Table des matières

Atténuer les attaques VLAN

1. Révision des attaques de VLAN

En bref**,** Une attaque par saut de VLAN peut être lancée de trois manières :

- Usurpation des messages DTP (Dynamic Trunk Protocol) de l'hôte attaquant pour que le commutateur passe en mode trunking. À partir de là, l'attaquant peut envoyer du trafic étiqueté avec le VLAN cible, et le commutateur délivre ensuite les paquets à la destination.
- Présentation d'un commutateur indésirable et activation de trunking. L'attaquant peut alors accéder à tous les VLAN sur le commutateur victime à partir du commutateur non autorisé.
- Un autre type d'attaque par saut de VLAN est une attaque à double étiquette (ou à double encapsulation). Cette attaque profite de la façon dont le matériel de la plupart des commutateurs fonctionne.

2. Les Étapes pour atténuer les attaques par sauts de VLAN

Utilisez les étapes suivantes pour atténuer les attaques par saut de VLAN:

Étape 1: désactivez les négociations DTP (jonction automatique) sur les ports sans trunk à l'aide de la commande de configuration de l'interface **switchport mode access** .

Étape 2: désactivez les ports inutilisés et placez-les dans un VLAN inutilisé.

Étape 3: Activez manuellement la liaison de jonction sur un port de jonction à l'aide de la commande **switchport mode trunk** .

Étape 4: désactivez les négociations DTP (trunking automatique) sur les ports de jonction à l'aide de la commande **switchport nonegotiate** .

Étape 5: définissez le VLAN natif sur un VLAN autre que VLAN 1 à l'aide de la commande **switchport trunk native vlan** _vlan_number.

Par exemple, supposez ce qui suit:

- Les ports FastEthernet 0/1 à fa 0/16 sont des ports d'accès actifs
- Les ports FastEthernet 0/17 à 0/24 ne sont pas actuellement utilisés
- Sur les swirches 53/5000 Les ports FastEthernet 0/21 à 0/20 sont des ports de trunk.

Le saut de VLAN peut être atténué en mettant en œuvre la configuration suivante.

```
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#
```

- Les ports FastEthernet 0/1 à 0/16 sont des ports d'accès (ACCESS) donc le trunking est désactivé en leur faisant explicitement des ports d'accès.
- Les ports FastEthernet 0/17 à 0/20 sont des ports inutilisés et sont désactivés et affectés à un VLAN inutilisé.
- Les ports FastEthernet 0/21 à 0/24 sont des liaisons de trunk et sont activés manuellement en tant que trunks avec DTP désactivé. Le VLAN natif passe également du VLAN 1 par défaut à un VLAN 999 inutilisé.

3. Vérificateur de syntaxe - Atténuer les attaques par sauts de VLAN

Atténuez les attaques par sauts de VLAN sur le commutateur en fonction des exigences spécifiées.

Vous êtes actuellement connecté à S1. L'état des ports est comme suivant:

- Les ports FastEthernet 0/1 à 0/4 sont utilisés pour le trunc avec d'autres commutateurs.
- Les ports FastEthernet 0/5 à 0/10 ne sont pas utilisés.
- Les ports FastEthernet 0/11 à 0/24 ne sont pas actuellement utilisés

Utilisez **interface range fa0/1 - 4** pour passer en mode de configuration d'interface pour les truncs.

```
S1(config)#
```