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

Corrélation d'évènements dans un environnement VoIP avec ExaProtect

Origines de l'étude

D'un côté, les composants d'un réseau informatique produisent depuis longtemps quantité de journaux d'évènements, appelés aussi logs. Ceux-ci sont une source extraordinaire de données pertinentes – souvent noyées dans la masse d'informations – sur les activités et évènements se déroulant autour d'eux.

« La pertinence des logs… »

De l'autre, la voix sur IP, formidable révolution de la téléphonie, est aujourd'hui en cours de déploiement à grande échelle. Mais cela, trop souvent sans les précautions essentielles en matière de sécurité élémentaire. Certes, les risques concrets ne sont pour l'heure que relativement limités, pourtant, avec la démocratisation croissante de cette technologie, il y a de fortes raisons de penser que le calme apparent ne perdurera pas.

« …appliquée à la sécurité de la VoIP »

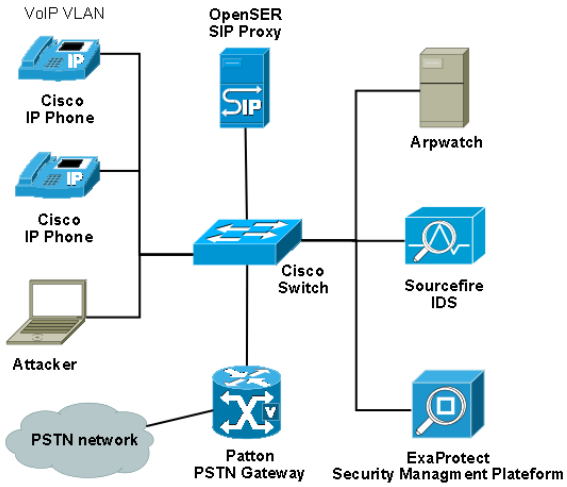
Corrélation et ExaProtect

Des liens existent assurément entre ces deux mondes, il suffit de disposer de l'outil qui permettra une analyse suffisamment avancée des évènements complexes liés à la VoIP. Cet outil pourrait bien être ExaProtect, un SIEM (Security Information & Event Management) connu du monde de la sécurité et qui, sur le papier, dispose de nombreux atouts pour y parvenir. Les systèmes SIEM ont fait leurs preuves en matière d'analyse globale de la sécurité, ils apportent un moyen extrêmement efficace d'extraction et de corrélation des informations à partir de nombreuses données multi-sources et hétérogènes.

exaprotect

Réalisation

Un modèle d'environnement VoIP représentatif de celui d'une petite entreprise a été mis en place.



Le premier but consiste à récupérer des informations sur ces composants :

- le proxy SIP fournit toutes les données sur la signalisation des appels,
- l'IDS indique la présence de messages RTP entre les téléphones,
- l'application Arpwatch qui va informer de toute attaque sur ce protocole.

Rassemblés via Syslog, SNMP ou avec un agent spécialisé, ces évènements vont être dans un deuxième temps analysés avec ExaProtect sur trois niveaux :

- analyse comportementale « connue » (appels standards, actions régulières),
- par scénarios d'attaques (dénis de service, écoutes clandestines, redirections…),
- analyse d'attaques inconnues ou comportementales telles que le SPIT.

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

Hes·so
Haute Ecole Spécialisée
de Suisse occidentale