Laborator - Configurarea Caracteristicilor de Securitate ale Switch-ului

Topologie

Tabela de Adresare

Echipament	Interfață	Adresă IP	Masca de subreţea	Default Gateway
R1	G0/1	172.16.99.1	255.255.255.0	N/A
S1	VLAN 99	172.16.99.11	255.255.255.0	172.16.99.1
PC-A	NIC	172.16.99.3	255.255.255.0	172.16.99.1

Obiective

Partea 1: Configurați Topologia și Inițializați Dispozitivele

Partea 2: Configuraţi Setările de Bază ale Dispozitivului şi Verificaţi Conectivitatea

Partea 3: Configuraţi şi Verificaţi Accesul SSH pe S1

- Configurați accesul SSH.
- Modificați parametrii SSH.
- Verificați configurarea SSH.

Partea 4: Configuraţi şi Verificaţi Caracteristicile Securităţii pe S1

- Configurați și verificați caracteristicile de securitate generale.
- Configurați și verificați securitatea portului.

Context/Scenariu

Este un lucru destul de comun să blocați accesul și să instalați opțiuni de securitate bune pe calculatoare și servere. Este important ca dispozitivele dumneavoastră de rețea, cum ar fi switchurile și routerele, să fie și ele configurate cu opțiuni de securitate.

În acest laborator, veți urmări câteva practici utile pentru configurarea opțiunilor de securitate pe switchurile LAN. Veți permite doar sesiuni SSH și HTTPS sigure. De asemenea, veți configura și veți verifica securitatea portului pentru a bloca orice echipament cu o adresă MAC care nu este recunoscută de switch.

Notă: Router-ul folosit la laboratoarele practice de CCNA sunt: Cisco 1941 Integrated Services Routers (ISR-uri)și Cisco IOS Release 15.2(4)M3 (universalk9 image). Switch-ul utilizat este un Cisco Catalyst 2960 cu Cisco IOS Release 15.0(2) (lanbasek9 image). Pot fi folosite și alte routere, switchuri și versiuni IOS. În funcție de model și de versiunea Cisco IOS, comenzile disponibile și rezultatele produse pot fi diferite față de cele arătate la laboratoare. Pentru a vizualiza identificatorii corecți ai interfeței, puteți consulta Tabelul cu Interfețele Routerelor de la sfârșitul laboratorului.

Notă: Asigurați-vă că routerele și switchurile au fost șterse și că nu au configurații de pornire. Dacă nu sunteți sigur, contactați instructorul sau consultați laboratorul precedent pentru procedurile necesare inițializării și reîncărcațării dispozitivelor.

Resurse necesare

- 1 Router (Cisco 1941 cu software Cisco IOS , Release 15.2(4)M3 imagine universală sau comparabilă)
- 1 Switch (Cisco 2960 cu Cisco IOS Release 15.0(2) imagine lanbasek9 sau comparabilă)
- 1 Calculator (Windows 7, Vista sau XP cu program de emulare a terminalului, cum ar fi Tera Term)
- Cabluri de consolă pentru a configura echipamentele Cisco IOS prin intermediul porturilor de consolă
- Cabluri Ethernet așa cum se arată în topologie

Part 1: Configurați Topologia și Inițializați Dispozitivele

În partea 1, veți configura topologia rețelei și veți elimina orice configurații dacă este necesar.

Step 1: Cablați rețeaua așa cum se arată în topologie.

Step 2: Inițializați și reîncărcați routerul și switchul.

Dacă fișierele de configurare au fost salvate anterior pe router și switch, inițializați și reîncărcați aceste dispozitive folosind configurările lor de bază.

Part 2: Configuraţi Setările de Bază ale Dispozitivului şi Verificaţi Conectivitatea

În Partea 2, veți configura setările de bază de pe router, switch și calculator. Consultați Topologia și Tabela de Adresare la începutul acestui laborator pentru informații despre adrese și numele dispozitivelor.

Step 1: Configurați o adresă IP pe PC-A.

Step 2: Configurarți setările de bază pe R1.

a. Configurați numele echipamentului.

b. Dezactivați DNS lookup.

c. Configurați adresa IP interfața așa cum se arată în Tabela de Adresare.

d. Folosiți **class** ca parolă pentru modul EXEC privilegiat.

e. Folosiți **cisco** pentru parola vty și de conolă și activați autentificarea.

f. Criptați parolele în text clar

g. Salvați configurarea curentă în fișierul de configurare inițială.

Step 3: Configurați setările de bază pe S1.

O practică utilă de securitate este alocarea adresei IP de management a switchului la un alt VLAN, nu la VLAN 1 (sau la orice alt VLAN de date cu utilizatori finali). În acest pas, veți crea VLAN 99 pe switch și veți aloca o adresă IP.

a. Configurați numele echipamentului.

b. Dezactivați DNS lookup.

c. Folosiți **class** ca parolă pentru modul EXEC privilegiat.

d. Folosiți **cisco** pentru parola vty și de consolă și activați autentificarea.

e. Configurați un gateway default IP pentru S1 folosind adresa IP a lui R1.

f. Criptați parolele în text clar

g. Salvați configurarea curentă în fișierul de configurare inițială.

h. Creați VLAN 99 pe switch și denumiți-l Management.

```
S1(config)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# exit
S1(config)#
```

i. Configurați adresa IP a interfeței de management VLAN 99, așa cum se arată în Tabela de Adresare și activați interfața.

```
S1(config)# interface vlan 99
S1(config-if)# ip address 172.16.99.11 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# end
S1#
```

j. Lansați comanda **show vlan** pe S1. Care este statusul lui VLAN 99? _____ Activ

k. Lansați comanda **show ip interface brief** pe S1. Care este statusul și protocolul pentru VLAN 99?

_____

De ce protocolul este down, deși ați lansat comanda **no shutdown** pentru interfața VLAN 99?

_____

l. Alocați porturi F0/5 și F0/6 la VLAN 99 pe switch.

```
S1# config t
S1(config)# interface f0/5
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 99
S1(config-if)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 99
S1(config-if)# end
```

m. Lansați comanda **show ip interface brief** pe S1. Care este statusul și protocolul pentru interfața VLAN 99? _____

Notă: Poate exista un delay în timp ce stările portului converg.

Step 4: Verificați conectivitatea dintre echipamente.

a. Din PC-A, dați ping la adresa gateway-ului default pe R1. Comenzile ping s-au realizat cu succes? _____

b. Din PC-A, dați ping la adresa de management a lui S1. Comenzile ping s-au realizat cu succes? _____
Din S1, dați ping la adresa gateway-ului implicit pe R1. Comenzile ping s-au realizat cu succes? _____

c. Din PC-A, deschideți un browser și accesați http://172.16.99.11. Dacă vi se cere un username și o parolă, lăsați gol la username și folosiți **class** pentru parolă. Dacă vi se cere o conexiune securizată răspundeți cu Nu. Ați putut accesa interfața web pe S1? _____

d. Închideți sesiunea browser-ului pe PC-A.

Notă: Interfața web nesigurizată (server HTTP) de pe un switch Cisco 2960 este activată în mod implicit. O măsură de securitate uzuală este dezactivarea acestul serviciu, așa cum ni se descrie în Partea 4.

Part 3: Configuraţi şi Verificaţi Accesul SSH pe S1

Step 1: Configurarți accesul SSH pe S1.

a. Activați SSH pe S1. Din modul de configurare global, creați un nume de domeniu CCNA-Lab.com.

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

b. Creați o intrare în baza de date cu utilizatori locali pentru a fi utilizată la conectarea la switch prin SSH. Utilizatorul ar trebui să dețină acces la nivel administrativ.

Notă: Parola utilizată aici NU este o parolă puternică. Este pur și simplu folosită în scopuri didactice.

```
S1(config)# username admin privilege 15 secret sshadmin
```

c. Configurați intrarea transportului pentru liniile vty pentru a permite doar conexiuni SSH și utilizați baza de date locală pentru autentificare.

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

d. Generați o cheie crypto RSA folosind un modul de 1024 biți.

```
S1(config)# crypto key generate rsa modulus 1024
Numele cheilor va fi: S1.CCNA-Lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 3 seconds)

S1(config)#
S1(config)# end
```

e. Verificați configurarea SSH și răspundeți la întrebările de mai jos.

```
S1# show ip ssh
```

Ce versiune de SSH folosește switchul? _____

Câte încercări de autentificare permite SSH? _____

Care este setarea de expirare implicită pentru SSH? _____

Modificați configurarea SSH pe S1.

Modificați configurarea SSH implicită.

Câte încercări de autentificare permite SSH? _____

Care este setarea de expirare pentur SSH? _____

Step 2: Verificați configurația SSH pe S1.

a. Folosind un clientu SSH pe PC-A (cum ar fi Tera Term), deschideți o conexiune SSH la S1. Dacă primiți un mesaj pe clientul dumneavoastră SSH cu privire la cheia hostului, acceptați-l. Autentificați-vă cu **admin** ca nume de utilizator și **cisco** pentru parolă.

Conexiunea s-a realizat cu succes? _____

Ce prompt s-a afișat pe S1? De ce?

b. Tastați **exit** pentru a încheia sesiunea SSH de pe S1.

Part 4: Configuraţi şi Verificaţi Caracteristicile Securităţii pe S1

În Partea 4, veți închide porturile neutilizate, veți opri anumite servicii care rulează pe switch și veți configura securitatea portului bazându-vă pe adrese MAC. Switchurile pot fi supuse la atacuri de supraîncărcare a tabelei cu adrese MAC, la atacuri de spoofing ale MAC-ului și la conexiuni neautorizate la porturile switchului. Veți configura securitatea portului pentru a limita numărul de adrese MAC ce pot fi învățate pe un port de switch și veți dezactiva portului dacă acel număr este depășit.

Step 1: Configurați caracteristicile generale de securitate pe S1.

a. Configurați un banner MOTD pe S1 cu un mesaj adecvat de avertizare.

b. Lansați o **comandă show ip interface brief** pe S1. Ce porturi fizice sunt up?

_____

c. Închideți toate porturile fizice neutilizate de pe switch. Folosiți comanda **interface range**.

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

d. Lansați comanda **show ip interface brief** pe S1. Care este statusul porturilor F0/1 și F0/4?

_____

Down din punct de vedere administrativ.

e. Lansați comanda **show ip http server status**.

Care este statusul serverului HHTP? _____

Ce port de server folosește? _____

Care este statusul serverului HTTP securizat? _____

Ce port de server securizat folosește? _____

f. Sesiunile HTTP trimit totul în text clar. Veți dezactiva serviciul HTTP care rulează pe S1.

```
S1(config)# no ip http server
```

g. Din PC-A, deschideți o sesiune a browser-ului pentru http://172.16.99.11. Care este rezultatul?

_____

h. Din PC-A, deschideți o sesiune de browser la https://172.16.99.11. Acceptați certificatul. Autentificați-vă fără a folosi un nume de utilizator și cu parola class. Care este rezultatul?

_____

i. Închideți sesiunea web de pe PC-A.

Step 2: Configurați și verificați securitatea portului pe S1.

a. Înregistrați MAC a lui G0/1 din R1. Din CLI-ul de pe R1, **folosiți comanda show interface** g0/1 și înregistrați adresa MAC a interfeței.

```
R1# show interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is 30f7.0da3.1821 (bia
3047.0da3.1821)
```

Care este adresa MAC a interfeței G0/1 de pe R1?

_____

b. Din CLI-ul lui S1, dați **comanda show mac address-**table din modul EXEC privilegiat. Găsiți intrările dinamice pentru porturile F0/5 și F0/6. Notați-le mai jos.

Adresa MAC F0/5 MAC: _____

Adresa MAC F0/6: _____

c. Configurați securitatea de bază a portului.

Notă: Această procedură ar fi efectuată în mod normal pe toate porturile de acces de pe switch. F0/5 este dat ca un exemplu.

1) Din CLI-ul de pe S1, intrați în modul de configurare al interfeței pentru portul care se conectează la R1.

```
S1(config)# interface f0/5
```

2) Închideți portul.

```
S1(config-if)# shutdown
```

3) Activați securitatea portului pe F0/5.

```
S1(config-if)# switchport port-security
```

Notă: Prin introducerea **comenzii switchport port**-security se setează adresele MAC maxime la 1 și oprirea acțiunii de violare. Comenzile **switchport port-security maximum** și **switchport port-security violation** pot fi utilizate pentru a schimba comportamentul implicit.

4) Configurați o intrare statică pentru adresa MAC a interfeței G0/1 din R1 înregistrată în Pasul 2a.

```
S1(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx
```

(xxxx.xxxx.xxxx este adresa MAC actuală a interfeței G0/1 a routerului)

Notă: Opțional, puteți utiliza comanda **switchport port-security mac-address sticky** pentru a adăuga toate adresele MAC sigure care sunt învățate dinamic pe un port (până la maximul setat) la configurarea curentă a switchului.

5) Activați portul switchului.

```
S1(config-if)# no shutdown
S1(config-if)# end
```

d. Verificați securitatea portului pe F0/5 din S1 lansând comanda **show port-security interface**.

```
S1# show port-security interface f0/5
```

```
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

Care este statusul portului pe F0/5?

_____

e. Din promptul de comandă R1, dați ping la PC-A pentru a verifica conectivitatea.

```
R1# ping 172.16.99.3
```

f. Acum veți viola securitatea modificând adresa MAC pe interfața routerului. Intrați în modul de configurare al interfeței pentru G0/1 și opriți-o.

```
R1# config t
R1(config)# interface g0/1
R1(config-if)# shutdown
```

g. Configurați o nouă adresă MAC pentru interfață, folosind aaaa.bbbb.cccc **ca** adresă.

```
R1(config-if)# mac-address aaaa.bbbb.cccc
```

h. Dacă este posibil, deschideți o sesiune de consolă pe S1 în timp ce faceți acest pas. Veți vedea diverse mesaje afișate în conexiunea de consolă la S1 indicând o încălcare de securitate. Activați interfața G0/1 pe R1.

```
R1(config-if)# no shutdown
```

i. Din modul EXEC privilegiat R1, dați ping la PC-A. Ping-ul s-a realizat cu succes? De ce sau de ce nu?

_____

j. Pe switch, verificați securitatea portului cu următoarele comenzi arătate mai jos.

```
S1# show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
---------------------------------------------------------------------
      Fa0/5           1           1                1         Shutdown
---------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     :0
Max Addresses limit in System (excluding one mac per port) :8192

S1# show port-security interface f0/5
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
```

```
Aging Type                  : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses       : 1
Total MAC Addresses         : 1
Configured MAC Addresses    : 1
Sticky MAC Addresses        : 0
Last Source Address:Vlan    : aaaa.bbbb.cccc:99
Security Violation Count    : 1

S1# show interface f0/5
FastEthernet0/5 is down, line protocol is down (err-disabled)
  Hardware is Fast Ethernet, address is 0cd9.96e2.3d05 (bia 0cd9.96e2.3d05)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
<output omitted>

S1# show port-security address
               Secure Mac Address Table
------------------------------------------------------------------------
Vlan     Mac Address       Type                  Ports      Remaining Age
                                                             (mins)
----     -----------       ----                  -----   -------------
  99     30f7.0da3.1821    SecureConfigured      Fa0/5         -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     :0
Max Addresses limit in System (excluding one mac per port) :8192
```

k. Închideți interfața G0/1 de pe router, ștergeți adresa MAC hard-coded din router și reactivați interfața G0/1.

```
R1(config-if)# shutdown
R1(config-if)# no mac-address aaaa.bbbb.cccc
R1(config-if)# no shutdown
R1(config-if)# end
```

l. Din R1, dați ping din nou la PC-A la 172.16.99.3. Ping-ul s-a realizat cu succes? _____Nu

m. Lansați comanda **show interface f0/5** pentru a determina cauza eșecului comenzii ping. Înregistrați-vă căutările.

_____

n. Ștergeți statusul error-disabled de pe F0/5 de pe S1.

```
S1# config t
S1(config)# interface f0/5
S1(config-if)# shutdown
S1(config-if)# no shutdown
```

Notă: Poate exista un delay în timp ce stările portului converg.

o. Lansați comanda **show interface f0/5** pe S1 pentru a verifica dacă F0/5 mai este în modul error disabled.

```
S1# show interface f0/5
FastEthernet0/5 is up, line protocol is up (connected)
```

```
Hardware is Fast Ethernet, address is 0023.5d59.9185 (bia 0023.5d59.9185)
MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
   reliability 255/255, txload 1/255, rxload 1/255
```

p. Din prompt-ul de comandă R1, dați din nou ping la PC-A. Ar trebui să se realizeze cu succes.

Reflecție

1. De ce ați activa securitatea portului pe un switch?

   _____

2. De ce ar trebui dezactivate porturile de pe un switch?

   _____

Tabela Interfețelor Routerului

Rezumatul Interfețelor Routerului				
Modelul Routerului	**Interfața Ethernet #1**	**Interfața Ethernet #2**	**Interfața Serială #1**	**Interfața Serială #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 (S0/1/0)	Serial 0/1/1 (S0/1/1)
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)

Notă: Pentru a afla cum este configurat routerul, uitați-vă la interfețe pentru a identifica tipul routerului și câte interfețe are routerul. Nu există o listă efectivă cu toate combinațiile configurărilor pentru fiecare clasă de routere. Acest tabel include identificatorii pentru combinațiile posibile de interfețe Seriale și Ethernet din dispozitiv. Tabelul nu include nici un alt tip de interfață, chiar dacă un anumit router poate. Un astfel de exemplu poate fi interfața ISND BRI. Denumirea din paranteză este prescurtarea legală care poate fi folosită în comenzile Cisco IOS pentru a reprezenta interfața.