Packet Tracer - Zabezpieczanie urządzeń sieciowych

Tabela adresowania

Urządzenie	Interfejs	Adres	Maska	Brama
RTR-A	G0/0/0	192.168.1.1	255.255.255.0	nd.
	G0/0/1	192.168.2.1	255.255.255.0	nd.
SW-1	SVI	192.168.1.254	255.255.255.0	
PC	karta sieciowa	192.168.1.2	255.255.255.0	
Laptop	karta sieciowa	192.168.1.10	255.255.255.0	
Remote PC	karta sieciowa	192.168.2.10	255.255.255.0	

Wymagania

Uwaga: Aby to ćwiczenie było krótkie i łatwe w zarządzaniu, niektóre ustawienia konfiguracji zabezpieczeń nie zostały wprowadzone. Innymi słowy nie przestrzegane są najlepsze praktyki w zakresie bezpieczeństwa**.**

W tym ćwiczeniu skonfigurujesz router i przełącznik na podstawie listy wymagań.

Instrukcje

Krok1: Tworzenie dokumentacji sieci.

Uzupełnij tabelę adresową z brakującymi informacjami.

Krok2: Wymagania dotyczące konfiguracji routera:

- Zapobiegnij próbowaniu przez IOS odwzorowania błędnie wpisanych poleceń jako nazw domen.
- Nazwy hostów mają pasować do wartości w tabeli adresowania.
- Wymagaj, aby nowo utworzone hasła miały co najmniej 10 znaków długości.
- Zastosuj silne dziesięcioznakowe hasło dla linii konsoli. Użyj **@Cons1234!**
- Zapewnij, że konsola i sesje VTY zamkną się dokładnie po 7 minutach.
- Zastosuj silne, zaszyfrowane 10-znakowe hasło dla uprzywilejowanego trybu EXEC. W przypadku tego ćwiczenia dopuszczalne jest użycie tego samego hasła co na linii konsoli.
- Skonfiguruj baner MOTD ostrzegający o nieautoryzowanym dostępie do urządzeń.
- Zastosuj password encryption dla wszystkich haseł.
- Nazwa użytkownika **NetAdmin** z zaszyfrowanym hasłem **LogAdmin! 9**.
- Włącz SSH.
  - Użyj **security.com** jako nazwy domeny.
  - Użyj modułów długości **1024**.

- Linie VTY powinny używać SSH dla połączeń przychodzących.
- Linie VTY powinny używać nazwy użytkownika i hasła skonfigurowanego do uwierzytelniania.
- Utrudnij próby siłowego włamania za pomocą polecenia blokującego próby logowania przez 45 sekund, przy trzech nieudanych próbach w ciągu 100 sekund.

Krok3: Wymagania dotyczące konfiguracji przełącznika:

- Wszystkie nieużywane porty przełącznika powinny być wyłączone.
- Domyślny interfejs zarządzania SW-1 powinien akceptować połączenia z sieci. Skorzystaj z informacji pokazanych w tabeli adresowej. Przełącznik powinien być dostępny ze zdalnych sieci.
- Zastosuj słowo **@Cons1234!** jako hasło dostępu do trybu uprzywilejowanego EXEC.
- Skonfiguruj SSH, jak to zostało zrobione dla routera.
- Utwórz nazwę użytkownika **NETAdmin** z zaszyfrowanym tajnym hasłem **LogAdmin!9**
- Linie VTY powinny akceptować tylko połączenia SSH.
- Linie VTY powinny zezwalać na dostęp do interfejsu zarządzania przełącznikiem tylko z konta administratora sieci.
- Test ping z hostów obu sieci LAN powinny zakończyć się pomyślnie do interfejsu zarządzania przełącznikiem.