

Ćwiczenie 1 – Bezpieczeństwo na liniach VTY

Topologia



Tabela adresów:

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
R1	G0/1	192.168.x.1	255.255.255.0	n/d
R1	G0/0	172.16.x.1	255.255.255.252	n/d
PC-A	NIC	192.168.x.1x	255.255.255.0	192.168.x.1
PC-B	NIC	172.16.x.100	255.255.255.128	172.16.x.1
S1	VLAN 1	192.168.x.2	255.255.255.0	192.168.x.1

Wprowadzenie

Dobłą praktyką jest ograniczanie dostępu do interfejsów, przez które możliwe jest zarządzanie routerem np. port konsolowy czy linie vty. Listy kontroli dostępu mogą być użyte do zezwolenia na ruch z konkretnych adresów IP, zapewniając, że tylko administrator ma dostęp do routera poprzez Telnet lub SSH.

Podstawowa konfiguracja urządzeń:

1. Stwórz i zaadresuj topologię zgodnie z powyższym schematem
2. Wyłącz niepożądane zapytania DNS (DNS lookup)
3. Skonfiguruj nazwy urządzeń zgodnie z topologią (hostname)
4. Ustaw „*swoje imię*” jako hasło do trybu uprzywilejowanego EXEC
5. Ustaw *cisco* jako hasło do połączeń konsolowych i wymuś logowanie
6. Ustaw *sieci* jako hasło do połączeń wirtualnych w celu uruchomienia dostępu przez telnet i wymuś logowanie

Uwaga: SSH jest bezpieczniejszy od Telnetu; jednakże SSH wymaga aby urządzenia sieciowe były odpowiednio skonfigurowane. W tym ćwiczeniu Telnet używany jest dla wygody

7. Włącz szyfrowanie haseł
8. Ustaw baner MODT ostrzegający przed nieautoryzowanym dostępem
9. Zapisz bieżącą konfigurację urządzeń jako startową
10. Sprawdź czy komputery PC-A i PC-B pingują router i switch, sprawdź również czy możesz zrobić telnet z obu komputerów do routera i switcha.

Jeżeli wszystko działa można przejść dalej

Konfiguracja standardowej listy kontroli dostępu (ACL) na routerze:

1. Przygotuj ACL standardową (*access-list x*) umożliwiającą komputerowi PC-A dostęp do routera
2. Przypisz utworzoną ACL do wszystkich linii vty
3. Sprawdź, czy lista ACL działa poprawnie - oba komputery powinny odpowiadać na komunikaty ping do Router, ale tylko komputer PC-A powinien mieć dostęp poprzez usługę TELNET do tego routera
4. W trybie uprzywilejowanym routera R1 użyj komendy show ip access-lists i naciśnij Enter. Zauważ jak system IOS pokazuje liczbę poprawnych powiązań do danego wpisu ACE (w nawiasie).
5. Dodaj do swojej ACL na końcu wpis **deny any**
Uwaga: Ze względu na niejawną wpis deny any na końcu każdej listy nie ma potrzeby dodawania wyraźnego wpisu deny any. Jednakże wpis ten może być przydatny administratorowi w celu sprawdzenia ile razy wykonano połączenia, które zostały zablokowane.
6. Ponownie sprawdź usługę telnet na PC-A i PC-B
7. W trybie uprzywilejowanym użyj komendy show ip access-lists i naciśnij Enter. Powinny być teraz widoczne powiązania do wpisu deny any.

Wyzwanie – Konfiguracja list kontroli dostępu na przełączniku S1

1. Bez odnoszenia się do konfiguracji routera R1 spróbuj skonfigurować listę ACL nazywaną na przełączniku, zezwalającą na dostęp tylko z komputera PC-A
2. Przypisz listę ACL do linii vty przełącznika S1.
3. Połącz się do przełącznika przy użyciu protokołu Telnet z każdego z komputerów w celu sprawdzenia czy listy ACL działają poprawnie. Powinieneś połączyć się tylko z komputera PC-A, z komputera PC-B nie.