Mission Yersinia - Panique dans le laboratoire "R et D"... Attaque interne type DoS via le protocole STP. Comment s'en protéger ?

Le contexte

Les locaux hébergeant le labo. “R et D” ont été rénovés. L'infrastructure (équipements passifs et actifs) a été entièrement reconstruite. Cette infrastructure s'appuie sur la dorsale décrite dans la mission “BackBone”. Le proto. STP a été configuré sur les switchs fédérateurs de la dorsale.

Le lundi 7 septembre 2015, les utilisateurs du labo. constatent un effondrement du réseau en terme de performances qui impacte le travail des chercheurs pendant plusieurs heures.

Les premières investigations de Derrick laissent à penser qu'une attaque interne de type DoS via le protocole STP est à l'origine de cette catastrophe.

Une nouvelle fois, la DG de GSB demande des comptes à Derrick qui vous charge de résoudre techniquement le problème de manière définitive. Par ailleurs, Derrick participera en qualité d'expert à une commission d'enquête chargée de déterminer l'identité du ou des auteur(s) de l'attaque qui ne peut avoir qu'une origine interne.

La mission

Voue êtes chargé d'analyser l'attaque subie par le réseau (vraisemblablement via le logiciel **Yersinia**) et de reconfigurer les équipements actifs afin de se protéger contre ce type de malveillance.

Documentation

- Le protocole STP (couche 2)
- SECURITE COUCHE 2 (Port Security, STP Security)