Ecole d'ingénieurs
du Canton de Vaud

Tél. : + 41 24 423 21 11
Fax : + 41 24 425 00 50

mailto:info@eivd.ch
http://www.eivd.ch

Travail de diplôme 2003
Département E + I

Ecole d'ingénieurs du Canton de Vaud
Route de Cheseaux 1, case postale
CH - 1401 Yverdon - les - Bains

Hybrid IDS

Description

Il ne se passe pas un jour sans que l'on ne parle de virus, cheval de troie et autres intrusions dans les systèmes informatiques. La sécurité informatique est devenue une obligation. Il existe une panoplie d'appareils et de logiciels que l'on peut utiliser afin de combattre le cybercrime, dont les IDS. Un IDS, ou système de détection d'intrusion, est une solution informatique permettant de garder une trace des attaques perpétuées sur un réseau ou une machine par des hackers. Les IDS souffrent d'un grand problème: ils lèvent de nombreuses fausses alertes appelés "**false positive**". Des fichiers logs interminables sont remplis de fausses alertes que des spécialistes de la sécurité doivent analyser avec des moyens le plus souvent sommaires. Afin de minimiser les "**false positive**" on peut essayer de corréler différentes informations, comparer plusieurs sources afin de n'en ressortir que de véritables attaques et gagner du temps sur l'analyse. Cette corrélation peut se faire par une multitude de moyens dont une entre un IDS et un scanneur de vulnérabilité.

Snort est l'IDS le plus connu et utilisé

Mandat

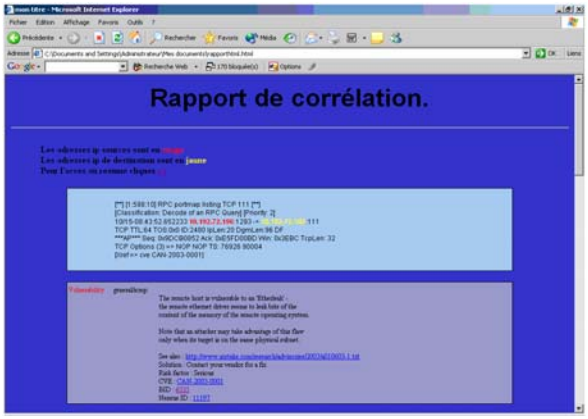
Le travail consiste à trouver un moyen de corréler de manière simple, un système de détection d'intrusions et un scanneur de vulnérabilités, ceci avec des moyens Open Source et sous Linux. Bien sûr il faudra aussi que cette solution soit le plus possible automatisée.

Outils pour la réalisation

La corrélation sera faite avec les outils Open Source les plus connus et utilisé dans le monde de la sécurité qui sont *Snort* et *Nessus*.

Nessus est un scanneur de vulnérabilité réputé également utilisé par les hackers.

La solution de corrélation utilisera des références que l'on trouve dans les fichiers logs des deux programmes. La partie programmation sera faite en Perl, qui est un langage de programmation puissant donc une des spécialités est la réalisation de rapport et la manipulation de chaînes de caractères.



Résultats

Le résultat donne un rapport en HTML regroupant les paquets corrélés suspects suivis des informations sur la vulnérabilité décelée et des moyens pour y remédier. La solution est fonctionnelle mais seule une petite partie des vulnérabilités actuelles sont traçables dû à la petite partie des vulnérabilités actuelles relevés par les deux programmes utilisés. Néanmoins une partie pénible du travail de l'analyste est ainsi réalisée.

Auteur: **Pierre Duc**
Répondant externe: **Christophe Gabioud**
Prof. responsable: **Stephan Robert**
Sujet proposé par: **Swisscom mobile**

Hes·so
Haute Ecole Spécialisée
de Suisse occidentale