0.1 Scanner de vulnérabilité : Nessus

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
- Vous pouvez effectuer les scans en parallèle (gain de rapidité et de performance)
- Vous pouvez utiliser les "safe checks" pour les plugins de test.

et j'en oublie. Comme il est d'usage en matière de sécurité sur trustonme, nous n'étudierons que l'installation à partir des sources. Ceci pour mettre toutes les distributions sur un pied d'égalité et être sûr que vous maîtrisiez tous les rouages de cette installation.

0.1.1 1. Pré-requis :

Pour utiliser, Nessus vous devez disposer des logiciels qui vont suivre, ils sont en principe présent sur les CDS de votre distribution et souvent installé par défaut :

- GTK 1.2, qui correspond à gnome 1.x
- Nmap, un scanner de ports
- OpenSSL une librairie utiliser pour les communications sécurisées.
- Les sources des logiciels de la suite Nessus : nessus-libraries, libnasl, nessus-core, nessus-plugins téléchargeables ici[1]. Téléchargez les sources de la version la plus récente de nessus. Au moment où j'écrivais ce document, c'était la 1.2.7, je suis donc allé dans : **nessus-1.2.7/src/**

0.1.2 2. Installation :

Commencez par décompresser les sources des logiciels :

```
tar -xzvf /où_est/nessus-libraries-1.2.7.tar.gz
tar -xzvf /où_est/libnasl-1.2.7.tar.gz
tar -xzvf /où_est/nessus-core-1.2.7.tar.gz
tar -xzvf /où_est/nessus-plugins-1.2.7.tar.gz
```

Compilez et installez nessus-librairies :

```
cd nessus-libraries/
./configure –prefix=/usr
make
make install
```

Compilez et installez libnasl :

```
cd ../libnasl/
./configure –prefix=/usr
make
make install
```

[1] ftp://ftp.nessus.org/pub/nessus/

Compilez et installez nessus-core :

```
cd ../nessus-core/
./configure –prefix=/usr
make
make install
```

Compilez et installez nessus-plugins :

```
cd ../nessus-plugins/
./configure –prefix=/usr
make
make install
```

0.1.3 3. Utilisation et Configuration :

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 nécesaire que le client et le serveur soit sur la même machine. Les paquetages que vous venez d'installer, comprennent les 2.

0.1.4 3.1 Configuration et lancement du serveur :

Avant de lancer le daemon nessusd, il faut rajouter, au moins, un utilisateur et son mot de passe. Vous êtes obligé d'être root pour ça, mais l'utilisateur peut ne pas s'appeler root. Pour ce faire tapez : **nessus-adduser** . Voici le détail du dialogue chez moi :

```
Using /var/tmp as a temporary file holder
Add a new nessusd user
————————-
Login : Kernel
Authentication (pass/cert) [pass] : pass
Login password : xxxxxx
User rules
———-
nessusd has a rules system which allows you to restrict the hosts
that Kernel has the right to test. For instance, you may want
him to be able to scan his own host only.
Please see the nessus-adduser(8) man page for the rules syntax
Enter the rules for this user, and hit ctrl-D once you are done :
(the user can have an empty rules set)
Login : kernel
Password : xxxxxx
DN :
Rules :
Is that ok ? (y/n) [y] y
user added.
```

Je n'ai mis aucune règle, cela signifie que l'utilisateur kernel a le droit de scanner n'importe quelle machine. Pour valider les règles c'est [ctrl]+[d] . Vous pouvez bien-sûr définir d'autres utilisateurs, avec des droits différents. Voici des exemples de règles : l'utilisateur a le droit de scanner uniquement les classes d'adresses sus-mentionnée :

```
accept 192.168.1.0/24
accept 192.168.3.0/24
accept 172.22.0.0/16
default deny
```

l'utilisateur peut scanner tout sauf le réseau : 192.168.1.0/24 :

```
deny 192.168.1.0/24
default accept
```

l'utilisateur n'a le droit de scanner que sa machine :

```
accept client_ip
default deny
```

A ce stade le serveur est presque finalisé, il vous faut maintenant générer, le certificat SSL et les clés privés. Pour ce faire, tapez :

```
nessus-mkcert
```

Répondez aux questions. Quand vous êtes satisfait, tapez :

```
nessusd -s
```

Il affichera le fichier de config de nessus, à savoir, /usr/etc/nessus/nessusd.conf. Maintenant, vous pouvez lancer le daemon par :

```
/usr/sbin/nessusd -D
```

Vérifiez que tout c'est bien passé en tapant :

```
ps aux | grep nessusd
root 16409 0.0 0.6 5400 3452 ? S 19 :04 0 :00 /usr/sbin/nessusd -D
```

Si vous obtenez cette dernière ligne c'est que tout s'est bien passé.

0.1.5 3.2 Configuration et lancement du client :

Nessus compilé avec le support gtk, propose un client graphique que vous pouvez lancer en simple utilisateur par :

```
nessus &
```

Vous obtenez une fenêtre comme celle-là : Il y'a 8 onglets. Le premier onglet est **"nessusd host"**. Vous pouvez à partir de là, vous connecter sur l'hôte nessusd en cliquant sur le bouton **"Log in"**. Là le module SSL se lance, choisissez la 2ème option : **"Trust the server certificate if and only if it is valid and certified by the CA"**. Le deuxième onglet concerne les plugins. Vous y sélectionnez (ou désélectionnez) les plugins à utiliser pendant le scan. Cochez, **"Enable dependencies at runtime"**. En cliquant sur un plugin vous avez la description du contenu. Pensez à enlever ce qui est inutile ou dangereux. Le troisième onglet définit les préférences des plugins : FTP, plugins ... Le quatrième onglet permet de définir les options de scan et le port scanner, assurez-vous d'avoir cocher nmap. Dans le

cinquième onglet vous indiquez à nessus la cible à scanner. Dans le champ **"target"** vous pouvez écrire le nom d'un ou plusieurs hôtes, séparés par des virgules. Ou une ou plusieurs adresses IP, toujours séparées par des virgules. Ou encore une classe d'adresse, exemple : 192.168.0.1/24 Le sixième onglet permet à l'utilisateur de gérer ses paramètres. Le septième concerne le KB (Knowledge base), la base de connaissances. La huitième et dernière affiche la page Crédits.

0.1.6 3.3 Un scan :

Quand tout est au point, toujours dans la fenêtre de nessus, cliquez sur **"start the scan"** pour lancer le scan. Il apparaît alors la fenêtre suivante : Quand le scan est finit, il vous affiche une fenêtre récapitulative. En cliquant sur un hôte vous obtenez les résultats de son scan. En cliquant sur **"save report"** vous pouvez sauvegarder le rapport dans le format de votre choix. Si vous choisissez html avec graphe, il vous suffit d'indiquer un répertoire et il créera lui-même les fichiers html et les images qui vont avec.

0.1.7 3.4 Post-installation :

Si vous souhaitez que nessusd soit lancé au démarrage de l'ordinateur, il vous suffit de rajouter la ligne suivante :

```
/usr/sbin/nessusd -D
```

Dans votre /etc/rc.d/rc.local. Vous pouvez supprimer un utilisateur, en utilisant la commande :

```
/usr/sbin/nessus-rmuser
```

Pour finir, le fichier /usr/etc/nessus/nessusd.conf, fourni de précieuses informations sur votre installation, il vous indique notamment que vos logs sont consignés dans /usr/var/nessus/logs/nessusd.mes

0.1.8 4. Conclusion :

C'est grâce aux plugins que vous pouvez tester vos machines, ils occupent donc une place de choix. Ils sont écrit dans un langage de scripts nommé : NASL (Nessus Attack Scripting Language). Ils sont localisés dans /usr/lib/nessus/plugin/. Vous avez bien-sûr la possibilité d'en écrire vous-même, pour ce faire, consultez le document suivant[2]. Si vous souhaitez mettre à jour vos scripts, rendez-vous ici[3] Ceci ne constitue qu'une introduction à Nessus, si vous êtes intéressé par ce logiciel, rendez-vous sur le site officiel[4] et consultez la doc en ligne.

[2] http://www.nessus.org/doc/nasl.html
[3] http://cgi.nessus.org/plugins/
[4] http://www.nessus.org/