Nessus

Nessus est un outil d'audit "externe", dans le sens où il simule des attaques depuis un réseau vers un serveur.
Il vérifie la version des serveurs associés, leur configuration, et teste les failles de sécurité connues.
Il s'adresse à l'audit de machines très diverses : routeurs CISCO, serveurs Windows, Unix...

Nessus est une aplication client/serveur

- serveur Nessus : exécute les attaques
- client Nessus : sélectionne les attaques et machines à tester

Le serveur n'est disponible que pour Unix, le client existe pour Unix et Windows.

Modulabilité

Le serveur Nessus est constitué d'un démon et de plugins, qui exécutent les attaques vers les services.

Nessus est livré avec près de 2000 plugins différents. La mise à jour des plugins est facilitée afin de détecter de nouvelles failles de sécurité :

```
nessus-update-plugins
```

nessus - installation

Packages prérequis

Télécharger sur `http://atrpms.net/dist/el5/nessus/` les paquets nécessaires à l'installation (pour une RedHat 6, utilisez le répertoire el6) :

```
libnasl-2.2.xxxxx.at.i386.rpm
nessus-server-2.2.xxxxx.at.i386.rpm
nessus-2.2.xxxxx.at.i386.rpm
libnessus-2.2.xxxxx.at.i386.rpm
```

nessus - installation

Mise en place du serveur

créer le certificat du serveur :

```
[root@ServPort09 ~]# nessus-mkcert
-------------------------------------------------------------------------------
                        Creation of the Nessus SSL Certificate
-------------------------------------------------------------------------------

This script will now ask you the relevant information to create the SSL
certificate of Nessus. Note that this information will *NOT* be sent to
...
Congratulations. Your server certificate was properly created.

/usr/local/etc/nessus/nessusd.conf updated

The following files were created :

. Certification authority :
   Certificate = /usr/local/com/nessus/CA/cacert.pem
   Private key = /usr/local/var/nessus/CA/cakey.pem

. Nessus Server :
    Certificate = /usr/local/com/nessus/CA/servercert.pem
    Private key = /usr/local/var/nessus/CA/serverkey.pem

Press [ENTER] to exit
```

nessus - exploitation

Ajout d'utilisateurs autorisés à se connecter au serveur

créer un compte d'utilisateur nessus :

```
[root@ServPort09 ~]# nessus-adduser
Using /var/tmp as a temporary file holder

Add a new nessusd user
----------------------
Login : audit
Authentication (pass/cert) [pass] :
Login password : bonjour

User rules
----------
nessusd has a rules system which allows you to restrict the hosts
that audit 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             : audit
Password          : bonjour
DN                :
Rules             :

Is that ok ? (y/n) [y] y
user added.
```

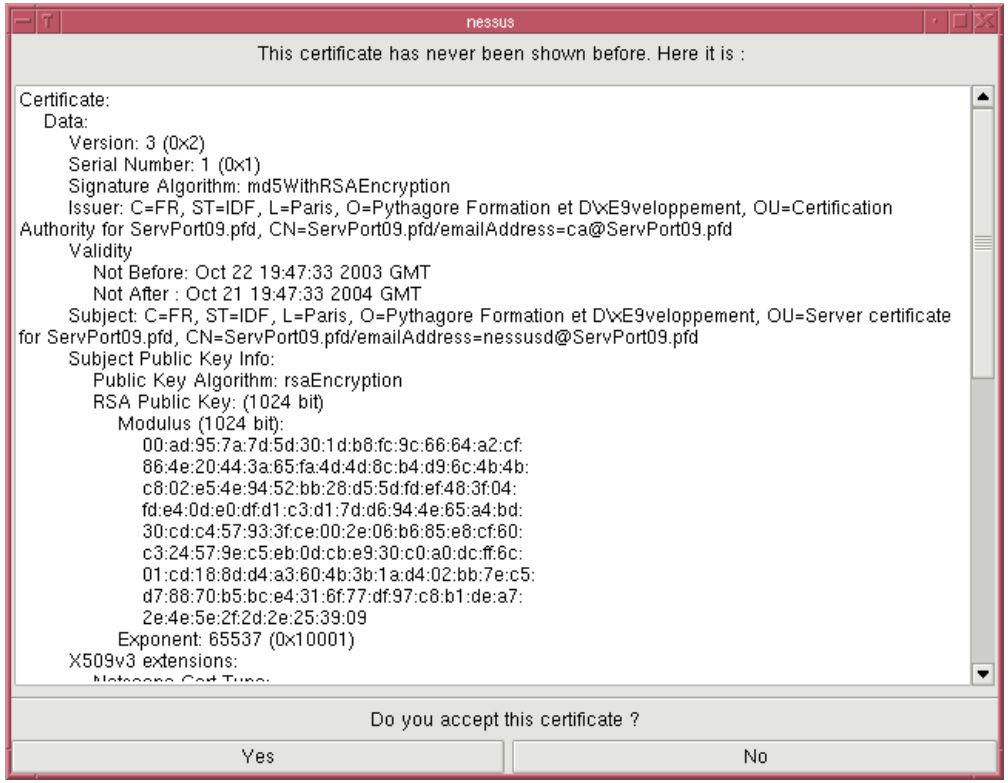
nessus - exploitation

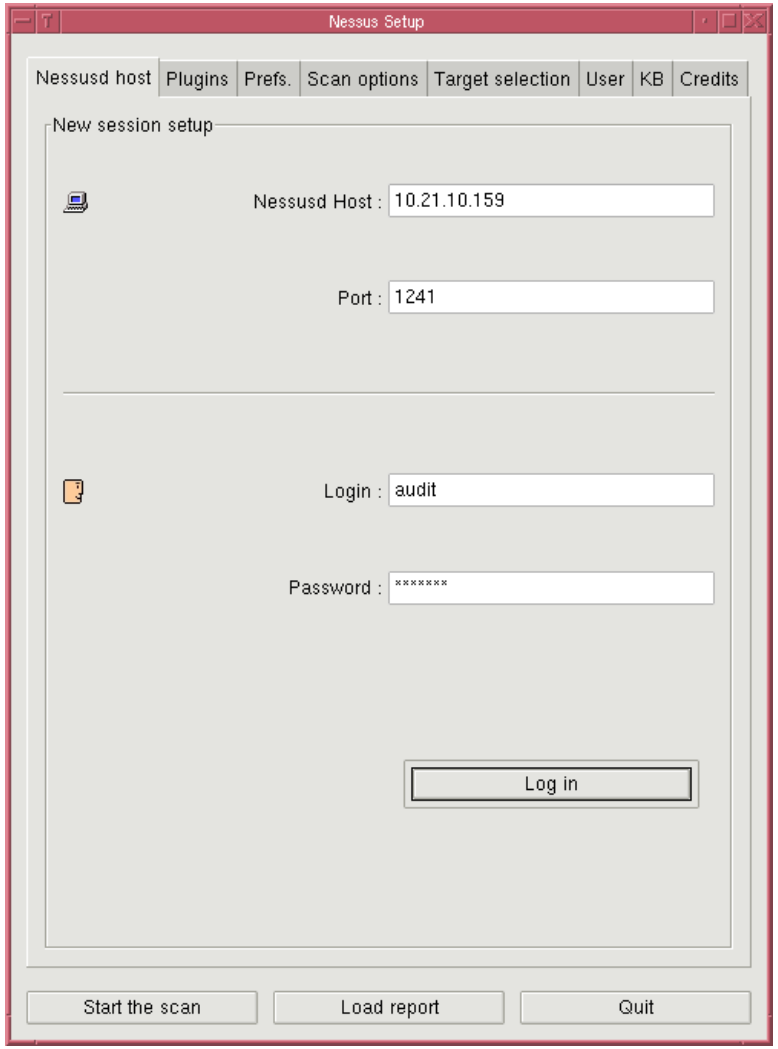
lancer Nessus en démon :

```
service nessusd start
```

lancer un client Nessus

depuis n'importe quelle machine cliente :





nessus - exploitation

Sélectionner les plugins en fonction de la machine à auditer, puis choisir la (ou les cibles) :