GSB

Sécurisation des VLAN

Version <1.0>

Sécurisation des VLAN

Historique des révisions

Date	Version	Description	Auteur
06/10/2015	<1.0>	Sécurisation des vlans	Legrand Julien, Brice Harismendy

Table des matières

Sécurisation des vlans

1. Introduction

L'un des principaux avantages des commutateurs est le vlan, mais comme tout dans un réseau il faut le sécuriser sinon des risques d'attaque existe.

1.1 Contexte du projet

Nous avons un switch d'ont on viens juste de configurer les vlans sans mettre en place la moindre sécurité.

1.2 Objectifs du document

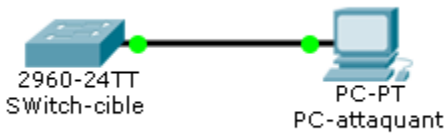
Ce document à pour objectif d'expliquer et de démontrer la sécurisation de ports en mode access sur le switch et éviter ainsi qu'ils soient passés en mode trunk.

1.3 Portée

Ce document est destiné aux administrateurs et techniciens réseau.

2. Éléments de configuration

2.1 schéma réseau



2.2 Configuration par défaut

```
sw2.2#sh int fa 0/16 switchport
Name: Fa0/16
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 27 (VLAN0027)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
```

Nous allons donc réaliser une attaque depuis Kali Linux sur Yersinia (voir 3.1)

2.3 Mise en place de la sécurité

```
sw2.2#conf t
sw2.2(config)#int fastEthernet 0/16
sw2.2(config-if)#switchport mode access
sw2.2(config-if)#switchport access vlan 27
sw2.2(config-if)#switchport nonegotiate
```

Voici la nouvelle configuration du port :

```
sw2.2#sh int fa 0/16 switchport
Name: Fa0/16
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 27 (VLAN0027)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

3. Tests / Validations

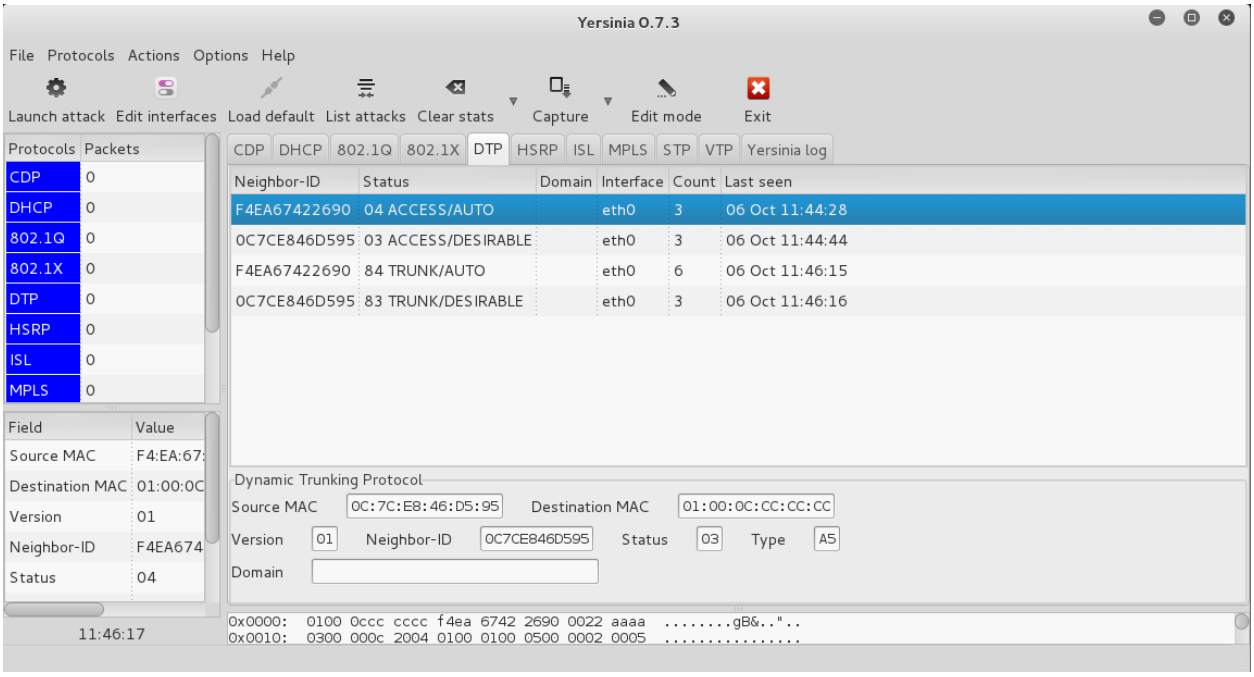
3.1 Attaque DTP d'une interface en acces sur le vlan 27 mal configuré :

Après le lancement de l'attaque le port est passé en mode trunk ce qui est très dangereux :

```
sw2.2#sh int fa 0/16 switchport
Name: Fa0/16
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 27 (VLAN0027)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Sur kali linux :


Yersinia 0.7.3
File Protocols Actions Options Help
Launch attack
Edit interfaces
Load default
List attacks
Clear stats
Capture
Edit mode
Exit
Protocols Packets
CDP 0
DHCP 0
802.1Q 0
802.1X 0
DTP 0
HSRP 0
ISL 0
MPLS 0
Field Value
Source MAC F4:EA:67:
Destination MAC 01:00:0C
Version 01
Neighbor-ID F4EA674
Status 04
11:46:17
CDP DHCP 802.1Q 802.1X DTP HSRP ISL MPLS STP VTP Yersinia log
Neighbor-ID Status Domain Interface Count Last seen
F4EA67422690 04 ACCESS/AUTO eth0 3 06 Oct 11:44:28
0C7CE846D595 03 ACCESS/DESIRABLE eth0 3 06 Oct 11:44:44
F4EA67422690 84 TRUNK/AUTO eth0 6 06 Oct 11:46:15
0C7CE846D595 83 TRUNK/DESIRABLE eth0 3 06 Oct 11:46:16
Dynamic Trunking Protocol
Source MAC 0C:7C:E8:46:D5:95
Destination MAC 01:00:0C:CC:CC:CC
Version 01
Neighbor-ID 0C7CE846D595
Status 03
Type A5
Domain
0x0000: 0100 0ccc cccc f4ea 6742 2690 0022 aaaa ....gB&.."..
0x0010: 0300 000c 2004 0100 0100 0500 0002 0005 ....

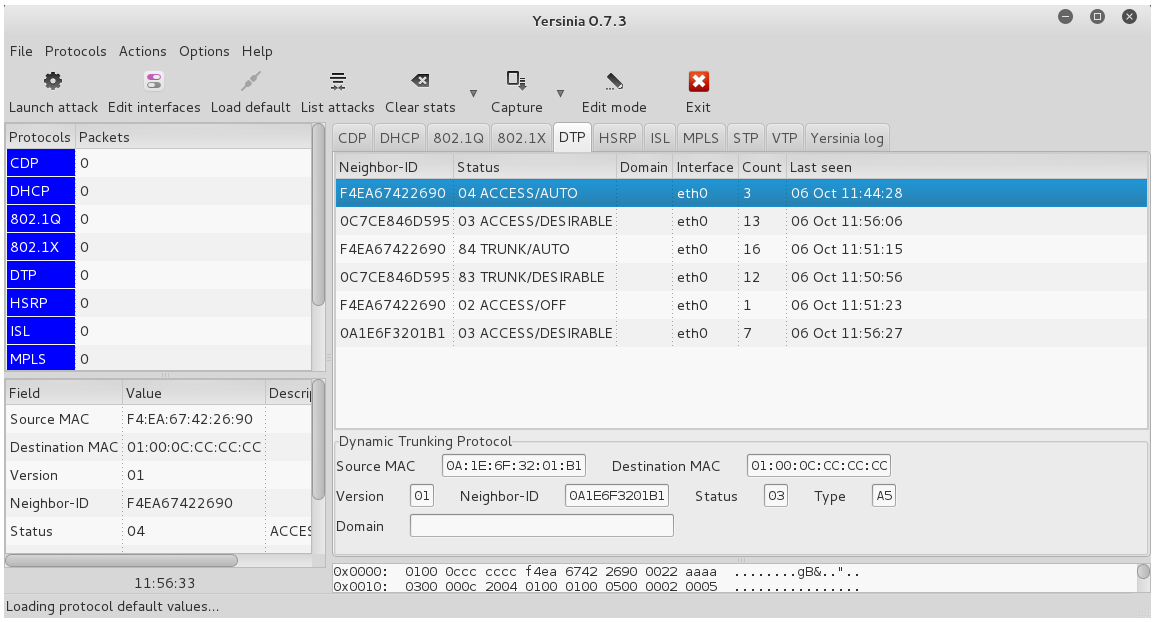
3.2 Attaque relancé une fois le port sécurisé :

Cette fois le port ne passe pas en mode trunk :

```
sw2.2#sh int fa 0/16 switchport
Name: Fa0/16
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 27 (VLAN0027)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Sur kali linux :



4. Conclusion

Il ne faut pas activer le protocole DTP et il faut forcer le mode access. Bien que simple à mettre en place, cette sécurité est essentielle dans un réseau et empêche qu'un utilisateur mal intentionné ne passe sont port sur le switch en mode trunk et ne puisse voir toutes les trames passant par le switch.