Packet Tracer - Konfiguracja bezpiecznych haseł i SSH

Tabela adresowania

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
RTA	G0/0	172.16.1.1	255.255.255.0	nd.
PCA	karta sieciowa	172.16.1.10	255.255.255.0	172.16.1.1
SW1	VLAN 1	172.16.1.2	255.255.255.0	172.16.1.1

Scenariusz

Administrator sieci poprosił o przygotowanie **RTA** i **SW1** do wdrożenia. Zanim zostaną one podłączone do sieci, muszą być włączone środki bezpieczeństwa.

Intrukcje

Krok 1: Skonfiguruj podstawowe zabezpieczenia na routerze

a. Skonfiguruj adresowanie IP na **PCA** zgodnie z tabelą adresowania.

b. Połącz się z konsolą RTA z terminala PCA.

c. Skonfiguruj nazwę hosta jako **RTA**.

d. Skonfiguruj adresowanie IP w **RTA** i włącz interfejs.

e. Zaszyfruj hasła zapisane jawnym tekstem.

```
RTA(config)# service password-encryption
```

f. Ustaw minimalną długość hasła na 10.

```
RTA(config)# security password min-length 10
```

g. Wymyśl i ustaw silne zaszyfrowane hasło. **Uwaga**: Wybierz hasło, które zapamiętasz, w przeciwnym razie będziesz musiał zresetować ćwiczenie, jeśli zablokujesz urządzenie.

h. Wyłącz rozwiązywanie nazw domenowych (DNS lookup).

```
RTA(config)# no ip domain-lookup
```

i. Ustaw nazwę domeny na **CCNA.com** (wielkość liter istotna dla punktacji w PT).

```
RTA(config)# ip domain-name CCNA.com
```

j. Utwórz konto użytkownika o dowolnej nazwie, zabezpieczone silnym hasłem.

```
RTA(config)# username any_user secret any_password
```

k. Wygeneruj 1024-bitowe klucze RSA.

Uwaga: W programie Packet Tracer wprowadź polecenie crypto key generate rsa, a następnie naciśnij Enter, aby kontynuować.

```
RTA(config)# crypto key generate rsa
The name for the keys will be: RTA.CCNA.com
Choose the size of the key modulus in the range of 360 to 2048 for your
```

```
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
```

l. Ustaw blokowanie na trzy minuty konta użytkownika, który w ciągu dwóch minut dokonał czterech nieudanych prób logowania.

```
RTA(config)# login block-for 180 attempts 4 within 120
```

m. Skonfiguruj wszystkie linie VTY dla dostępu SSH i użyj lokalnych profili użytkowników do uwierzytelnienia.

```
RTA(config)# line vty 0 4
RTA(config-line)# transport input ssh
RTA(config-line)# login local
```

n. Ustaw limit czasu w trybie EXEC na 6 minut na liniach VTY.

```
RTA(config-line)# exec-timeout 6
```

o. Zapisz konfigurację do NVRAM.

p. Uzyskaj dostęp do wiersza polecenia na pulpicie **PCA** , aby nawiązać połączenie SSH z **RTA** .

```
C:\> ssh /?
Packet Tracer PC SSH
Usage: SSH -l username target
C:\>
```

Krok 2: Skonfiguruj podstawowe zabezpieczenia na przełączniku

Skonfiguruj przełącznik **SW1** z odpowiednimi środkami bezpieczeństwa. Jeśli potrzebujesz dodatkowej pomocy, zapoznaj się z krokami konfiguracji routera.

a. Kliknij **SW1** i wybierz kartę **CLI**.

b. Skonfiguruj nazwę hosta jako **RTA**.

c. Skonfiguruj adresowanie IP w SW1 **VLAN1** i włącz interfejs.

d. Skonfiguruj adres IP bramy domyślnej.

e. Wyłącz wszystkie nieużywane porty.

Uwaga: Na przełączniku dobrą praktyką bezpieczeństwa jest wyłączanie nieużywanych portów. Jednym ze sposobów na to jest po prostu zamknięcie każdego portu za pomocą polecenia „**shutdown**”. Wymagałoby to dostępu do każdego portu indywidualnie. Istnieje metoda skrócona do wprowadzania modyfikacji do kilku portów naraz za pomocą polecenia **interface range** . W **SW1** wszystkie porty oprócz FastEthernet0/1 i GigabitEthernet0/1 można zamknąć za pomocą następującego polecenia:

```
SW1(config)# interface range F0/2-24, G0/2
SW1(config-if-range)# shutdown
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
<Output omitted>
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
```

W poleceniu wykorzystano zakres portów 2-24 dla portów FastEthernet, a następnie pojedynczy port GigabitEthernet0/2.

f. Zaszyfruj hasła zapisane jawnym tekstem.

g. Wymyśl i ustaw silne zaszyfrowane hasło.

h. Wyłącz rozwiązywanie nazw domenowych (DNS lookup).

i. Ustaw nazwę domeny na **CCNA.com** (wielkość liter istotna dla punktacji w PT).

j. Utwórz konto użytkownika o dowolnej nazwie, zabezpieczone silnym hasłem.

k. Wygeneruj 1024-bitowe klucze RSA.

l. Skonfiguruj wszystkie linie VTY dla dostępu SSH i użyj lokalnych profili użytkowników do uwierzytelnienia.

m. Ustaw limit czasu w trybie EXEC na 6 minut na wszystkich liniach VTY.

n. Zapisz konfigurację do NVRAM.