GSB

STP

Version <1.5>

Sécurisation Spanning-Tree Protocol

Historique des révisions

Date	Version	Description	Auteur
29/09/2015	<1.0>	Mise en place de Spanning-Tree et Attaque avec Yersinia pour détournement du trafic.	Legrand Julien Harismendy Brice
10/10/15	<1.5>	Finalisation de la documentation.	Legrand Julien Harismendy Brice

Table des matières

Sécurisation de Spanning-Tree

1. Introduction

Le protocole Spanning-Tree est un protocole réseau activé par défaut sur les switchs Cisco il sert à éviter les redondances réseau mais n'est pas sécurisé par défaut.

1.1 Contexte du projet

Le réseau est constitué d'un switchs et d'un PC sous Kali Linux no_us allons essayer de passer le port sur lequel le pc est connecté.

1.2 Objectifs du document

Le protocole STP permet d'éviter qu'un réseau soit saturé et donc d'éviter des phénomènes comme les 'tempêtes de broadcast'; Le protocole permet aussi le changement de route, et forme un réseau en 'arbre', c'est-à-dire que l'un des switchs devient (après la découverte du réseau) ' ROOT ' et les autres switchs du réseau le prennent pour modèle (possibilité de configuration manuelle). L' objectif premier est de démontrer la faille de ce protocole lors d'un détournement de trafic, avec le logiciel 'Yersinia' qui aura pour but de lancer des trames réseau et se placer en tant que racine (ROOT). Le second objectif sera donc de voir les possibilités de sécurisation du réseau qui utilise le protocole STP.

1.3 Portée

La portée de ce document est scolaire, mais adressée aussi aux entreprises qui possèdent ce modèle 'spanning-tree' et souhaitent sécuriser leur réseau.

1.4 Définitions, Acronymes et Abréviations

STP : Spanning-Tree Protocol

1.5 Références

Aide sur la configuration Spanning-tree (site Cisco) : http://goo.gl/HvJg00
err-disable : https://aacable.wordpress.com/2012/12/07/cisco-3750-howto-enable-err-disabled-ports/

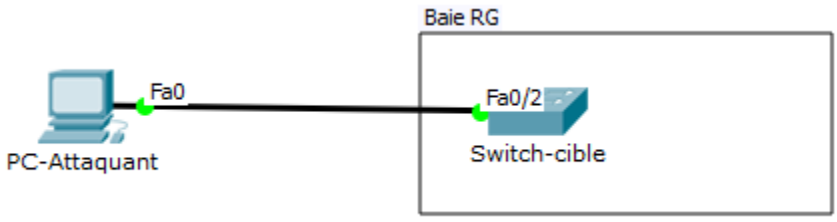
https://www.ciscomadesimple.be/2013/01/29/spanning-tree-portfast-bpduguard/

1.6 Vue générale

Dans un premier temps nous allons attaquer le switch « sans défense » puis nous le sécuriserons et enfin nous validerons ces sécurités en le ré-attaquant de nouveau.

2. Éléments de configuration

2.1 schéma réseau



2.2 Assignation des ports

Vlan 20	Fa 0/1, Fa 0/2
Vlan 21	Fa 0/3, Fa 0/4
Vlan 22	Fa 0/5, Fa 0/6
Vlan 23	Fa 0/7, Fa 0/8
Vlan 24	Fa 0/9, Fa 0/10
Vlan 25	Fa 0/11, Fa 0/12
Vlan 26	Fa 0/13, Fa 0/14
Vlan 27	Fa 0/15, Fa 0/16
Vlan 28	Fa 0/17, Fa 0/18
Vlan 29	Fa 0/19, Fa 0/20
Trunk	Gi 0/1, Gi 0/2

2.3 Materiel utilisé

On a :
-un switch Cisco catalyst 2960
-une clé usb contenant une version live de kali linux

2.4 sécurisation du switch

Sur le port fa0/20 (que l'on veut en tant que port “ROOT”) :

```
sw2.2(config)#int fa0/20
sw2.2(config-if)#spanning-tree bpduguard disable
```
→ permet a ce que le switch recoivent des trames bpdu (mise à jour de la topologie)
```
sw2.2(config)#spanning-tree vlan 20-29 root primary
```
→ c'est le port root pour le VLAN 29
```
sw2.2(config)#int fa0/20
sw2.2(config-if)#spanning-tree guard root
```

Et on interdit les bpdu sur tout les autres ports :

```
sw2.2(config)#int range fa0/1-19
sw2.2(config-if-range)#spanning-tree bpduguard enable
sw2.2(config-if-range)#exit
sw2.2(config)#int range fa0/21-24
sw2.2(config-if-range)#spanning-tree bpduguard enable
```
→ permet de couper immédiatement l'interface si elle reçois un paquet bpdu
```
sw2.2(config-if-range)#int range gi0/1-2
sw2.2(config-if-range)#spanning-tree bpduguard disable
```
→ on le désactive car ce sont des liens trunk et il est donc normal qu'ils recoivent des trames bpdu car ils peuvent être relier à d'autre switch.

On relance l'attaque : voir 3.2

Pour réactiver une interface en err-disabled :
soit il faut attendre 300 secondes par défaut ou on peut forcer le retour en éteignant et en réactivant l'interface.

réactivation de l'interface fa 0/2 alors qu'elle est en err-disabled (suite a la tentative d'attaque) :

```
sw2.2(config)#int fa0/2
sw2.2(config-if)#shut
sw2.2(config-if)#no sh
```

2.5 Désactiver STP

Pour désactiver Spanning-tree il faut mettre le port en mode portfast :
exemple :
```
sw2.2(config)#int fa0/10
sw2.2(config-if)#spanning-tree portfast → permet
```

3. Tests / Validations

3.1 attaque sur le switch non protégé :

Après avoir mis en place l'infrastructure réseau nous allons tenter une attaque spanning tree :

nous allons forger des trames en utilisant du code en python combiné à la bibliothèque Scapy dont voici la syntaxe :

sendp(Dot3(src="C4:E6:1F:04:84:A4",dest="01:80:02:00:00:00")/LLC()/STP(bdutype=0,rootid=100,root mac="C4:E6:1F::04:84:FF",bridgeid=100,bridgemac="01:02:03:04:05:06"),iface="eth0",count=1000)

Explication de la commande :

sendp : send paquet

dot3 : paquet ethernet

src : adresse MAC source

dest : adresse MAC de destination

LLC : sous couche de la couche 2

bpdutype : la topologie a changer

rootid :plus le numéro est petit plus la source est prioritaire

root mac : adresse MAC du nouveau appareil root

iface : interface par laquelle est envoyé la trame

count : nombre de fois que la trame est envoyé

On exécute cette commande on voit alors le pc passer root du protocole STP dans le switch (il est branché sur fa0/2) :

```
sw2.2#sh spanning-tree

VLAN0020
  Spanning tree enabled protocol ieee
  Root ID     Priority    100
              Address     c46e.1f04.84a4
              Cost        19
              Port        2 (FastEthernet0/2)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32788  (priority 32768 sys-id-ext 20)
              Address     f4ea.6742.2680
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/2               Root FWD 19        128.2    P2p
```

3.2 test de la même attaque avec spanning tree protégé :

On relance la première attaque :

Cela désactive l'interface attaqué :

```
sw2.2#sh int fa0/2
FastEthernet0/2 is down, line protocol is down (err-disabled)
  Hardware is Fast Ethernet, address is f4ea.6742.2682 (bia f4ea.6742.2682)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

Le port spanning tree reste fa0/20 :

```
sw2.2#sh spanning-tree

VLAN0029
  Spanning tree enabled protocol ieee
  Root ID     Priority    24605
              Address     f4ea.6742.2680
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24605  (priority 24576 sys-id-ext 29)
              Address     f4ea.6742.2680
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/20              Desg FWD 19        128.20   P2p Edge
```

4. Conclusion

Maintenant notre commutateur est sécurisé au niveau du protocole stp et aucun autre switch ne peut prendre sa position de “root”.