , możesz na przykład ustalić, że użytkownik o adresie IP 193.1.2.3 ma adres klasy C, a użytkownik o adresie IP 9.1.2.3 ma adres klasy A. Adres IP składa się z 4 bajtów. Bajt jest równy 8 bitom. Osiem bitów można również nazwać oktetem, więc czasami adres IP jest definiowany jako cztery oktety zamiast 4 bajtów. Poniższa lista opisuje każdą klasę adresu:

• Klasa A - pierwszy bajt adresu klasy A jest zarezerwowany dla adresu sieciowego, dzięki czemu ostatnie 3 bajty są dostępne do przypisania komputerom hosta. Ponieważ adres klasy A ma trzyoktetowy adres hosta, sieci klasy A mogą obsługiwać ponad 16 milionów hostów. Liczba adresów klasy A jest ograniczona, więc te adresy są zarezerwowane dla dużych korporacji i rządów. Adresy klasy A mają format sieć.węzeł.węzeł.węzeł.

• Klasa B - te adresy są równo podzielone między dwuoktetowy adres sieciowy i dwuoktetowy adres hosta, co pozwala na ponad 65 000 hostów na adres sieciowy klasy B. Dużym organizacjom i dostawcom usług internetowych często przypisuje się adresy klasy B, które mają format sieć.sieć.węzeł.węzeł.

• Klasa C - te adresy mają trzyoktetowy adres sieciowy i jednooktetowy adres hosta, co daje ponad dwa miliony adresów klasy C. Każdy adres obsługuje do 254 hostów. Te adresy, zwykle dostępne dla małych firm i użytku domowego, mają format sieć.sieć.sieć.węzeł.

Podsieci umożliwiają administratorowi sieci podzielenie tych sieci na mniejsze segmenty. Użycie podsieci jest ważne zarówno ze względu na wydajność, jak i bezpieczeństwo. Oprócz unikalnego adresu sieciowego, każdej sieci musi zostać przypisana maska podsieci, która pomaga odróżnić bity adresu sieciowego od bitów adresu hosta. Rozważ następujący przykład. Adres IP 128.214.018.016 przedstawiony w systemie binarnym to 10000000.11010110.00010010.00010000

Jeśli zdefiniujesz maskę podsieci 255.255.255.0, zostanie ona wyrażona w systemie binarnym jako 11111111.11111111.11111111.00000000

Część podsieci adresu IP to

10000000.11010110.00010010

Adres hosta to

00010000

Możesz określić, do której podsieci należy adres IP, wykonując operację bitową AND na adresie IP i masce podsieci. Obliczenie to jest pionowe dla każdej kolumny. W przypadku operacji AND, jeśli oba bity mają wartość 1, wynikowa wartość wynosi 1. W przeciwnym razie wynikowa wartość wynosi 0.

10000000.11010110.00010010.00010000 AND

11111111.11111111.11111111.00000000 =

10000000.11010110.00010010.00000000

Obliczenie to daje podsieć 128.215.018.0, co oznacza, że oryginalny adres IP 128.214.018.016 z maską podsieci 255.255.255.0 należy do podsieci 128.214.018.0. Zrozumienie tych koncepcji jest istotne dla specjalisty ds. bezpieczeństwa, ale w Internecie można znaleźć wiele bezpłatnych kalkulatorów podsieci.

Notacja CIDR

IPv4 umożliwia około 4,3 miliarda unikalnych adresów IP. Brzmi to jak dużo adresów. Jednak wraz ze wzrostem liczby urządzeń podłączonych do Internetu, prawie wszystkie adresy IPv4 na świecie są w użyciu. Długoterminowym rozwiązaniem jest adresowanie IPv6. Jednym z krótkoterminowych rozwiązań było CIDR (Classless Inter-Domain Routing), które zostało opracowane w 1993 roku i pomogło przedłużyć żywotność IPv4, umożliwiając bardziej wydajną przestrzeń przypisywania adresów IP. Oto przykład podsieci w notacji CIDR: 192.168.1.0/24. W CIDR liczba po „/" jest prefiksem. Podsieć używająca prefiksu CIDR 24 jest analogiczna do podsieci klasy C. Prefiks CIDR /16 jest domyślną maską podsieci dla adresów klasy B, a prefiks CIDR /8 jest domyślną maską podsieci dla adresów klasy A. CIDR optymalizuje sposób, w jaki przestrzeń IP była przydzielana lub alokowana, dając inżynierom więcej opcji na dostosowanie rozmiaru przypisań. Przypisując /23 zawierające 512 adresów do organizacji, która wymaga 400 adresów IP, CIDR oszczędza ponad 65 000 adresów (prawie całą klasę B), które byłyby wymagane w ramach przypisania klasowego.

Planowanie przydziałów adresów IP

Kiedy firmy przydzielają adresy IP, muszą nadać unikalny adres IP każdemu segmentowi sieci oddzielonemu routerem. Na przykład, firmie przyznano dwa adresy IP: 193.145.85.0 i 193.145.86.0 (lub 193.145.85.0/24 i 193.154.86.0/24 w notacji CIDR). Patrząc na pierwszy bajt każdego adresu, firma ustala, że oba są adresami klasy C. Przy domyślnej masce podsieci 255.255.255.0, do każdego segmentu można przypisać 254 adresy hosta. Do tego obliczenia używasz wzoru 2x 2 2, gdzie x reprezentuje liczbę niezamaskowanych bitów. W tym przykładzie x jest równe 8, ponieważ w czwartym oktecie znajduje się 8 bitów:

$2^8 – 2 = 254$

Musisz odjąć 2 w formule, ponieważ część sieciowa i część hosta adresu IP nie mogą zawierać samych 1 ani samych 0. Pamiętaj, że nie możesz przypisać użytkownikowi sieci adresu IP 192.168.8.0, jeśli użyłeś maski 255.255.255.0. Ponadto nie możesz nadać użytkownikowi adresu 192.168.8.255, ponieważ spowodowałoby to wytworzenie samych 1 w części hosta adresu IP; ten adres jest zarezerwowany jako adres rozgłoszeniowy dla wszystkich węzłów w segmencie 192.168.8.0. Aby uzyskać dostęp do jednostek i usług w innych sieciach, każdy komputer musi również mieć adres IP swojej bramy. Przed wysłaniem pakietu do innego komputera warstwa internetowa TCP/IP używa maski podsieci komputera wysyłającego, aby określić adres sieciowy komputera docelowego. Jeśli ten adres jest inny niż adres sieciowy komputera wysyłającego, komputer wysyłający przekazuje pakiet na adres IP określony w parametrze bramy. Następnie komputer bramy przesyła pakiet do następnego miejsca docelowego. W ten sposób pakiet ostatecznie dociera do komputera docelowego. Na przykład, jeśli serwer Linux ma adres IP 192.168.8.2 i maskę podsieci 255.255.255.0, a użytkownik ma komputer o adresie IP 192.168.9.200 i masce podsieci 255.255.255.0, firma musi skonfigurować adres domyślnej bramy. Domyślna brama wysyła wiadomość do routera, który kieruje ją do innego segmentu sieci. Jeśli domyślna brama nie jest skonfigurowana na komputerze użytkownika, a użytkownik ten próbuje użyć polecenia ping, aby skontaktować się z serwerem, użytkownik otrzymuje komunikat „Destination Unreachable" (patrz Tabela 2-2). Komputer użytkownika nie może połączyć się z innym hostem — serwerem Linux znajdującym się w innym segmencie sieci — ponieważ nie ma routera, który mógłby mu pomóc. Zadaniem routera jest przyjmowanie pakietów przeznaczonych dla komputera w innym segmencie sieci niż komputer wysyłający i wysyłanie ich dalej. Specjaliści ds. bezpieczeństwa muszą zrozumieć te podstawowe koncepcje sieciowe, zanim podejmą próbę przeprowadzenia testu penetracyjnego w sieci, zwłaszcza takiej, która została podzielona na podsieci. W sieci podzielonej na podsieci łatwo pomylić adres rozgłoszeniowy z prawidłowym adresem hosta, co jest poważnym

błędem, który może spowodować atak typu „odmowa usługi” po wysłaniu tysięcy pakietów do wszystkich hostów w sieci zamiast do jednego hosta, do którego próbowałeś dotrzeć. Pamiętaj tylko, aby zweryfikować adres IP, do którego wysyłasz pakiety, zanim naciśniesz Enter.

Adresowanie IPv6

Jako specjalista ds. bezpieczeństwa powinieneś poświęcić trochę czasu na zapoznanie się z systemem adresowania IP Internet Protocol w wersji 6 (IPv6). Jak wspomniano, IPv4 nie został zaprojektowany z myślą o bezpieczeństwie, a wiele obecnych luk w sieci jest spowodowanych tym niedopatrzeniem. Ta sekcja zawiera podstawowe informacje o protokole IPv6, ale zaleca się zapoznanie się z dokumentem RFC 2460 (www.ietf.org/rfc/rfc2460. txt), aby uzyskać więcej szczegółów. Protokół IPv6 został opracowany w celu zwiększenia przestrzeni adresowej IP i zapewnienia dodatkowego bezpieczeństwa. Zamiast 4 bajtów używanych w protokole IPv4, protokół IPv6 używa 16 bajtów, czyli adresu 128-bitowego, więc dostępnych jest 2128 adresów — około 2000 adresów IP na każdy metr kwadratowy na planecie. Możesz pomyśleć, że tak wiele adresów IP nie jest koniecznych, ale będą one potrzebne do obsługi Internetu rzeczy (IoT). Wiele nowych produktów — takich jak tostery, kuchenki mikrofalowe, lodówki i telewizory — może być dostępnych przez Internet i wymaga adresów IP. Oto przykład numeru protokołu IPv6: 1111:0cb7:75a2:0110:1234:3a2e:1113:7777. Jeśli wydaje Ci się to dziwne, przegląd liczb szesnastkowych może odświeżyć Twoją pamięć. Dwukropki oddzielają każdą grupę czterech liczb szesnastkowych. Dobra wiadomość jest taka, że bycie skutecznym testerem bezpieczeństwa nie wymaga bycia ekspertem w tłumaczeniu lub zapamiętywaniu tych długich liczb. Jako tester bezpieczeństwa powinieneś wiedzieć, że wszystkie nowsze systemy operacyjne są skonfigurowane do obsługi protokołu IPv6, ale niektóre urządzenia filtrujące routery, zapory sieciowe i systemy wykrywania włamań (IDS) nie są. Umożliwia to hakerom omijanie tych systemów bezpieczeństwa za pomocą protokołu IPv6. W Internecie można znaleźć wiele artykułów omawiających słabości protokołu IPv4, IPv6 i protokołów, które je obsługują. Cyberprzestępcy spędzają godziny na czytaniu tego typu artykułów. Testerzy bezpieczeństwa również powinni.

Ćwiczenie 2-5: Praca z adresami IP i maskami podsieci

Czas trwania: 30 minut

Cel: Zastosuj swoją wiedzę na temat adresów IP i masek podsieci, aby odpowiedzieć na serię pytań dotyczących sieci.

Opis: Jako specjalista ds. bezpieczeństwa musisz rozumieć adresy IP, klasy i maski podsieci z wielu przydatnych powodów. Jednym z takich celów jest identyfikacja sieci, w której znajduje się określone urządzenie.

1. Zidentyfikuj klasy następujących adresów IP: 10.20.0.1, 172.16.42.42 i 192.168.255.255

2. Jaki jest odpowiednik notacji CIDR sieci 192.168.1.0 255.255.255.0?

3. Mając adres IP 192.168.1.128 i maskę podsieci 255.255.255.128, jaka jest część podsieci adresu i część hosta adresu?

4. Komputer A ma adres IP 192.168.1.10 i maskę podsieci 255.255.255.128. Komputer B ma adres IP 192.168.1.200 i maskę podsieci 255.255.255.128. Czy komputer A i komputer B znajdują się w tej samej podsieci?

5. Ile hostów może znajdować się w podsieci z maską podsieci 255.255.255.128?

6. Ile bitów ma adres IPv6?

PRZEGLĄD SYSTEMÓW LICZBOWYCH

Twoja wiedza na temat systemów liczbowych odgrywa rolę jako profesjonalisty ds. bezpieczeństwa. Poniższe sekcje oferują szybki przegląd systemów liczbowych binarnych, ósemkowych i szesnastkowych.

Przegląd systemu liczbowego binarnego

Nauczyłeś się matematyki dziesiętnej w szkole podstawowej, chociaż mogłeś nie zdawać sobie z tego sprawy w tamtym czasie. Kiedy widzisz na przykład liczbę 3742, rozpoznajesz ją jako „trzy tysiące siedemset czterdzieści dwa". Umieszczając każdą liczbę w kolumnie, jak pokazano w poniższych wierszach, możesz zobaczyć, że każda liczba ma inną wartość i wielkość. Ten system liczbowy używa 10 jako swojej podstawy i idzie od prawej do lewej, mnożąc liczbę podstawy w każdej kolumnie przez wykładnik, zaczynając od zera. Prawidłowe liczby w podstawie 10 to od 0 do 9. Oznacza to, że każda kolumna może zawierać dowolną liczbę od 0 do 9.

```
1000    100    10     1
10³     10²    10¹    10⁰
3       7      4      2
```

Jak widać, mnożąc 2 przez 1, 4 przez 10, 7 przez 100 i 3 przez 1000, a następnie dodając wszystkie te wartości, otrzymujemy 3742. Z drugiej strony, system liczbowy binarny używa 2 jako swojej podstawy. Każda cyfra binarna (bit) jest reprezentowana przez 1 lub 0. Bity są zwykle grupowane po osiem, ponieważ bajt zawiera 8 bitów. Inżynierowie komputerowi wybrali ten system liczbowy, ponieważ układy logiczne podejmują decyzje binarne na podstawie prawda lub fałsz, włączony lub wyłączony i podobnych warunków. Przy 8 bitach programista może przedstawić na przykład 256 różnych kolorów dla karty graficznej. (Dwa do potęgi ósmej, czyli 28, równa się 256.) Dlatego czerń można przedstawić jako 00000000, biel jako 11111111 i tak dalej. Innym przykładem użycia numeracji binarnej są uprawnienia użytkowników do plików: r (odczyt), w (zapis) i x (wykonywanie). 1 oznacza posiadanie uprawnienia, a 0 je usuwa. Dlatego 111 (rwx) oznacza, że obowiązują wszystkie uprawnienia, a 101 (r-x) oznacza, że użytkownik może odczytać i wykonać plik, ale nie może do niego zapisywać. (Symbol - oznacza, że uprawnienie nie zostało przyznane). Osoby zaznajomione z Uniksem rozpoznają ten system numeracji. Unix pozwala na używanie dziesiętnego odpowiednika liczb binarnych, więc dla binarnej liczby 111 wprowadzasz liczbę dziesiętną 7. Dla binarnej liczby 101 wprowadzasz liczbę dziesiętną 5. Jesteś zdezorientowany? Za kilka minut zostaniesz ekspertem od liczb binarnych, więc wytrzymaj. Aby uprościć koncepcję liczb binarnych, pomyśl o pokoju z dwoma przełącznikami światła i zastanów się, ile różnych kombinacji pozycji mógłbyś użyć dla przełączników. Na przykład oba przełączniki mogą być wyłączone, Switch 1 może być wyłączony, a Switch 2 może być włączony itd. Oto binarna reprezentacja tych pozycji przełączników:

```
0    0    (off, off)
0    1    (off, on)
1    0    (on, off)
1    1    (on, on)
```

Dwa przełączniki mają cztery możliwe wystąpienia, czyli 2x mocy; x oznacza liczbę dostępnych przełączników (bitów). W przypadku przełączników światła x równa się 2.

Przykłady określania wartości binarnych

Teraz, gdy zapoznałeś się z podstawowymi koncepcjami, możesz zobaczyć, jak bity są używane do zapisywania liczb binarnych. Najpierw jednak musisz nauczyć się i zapamiętać kolumny liczb binarnych, tak jak zrobiłeś to w przypadku numeracji dziesiętnej:

128 64 32 16 8 4 2 1

Od prawej do lewej liczby te oznaczają rosnące potęgi dwójki. Używając poprzednich kolumn, spróbuj określić wartość liczby binarnej 01000001:

128	64	32	16	8	4	2	1
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
0	1	0	0	0	0	0	1

Bajt w poprzednim przykładzie reprezentuje liczbę dziesiętną 65. Obliczasz tę wartość, dodając każdą kolumnę zawierającą 1 (64 1 1). Teraz wypróbuj inny przykład z liczbą binarną 11000001:

128	64	32	16	8	4	2	1
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1	1	0	0	0	0	0	1

Aby przekonwertować liczbę binarną na dziesiętną (podstawa 10), dodaj kolumny zawierające 1:

128 + 64 + 1 = 193

Dodawanie wartości w tych kolumnach może być żmudne, ale możesz nauczyć się kilku sztuczek, które pomogą Ci szybko przekonwertować liczbę binarną na dziesiętną. Pamiętaj jednak, aby zapamiętać każdą kolumnę binarną przed przejściem do pozostałych przykładów.

Zrozumienie Nibbles

Psychologowie odkryli, że ludzie mają trudności z zapamiętywaniem liczb siedmiocyfrowych lub większych. Ta trudność jest powodem, dla którego numery telefonów mają tylko siedem cyfr, a myślnik następuje po pierwszych trzech liczbach; myślnik daje mózgowi szansę na zatrzymanie się przed przejściem do następnych czterech liczb. Podobnie liczby binarne są łatwiejsze do odczytania, gdy są oddzielone spacją. Na przykład 1111 1010 jest łatwiejsze do odczytania niż 11111010. Jeśli musisz przekonwertować liczbę binarną zapisaną jako 11111010, powinieneś ją sobie wyobrazić jako 1111 1010. Innymi słowy, dzielisz bajt na dwa nibble (czasami pisane jako „nybbles”). Nibble to pół bajtu lub 4 bity. 4 bity po lewej stronie nazywane są nibblem wyższego rzędu, a 4 bity po prawej stronie to nibble niskiego rzędu. Poniższe przykłady pokazują, jak przekonwertować nibble niskiego rzędu na liczbę dziesiętną. Zwróć uwagę na wzór w liczbach binarnych, gdy przechodzisz przez przykłady:

```
0000 = 0
0001 = 1
0010 = 2
0011 = 3
0100 = 4
0101 = 5
0110 = 6
0111 = 7
1000 = 8
1001 = 9
1010 = 10
1011 = 11
1100 = 12
1101 = 13
1110 = 14
1111 = 15
```

Największa liczba dziesiętna, jaką możesz przedstawić za pomocą czterech bitów niższego rzędu, to 15. Powinieneś zapamiętać te liczby, jeśli możesz, zwłaszcza te, które mają wygodne pomoce pamięciowe. Na przykład 1010 jest równe liczbie dziesiętnej 10. Zapamiętaj tylko frazę „To 10, głuptasie, 10!" 1011 jest równie łatwe: „Nie 10, ale 11". Możesz wymyślić własne sztuczki, ale zawsze możesz po prostu dodać kolumny, jeśli zapomnisz. Możesz również ćwiczyć zamianę liczb dziesiętnych na liczby binarne, używając numerów tablic rejestracyjnych. Na przykład, jeśli numer tablicy rejestracyjnej kończy się na 742, powinieneś zwizualizować 0111, 0100, 0010. (Możesz wyeliminować zera wiodące po kilku dniach ćwiczeń). Kiedy poczujesz się komfortowo z nibblem niższego rzędu i będziesz w stanie szybko zidentyfikować sekwencję 4 bitów, możesz przejść do strony wyższego rzędu. Na przykład, ile wynosi liczba binarna 1010 1010 w systemie dziesiętnym? Po stronie niskiego rzędu możesz szybko przekonwertować 1010 na liczbę dziesiętną 10. Strona wyższego rzędu to również 10, ale to 10 razy 16, czyli 160. Następnie dodaj stronę niższego rzędu 10 do strony wyższego rzędu 160, aby uzyskać odpowiedź 170. Zawsze możesz dodać kolumny, jeśli jesteś zdezorientowany:

128 + 32 = 160

Każda wartość w półbajcie wyższego rzędu jest mnożona przez liczbę 16. Na przykład liczba binarna 0010 0000 jest równa 32. Możesz pomnożyć wartość półbajtu 2 przez 16, ale w tym przypadku łatwiej jest rozpoznać 1 w kolumnie 32, co daje odpowiedź 32. Powinieneś zapamiętać następujące wartości półbajtów wyższego rzędu, co pomoże Ci w podsieciach. Jak zapewne pamiętasz z podstaw podziału na podsieci, jako maski podsieci stosuje się numery 128, 192, 224 itd.

```
1000 = 128
1100 = 192
1110 = 224
1111 = 240
```

Jeśli rozpoznajesz 1111 0000 jako 240, liczba binarna 1111 1000 powinna być łatwa do obliczenia jako 248. Podobnie liczba binarna 1111 1111 jest równa dziesiętnej liczbie 255 lub 240 1 15, największej liczbie, jaką można przedstawić za pomocą 8 bitów.

UWAGA

Aby pomóc Ci poprawnie przekonwertować liczby, zwróć uwagę, że wszystkie liczby nieparzyste mają włączony bit najniższego rzędu. Na przykład 1001 nie może być liczbą parzystą, taką jak 10 lub 8, ponieważ bit najniższego rzędu jest włączony. Możesz również zgadnąć, że liczba jest większa niż 8,

ponieważ bit 8-kolumnowy jest włączony. Podobnie możesz zidentyfikować 0101 jako konwertowane na liczbę dziesiętną niższą niż 8, ponieważ kolumna 8 nie jest włączona i zidentyfikować ją jako liczbę nieparzystą, ponieważ bit najniższego rzędu jest włączony.

UWAGA

Możesz użyć innych prostych sposobów zapamiętywania i rozkładania liczb binarnych. Na przykład 1010 to 10, a 0101 to połowa 10: 5. Te dwie liczby są swoimi lustrzanymi odbiciami w systemie binarnym, a jedna liczba to połowa drugiej w systemie dziesiętnym. W ten sam sposób 1110 to 14, a 0111 to 7. W półbajcie wyższego rzędu 1110 to 224, a 0111 w półbajcie wyższego rzędu to 112 (połowa 224). Ta sztuczka pomaga szybko przekonwertować liczby binarne. Na przykład liczba binarna 0101 1010 to 90. W tej liczbie półbajt wyższego rzędu to 80, ponieważ 1010 to 160. Półbajt niższego rzędu to 10, a szybkie dodawanie daje ostateczną odpowiedź 90.

Przegląd systemu liczb ósemkowych

Liczba ósemkowa to liczba w systemie ósemkowym, więc jest zapisywana przy użyciu tych ośmiu wartości: 0, 1, 2, 3, 4, 5, 6 i 7. Ponieważ jesteś teraz ekspertem od liczb binarnych, łatwo jest zobaczyć, jak liczba binarna jest konwertowana na ósemkową. Cyfrę ósemkową można przedstawić za pomocą tylko 3 bitów, ponieważ największą cyfrą w systemie ósemkowym jest 7. Liczba 7 jest zapisywana jako 00000111 lub 111, jeśli usuniesz zera wiodące. Binarny odpowiednik liczby ósemkowej 5 to 101. Aby zobaczyć, jak ta koncepcja odnosi się do bezpieczeństwa sieci, spójrz ponownie na uprawnienia Uniksa. Numeracja ósemkowa jest używana do wyrażania następujących uprawnień do katalogu lub pliku: uprawnienia właściciela, uprawnienia grupy i inne uprawnienia. Ustawienie uprawnień (rwxrwxrwx) dla katalogu oznacza, że właściciel katalogu, członkowie grupy i wszyscy inni (inni) mają uprawnienia do odczytu, zapisu i wykonywania dla tego katalogu. Ponieważ każda kategoria ma trzy unikalne uprawnienia, a ponieważ każde uprawnienie można wyrazić jako prawda lub fałsz (włączone lub wyłączone), używane są 3 bity. Nie potrzebujesz wszystkich 8 bitów, ponieważ 3 bity (rwx) są wystarczające. Przypomnij sobie z numeracji binarnej, że 0 jest liczone jako liczba, więc przy 3 bitach istnieje osiem możliwych wystąpień: 000, 001, 010, 011, 100, 101, 110 i 111. Używając numeracji ósemkowej, 001 oznacza, że przyznano uprawnienie do wykonywania (x), 010 oznacza, że przyznano uprawnienie do zapisu (w), ale nie do odczytu i wykonywania itd. Liczba ósemkowa 7 oznacza same jedynki (111) lub 1 1 2 1 4. Tak więc w systemach Unix i Linux 777 (w systemie binarnym 111 111 111) oznacza, że właściciel, grupa i inni mają wszystkie uprawnienia (rwx) do pliku lub katalogu. Rysunek 2-17 przedstawia listę plików z ustawieniami uprawnień. Nazwy plików i katalogów opisują, co oznaczają ich ustawienia uprawnień.

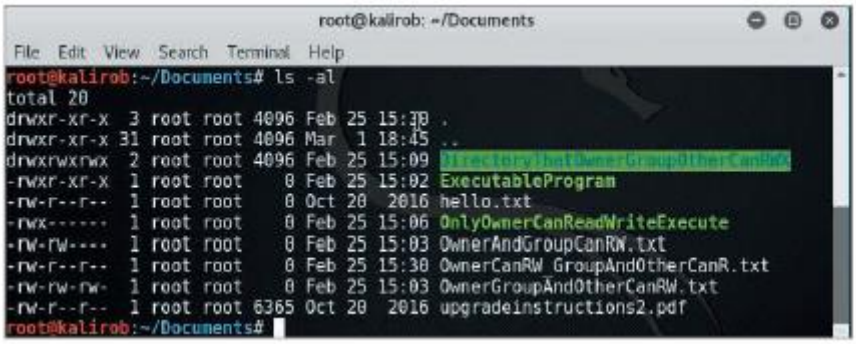


Tabela szczegółowo wyjaśnia uprawnienia

Nazwa pliku : Uprawnienia : Właściciel : Grupa : Inne : Opis

DirectoryThatOwnerGroupOtherCanRWX : drwxrwxrwx :rwx: rwx: rwx : Katalog z pełnymi uprawnieniami dla właściciela, grupy i innych

ExecutableProgram : rwxr-xr-x : rwx :r-x : r-x : Program wykonywalny, do którego

właściciel ma pełne uprawnienia — grupa i inni mogą wykonywać

hello.txt : rw-r—r-- : rw- : r-- : r-- : Plik niewykonywalny, który właściciel może

odczytować i zapisać — grupa i inni mogą tylko odczytywać

OnlyOwnerCanReadWriteExecute : rwx------ : rwx : --- : --- : Właściciel może

odczytować, zapisać i wykonać — grupa i inni nie mają uprawnienia

OwnerAndGroupCanRW.txt : rw-rw---- : rw- : rw- : --- : Właściciel i grupa

mogą czytać i pisać — inni nie mają uprawnień

OwnerCanRW_GroupAndOtherCanR.txt : rw-r—r-- : rw- : r-- : -- : Właściciel może czytać i pisać — grupa i inni mogą tylko czytać

OwnerGroupAndOtherCanRW.txt : rw-rw-rw- : rw- : rw- : rw- : rw- : Właściciel, grupa i inni mogą czytać i pisać — nikt nie może wykonywać

Zmiana uprawnień za pomocą polecenia chmod

W systemach Unix i Linux polecenie chmod umożliwia zmianę uprawnień plików i katalogów. Jest to przydatne, jeśli musisz nadać plikowi lub katalogowi więcej lub mniej uprawnień ze względów bezpieczeństwa. Możesz użyć polecenia chmod do zmiany uprawnień na dwa główne sposoby. Jednym ze sposobów jest podanie uprawnień jako liczby ósemkowej. Na przykład, aby zmienić uprawnienia pliku hello.txt tak, aby właściciel, grupa i inni członkowie mieli pełne uprawnienia do odczytu, zapisu i wykonywania, wprowadź następujące polecenie:

chmod 777 hello.txt

Pamiętaj, że ósemkowa liczba 7 w systemie binarnym to 111, co oznacza, że wszystkie bity r, w i x są włączone, co daje uprawnienia do odczytu, zapisu i wykonywania. Pierwsza liczba 7 w 777 daje właścicielowi pełne uprawnienia rwx, druga liczba 7 daje grupie pełne uprawnienia rwx, a ostatnia liczba 7 daje innym pełne uprawnienia rwx. Jeśli chcesz zmienić uprawnienia tak, aby inni użytkownicy nie mieli żadnych uprawnień do pliku hello.txt, użyj następującego polecenia:

chmod 770 hello.txt

Jeśli chcesz zmienić uprawnienia tak, aby właściciel miał uprawnienia do odczytu i zapisu, grupa miała uprawnienia do odczytu, a inni mieli uprawnienia do wykonywania, użyj następującego polecenia:

chmod 641 hello.txt

Pamiętaj, że polecenie chmod 641 hello.txt całkowicie zmienia wszystkie uprawnienia ustawione za pomocą polecenia chmod 770 hello.txt.

Oprócz podania pełnego trzycyfrowego numeru uprawnienia w systemie ósemkowym, polecenie chmod umożliwia określenie konkretnych zestawów uprawnień (właściciela, grupy lub innych) i włączenie lub wyłączenie poszczególnych uprawnień do odczytu, zapisu lub wykonywania. Aby to zrobić, musisz określić, dla kogo ustawiasz uprawnienia, jaką zmianę wprowadzasz (dodajesz lub

usuwasz uprawnienie) i jakie uprawnienie ustawiasz. To ukierunkowane podejście może okazać się wygodniejsze. Wartości „who”, których możesz użyć, to:

u: Użytkownik, oznaczający właściciela pliku

g: Grupa, oznaczająca członków grupy, do której należy plik

o: Inni, oznaczający osoby nieobjęte uprawnieniami u i g

a: Wszyscy, oznaczający wszystkie powyższe

Wartości „what”, których możesz użyć, to:

2 Znak minus, aby usunąć uprawnienie

1 Znak plus, aby przyznać uprawnienie

5 Znak równości, aby ustawić uprawnienie i usunąć inne.

Wartości „which”, których możesz użyć, to:

r: Uprawnienie do odczytu

w: Uprawnienie do zapisu

x: Uprawnienie do wykonywania

Na przykład, jeśli chcesz zmienić uprawnienia do pliku hello.txt, aby inni użytkownicy mogli ponownie mieć uprawnienia do odczytu, użyj następującego polecenia:

chmod o+r hello.txt

Aby odebrać uprawnienia do wykonywania członkom grupy, użyj następującego polecenia:

chmod g-x hello.txt

Przeglądanie systemu liczbowego heksadecymalnego

Liczba szesnastkowa (lub w skrócie hex) jest zapisywana za pomocą dwóch znaków, z których każdy reprezentuje nibble. System szesnastkowy to system liczbowy o podstawie 16, więc jego prawidłowe liczby mieszczą się w zakresie od 0 do 15. Podobnie jak system o podstawie 2 (binarny), hex używa wykładników, które zaczynają się od 0 i rosną od prawej do lewej:

4096	256	16	1
16^3	16^2	16^1	16^0
A	0	C	1

Na szczęście w systemie szesnastkowym musisz zapamiętać tylko dwie ostatnie kolumny: 1 i 16. Jak widać w poprzednim przykładzie, wartość zawiera znaki alfabetyczne — prawidłowe liczby szesnastkowe mieszczą się w zakresie od 0 do 15, a system szesnastkowy rozwiązuje problem wyrażania dwucyfrowych liczb w jednym slocie za pomocą liter. Na przykład A oznacza liczbę 10, B oznacza 11, C oznacza 12, D oznacza 13, E oznacza 14, a F oznacza 15. Liczby szesnastkowe są czasami wyrażane z „03” przed nimi. Na przykład 0x10 równa się liczbie dziesiętnej 16. Podobnie jak w przypadku liczb dziesiętnych i binarnych, mnożysz wartość w każdej kolumnie przez wartość kolumny, aby określić liczby szesnastkowe. W poprzednim przykładzie po prostu mnożysz 1 przez 16, aby uzyskać

16. Aby przekonwertować liczbę szesnastkową na binarną, wpisujesz każdy nibble od lewej do prawej. Na przykład 0310 to 0001 0000 w systemie binarnym, a 0324 to 0010 0100. Jako specjalista ds. bezpieczeństwa czasami musisz przeglądać dane wyjściowe z oprogramowania, które wyświetla wartości w postaci liczb szesnastkowych. Na przykład narzędzie tcpdump używa liczb szesnastkowych w większości swoich danych wyjściowych, zwłaszcza jeśli analizowane systemy używają protokołu IPv6. Jak wyjaśniono, wszystkie adresy IPv6 są w notacji szesnastkowej.

BAJTY BEZPIECZEŃSTWA

Czy znajomość systemu szesnastkowego może uratować ci życie, jeśli zostaniesz uwięziony na Marsie? Uwaga, spoiler: To zadziałało w przypadku postaci Matta Damona, astronauty Marka Watneya, w filmie Marsjanin z 2015 roku. Watney potrzebował sposobu na komunikację z NASA, który wykorzystywałby karty umieszczone wokół okręgu i kamerę obracającą się o 360 stopni. Jednak 26-znakowy alfabet stwarzał problemy z kątami kamery. Potrzebował mniejszego alfabetu. Na szczęście heksadecymalny ma tylko 16 znaków. Pisząc heksadecymalne znaki, które otrzymał z tabeli ASCII, zawierającej 255 znaków, mógł komunikować się z NASA. Na przykład litera A w ASCII jest równoważna 41 w heksadecymalnym. Wiele darmowych konwerterów ASCII na heksadecymalny jest dostępnych online. Możesz ich użyć, aby wprowadzić dwucyfrową liczbę heksadecymalną i uzyskać odpowiednik litery ASCII. (Jest jeden na stronie www.rapidtables.com/convert/number/ascii-to-hex.htm. Spróbuj napisać słowo HELP! w heksadecymalnym. Nie zapomnij o wykrzykniku.)

Przegląd systemu numeracji Base-64

Base-64 ma wiele zastosowań, zarówno legalnych, jak i nielegalnych. Typowym zastosowaniem bazy 64 jest kodowanie i przesyłanie plików binarnych wysyłanych pocztą e-mail. Wszystko, co musisz teraz wiedzieć, to to, że atakujący mogą używać bazy 64 na wiele sposobów, aby zaciemnić swoje działania.

Mapowania znaków bazy 64 przedstawiono w tabeli .

Znak lub symbol: Reprezentacja w bazie 64

Wielkie litery od A do Z: 0–25

Małe litery od a do z: –51

Cyfry od 0 do 9: 52–61

1 i / symbole: 62, 63

Aby przedstawić od 0 do 63 znaków, potrzebujesz tylko 6 bitów, czyli 26. Tak więc binarna reprezentacja litery A to 000000, B to 000001, C to 000010 itd. Z jest reprezentowane jako 011001. Pamiętaj tylko, że bit najwyższego rzędu to kolumna 32, a nie 128, jak w przypadku 8 bitów. Najniższa liczba, jaką możesz przedstawić za pomocą 6 bitów, to 000000 (0), a najwyższa to 111111 (63). Aby przekonwertować liczbę w systemie 64-bitowym na jej dziesiętny odpowiednik, po prostu podziel sekwencję na grupy po cztery znaki i przedstaw każdy znak za pomocą 6 bitów (24 bity -6 x 4).

Jako przykład, oto jak przekonwertować ciąg SGFwcHkgQmlydGh-kYXk5 w systemie base-64 na jego dziesiętny odpowiednik. W tym przykładzie pierwsze cztery znaki — S, G, F i w — są zapisane jako trzy 8-bitowe liczby (24 bity – 3 x 8).

1. Przekonwertuj wartość dziesiętną każdej litery na binarną:

S = 18 dziesiętny, binarny 010010

G = 6 dziesiętny, binarny 000110

F = 5 dziesiętny, binarny 000101

w = 48 dziesiętny, binarny 110000

2. Przepisz cztery grupy binarne na trzy grupy po 8 bitów. Na przykład, zaczynając od bitu niższego rzędu binarnego odpowiednika „w", zapisanie od prawej do lewej daje [01]110000. Liczby binarne w nawiasach reprezentują pierwsze dwa bity niższego rzędu z odpowiednika binarnego F, 1 i 0:

01001000 01100001 01110000

3. Przekształć liczbę binarną na jej odpowiednik dziesiętny:

01001000 = 72 ASCII H

01100001 = 97 ASCII a

01110000 = 112 ASCII p

Powtórz kroki od 1 do 3 dla następnych czterech liczb w systemie 64, cHkg, aż liczba w systemie 64 każdej litery zostanie przekonwertowana. (Używasz jednego lub dwóch znaków równości, gdy 3 bajty [24 bity] nie są potrzebne do przedstawienia liczby całkowitej). Na co konwertuje się ciąg w systemie 64? Twoja odpowiedź powinna brzmieć „Wszystkiego najlepszego z okazji urodzin". Dekodery w systemie 64 są dostępne bezpłatnie online. Jako specjalista ds. bezpieczeństwa nie musisz wiedzieć, jak ręcznie konwertować kod Base-64, ale ważne jest, aby wiedzieć, jak systemy numeracji są wykorzystywane w zastosowaniach praktycznych, a nie tylko w ćwiczeniach akademickich.

Ćwiczenie 2-6: Praca z numeracją binarną i ósemkową

Czas trwania: 30 minut

Cel: Zastosuj swoje umiejętności w zakresie numeracji binarnej i ósemkowej do konfigurowania uprawnień do katalogów i plików *nix.

Opis: Jako specjalista ds. bezpieczeństwa musisz rozumieć różne systemy numeracji. Na przykład, jeśli pracujesz z routerami, możesz musieć utworzyć listy kontroli dostępu (ACL), które filtrują przychodzący i wychodzący ruch sieciowy, a większość ACL wymaga zrozumienia numeracji binarnej. Podobnie, jeśli wzmacniasz system Linux, Twoja znajomość systemu binarnego pomoże Ci utworzyć prawidłową maskę umask i uprawnienia. Unix używa numeracji ósemkowej (ósemkowej) do tworzenia uprawnień do katalogów i plików. Nie musisz wykonywać tej czynności na komputerze; możesz po prostu użyć ołówka i papieru.

1. Napisz ósemkowe odpowiedniki następujących liczb binarnych: 100, 111, 101, 011 i 010.

2. Napisz, jak wyrazić uprawnienia właściciela *nix r-x w systemie binarnym. (Pamiętaj, że symbol - oznacza, że uprawnienie nie zostało przyznane.) Jaka jest ósemkowa reprezentacja obliczonej liczby binarnej? (Zakres liczb wyrażonych w systemie ósemkowym wynosi od 0 do 7. Ponieważ *nix ma trzy zestawy uprawnień, trzy zestawy 3 bitów binarnych logicznie reprezentują wszystkie możliwe uprawnienia.)

3. W numeracji binarnej i ósemkowej, jak wyrażasz udzielenie uprawnień do odczytu, zapisu i wykonywania właścicielowi pliku i żadnych uprawnień nikomu innemu?

4. W numeracji binarnej i ósemkowej, jak wyrażasz udzielenie uprawnień do odczytu, zapisu i wykonywania właścicielowi pliku; uprawnień do odczytu i zapisu grupie; i uprawnień do odczytu

innym? 5. W systemie Unix plik można utworzyć, używając umask, który umożliwia modyfikację domyślnych uprawnień dla pliku lub katalogu. Na przykład katalog ma domyślne uprawnienia ósemkowe 777. Jeśli administrator systemu Unix utworzy katalog z umask ósemkowym 020, jaki wpływ to ustawienie będzie miało na katalog? Wskazówka: Aby obliczyć rozwiązanie, możesz odjąć ósemkową wartość umask od ósemkowych domyślnych uprawnień.

6. Domyślne uprawnienia dla pliku w systemie Unix to ósemkowe 666. Jeśli plik zostanie utworzony z umask ósemkowym 022, jakie będą efektywne uprawnienia? Oblicz swoje wyniki.

PODSUMOWANIE MODUŁU

• TCP/IP jest najszerzej stosowanym protokołem do komunikacji przez Internet. Stos TCP/IP składa się z czterech warstw, które wykonują różne funkcje: Sieć, Aplikacja, Transport i Internet.

• Protokoły warstwy aplikacji są front-endem protokołów niższej warstwy. Przykładami protokołów działających na tej warstwie są HTTP, SMTP, Telnet i SNMP.

• Warstwa transportu odpowiada za kapsułkowanie danych w segmenty i używa nagłówków UDP lub TCP do zarządzania transmisją danych. TCP jest protokołem zorientowanym na połączenie. UDP jest protokołem bezpołączeniowym. TCP zapewnia gwarantowaną dostawę pakietów danych, ale jest wolniejszy niż UDP, który nie gwarantuje dostawy.

• Krytycznymi składnikami nagłówków segmentów TCP są flagi TCP, ISN oraz numery portów źródłowych i docelowych.

• Porty TCP identyfikują usługi działające w systemie. Numery portów od 1 do 1023 są uważane za dobrze znane porty. Łącznie dostępnych jest 65 535 numerów portów.

• Warstwa internetowa odpowiada za kierowanie pakietu do adresu docelowego. W tej warstwie używane są adresy IP, a także komunikaty ICMP. IP, podobnie jak UDP, jest protokołem bezpołączeniowym. ICMP jest używany do wysyłania komunikatów związanych z operacjami sieciowymi.

• Kod typu identyfikuje typ komunikatu ICMP i może być używany do filtrowania ruchu sieciowego.

• Adresy IP składają się z 4 bajtów, zwanych również oktetami, które są podzielone na dwa komponenty: adres sieciowy i adres hosta. W Internecie używane są trzy klasy adresów: A, B i C.

• Adresy IPv6 składają się z 16 bajtów i są zapisywane w notacji szesnastkowej.

• Urządzenia cyfrowe używają binarnego systemu numeracji głównie dlatego, że układy scalone Ogic podejmują decyzje binarne w oparciu o ustawienia prawda lub fałsz, włączony lub wyłączony, tak lub nie. Liczby binarne są reprezentowane przez 0 lub 1.

• Ósemkowy system liczbowy (podstawa 8) używa liczb od 0 do 7. Używa tylko 3 bitów binarnego systemu liczbowego, ponieważ najwyższą liczbą w podstawie 8 jest liczba 7, którą można zapisać za pomocą 3 bitów binarnych: 111.

• Systemy Unix i Linux używają ósemkowego systemu liczbowego do wyrażania ustawień uprawnień plików i katalogów. Możesz użyć polecenia chmod, aby dostosować ustawienia uprawnień.

• Szesnastkowy to szesnastkowy system liczbowy, który używa liczb od 0 do 15. Po 9 liczby 10, 11, 12, 13, 14 i 15 są reprezentowane jako A, B, C, D, E i F.

• Base64 to system liczbowy, który używa liczb od 0 do 63. Liczby od 0 do 61 są reprezentowane za pomocą znaków alfanumerycznych; 62 i 63 są symbolami.