

Intrusion Management

Description

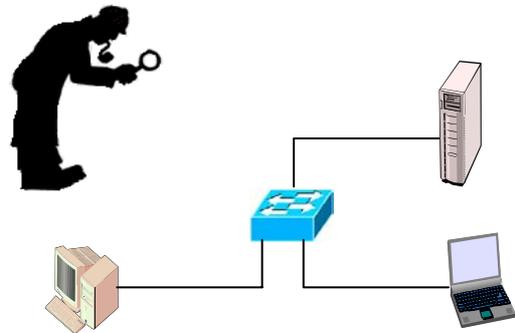
L'intrusion est une technique permettant à une personne désirant exécuter une attaque. Dans le but de nuire à une victime que ce soit par un déni de service ou une autre méthode.



Test de vulnérabilité sur un utilisateur.

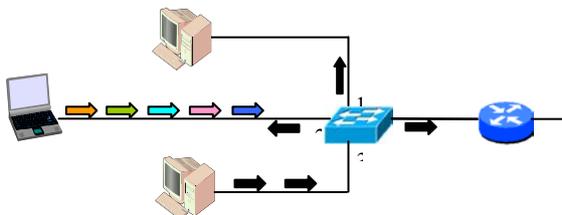
Réalisation

Mise en place de banc de test permettant de tester différentes attaques ; comment attaquer un switch, man in the middle, interception de mot de passe etc ...



Mandat

"Ce travail a pour objet les intrusions à l'intérieur et l'extérieur de l'entreprise. Le terme d'"Intrusion Management" englobe quatre types d'activité qui assurent la prévention contre les intrusions (Avoidance, Assurance, Detection) ou les mesures de réparation à prendre en cas d'intrusion réussie (Investigation). Les objectifs de ce travail concernent uniquement certains aspects du management de l'intrusion à savoir : l'étude et présentation des différentes stratégies d'intrusion à l'extérieur et l'intérieur de l'entreprise (layer 2 hacking) et les aspects de prévention (avoidance) basés sur une authentification forte."



Solution testée

Mise en place de détecteurs d'intrusions, permettant de renifler le réseau pour détecter les intrusions. Application de la sécurité sur les switch Cisco Catalyst. Utilisation de protocole sécurisé employant la cryptographie pour garantir la confidentialité. Investigation permettant de déterminer la source de l'attaque.

Résultats

Les méthodes testées permettent de retrouver la source de l'attaque ainsi que l'auteur. La cryptographie permet de garantir la confidentialité.

Auteur: Massimo Iritano
Répondant externe: Sylvain Maret
Répondant interne: Stefano Ventura
Sujet proposé par: Centre de compétence CCTI