

Nessus Lab

Installation:

Nessus is made up of two parts : a client and a server. You need a Unix-like system to use the server (Linux is just fine). In this test, I used the standard client *nessus*, mainly because I wrote it and because it is the only one that supports the cipher layer.

The Nessus Security Scanner relies on the following items:

- **GTK** - The Gimp Toolkit, version 1.2

GTK is a set of Widgets (like Motif) which are used by many open-sourced programs such as [The Gimp](#). GTK is used by the POSIX client *nessus*.

Download it at : <ftp://ftp.gimp.org/pub/gtk/v1.2>.

Note : If your system comes with GTK, make sure that you have the *gtk-config* program installed. If you do not, install the *gtk-devel* package that should come on your distribution CDROM.

Note #2: If you do not want to install GTK and/or if your system lacks X11, then you can compile a command-line client by doing

```
./configure --disable-gtk
```

in *nessus-core*

- **Nmap** which is an excellent portscanner and which is available at <http://www.insecure.org/nmap/>. I recommend you use Nmap 3.00 or 2.54.
- **OpenSSL** (optional but heavily recommended). OpenSSL is used for the client - server communication as well as in the testing of SSL-enabled services. Get it at <http://www.openssl.org>.

Nessus also comes as a standalone package that auto-installs itself. To use it, download the script *nessus-installer.sh*

<http://www.nessus.org/download.html>

```
# sh nessus-installer.sh
```

Choose the default locations to install the nessus files: /usr/local

Using Nessus:

1. Create a nessusd account

The nessusd server has its own users database, each user having a set of restrictions. This allows you to share a single nessusd server for a whole network and different administrators who will only test their part of the network.

The utility *nessus-adduser* takes care of the creation of a new account :

```
# nessus-adduser
Using /var/tmp as a temporary file holder

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

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

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

2. Configure your nessus daemon / run command 'nessus-mkcert' to create certificates

In the file `/usr/local/etc/nessus/nessusd.conf`, I can set several options for nessusd. Typically this is where you can define that you want nessusd to use your favorite language (french for me). Anyway, I kept the standard configuration file for this demonstration.

3. Start *nessusd*

Once all of this is done, I can safely start nessusd as root :

```
nessusd -D
```

4. Fire up *nessus* in X windows graphical environment

Click on **Login**, since this setup is correct. Since this is the first time connecting to this server, it will ask the password. The next time you connect to it, the public key will be enough.

Once connected, the **Log in** button changes to **Log out**, and a **Connected** label appears at its left.

5. The security checks configuration

Let all the security check to be performed, except the Denial of Service attacks, because you do not want hosts to crash.

Clicking on a plugin name will pop up a window explaining what the plugin does.

6. The plugins preferences

Some security checks will require extra arguments. For instance, the pop2 overflow security test needs a valid pop account. The plugin which tests whether a FTP directory is writeable or not asks if it should just trust the permissions or really attempt to store a file. And so on... This screen shot shows the configuration of Nmap.

7. The scan options

Here you choose which port scanner you want to use. Prefer to use the Nmap tcp connect scanner, since it's the fastest.

8. Define the targets

Uncheck the 'Perform a DNS transfer zone' option, since it would make DNS transfer on *fr.nessus.org* and *nessus.org*, and it would be useless, since it would not gain any new hosts.

Use the following options to define the targets:

192.168.1.1	A single IP address.
192.168.1.1-7	A range of IP addresses.
192.168.2.1-192.168.2.50	Another range of IP addresses.
192.168.1.1/29	Again a range of IP addresses in CIDR notation.
prof.fr.nessus.org	A hostname in Full Qualified Domain Name notation.
prof	A hostname (as long as it is resolvable on the server).
prof, 192.168.1.1/29, ...	Any combination of the above mentioned forms separated by a comma.

9. The rules section

The rules allow a user to restrict his test. For instance, if you want to test 192.168.1.0/29, except 192.168.1.2. The ruleset entered allows you to do that. Once all of this is done, start the scan...

10. The Nessus scan report

Now that the scan is over, the report window just pops up

11. Resolving the security issues

Go through the scan report and try to resolve reported security holes on the respective servers by following the suggestions given in the report OR by referring to the vendor's site.