heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud
http://www.heig-vd.ch

Travail de diplôme 2007

HEIG-VD
Route de Cheseaux 1
CH - 1401 Yverdon-les-Bains

Déploiement et Test d'un système de détection IDS appliqué à la VoIP : Etude de cas IPS-1 de Check Point

Description :
Depuis quelques années, nous vivons dans l'époque numérique, où tout passe par internet. Ainsi la télècommunication ne fait pas exception à cette règle donnant naissance à une nouvelle technologie : VoIP. Elle permet de transporter de la voix à travers un réseau utilisant le protocole IP.
Cependant, l'intégration de la téléphonie dans le monde Internet, l'expose à divers problèmes particulièrement au niveau de la sécurité. Des outils appelés système de détection d'intrusions (IDS) ont été développées dans le but de résoudre la problématique de la sécurité des services voix et multimédia.

Mandat :

Ce projet est né d'une initiative d'e-Xpert Solutions SA et IICT qui désiraient collaborer dans le domaine de la sécurité VoIP. En effet grâce à l'aboutissement de la première étape du projet Vadese (www.vadese.org), IICT souhaitait étendre les fonctionnalités des IDS conventionnels au trafic VoIP et étendre ainsi les services SIEM (Security Information and Event Management) à la VoIP. Dans le cadre de ce travail de diplôme Il s'agirat de tester et compléter les filtres VoIP de l'IDS mis à disposition de CheckPoint (désigné par la suite IPS1). Cette extension ayant pour objectif de démontrer l'utilité et l'efficacité d'une sécurisation du service VoIP au sein d'une PME.

Réalisation :
IPS-1 se décompose en quatre composants qui sont : l'IPS-1 Sensor, l'IPS-1 Alert concentrator, l'IPS-1 Server et l'IPS-1 Management Dashboard. Un réseau de test, contenant ces composants, des téléphones Cisco et softphones, est mis en place afin de tester les filtres développés sur l'IPS-1.

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

Résultat :

Suite aux tests effectués, l'IPS détecte les paquets qui ne respectent pas la RFC SIP. Ainsi des alertes sont émises vers l' IPS-1 Management Dashboard afin de prévenir l'administrateur réseau de toute intrusion.

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

Auteur: **Marie Thérèse Gomes**
Répondant externe: **Sylvain Maret**
Prof. responsable: **Stefano Ventura**
Sujet proposé par: **e-Xpert Solutions SA**

Hes·so
Haute Ecole Spécialisée
de Suisse occidentale