



The **Nessus Security Scanner** is a security auditing tool made up of two parts: a server, and a client. The server, **nessusd** is in charge of the attacks, while the client **nessus** interfaces with the user.

**nessusd** inspect the remote hosts and attempts to list all the vulnerabilities and common misconfigurations that affects them.

You can download Nessus from [www.nessus.org](http://www.nessus.org) . There are two ways to install Nessus:

- Automatic with script “nessus.installer.sh”
- Manual compilations and installation

My notebook is running Kernel 2.4.18-14, based on Red Hat Linux.

### *Manual Installation Steps of the Client*

Download following libraries from [www.nessus.org/nessus\\_2\\_0.html](http://www.nessus.org/nessus_2_0.html)

- nessus-libraries-2.0.10a.tar.gz
- libnasl-2.0.10a.tar.gz
- nessus-core-2.0.10a.tar.gz
- nessus-plugins-2.0.10a.tar.gz

#### Download Extract the Tarballs

```
tar -xvzf nessus-libraries-2.0.10a.tar.gz
tar -xvzf libnasl-2.0.10a.tar.gz
tar -xvzf nessus-core-2.0.10a.tar.gz
tar -xvzf nessus-plugins-2.0.10a.tar.gz
```

You must compile and install them in following order

### *1. Compiling and installing nessus-libraries*

Compiling nessus-libraries is a simple operation :

```
cd nessus-libraries
./configure
make
```

After this, execute this command as root :

```
make install
```



#### DISCLAIMER

This Technical Tip or TechNote is provided as information only. I cannot make any guarantee, either explicit or implied, as to its accuracy to specific system installations / configurations. Readers should consult each Vendor for further information or support.

Although I believe the information provided in this document to be accurate at the time of writing, I reserve the right to modify, update, retract or otherwise change the information contained within for any reason and without notice. This technote has been created after studying the material and / or practical evaluation by myself. All liability for use of the information presented here remains with the user.

## 2. Compiling and installing libnasl

```
cd libnasl
./configure
make
```

After this, execute this command as root :

```
make install
```

## 3. Compiling and installing nessus-core

```
cd nessus-core
./configure
make
```

After this, execute this command as root :

```
make install
```

## 4. Compiling and installing nessus-plugins

```
cd nessus-core
./configure
make
```

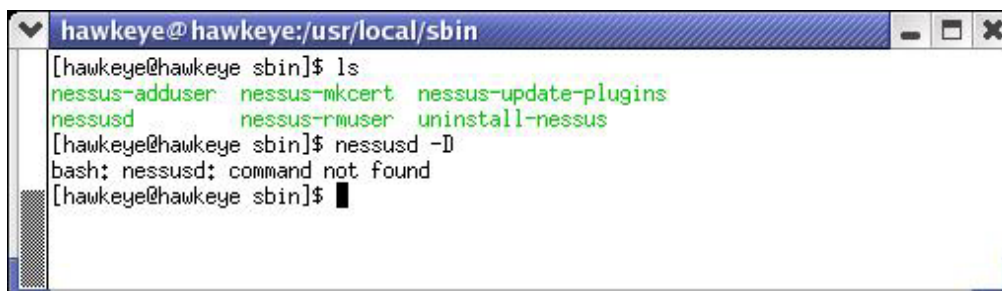
After this, execute this command as root :

```
make install
```

### Setting Library Path

Make sure, that Library path “*/usr/local/lib*” is set in */etc/ld.so.conf*.

Now, you are ready to fire up NESSUS



```
hawkeye@hawkeye:/usr/local/sbin
[hawkeye@hawkeye sbin]$ ls
nessus-adduser  nessus-mkcert  nessus-update-plugins
nessusd         nessus-rmuser  uninstall-nessus
[hawkeye@hawkeye sbin]$ nessusd -D
bash: nessusd: command not found
[hawkeye@hawkeye sbin]$
```

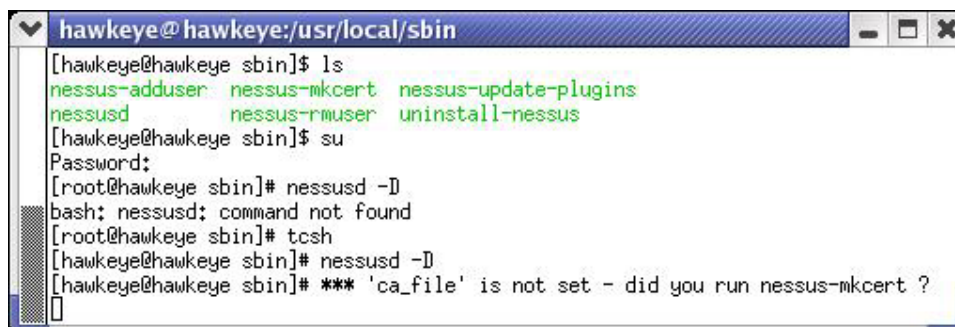


## Command not found

It's not Murphy, when you just have installed a Program, such as Nessus in this case and you try to run it. Sometimes you found a message, like "Command not found". OK, you verified the Path settings and they look good – next, you move your prompt into the directory to make sure the files are there. Still stuck with "Command not found"?

To remember, you have to be root in order to run NESSUS.

Probably, you use `tcsh` or `csh`, which caches program names and paths. Try to change the shell and restart the program again.



```
hawkeye@hawkeye:/usr/local/sbin
[hawkeye@hawkeye sbin]$ ls
nessus-adduser  nessus-mkcert  nessus-update-plugins
nessusd         nessus-rmuser  uninstall-nessus
[hawkeye@hawkeye sbin]$ su
Password:
[root@hawkeye sbin]# nessusd -D
bash: nessusd: command not found
[root@hawkeye sbin]# tcsh
[hawkeye@hawkeye sbin]# nessusd -D
[hawkeye@hawkeye sbin]# *** 'ca_file' is not set - did you run nessus-mkcert ?

```

## Create Certificate

```
# nessusd -D
```

A script will help to create a NESSUS SSL Certificate.

```
CA certificate life time in days [1460]: <return>
Server certificate life time in days [365]: <return>
Your country (two letter code): DE
Your state or province name [none]:
Your location (e.g. town) [Paris]: Munich
Your organization [Nessus Users United]: McAfee Security
```

You should get a similar message like this:



```
hawkeye@hawkeye:/usr/local/sbin
-----
Creation of the Nessus SSL Certificate
-----
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

```

## Add Nessus User

```
Login: McNessus
Authentication: (pass/cert) [pass]: <return>
Login password: password
```

You could either add rules or hit CTRL-D once you are done

```
hawkeye@hawkeye:/usr/local/sbin
-----
nessusd has a rules system which allows you to restrict the hosts
that McNessus 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)

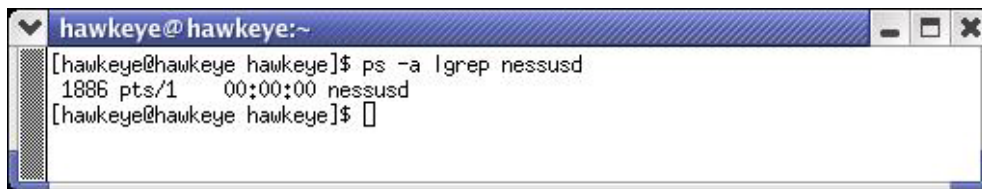
Login          : McNessus
Password       : password
DN             :
Rules          :

Is that ok ? (y/n) [y] y
user added.
[hawkeye@hawkeye sbin]#
```

Now, you are really ready to run NESSUS for the first time.



Verify, if NISSUS Daemon is running



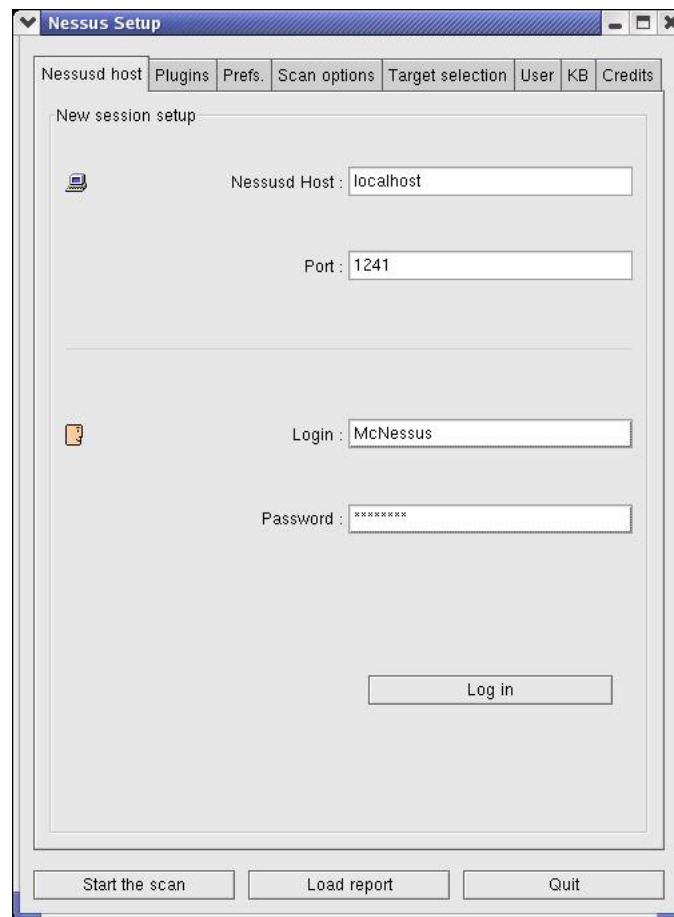
```
hawkeye@hawkeye:~  
[hawkeye@hawkeye hawkeye]$ ps -a | grep nessusd  
1886 pts/1    00:00:00 nessusd  
[hawkeye@hawkeye hawkeye]$
```

When getting a positive result, you are ready to start the Nessus client by executing nessus.



```
hawkeye@hawkeye:~  
[hawkeye@hawkeye hawkeye]$ nessus
```

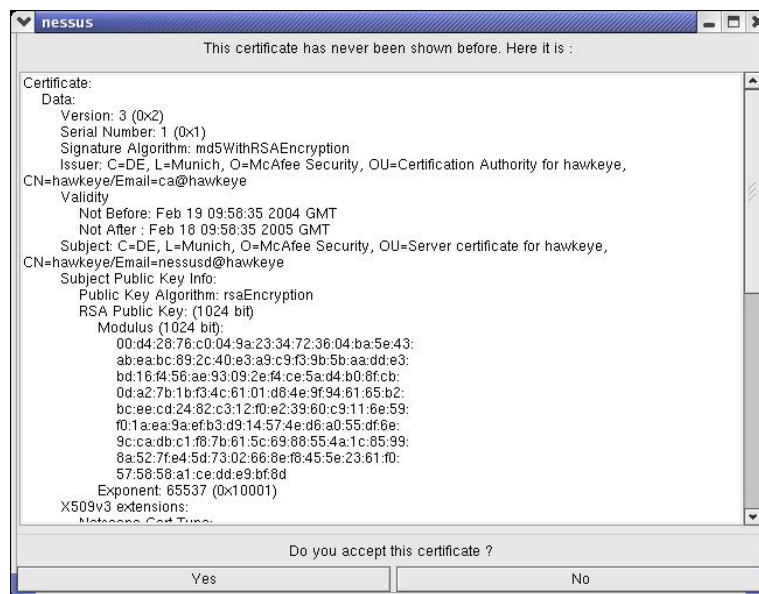
Type the user credentials and hit Log in button



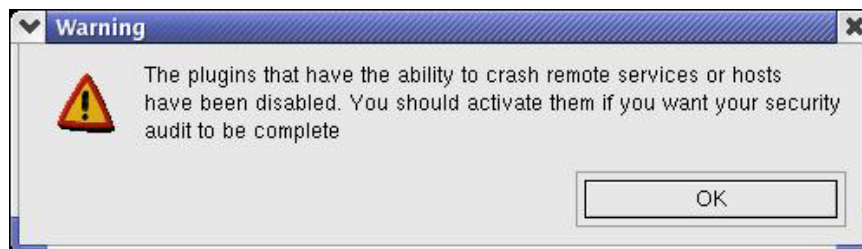
You will get a first time certificate info. You have to accept this certificate in order to continue logon process



Choose and click on OK

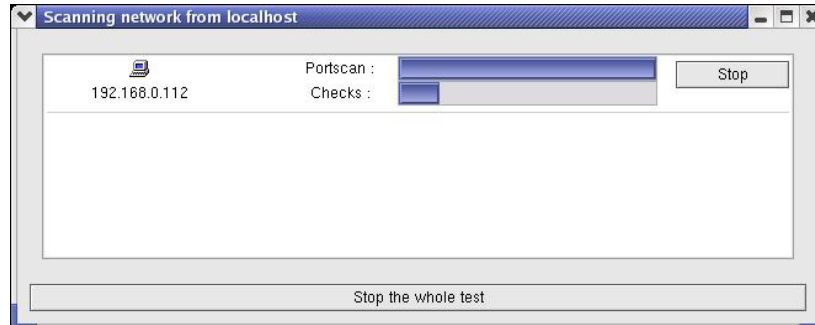


You should get a warning about the plugins, which may be able to crash remote services or hosts. Usually, they are disabled by default.

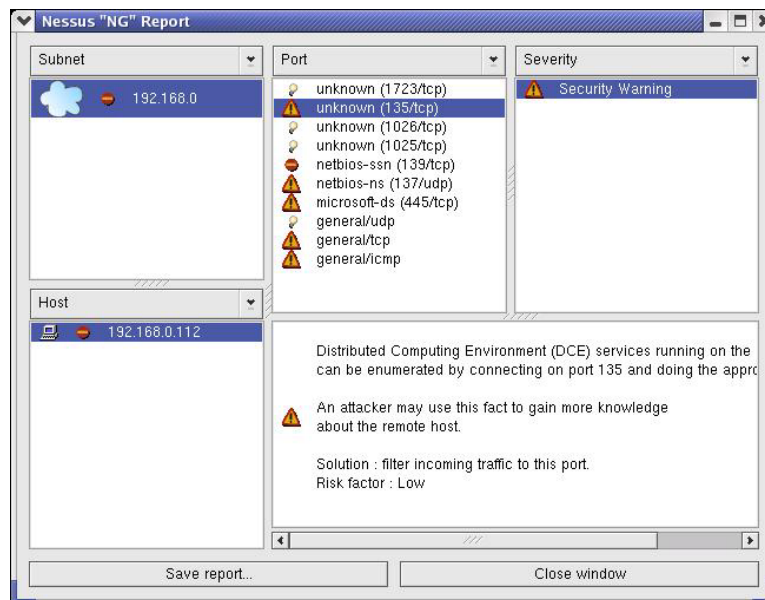


**You are done!**

You can run a first scan with SCAN OPTIONS and TARGET SELECTION



When done, you could see a report of your scan



If you got any issues or problems, please refer to NISSUS FAQs or Documentation

### *Nessus FAQs*

<http://www.nessus.org/doc/faq.html>

### *Nessus Documentation*

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

