Ecole d'ingénieurs
du Canton de Vaud

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

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

Travail de diplôme 2004

Département Electricité et Informatique

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

Sécurité UNIX - Automatisation d'un audit système

Description

Unicible développe et intègre des solutions d'informatique bancaire pour les banques cantonales romandes.

La sécurité est une composante primordiale dans ces environnements et Unicible recherche et déploie les meilleures solutions pour implémenter sa politique de sécurité.

En 2001, un modèle d'audit des systèmes Unix a été proposé avec une liste de critères exhaustive selon le concept de sécurité Unix d'Unicible.

Afin d'optimiser l'audit système pour un parc large et complexe, Unicible souhaite automatiser les audits et reporting d'une manière pragmatique en utilisant le modèle proposé.

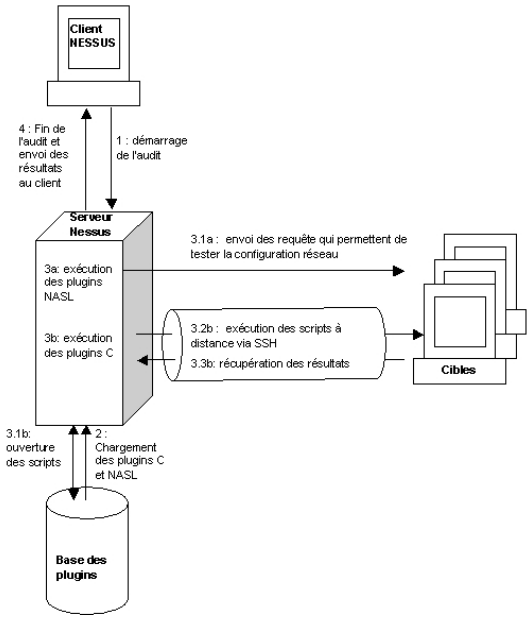
L'outil Nessus a été choisi parmi plusieurs outils "open source" et étendu pour parvenir à ce but. Le reporting a été également adapté de manière à répondre au standard de documentation d'Unicible.

Automatisation d'un échantillon de 20 tests

Nessus permet le développement de ses propres tests de vulnérabilités à l'aide de deux langages : NASL (Nessus Attack Scripting Language) et C. NASL ne permet pas de réaliser des contrôles locaux à un système. Le langage C a été utilisé pour implémenter ces tests.

Ces examens, réalisés sous la forme de scripts shells, sont réalisés de manière totalement sécurisée grâce à l'utilisation de SSH qui les exécute depuis un serveur sans avoir à copier des données sur les machines cibles.

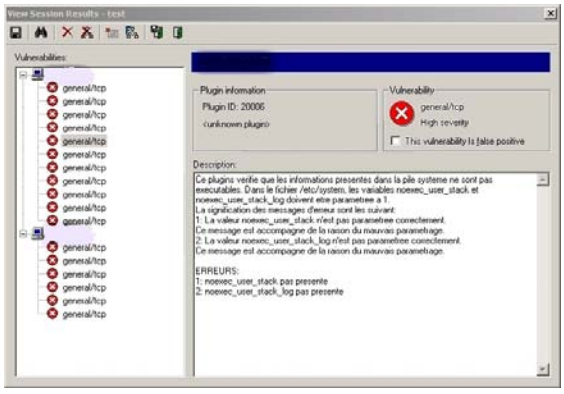
Un client permet de paramétrer, d'exécuter et de visualiser les résultats de l'audit depuis n'importe quel endroit pour autant que le serveur soit atteignable par un réseau informatique, via SSH.



Architecture de l'audit

Résultat

L'exécution de Nessus couplé à des contrôles de vulnérabilités systèmes permet d'avoir une vision réseau et systèmes des failles répertoriées sur une machine donnée.



Résultat de l'exécution de Nessus

Auteur: **Guye Benoît**
Répondant externe: **Minh Richoz**
Prof. responsable: **Buchs Christian**
Sujet proposé par: **Minh Richoz, Unicible SA**

Hes·so
Haute Ecole Spécialisée
de Suisse occidentale