Laboratorium - Zabezpieczenie urządzeń sieciowych
Topologia sieci

Tabela adresowania

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
R1	G0/0/1	192.168.1.1	255.255.255.0	nd.
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	karta sieciowa	192.168.1.3	255.255.255.0	192.168.1.1

Cele

Część 1: Konfiguracja podstawowych ustawień urządzenia

Część 2: Konfiguracja podstawowych zabezpieczeń routera

Część 3: Konfiguracja podstawowych zabezpieczeń przełącznika

Wprowadzenie

Zaleca się, aby wszystkie urządzenia sieciowe były skonfigurowane za pomocą co najmniej minimalnego zestawu poleceń oferującego najlepsze zabezpieczenia. Zalecenie dotyczy urządzeń końcowych (komputerów stacjonarnych), serwerów oraz urządzeń sieciowych takich jak routery i przełączniki.

W tym laboratorium będziesz skonfigurować urządzenia sieciowe znajdujące się w topologii w celu używania sesji SSH do zdalnego zarządzania. Będziesz używać również wiersza poleceń IOS CLI w celu konfigurowania środków bezpieczeństwa zgodnych z podstawowymi najlepszymi praktykami. Następnie będziesz testować środki bezpieczeństwa w celu sprawdzenia, czy są one właściwie realizowane i czy działają poprawnie.

Uwaga: Routery używane w praktycznych laboratoriach CCNA to Cisco 4221 z Cisco IOS XE wydanie 16.9.4 (obraz universalk9).Przełączniki używane w laboratoriach to Cisco Catalyst 2960 z Cisco IOS wydanie 15.2 (2) (obraz lanbasek9).Można użyć również innych routerów i przełączników Cisco z różnymi wersjami Cisco IOS. Zależnie od modelu urządzenia i wersji systemu IOS, dostępne polecenia i wyniki ich działania mogą się różnić od prezentowanych w niniejszej instrukcji. Przejrzyj tabelę podsumowującą interfejsy routera w celu określenia poprawnych identyfikatorów interfejsów.

Uwaga: Upewnij się, czy konfiguracje routerów oraz przełączników zostały wymazane i nie posiadają konfiguracji początkowej. Jeśli nie jesteś pewien, to poproś o pomoc instruktora.

\Wymagane zasoby

- 1 router (Cisco 4221 z uniwersalnym obrazem Cisco IOS XE Release 16.9.4 lub porównywalnym)
- 1 przełącznik (Cisco 2960 z systemem Cisco IOS wersja15.2 (2) obraz lanbasek9 lub porównywalny)
- 1 komputer PC (Windows z emulatorem terminala takim jak Tera Term)

- Kable konsolowe do konfiguracji urządzeń Cisco przez porty konsolowe
- Kable Ethernet zgodnie z przedstawioną topologią

Instrukcje

Część 1: Konfigurowanie podstawowych ustawień urządzenia

W części 1 będziesz tworzyć topologię sieci i konfigurować podstawowe ustawienia takie jak adresy IP dla interfejsu, dostęp do urządzenia oraz hasła urządzeń.

Krok 1: Zbuduj sieć zgodnie z topologią.

Połącz wymagane urządzenia oraz kable, tak jak pokazano na schemacie topologii.

Krok 2: Zainicjuj i zrestartuj router i przełącznik.

Krok 3: Skonfiguruj router i przełącznik.

a. Połącz się do konsoli urządzenia i przejdź do trybu uprzywilejowanego.

b. Przypisz nazwę urządzenia zgodnie z tabelą adresowania.

c. Wyłącz DNS lookup aby zapobiec próbom tłumaczenia przez router niepoprawnie wprowadzonych poleceń jako nazw hostów.

d. Przypisz class jako zaszyfrowane hasło trybu uprzywilejowanego EXEC.

e. Przypisz cisco jako hasło konsoli i włącz logowanie.

f. Przypisz cisco jako hasło do VTY oraz włącz logowanie.

g. Utwórz baner, który będzie ostrzegał osoby łączące się z urządzeniem, że nieautoryzowany dostęp jest zabroniony.

h. Skonfiguruj i włącz interfejs G0/0/1 w routerze przy użyciu informacji zawartych w tabeli adresowania.

i. Skonfiguruj domyślny SVI na przełączniku z informacjami o adresie IP zgodnie z tabelą adresowania.

j. Zapisz konfigurację bieżącą (running-configuration) jako plik konfiguracji startowej (startup-configuration).

Krok 4: Skonfiguruj PC-A.

a. Skonfiguruj adres IP i maskę podsieci dla komputera PC-A.

b. Skonfiguruj bramę domyślną dla komputera PC-A.

Krok 5: Sprawdzanie połączenia sieci.

Wykonaj ping z PC-A do R1 i S1. Jeżeli ping nie powiedzie się, to poszukaj rozwiązania problemu.

Część 2: Skonfiguruj podstawowe zabezpieczenia routera

Krok 1: Skonfiguruj środki bezpieczeństwa.

a. Zaszyfruj wszystkie hasła.

b. Skonfiguruj system tak, aby wymagał co najmniej 12-znakowego hasła.

c. Zmień hasła (uprzywilejowany exec, konsola i vty), aby spełnić nowe wymagania dotyczące długości.

1) Ustaw hasło dostępu do trybu uprzywilejowanego jako **$cisco!PRIV***.

2) Ustaw hasło konsoli jako **$cisco!!CON***.

3) Ustaw hasło terminala wirtualnego jako **$cisco!!VTY***

d. Skonfiguruj router tak, aby akceptował tylko połączenia SSH z lokalizacji zdalnych

   1) Skonfiguruj nazwę użytkownika **SShadmin** z zaszyfrowanym hasłem **55HAdm!n2020**

   2) Nazwa domeny routera powinna być ustawiona na ccna-lab.com

   3) Moduł klucza powinien wynosić 1024 bitów.

e. Ustaw konfiguracje zabezpieczeń i najlepszych praktyk na konsoli i liniach vty.

   1) Użytkownicy powinni zostać odłączeni po 5 minutach bezczynności.

   2) Router nie powinien zezwalać na logowanie vty przez 2 minuty, jeśli 3 nieudane próby logowania wystąpią w ciągu 1 minuty.

Część 3: Skonfiguruj środki bezpieczeństwa.

Krok 1: Sprawdź, czy wszystkie nieużywane porty są wyłączone.

Porty routera są wyłączone domyślnie, ale zawsze należy sprawdzić, czy wszystkie nieużywane porty są w stanie "administratively down". Można to szybko sprawdzić za pomocą polecenia **show ip interface brief**. Nieużywane porty, które nie są w stanie administracyjnym down powinny zostać wyłączone za pomocą polecenia **shutdown** w trybie konfiguracji interfejsu.

Krok 2: Sprawdź, czy środki bezpieczeństwa są właściwie zaimplementowane.

a. Użyj Tera Term aby połączyć do R1 za pomocą Telnet.

   Czy R1 akceptuje połączenie Telnet? Wyjaśnij.

b. Użyj programu Tera Term do zalogowania do R1 poprzez SSH.

   Czy R1 zaakceptował połączenie SSH?

c. Celowo błędnie wpisz dane użytkownika i hasło, aby sprawdzić, czy dostęp do logowania jest zablokowany po dwóch próbach.

   Co się stało po tym jak nie udało się zalogować po raz drugi?

d. Aby wyświetlić status logowania należy wykonać w konsoli routera polecenie **show login**. W poniższym przykładzie polecenie **show login** zostało wykonane w okresie blokowania (30 sekundowym) i pokazuje, że router jest w stanie Quiet-Mode. Router nie będzie przyjmował żadnych prób logowania przez okres 111 sekund.

e. Po upływie 120 sekund, użyj SSH ponownie do R1 i zaloguj się przy użyciu nazwy użytkownika **SSHadmin** i hasła **55HAdm!n2020**.

   Co pokazało się na ekranie po pomyślnym zalogowaniu się?

f. Przejdź do trybu uprzywilejowanego i użyj hasła **$cisco!PRIV***.

   Jeżeli popełnisz błąd w haśle, to czy zostaniesz odłączony od sesji SSH po dwóch nieudanych próbach w ciągu 60 sekund? Wyjaśnij.

g. Aby wyświetlić wykonane przez ciebie ustawienia zabezpieczeń, wykonaj polecenie **show running-config** w wierszu trybu uprzywilejowanego.

Część 4: Konfiguracja podstawowych zabezpieczeń przełącznika

Krok 1: Skonfiguruj środki bezpieczeństwa.

a. Zaszyfruj wszystkie hasła.

b. Skonfiguruj system tak, aby wymagał hasła z co najmniej 12 znaków

c. Zmień hasła (uprzywilejowany exec, konsola i vty), aby spełnić nowe wymagania dotyczące długości.

1) Ustaw hasło dostępu do trybu uprzywilejowanego jako **$cisco!PRIV***.

2) Ustaw hasło konsoli jako **$cisco!!CON***.

3) Ustaw hasło terminala wirtualnego jako **$cisco!!VTY***

d. Skonfiguruj przełącznik tak, aby akceptował tylko połączenia SSH z lokalizacji zdalnych.

1) Skonfiguruj nazwę użytkownika **SShadmin** z zaszyfrowanym hasłem **55HAdm!n2020**

2) Nazwa domeny przełączników powinna być ustawiona na ccna-lab.com

3) Moduł klucza powinien wynosić 1024 bitów.

e. Ustaw konfiguracje zabezpieczeń i najlepszych praktyk na konsoli i liniach vty.

1) Użytkownicy powinni zostać odłączeni po 5 minutach bezczynności.

2) Przełącznik nie powinien umożliwiać logowania przez 2 minuty, jeśli 3 nieudane próby logowania wystąpią w ciągu 1 minuty.

f. Wyłącz wszystkie nieużywane porty.

Krok 2: Sprawdź, czy wszystkie nieużywane porty są wyłączone.

Porty przełącznika są domyślnie włączone. Zamknij wszystkie porty, które nie są używane w przełączniku.

a. Możesz sprawdzić stan portów przełącznika za pomocą polecenia **show ip interface brief**.

b. Za pomocą polecenia **interface range** możesz wyłączać jednocześnie wiele interfejsów.

c. Upewnij się, że wszystkie nieaktywne interfejsy zostały administracyjnie wyłączone.

Krok 3: Sprawdź, czy środki bezpieczeństwa są właściwie zaimplementowane.

a. Sprawdź, czy usługa Telnet została wyłączona w przełączniku.

b. Połącz się do przełącznika przez SSH i celowo błędnie wpisz nazwę użytkownika i hasło, aby zobaczyć, czy dostęp do logowania jest zablokowany.

c. Po upływie 30 sekund, użyj SSH ponownie do S1 i zaloguj się przy użyciu nazwy użytkownika **SSHadmin** i hasła **55HAdm!n2020**.

Czy pokazał się baner na ekranie po pomyślnym zalogowaniu się?

d. Przejdź do uprzywilejowanego trybu EXEC, używając hasła **$cisco!PRIV***.

e. Aby wyświetlić wykonane przez ciebie ustawienia zabezpieczeń, wykonaj polecenie **show running-config** w wierszu trybu uprzywilejowanego.

Pytania do przemyślenia

1. W części 1 dotyczącej podstawowej konfiguracji dla konsoli i linii VTY zostało wpisane polecenie **password cisco**. Kiedy zostało to hasło użyte, czy po zaimplementowaniu zabezpieczeń według założeń dotyczących najlepszych praktycznych środków bezpieczeństwa?

2. Czy hasła wstępnie skonfigurowane i krótsze niż 10 znaków są analizowane przez polecenie **security passwords min-length 12**?

Tabela zbiorcza interfejsów routerów

Model routera	Interfejs Ethernet nr 1	Interfejs Ethernet nr 2	Interfejs szeregowy nr 1	Interfejs szeregowy nr 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Uwaga: Aby stwierdzić jak router jest skonfigurowany, spójrz na interfejsy, aby zidentyfikować typ routera oraz liczbę jego interfejsów. Nie ma jednego sposobu na skuteczne opisanie wszystkich kombinacji konfiguracji dla każdego modelu routera. Tabela zawiera identyfikatory możliwych kombinacji interfejsów Ethernet i Serial w urządzeniu. W tabeli nie podano żadnych innych rodzajów interfejsów, pomimo iż dany router może być w nie wyposażony. Przykładem takiego interfejsu może być ISDN BRI. Informacje umieszczone w nawiasach są dozwolonym skrótem, którego można używać w poleceniach IOS w celu odwołania się do interfejsu.