Packet Tracer – Konfigurowanie SSH

Topologia

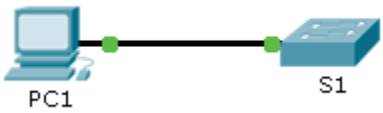

Tabela adresacji

Urządzenie	Interfejs	Adres IP	Maska podsieci
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	Karta sieciowa	10.10.10.10	255.255.255.0

Cele

Część 1: Zabezpieczanie haseł

Część 2: Szyfrowanie komunikacji

Część 3: Weryfikowanie implementacji SSH

Wprowadzenie

Protokół SSH powinien zastąpić Telnet przy zarządzaniu urządzeniami. Telnet przesyła dane w postaci niezabezpieczonej - jawnym tekstem. SSH zapewnia bezpieczeństwo zdalnych połączeń, szyfrując wszystkie dane transmitowane pomiędzy urządzeniami. W tym ćwiczeniu zabezpieczysz zdalny przełącznik za pomocą szyfrowania hasła i SSH.

Część 1: Zabezpieczanie haseł

a. Używając linii komend na **PC1**, wykonaj Telnet do **S1**. Hasło do trybu EXEC użytkownika oraz trybu uprzywilejowanego EXEC to **cisco**.

b. Zapisz bieżącą konfigurację, aby można było cofnąć ewentualne pomyłki, wyłączając i włączając zasilanie **S1**.

c. Wyświetl bieżącą konfigurację i zwróć uwagę, że hasła widać w sposób jawny. Wpisz komendę, która zaszyfruje hasła**: service password-encryption**

d. Sprawdź, czy hasła zostały zaszyfrowane.

Część 2: Szyfrowanie komunikacji

Krok 1: Ustaw nazwę domeny i wygeneruj klucze bezpieczeństwa.

Zwykle używanie Telnetu nie jest bezpieczne, ponieważ dane są przesyłane jawnym tekstem. W związku z tym używaj SSH, gdzie to tylko możliwe.

a. Skonfiguruj nazwę domeny jako **netacad.pka**.

b. Klucze bezpieczeństwa są potrzebne do zaszyfrowania danych. Wygeneruj klucze RSA używając długości klucza 1024.

Krok 2: Stwórz użytkownika i zmień konfigurację linii VTY, umożliwiając dostęp wyłącznie przez SSH.

a. Utwórz użytkownika **administrator** z hasłem **cisco**.

b. Skonfiguruj linie VTY, aby login i hasło były sprawdzane w lokalnej bazie użytkowników oraz aby pozwolić na dostęp tylko przez SSH. Usuń istniejące hasło z linii vty.

Część 3: Weryfikowanie implementacji SSH

a. Wyjdź z sesji Telnet i spróbuj zalogować się ponownie używając Telnetu. Nie powinno się udać.

b. Spróbuj zalogować się używając SSH. Wpisz **ssh** i naciśnij **Enter** bez żadnych parametrów, aby wyświetlić instrukcje użycia komendy. Uwaga: Opcja `-l` to litera "L", a nie cyfra 1.

c. Po udanym logowaniu, wejdź do trybu uprzywilejowanego EXEC i zapisz konfigurację. Jeśli nie możesz zalogować się do **S1**, to wyłącz i włącz zasilanie, a następnie zacznij ponownie od Części 1.