heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

Tél. : 024 557 63 30
Fax : 024 557 64 04

info@heig-vd.ch
http://www.heig-vd.ch

Travail de diplôme 2005

Département Electricité et Informatique

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

VoIP & Security

Description

Le projet VoiSE (VoIP & Security) tente d'apporter une réponse à la problématique de la sécurisation des services voix et multimédia dans le cadre d'un déploiement en entreprise. Malgé le grand engouement pour la VoIP, beaucoup d'entreprises restent, pour des raisons de sécurité attachées aux PBX traditionnels.

Le téléphone restant le nerf de la guerre des entreprises, il est clair que les solutions de téléphonie sur IP doivent apporter des garanties de sécurité acceptables contres les principaux risques d'attaques.

Cahier des charges

Ce travail de diplôme étudie les points cités ci-dessous, l'étude d'un IDS (Intrusion Detection System) est le point principale:

1. Étude de la problématique de la sécurité VoIP : Il s'agit de de montrer les principales vulnérabilité et menaces de la VoIP pour les systèmes IP-PBX basées sur le protocole SIP
2. Étude des différentes stratégies des IDS (stateless, statefull, cross protocol) pour la VoIP.
3. Réalisation d'un IDS statefull

Réalisation

L'IDS a pour but de détecter les attaques SIP contre le proxy et les vulnérabilités du protocole.

Pour implémenter l'IDS, notre choix s'est porté sur la plate forme SNORT (www.snort.org) enrichie par deux préprocesseurs SIP que nous avons développé dans le cadre de ce travail de diplôme. Cela nous a permis de décomposer le problème en deux IDS différents.

Le premier est placé devant l'IP-PBX. Il vérifie les sessions SIP et détecte les attaques contre le serveur. On analyse les sessions SIP à l'aide d'un diagramme d'états.

Le deuxième est placé en monitoring sur les switchs ethernets. Sa vision du réseau est plus grande. Il peut détecter les attaques ne passant pas par l'IP-PBX et surveille les sessions des flux RTP.

Les sessions RTP et SIP sont enregistrées dans une base de données.

Conclusion

Ces deux IDS peuvent détecter une grande partie des attaques. La base de données permettra l'implémentation de la partie "cross protocole". En analysant les logs des deux bases de données, on peut faire une corrélation entre les protocoles SIP et RTP, ainsi détecter les fraudes de facturation par exemple. Ce travail de diplôme préconise aussi une interconnexion de l'IDS à la plateforme de gestions des Intrusions SIMS (Security Intrusion Management System) de l'Institut ICT

Auteur: **Christian THEVOZ**
Répondant externe:
Prof. responsable: **Stefano Ventura**
Sujet proposé par: **Stefano Ventura**

Hes·so
Haute Ecole Spécialisée
de Suisse occidentale