Hálózati eszközök biztonsága

Központi syslog szerver beállítása

1. Az UDP 514-es portra érkező forgalmat korlátozza a labor hálózatára:

```
iptables -A INPUT -s 192.168.100.0/24 -p UDP --dport 514 -j ACCEPT
iptables -A INPUT -p UDP --dport 514 -j DROP
```

2. A /etc/rsyslog.conf állomány végére írja a következő sorokat:

```
$template FILENAME,"/var/log/%fromhost-ip%/syslog.log"
*.* ?FILENAME
```

3. A /etc/rsyslog.conf állmányban távolítsa el a #-eket a következő sorok elejéről:

```
$ModLoad imudp
$UDPServerRun 514
```

4. Indítsa újra az rsyslog daemont:

```
/etc/init.d/rsyslog restart
```

Központi időszerver telepítése

1. Telepítse fel az ntp daemont:

```
apt-get install ntp
```

2. Győződjön meg az időszerver működéséről:

```
ntpq -p
```

Cisco switch üzembe helyezése

1. Csatlakoztassa a Cisco switch konzol kábelét számítógépe soros portjára.
2. Telepítsen számítógépére terminál emulátor programot. (Pl: apt-get install minicom)
3. Állítsa be a terminal emulátort a soros port kezelésére 9600,8,n,1 paraméterekkel.
4. Indítsa el a Cisco eszközt, és figyelje az indulás folyamatát.
5. Amennyiben szükséges, törölje a konfigurációt, majd indítsa újra az eszközt.
6. Iktassa közbe a switchet a laborhálózat és a számítógépe közé.
7. Rendeljen IP címet a switchez, valamint tiltsa le a domain lookup-ot:

```
enable
configure terminal
no ip domain lookup
interface vlan 1
ip address 192.168.100.X 255.255.255.0
```

```
no shutdown
```

Cisco switch hardening

1. Lássa el jelszóval a terminal portot:

```
enable
configure terminal
line console 0
password cisco
```

2. Hozzon létre egy falhasználót a hozzá tartozó jelszóval:

```
username student secret cisco
line console 0
login local
```

3. Állítsa be a vty-kre a belépés ellenőrzését:

```
line vty 0 15
login local
```

4. Állítsa be az enable secretet:

```
enable secret cisco
```

5. Tesztelje le a számítógépéről a csatlakozást telnet protokollal.

SSH engedélyezése

1. Győződjön meg róla, hogy az ön eszközének IOS verziója támogatja az SSH protokollt. (Az IOS nevének tartalmaznia kell a „k9” szöveget.) Ha nem támogatja, hagyja ki ezt a feladatrészt.

```
show version
```

2. Állítsa be a domain nevet sze.hu-ra:

```
enable ip domain-name sze.hu
```

3. Hozza létre a titkosításhoz szükséges kulcsot:

```
crypto key generate rsa
```

4. Állítsa át a vty vonalakat telnet-ről SSH-ra, és az SSH protokoll 2-es verziójára:

```
line vty 0 15
transport input ssh
exit
```

```
ip ssh version 2
```

5. Próbálja ki a csatlakozást számítógépéről telnet és SSH segítségével.

vty elérésének korlátozása

1. Hozzon létre ACL-t, mely csak az ön gépének IP címéről engedélyezi a hozzáférést a vty-khez, a többi címről érkező kéréseket logolja:

```
enable
configure terminal
access-list 1 permit host 192.168.100.X
access-list 1 deny any log
```

2. Rendelje hozzá az ACL-t a vty.khez:

```
line vty 0 15
access-class 1 in
```

3. Próbálja ki a saját és a szomszéd switch-re is a csatlakozást.

Nem használt portok korlátozása

1. Nézze meg eszközén, hogy mely portok nincsenek használatban, majd tiltsa le azokat:

```
enable
configure terminal
interface range FastEthernet 0/3-24 (Ez csak példa!)
shutdown
```

Trunk port mód tiltása

1. Nézze meg eszközén, hogy mely port csatlakozik számítógépéhez, majd azt állítsa fixen „access mode”-ba:

```
enable
configure terminal
interface FastEthernet 0/2 (Ez csak példa!)
swicthport mode access
```

2. Nézze meg eszközén, hogy mely port csatlakozik másik switchez, majd azon tiltsa le a VTP-t:

```
interface FastEthernet 0/1 (Ez csak példa!)
switchport mode trunk
swicthport nonegotiate
```

Nem használt szolgáltatások letiltása

1. Nézze meg, hogy eszköze milyen más Cisco eszközöket lát:

```
show cdp neighbors
```

2. Globálisan tiltsa le a CDP protokollt:

```
enable
configure terminal
no cdp run
```

3. Nézze meg ismét a CDP szomszédok listáját.

Időszerver beállítása

1. Írassa ki eszközén a pontos időt:

```
show clock
```

2. Állítsa be az időzónát, téli-nyári időszámítás szabályait, valamint időszerverként saját számítógépét:

```
enable
configure terminal
clock timezone CET 1
clock summer-time CET+DST recurring last Sun Mar 2:00 last Sun Oct 3:00
ntp server 192.168.100.X
```

3. Ellenőrizze ismét az időt, szükség esetén addig várjon, amíg az óra be nem állítódik.

Távoli log beállítása

1. Engedélyezze a log funkciót:

```
enable
configure terminal
logging enable
```

2. Állítsa be saját gépét syslog szervernek:

```
logging host 192.168.100.X
```

3. Állítsa be, hogy minden esemény logolásra kerüljön:

```
logging trap 7
```

4. Lépjen ki, és be az eszközre, végezzen sikertelen belépéseket is, majd tanulmányozza számítógépén a log tartalmát. (less /var/log/192.168.100.X/syslog.log)

Végleges konfiguráció

1. Tanulmányozza az eszköz konfigurációját:

```
enable

configure terminal

show running-config
```