Nessus

Outil d'exploration réseau et scanneur de ports/sécurité

1. Présentation

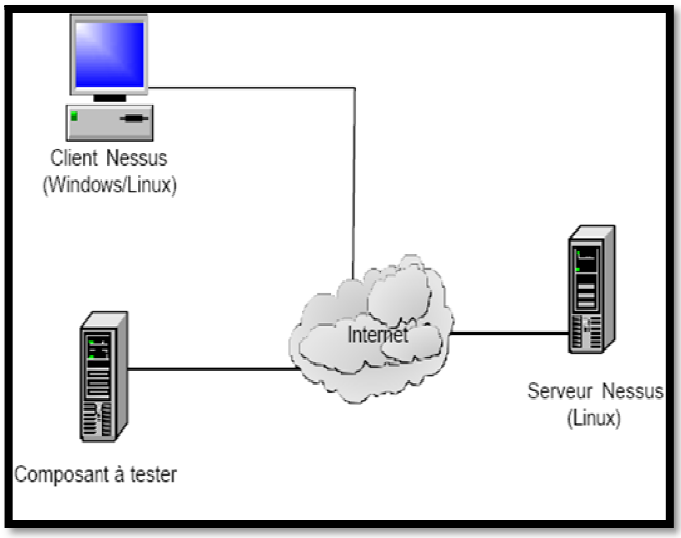
Nessus est un bon outil pour automatiser le test et découvrir les problèmes de sécurité.
Utilisé par: Simple utilisateur, hacker group, Security company, les chercheurs de violation de sécurité.
Environnement: Windows, Linux, Mac, OSX, BSD, Solaris..
Licence: GPL.
Nessus est ce qu'on appelle un scanner de vulnérabilité, c'est à dire qu'il va balayer une cible à la recherche des vulnérabilités : erreurs dans le code, backdoors ... Il produit un rapport étendu et propose même des solutions. Il propose une batterie de fonctionnalités avancées, citons :

- La possibilité d'utiliser les techniques classiques d'évasion d'IDS (encodage des séquences d'attaques...)
- Il peut sauvegarder des sessions de scan sur le serveur.
- Nous pouvons effectuer des scans en parallèle (gain de rapidité et de performance).
- Nous pouvons utiliser les "safe checks" pour les plugins de test.

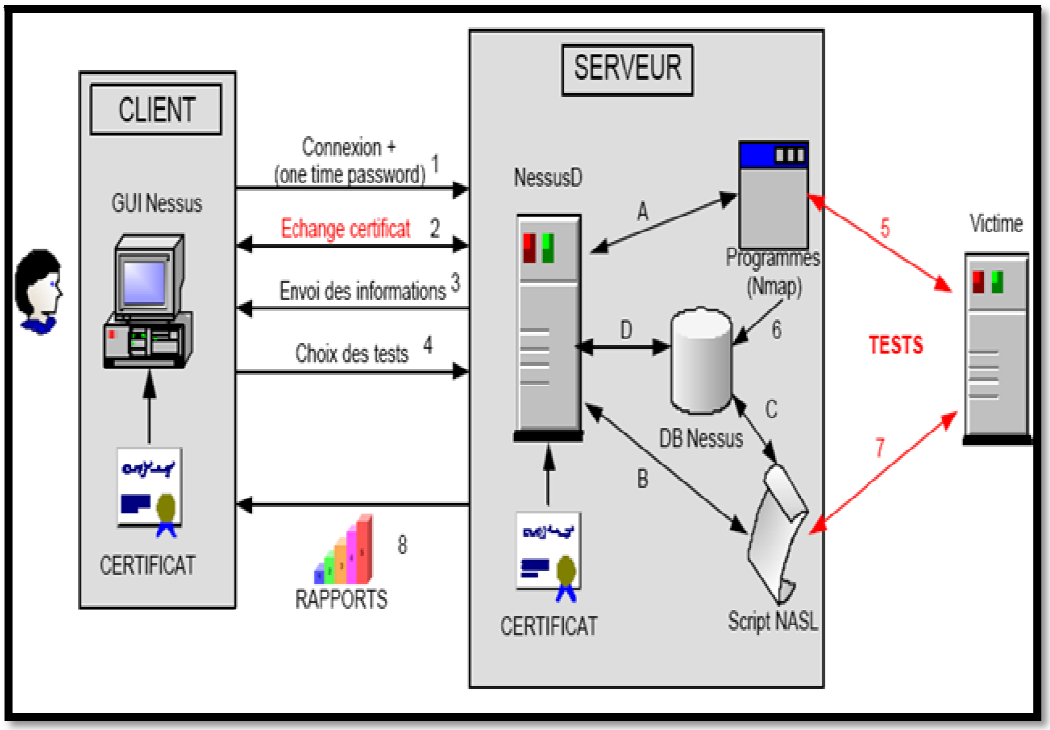
2. Fonctionnement

Nessus fonctionne en client/serveur. Le serveur s'appelle Nessusd, un daemon, et le client nessus. Le serveur est généralement sur une machine, Unix ou Linux. Le serveur pouvant être sous Windows. Il n'est pas nécessaire que le client et le serveur soit sur la même machine.

3. Topologie de NESSUS



4. Architecture de NESSUS



1) Le client se connecte pour la première fois au serveur et s'identifie avec un One Time password pré-programmé sur le serveur.
2) Le Client et le serveur s'échange leur certificat pour crypter les données et pour que le serveur authentifie le client grâce à ce certificat.
3) Le serveur envoie au client les divers tests possibles et les options.
4) Le client envoie les données choisies au serveur.

A- Nessusd enclenche Nmap pour scanner la victime avec les fonctions choisies.

5) Nmap réalise son scan.
6) Nmap enregistre les données dans la DataBase.

B- Nessusd démarre les scripts correspondants aux données recueillies par Nmap (si le port 80 est ouvert, Nessusd lance un http overflow).

7) Les scripts NASL testent le système de la victime grâce aux données dans la DataBase.

C- Les scripts enregistrent les données récupérées dans la DataBase.

A, B, D- Toutes les valeurs relatives aux tests et aux données récoltées sont envoyées à Nessusd durant les tests.

8) Nessusd génère un rapport qui sera transmis au Client.