Laboratorium – Zabezpieczanie urządzeń sieciowych

Topologia

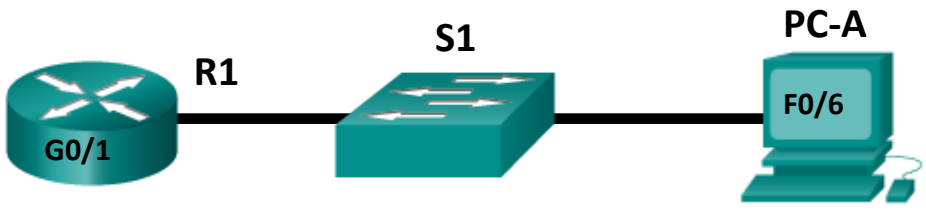

Tabela adresacji

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
R1	G0/1	192.168.1.1	255.255.255.0	Nie dotyczy
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

Scenariusz

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 laboratorium CCNA to Cisco 1941 ISR (Integrated Services Routers) z oprogramowaniem Cisco IOS 15.2(4)M3 (obraz universalk9). Przełączniki używane w laboratorium to Cisco Catalyst 2960 z oprogramowaniem Cisco IOS 15.0(2) (obraz lanbasek9). Inne routery, przełączniki i wersje systemu IOS również mogą być użyte. Zależnie od modelu urządzenia i wersji systemu IOS dostępne polecenia i wyniki ich działania mogą się różnic od prezentowanych w niniejszej instrukcji. Identyfikatory interfejsów znajdują się w tabeli interfejsów routerów na końcu tej instrukcji.

Uwaga: Upewnij się, że konfiguracje routerów i przełączników zostały usunięte i nie mają konfiguracji startowej. Jeśli nie jesteś pewien, poproś o pomoc instruktora.

Wymagane wyposażenie

- 1 Router (Cisco 1941 z systemem Cisco IOS wersja15.2(4)M3 uniwersalny lub porównywalny obraz)

- 1 przełącznik (Cisco 2960 Cisco IOS wersja15.0(2) obraz lanbasek9 lub porównywalny)
- 1 komputer PC (system Windows 7, Vista, lub XP z emulatorem terminala Tera Term)
- Kable konsolowe do konfiguracji urządzeń Cisco przez porty konsolowe
- Kable Ethernet zgodnie z pokazaną topologią

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 w routerze.

Krok 1: Połącz okablowanie zgodnie z topologią.

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

Krok 2: Uruchom i zrestartuj router i przełącznik.

Krok 3: Skonfiguruj router.

Skorzystaj z poprzedniego laboratorium jeśli potrzebujesz pomocy dotyczącej poleceń wymaganych dla SSH.

a. Połącz się przy użyciu konsoli z routerem i przejdź do uprzywilejowanego trybu EXEC.

b. Wejdź do trybu konfiguracji globalnej.

c. Ustaw nazwę routera jako R1.

d. Wyłącz wyszukiwanie DNS (DNS lookup), aby zapobiec próbom tłumaczenia niepoprawnie wprowadzonych poleceń.

e. Jako zaszyfrowane hasło trybu uprzywilejowanego ustaw **class** .

f. Jako hasło dostępu do konsoli ustaw **cisco** oraz włącz logowanie.

g. Jako hasło do VTY ustaw **cisco** oraz włącz logowanie.

h. Zaszyfruj wszystkie hasła podane otwartym tekstem.

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

j. Skonfiguruj i włącz interfejs G0/1 w routerze przy użyciu informacji zawartych w tabeli adresacji.

k. Zapisz konfigurację bieżącą do pliku konfiguracji startowej.

Krok 4: Skonfiguruj przełącznik.

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

b. Wejdź do trybu konfiguracji globalnej.

c. Ustaw nazwę przełącznika jako S1.

d. Wyłącz wyszukiwanie DNS (DNS lookup), aby zapobiec próbom tłumaczenia niepoprawnie wprowadzonych poleceń.

e. Jako zaszyfrowane hasło trybu uprzywilejowanego ustaw **class** .

f. Jako hasło dostępu do konsoli ustaw **cisco** oraz włącz logowanie.

g. Jako hasło do VTY ustaw **cisco** oraz włącz logowanie.

h. Zaszyfruj wszystkie hasła podane otwartym tekstem.

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

j. Skonfiguruj domyślny interfejs SVI za pomocą adresu IP znajdującego się w tabeli adresacji.

k. Zapisz konfigurację bieżącą do pliku konfiguracji startowej.

Część 2: Skonfiguruj podstawowe zabezpieczenia routera

Krok 1: Utwórz silne hasła.

Administrator powinien upewnić się, że hasła spełniają podstawowe standardowe założenia dotyczące silnych haseł. Założenia te mogą obejmować kombinacje liter, cyfr i znaków specjalnych w haśle oraz ustawienie minimalnej długości hasła.

Uwaga: Założenia dotyczące najlepszych praktyk w tym względzie wymagają stosowania silnych haseł, takich jak te pokazane tutaj, w środowisku produkcyjnym. Laboratoria w tym kursie używają haseł cisco i class, tylko w celu ułatwienia wykonywania ćwiczeń.

a. Zmień zaszyfrowane hasło trybu uprzywilejowanego tak aby spełnić założenia.

```
R1(config)# enable secret Enablep@55
```

b. Ustaw wymaganą długość dla wszystkich haseł na co najmniej 10 znaków .

```
R1(config)# security passwords min-length 10
```

Krok 2: Włącz połączenia SSH.

a. Ustaw nazwę domeny jako **CCNA-lab.com**.

```
R1(config)# ip domain-name CCNA-lab.com
```

b. Utwórz użytkownika w lokalnej bazie danych, który będzie używany do połączenia się z routerem poprzez SSH. Hasło powinno spełniać wysokie wymagania dotyczące standardów haseł a użytkownik powinien mieć dostęp do poziomu administratora.

```
R1(config)# username admin privilege 15 secret Admin15p@55
```

c. Skonfiguruj opcję "transport input" dla linii VTY tak aby one akceptowały połączenia SSH, ale nie pozwalały na połączenia Telnet.

```
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
```

d. Linie VTY powinny używać lokalnej bazy danych użytkowników do uwierzytelnienia.

```
R1(config-line)# login local
R1(config-line)# exit
```

e. Wygeneruj klucz szyfrujący RSA używając 1024 bity.

```
R1(config)# crypto key generate rsa modulus 1024
The name for the keys will be: R1.CCNA-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)

R1(config)#
*Jan 31 17:54:16.127: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Krok 3: Zabezpiecz konsolę i linie VTY.

f. Możesz ustawić router tak aby nastąpiło wylogowanie z połączenia po upływie określonego czasu bezczynności. Jeżeli administrator sieci był zalogowany do urządzenia sieciowego i został nagle gdzieś wezwany, to to polecenie automatycznie wylogowuje użytkownika po upływie określonego czasu. Następujące polecenia powodują automatyczne wylogowanie z konsoli po pięciu minutach bezczynności.

```
R1(config)# line console 0
R1(config-line)# exec-timeout 5 0
R1(config-line)# line vty 0 4
R1(config-line)# exec-timeout 5 0
R1(config-line)# exit
R1(config)#
```

g. Następujące polecenia utrudniają próby logowania za pomocą ataku siłowego. Router blokuje możliwość logowania przez czas 30 sekund, jeśli ktoś w ciągu 120 sekund dwa razy poda złe hasło. Czas ustawiony został specjalnie jako niski dla celów tego ćwiczenia.

```
R1(config)# login block-for 30 attempts 2 within 120
```

Co oznacza liczba **2 w odniesieniu do liczby 120** w powyższym poleceniu?

_____

Co oznacza **block-for 30** w powyższym poleceniu?

_____

Krok 4: Sprawdź, czy wszystkie nieużywane porty są wyłączone.

Porty routera są wyłączone domyślnie, ale zawsze należy sprawdzić, czy wszystkie nieużywane porty są w stanie administracyjnym "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.

```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet0/1         192.168.1.1     YES manual up                    up
Serial0/0/0                unassigned      YES NVRAM  administratively down down
Serial0/0/1                unassigned      YES NVRAM  administratively down down
R1#
```

Krok 5: Sprawdź, czy środki bezpieczeństwa są właściwie zaimplementowane.

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

Czy R1 zaakceptował połączenie przez Telnet? _____

Dlaczego tak się stało?

_____

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

Czy R1 zaakceptował połączenie SSH? _____

c. Jeżeli celowo błędnie wpiszesz użytkownika i hasło, aby zobaczyć, czy jest zablokowany dostęp logowania będzie 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". Router nie będzie przyjmował żadnych prób logowania przez okres 14 sekund.

```
R1# show login
     A default login delay of 1 second is applied.
     No Quiet-Mode access list has been configured.

     Router enabled to watch for login Attacks.
     If more than 2 login failures occur in 120 seconds or less,
     logins will be disabled for 30 seconds.

     Router presently in Quiet-Mode.
     Will remain in Quiet-Mode for 14 seconds.
     Denying logins from all sources.
R1#
```

e. Po 30 sekundach wygasła blokada i można zalogować się przez SSH do R1 ponownie za pomocą nazwy użytkownika **admin** oraz hasła **Admin15p@55**.

Co pokazało się na ekranie po pomyślnym zalogowaniu się? _____

f. Przejdź do trybu uprzywilejowanego i użyj hasła **Enablep@55**.

Jeżeli popełnisz błąd w haśle, to czy zostaniesz odłączony od sesji SSH po dwóch nieudanych próbach w ciągu 120 sekund, ? _____

Dlaczego tak albo dlaczego nie?

_____

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

Część 3: Konfiguracja podstawowych zabezpieczeń przełącznika

Krok 1: Utwórz silne hasła dla przełącznika.

Zmień zaszyfrowane hasło trybu uprzywilejowanego tak aby spełnić założenia dotyczące silnych haseł.

```
S1(config)# enable secret Enablep@55
```

Uwaga: Polecenie **password min-length** nie jest dostępne w przełączniku 2960.

Krok 2: Włącz połączenia SSH.

a. Ustaw nazwę domeny jako **CCNA-lab.com**.

```
S1(config)# ip domain-name CCNA-lab.com
```

b. Utwórz użytkownika w lokalnej bazie danych, który będzie używany do połączenia się z routerem poprzez SSH. Hasło powinno spełniać wysokie wymagania dotyczące standardów haseł a użytkownik powinien mieć dostęp do poziomu administratora.

```
S1(config)# username admin privilege 15 secret Admin15p@55
```

c. Skonfiguruj opcję "transport input" dla linii VTY tak aby one akceptowały połączenia SSH, ale nie pozwalały na połączenia Telnet.

```
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
```

d. Linie VTY powinny używać lokalnej bazy danych użytkowników do uwierzytelnienia.

```
S1(config-line)# login local
S1(config-line)# exit
```

e. Wygeneruj klucz szyfrujący RSA używając 1024 bity.

```
S1(config)# crypto key generate rsa modulus 1024
```

Krok 3: Zabezpiecz konsolę i linie VTY.

f. Możesz ustawić przełącznik tak aby nastąpiło wylogowanie z połączenia po upływie czasu bezczynności 10 minut.

```
S1(config)# line console 0
S1(config-line)# exec-timeout 10 0
S1(config-line)# line vty 0 15
S1(config-line)# exec-timeout 10 0
S1(config-line)# exit
S1(config)#
```

g. Aby utrudnić próby logowania za pomocą ataków brutalnych, skonfiguruj przełącznik tak, aby blokował możliwość logowania przez czas 30 sekund, po 2 próbach logowania w ciągu 120 sekund. Czas ustawiony został specjalnie jako niski dla celów tego ćwiczenia.

```
S1(config)# login block-for 30 attempts 2 within 120
S1(config)# end
```

Krok 4: 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** .

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.11    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  down                  down
FastEthernet0/2        unassigned      YES unset  down                  down
FastEthernet0/3        unassigned      YES unset  down                  down
FastEthernet0/4        unassigned      YES unset  down                  down
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  down                  down
FastEthernet0/8        unassigned      YES unset  down                  down
FastEthernet0/9        unassigned      YES unset  down                  down
FastEthernet0/10       unassigned      YES unset  down                  down
FastEthernet0/11       unassigned      YES unset  down                  down
FastEthernet0/12       unassigned      YES unset  down                  down
FastEthernet0/13       unassigned      YES unset  down                  down
FastEthernet0/14       unassigned      YES unset  down                  down
```

```
FastEthernet0/15       unassigned      YES unset  down                  down
FastEthernet0/16       unassigned      YES unset  down                  down
FastEthernet0/17       unassigned      YES unset  down                  down
FastEthernet0/18       unassigned      YES unset  down                  down
FastEthernet0/19       unassigned      YES unset  down                  down
FastEthernet0/20       unassigned      YES unset  down                  down
FastEthernet0/21       unassigned      YES unset  down                  down
FastEthernet0/22       unassigned      YES unset  down                  down
FastEthernet0/23       unassigned      YES unset  down                  down
FastEthernet0/24       unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  down                  down
GigabitEthernet0/2     unassigned      YES unset  down                  down
S1#
```

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

```
S1(config)# interface range f0/1-4 , f0/7-24 , g0/1-2
S1(config-if-range)# shutdown
S1(config-if-range)# end
S1#
```

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

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.11    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
FastEthernet0/2        unassigned      YES unset  administratively down down
FastEthernet0/3        unassigned      YES unset  administratively down down
FastEthernet0/4        unassigned      YES unset  administratively down down
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  administratively down down
FastEthernet0/8        unassigned      YES unset  administratively down down
FastEthernet0/9        unassigned      YES unset  administratively down down
FastEthernet0/10       unassigned      YES unset  administratively down down
FastEthernet0/11       unassigned      YES unset  administratively down down
FastEthernet0/12       unassigned      YES unset  administratively down down
FastEthernet0/13       unassigned      YES unset  administratively down down
FastEthernet0/14       unassigned      YES unset  administratively down down
FastEthernet0/15       unassigned      YES unset  administratively down down
FastEthernet0/16       unassigned      YES unset  administratively down down
FastEthernet0/17       unassigned      YES unset  administratively down down
FastEthernet0/18       unassigned      YES unset  administratively down down
FastEthernet0/19       unassigned      YES unset  administratively down down
FastEthernet0/20       unassigned      YES unset  administratively down down
FastEthernet0/21       unassigned      YES unset  administratively down down
FastEthernet0/22       unassigned      YES unset  administratively down down
FastEthernet0/23       unassigned      YES unset  administratively down down
FastEthernet0/24       unassigned      YES unset  administratively down down
GigabitEthernet0/1     unassigned      YES unset  administratively down down
```

```
GigabitEthernet0/2     unassigned      YES unset  administratively down down
S1#
```

Krok 5: 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 30 sekundach wygasła blokada i można zalogować się przez SSH do S1 ponownie za pomocą nazwy użytkownika **admin** oraz hasła **Admin15p@55**.

Czy pokazał się baner na ekranie po pomyślnym zalogowaniu się? _____

d. Przejdź do trybu uprzywilejowanego i użyj hasła **Enablep@55**.

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

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 10**?

_____

_____

_____

Tabela zbiorcza interfejsów routera

Zestawienie interfejsów routera				
Model routera	**Interfejs Ethernet #1**	**Interfejs Ethernet #2**	**Interfejs Serial #1**	**Interfejs Serial #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 (S0/0/0)	Serial 0/1/1 (S0/0/1)
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)
Uwaga: Aby stwierdzić jak router jest skonfigurowany, spójrz na interfejsy aby zidentyfikować typ routera oraz liczbę jego interfejsów. Nie ma sposobu na skuteczne opisanie wszystkich kombinacji konfiguracji dla każdej klasy routera. Ta tabela zawiera identyfikatory możliwych kombinacji interfejsów Ethernet oraz interfejsów Serial w urządzeniu. W tabeli nie podano żadnych innych rodzajów interfejsów, mimo iż dany router może być w nie wyposażony. Przykładem może być interfejs ISDN BRI. Informacja w nawiasach jest dozwolonym skrótem, którego można używać w poleceniach IOS w celu odwołania się do interfejsu.				