**Reduceți atacurile VLAN**

**Analiza atacurilor VLAN**

Ca o scurtă trecere în revistă **,** un atac de salt VLAN poate fi lansat în unul din trei moduri:

* Falsificarea mesajelor DTP de la gazda atacatoare pentru ca comutatorul să intre în modul trunking. De aici, atacatorul poate trimite trafic etichetat cu VLAN-ul țintă, iar comutatorul livrează apoi pachetele la destinație.
* Introducerea unui comutator necinstiți și activarea trunchiului. Atacatorul poate accesa apoi toate VLAN-urile de pe comutatorul victimă de la comutatorul necinstiți.
* Un alt tip de atac de salt VLAN este un atac cu etichetare dublă (sau dublu încapsulat). Acest atac profită de modul în care funcționează hardware-ul pe majoritatea switch-urilor.

**Pași pentru a atenua atacurile VLAN Hopping**

Utilizați următorii pași pentru a atenua atacurile de salt VLAN:

**Pasul 1** : Dezactivați negocierile DTP (trunking automat) pe porturile non-trunking utilizând comanda de configurare a interfeței de **switchport mode access.**

**Pasul 2** : Dezactivați porturile neutilizate și puneți-le într-un VLAN neutilizat.

**Pasul 3** : Activați manual legătura trunk pe un port trunk utilizând comanda **switchport trunk mode** .

**Pasul 4** : Dezactivați negocierile DTP (trunking automat) pe porturile de trunking utilizând comanda **switchport nonegotiate** .

**Pasul 5** : Setați VLAN-ul nativ la un alt VLAN decât VLAN 1 utilizând comanda **switchport trunk native vlan***vlan \_ number* .

De exemplu, presupuneți următoarele:

* Porturile FastEthernet de la 0/1 la fa0/16 sunt porturi de acces active
* Porturile FastEthernet de la 0/17 la 0/20 nu sunt utilizate în prezent
* Porturile FastEthernet de la 0/21 la 0/24 sunt porturi trunk.

Hoppingul VLAN poate fi atenuat prin implementarea următoarei configurații.

**S1(config)# interface range fa0/1 - 16**

**S1(config-if-range)# switchport mode access**

**S1(config-if-range)# exit**

**S1(config)#**

**S1(config)# interface range fa0/17 - 20**

**S1(config-if-range)# switchport mode access**

**S1(config-if-range)# switchport access vlan 1000**

**S1(config-if-range)# shutdown**

**S1(config-if-range)# exit**

**S1(config)#**

**S1(config)# interface range fa0/21 - 24**

**S1(config-if-range)# switchport mode trunk**

**S1(config-if-range)# switchport nonegotiate**

**S1(config-if-range)# switchport trunk native vlan 999**

**S1(config-if-range)# end**

**S1#**

* Porturile FastEthernet de la 0/1 la 0/16 sunt porturi de acces și, prin urmare, trunchiul este dezactivat făcându-le în mod explicit porturi de acces.
* Porturile FastEthernet de la 0/17 la 0/20 sunt porturi neutilizate și sunt dezactivate și atribuite unui VLAN neutilizat.
* Porturile FastEthernet de la 0/21 la 0/24 sunt legături trunchiuri și sunt activate manual ca trunchiuri cu DTP dezactivat. VLAN-ul nativ este, de asemenea, schimbat de la VLAN-ul implicit 1 la un VLAN 999 neutilizat.

**Syntax Checker - Atenuarea atacurilor VLAN Hopping**

**You are currently logged into S1. The ports status of the ports are as follows:**

**FastEthernet ports 0/1 through 0/4 are used for trunking with other switches.**

**FastEthernet ports 0/5 through 0/10 are unused.**

**FastEthernet ports 0/11 through 0/24 are active ports currently in use.**

**Use range fa0/1 - 4 to enter interface configuration mode for the trunks.**

**S1(config)#interface range fa0/1 - 4**

**Configure the interfaces as nonnegotiating trunks assigned to default VLAN 99.**

**S1(config-if-range)#switchport mode trunk**

**S1(config-if-range)#switchport nonegotiate**

**S1(config-if-range)#switchport trunk native vlan 99**

**S1(config-if-range)# exit**

**Use range fa0/5 - 10 to enter interface configuration mode for the unused ports.**

**S1(config)#interface range fa0/5 - 10**

**Configure the unused ports as access ports, assign them to VLAN 86, and shutdown the ports.**

**S1(config-if-range)#switchport mode access**

**S1(config-if-range)#switchport access vlan 86**

**% Access VLAN does not exist. Creating vlan 86**

**S1(config-if-range)#shutdown**

**\*Mar 1 00:28:48.883: %LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down**

**\*Mar 1 00:28:48.900: %LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down**

**\*Mar 1 00:28:48.908: %LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down**

**\*Mar 1 00:28:48.917: %LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down**

**\*Mar 1 00:28:48.942: %LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down**

**\*Mar 1 00:28:48.950: %LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down**

**\*Mar 1 00:28:49.890: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down**

**\*Mar 1 00:28:49.907: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to down**

**S1(config-if-range)# exit**

**Use range fa0/11 - 24 to enter interface configuration mode for the active ports and then configure them to prevent trunking.**

**S1(config)#interface range fa0/11 - 24**

**S1(config-if-range)#switchport mode access**

**S1(config-if-range)# end**

**S1#**

**You have successfully mitigated VLAN hopping attacks on this switch.**