Nessus Sever installation

I Downlading and Installing

The installation is easier when we download the self installer from the Nessus website[1]. In the download and installation section page, select the **'easy and less dangerous way'**. The link to the East coast server[2] will open an ftp session from which you can down load the following file:

Nessus-installer.sh

II Getting root access for a non-root user

If you are a user on the Linux machine[3], you might need the administative password to continue. Use the under mentioned command to get root access:

[menonrr@scinterface menonrr]$ **su -**
Password: **********
[root@scinterface root]#

Now we have the root privileges. It is important to navigate to the folder where you downloaded the installer file. I have downloaded the instller file in a folder called 'nessus'.

[root@scinterface root]# **cd /home/menonrr/**
[root@scinterface menonrr]# ls
Desktop Nessus Nessus-doc
[root@scinterface menonrr]# **cd Nessus ---> Folder in my home directory where nessus installer is downloaded**
[root@scinterface Nessus]# ls
nessus-installer.sh sharutils-4.2.1-14.i386.rpm
[root@scinterface Nessus]#

III Runnning the installer – nessus-installer.sh

The shell command for installation is as follows:

sh nessus-installer.sh

---

[1] www.nessus.org -->Download (left hand side) --> select link to Nessus 2.0 which is Nessus version 2.0.10
[2] For instance, http://ftp.nessus.org/nessus/nessus-2.0.10a/nessus-installer/
[3] We use Redhat 9.0

Note: *The installer did not install as it asked for an rpm that it depended on. It is noted below:*

s**harutils-4.2.1-14.i386.rpm**

The rpm was downloaded after a simple search in Google. To be more specific, we can download it from the rpmfind.net at:
<http://rpmfind.net/linux/RPM/redhat/9/i386/sharutils-4.2.1-14.i386.html>.

To install the rpm package, type the command:
rpm -Uvh sharutils-4.2.1-14.i386.rpm

After the rpm is installed, you can resume by running the Nessus installer.

Now run the installer with the command:
sh nessus-installer.sh

The installation is straight forward but included a few <Enter>s. The final message will appear similar to the following:

```
-----------------------------------------------------------------------
Nessus installation : Finished
-----------------------------------------------------------------------
Congratulations ! Nessus is now installed on this host
. Create a nessusd certificate using /usr/local/sbin/nessus-mkcert
. Add a nessusd user use /usr/local/sbin/nessus-adduser
. Start the Nessus daemon (nessusd) use /usr/local/sbin/nessusd -D
. Start the Nessus client (nessus) use /usr/local/bin/nessus
. To uninstall Nessus, use /usr/local/sbin/uninstall-nessus
. Remember to invoke 'nessus-update-plugins' periodically to update your
  list of plugins
. A step by step demo of Nessus is available at :
        http://www.nessus.org/demo/

Press ENTER to quit
```

IV Adding a User and Making a Certificate

The first thing to do is to add a user. The following steps may be followed:

i) User can be added as a root only. So use the **su** command.

ii) Navigate to the directory of the Nessus server:

[root@scinterface root]# cd /usr/local/sbin/

[root@scinterface sbin]# ./nessus-adduser

iii) Add the user and password.

Illustration:

Using /var/tmp as a temporary file holder
Add a new nessusd user

Login : **admin**
Authentication (pass/cert) [pass] : **pass**
Login password : **********

iv) Give the rules for the users

Illustration:

User rules
---
nessusd has a rules system which allows you to restrict the hosts
that **admin** 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)

accept 192.168.1.118/24
accept 192.168.1.111/24

Hit **<ctrl> D** here **.**

Login : admin
Password : ********
DN :
Rules :
accept 192.168.1.118/24
accept 192.168.1.111/24

Type Y for Yes here.

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

V) Adding the Certificate:

The server will prompt for making the certificate. Give Y for yes.

Illustration:

[root@scinterface sbin]# *** 'ca_file' is not set - did you run nessusmkcert
? **y**

If you missed the opportunity, don't fret yet!

Navigate to the nessus directory and run the command as shown.

Illustration:

[root@scinterface Nessus-doc]# cd /usr/local/sbin
[root@scinterface sbin]# ls
nessus-adduser **nessus-mkcert** nessus-update-plugins
nessusd nessus-rmuser uninstall-nessus

The command:

[root@scinterface sbin]# **./nessus-mkcert**

Enter the details for generating the certificate

/usr/local/var/nessus/CA created
/usr/local/com/nessus/CA created

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
anybody (everything stays local), but anyone with the ability to
connect to your Nessus daemon will be able to retrieve this information.

CA certificate life time in days [1460]: **<Enter>**
Server certificate life time in days [365]: **<Enter>**
Your country (two letter code) [FR]: **US**
Your state or province name [none]: **Virginia**
Your location (e.g. town) [Paris]: **Harrisonburg**
Your organization [Nessus Users United]: **CISC,JMU**

The output

Illustration:

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

V) Running the server and Checking if the Server is running

i) Navigate to the /usr/local/sbin directory. Use the command as shown to start the server.

Illutration:

[root@scinterface sbin]# **nessusd -D**

ii) To check if the server is running use this command as the root.

Illustration:

[root@scinterface sbin]# **ps -ef | grep "nessusd"**

root 7768 1 0 07:47 ? 00:00:00 nessusd: waiting for incoming connections
root 8742 7768 0 10:36 ? 00:00:01 nessusd: serving 192.168.1.111
root 8792 8557 0 10:48 pts/1 00:00:00 grep nessusd

The illustration shows that the Nessus server is running and also interacting with the Win2K client[4]

VI) Starting the client on Linux

The same installation procedure for the server was carried out for the client. But we navigate to the /usr/local/bin directory.

Illustration:
[root@scinterface local]# cd /usr/local/bin/
[root@scinterface bin]# ls
nasl **nessus** nessus-config nessus-mkrand

[4] Windows XP Professional Client named JMU1

nasl-config nessus-build nessus-mkcert-client

The client is run using the command **nessus** followed with options.

VII) Concerns in installation and basic configuration

The client does not support the easy GUI. Also I have not gone into the client interaction with the server. The client connectivity was tested with the server using the PING command.

Illustration of a command **./nessus -s -q <Server IP> <Username> <Password>**:

```
rajesh@Alex bin]$ ./nessus -s -q 192.168.1.10 1241 aboutabl ********

Please choose your level of SSL paranoia (Hint: if you want to manage many
servers from your client, choose 2. Otherwise, choose 1, or 3, if you are
paranoid.
2

[7140] SSL_CTX_load_verify_locations: error:02001002:system library:fopen:No such
file or directory
*** The plugins that have the ability to crash remote services or hosts
have been disabled. You should activate them if you want your security
audit to be complete
Remote sessions :
-----------------
Session ID  | Targets
==========================
```

Installation and using Nessus WX

Steps on how to download the NessusWX software

Before downloading the native Win32 Client, you must know that this software is only useful if you have installed Nessusd on a UNIX server.

To install the Nessus client software for Windows, follow this link:

1. Go to www.Nessus.org

2. Click **Download** on the left had of the screen.

3. When the **Download** window appears, click the packet name **NessusWX.** Make sure not to confuse this with the commercial packet that is available in the same table.

4. After you click **NessusWX**, the **NessusWX - Nessus Client for Win32** window will appear. Click **Download**.

5. Next the Download section will appear. Click the third option down which is **Installation program (self-extracting) for NessusWX 1.4.4 (Intel platform)**.

6. After downloading the **NessusWX** packet to the desired location, start the installation process by double clicking the downloaded file, **Nessuswx-1.4.4-install**.

Note: *We were unable to uninstall the NessusWX1.4.4 software through the normal administration process.*

Steps on how to connect and use the Nessus Windows client

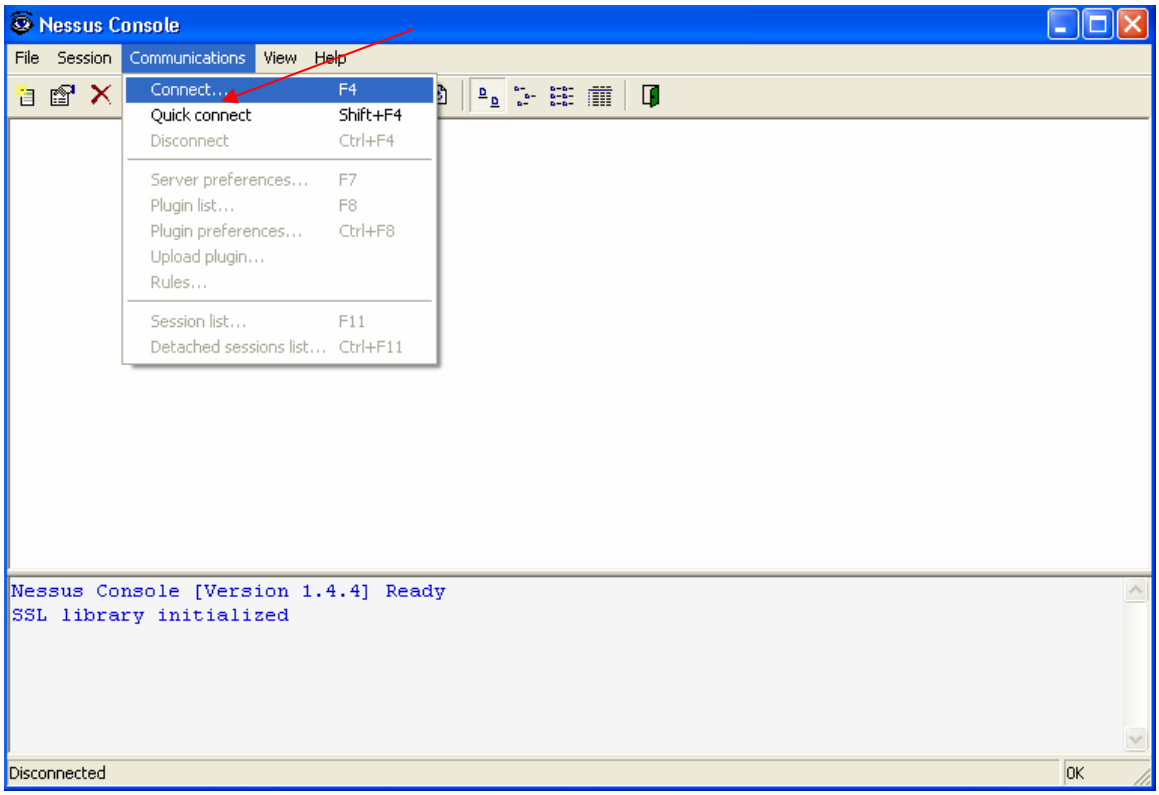
Before you start, check for basic connectivity between the Windows client and the Nessus server. You can do this using many options such as ping, tracerout, or telnet.

Follow these steps to connect the Windows client to the Nessus server:

1. Double click the Nessus icon from the desktop or press **Start** > **Programs** > **NessusWX**.

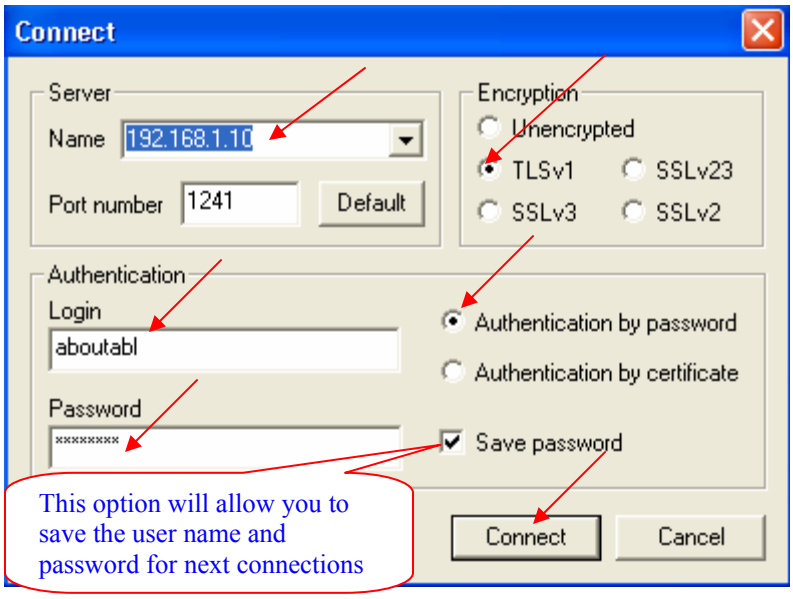
2. When the **Nessus Console** screen comes up, click **Communications** > **Connect**.

Note: *To disconnect the client form the server, click **Communications** > **Disconnect**.*

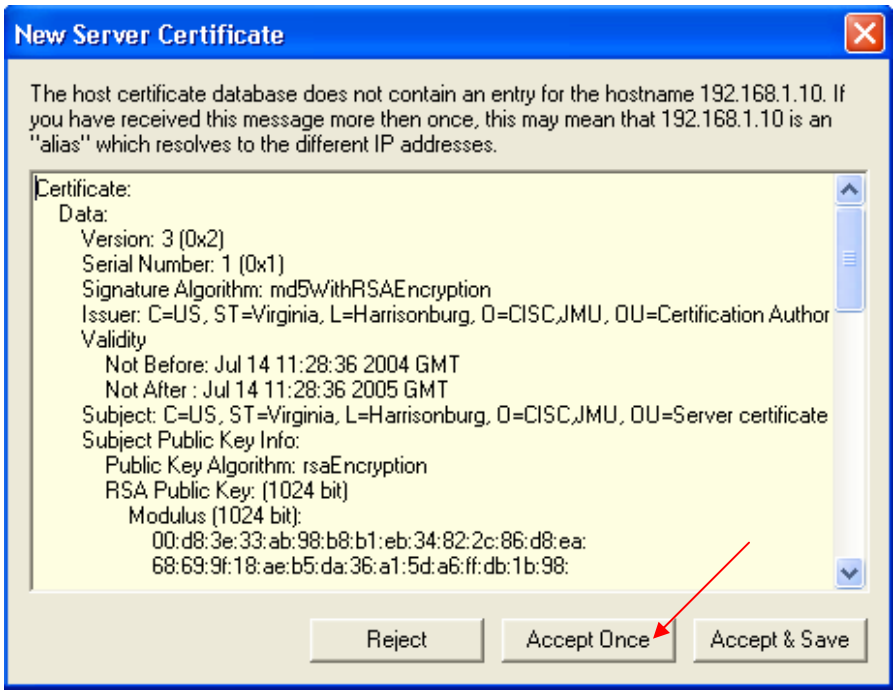


3. When the **Connect** window appears, type in the Nessus server's IP address in the **Name** text box, keep the default **Port number**. In the **Authentication** section, select the **Authenticate by password** radio button, and type in the user name and password that you assigned as you configured the server earlier. You could also choose to encrypt the client-server connection by selecting the encryption type from the **Encryption** section. Click **Connect**.

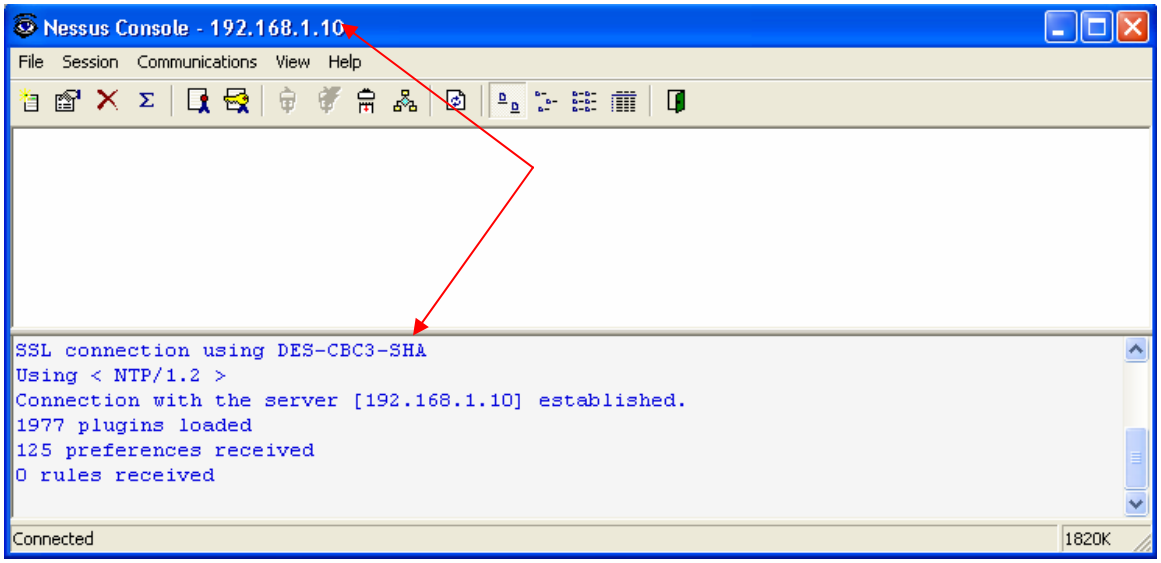
Note: *once the client is connected to the server, the connection will remain until terminated by the user. However, it is better practice to connect every time you run a new scan session, especially if there is a big time gap between the last session and the new one. New connections will help update the client, because as you connect to the server, all the new plugings available on the server will be downloaded to the client.*



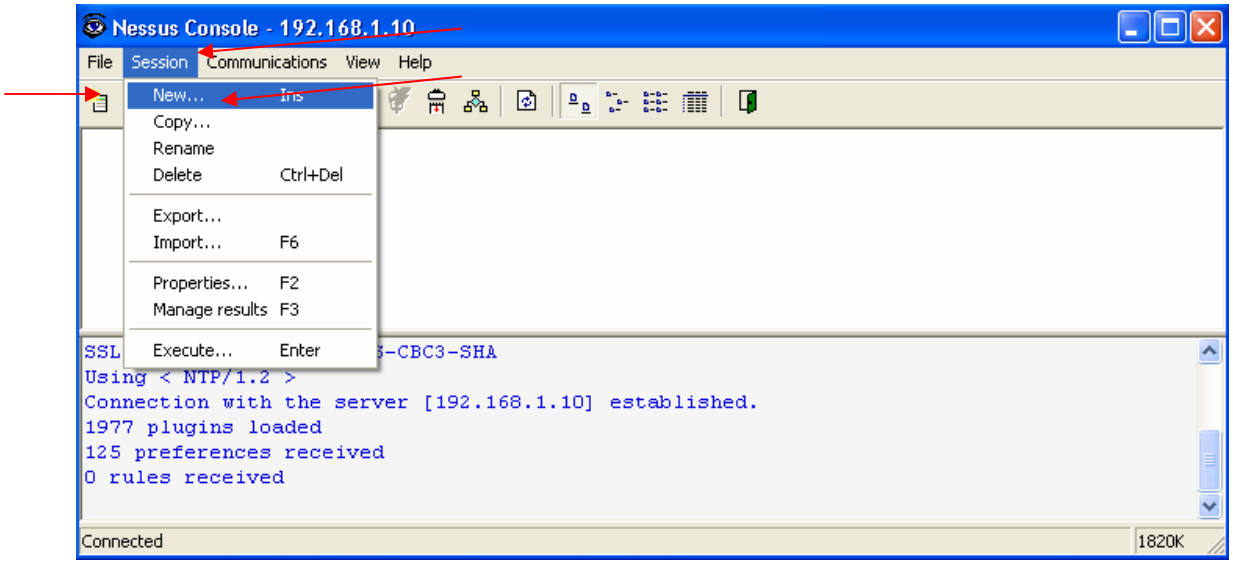
4. Next the **New Server Certificate** window will appear. Click **Accept Once**.



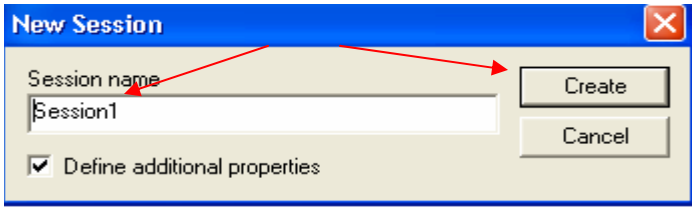
5. After clicking **Accept Once**, you will be taken back to the main screen. Check to see if you have been connected to the correct server.



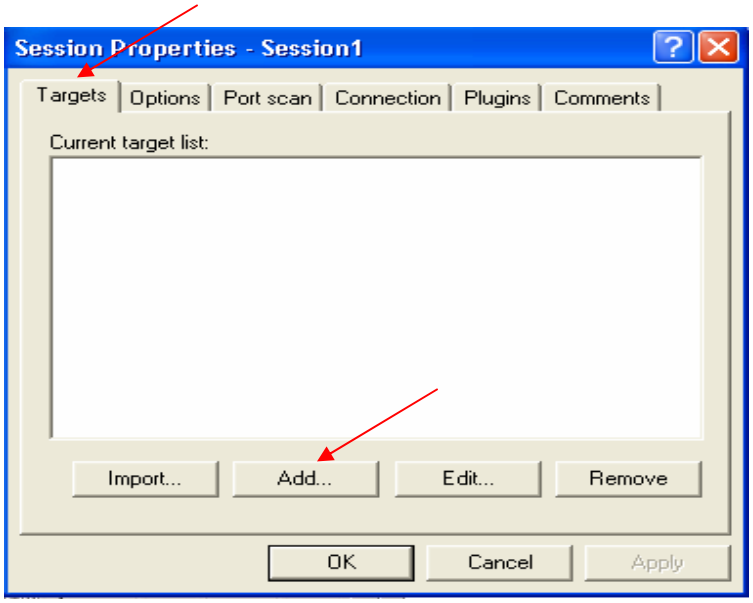
6. After you have established connectivity with the Nessus server, you should move on to create a new session. To do this, click **Session** > **New**, or click the create new session option from the menu bar.



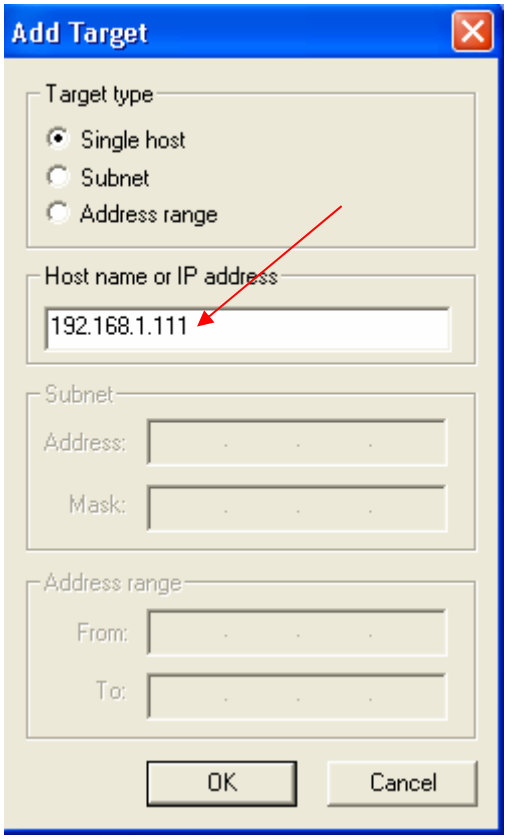
7. When the **New Session** panel appears, type in a unique session name, then click **Create**.



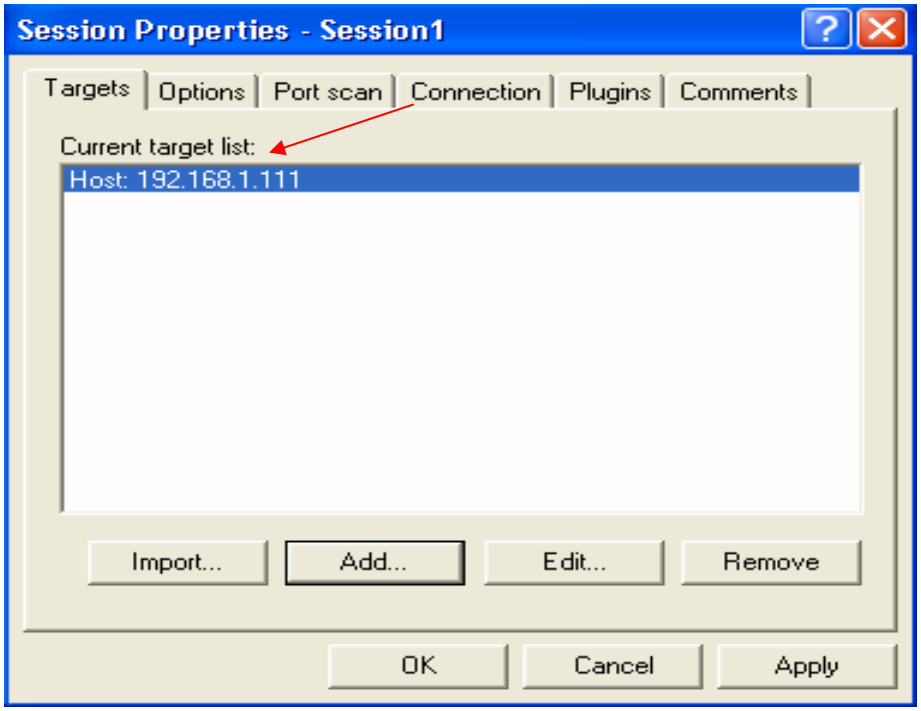
8. When the **Session Properties** window appears, make sure the **Target** Tab is clicked and click **Add**.



9. When the **Add Target** widow appears, type the targeted host's IP address or name and click **OK**.
You could also specify a range of IP addresses, or a complete subnet to be scanned, simultaneously. To scan the entire hosts of a specific subnet, select the **Subnet** radio button from the **Target type** section, and type in the subnet IP address in the **Address** box and the subnet mask in the **Mask** box, in the **Subnet** section. To scan a range of IP addresses, select the **Address range** radio button form the **Target type** section, and type in the IP address, from which the range starts form, in the **From** box and the IP address, where the address range stops, in the **To** box in the **Address range** section.



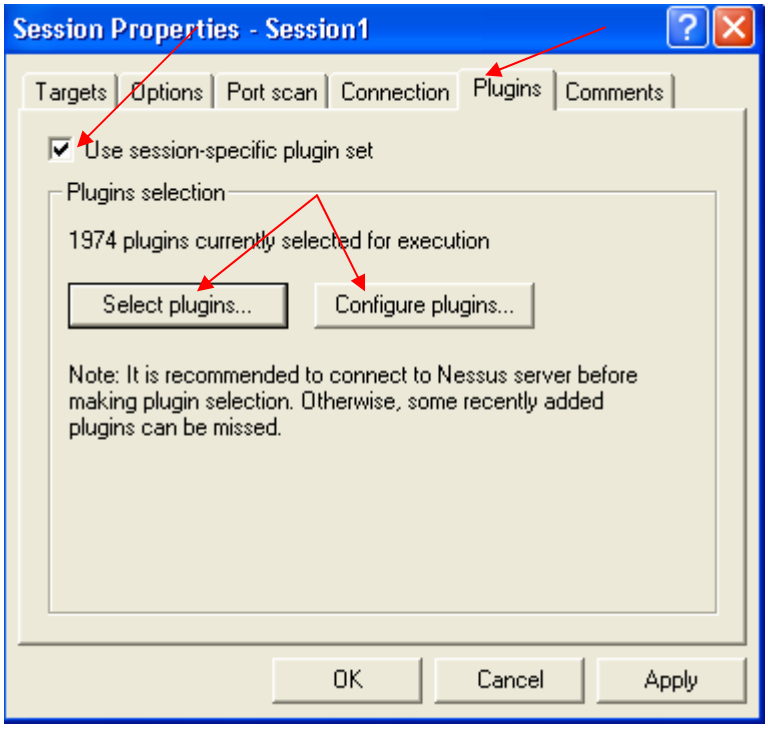
10. Next the **Session Properties** window will show the entered IP address in the **Current target list**.



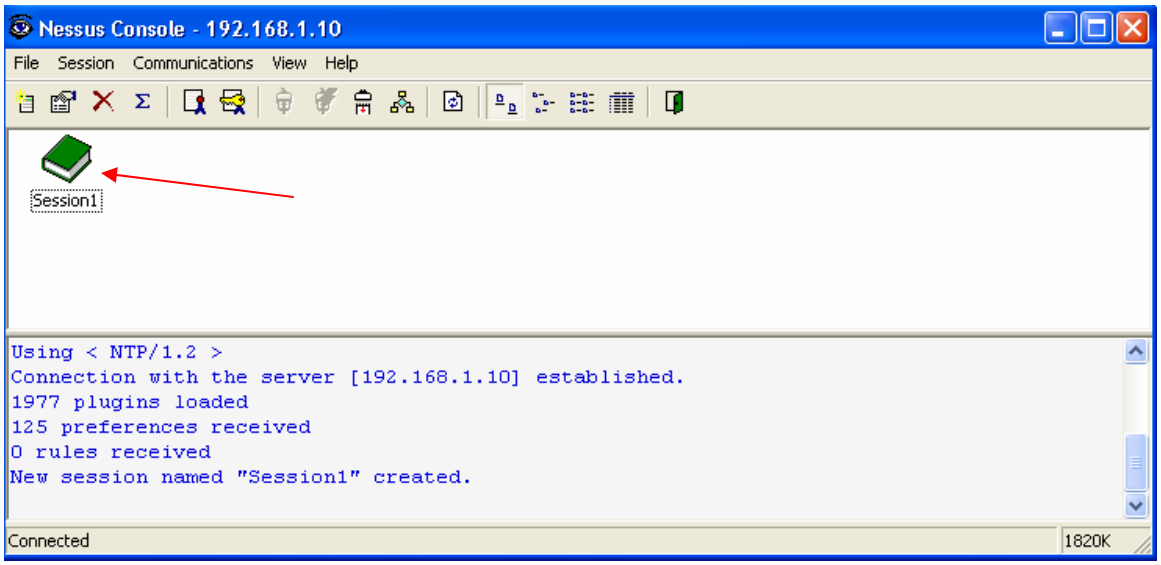
11. Click the **Plugins** tab and check mark the **Use session-specific plugin set** check box**.** Then you can click the **Select plugins** to select the kind of plugins you want (you can also leave it as default, selecting all), or you can click **Configure plugins** to customize a specific plugins.

    Note: *In the **Options** section, you can control the number of hosts scanned simultaneously and the number of the security checks per host. You could also make a general scan option selection to be implemented.*

    Note: *In the **Port scan** section, you can specify the range of the ports to be scanned. You could also decide to enable or disable each particular port scanner available.*

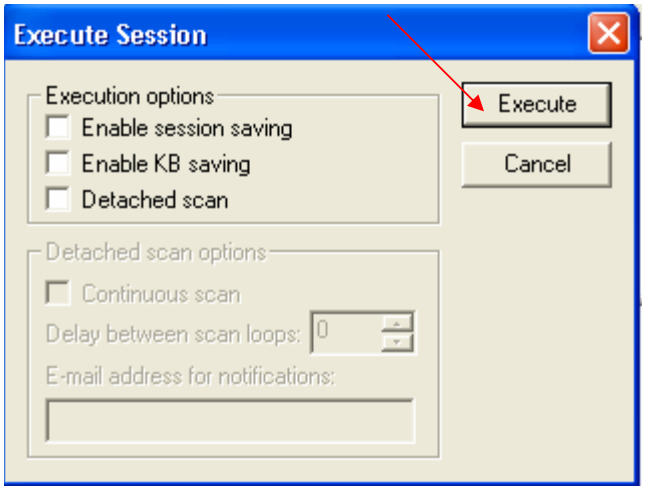


12. Right click on the session icon and click **Execute**.

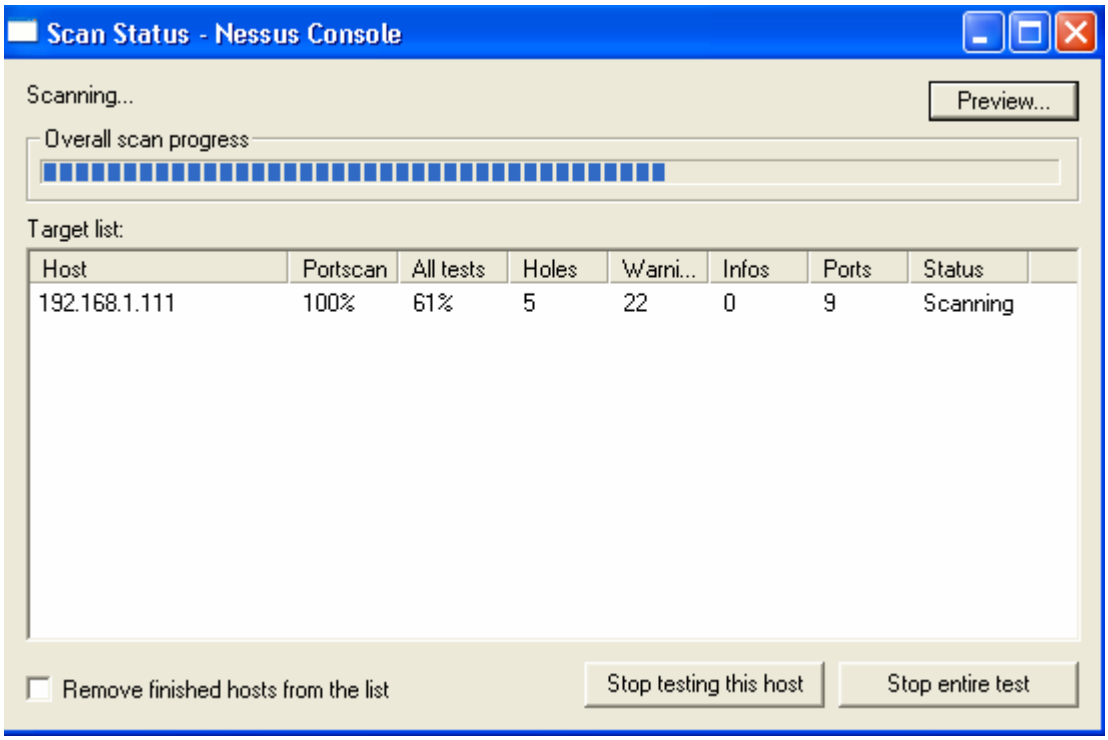


13. Click **Execute** in the **Execute Session** window.

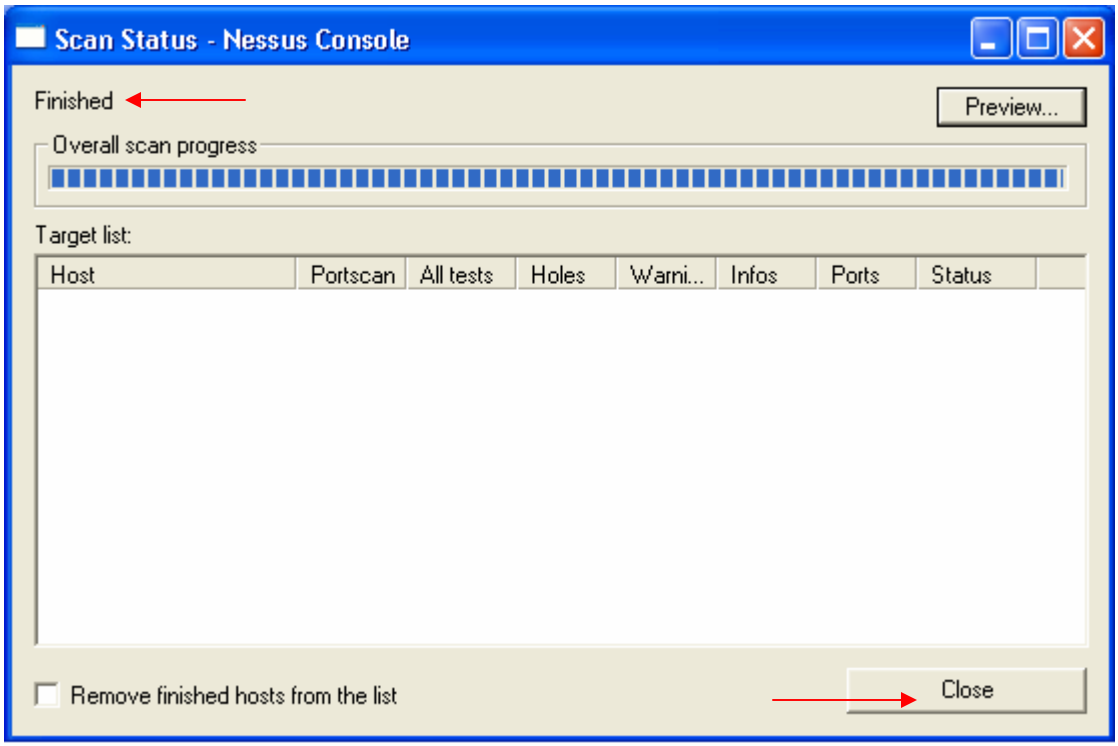
Note: *The **Detached scan** option should allow you to send the scan result to an email address of your choice, and control the time between the scans. However, these features were found underdeveloped according to this research.*



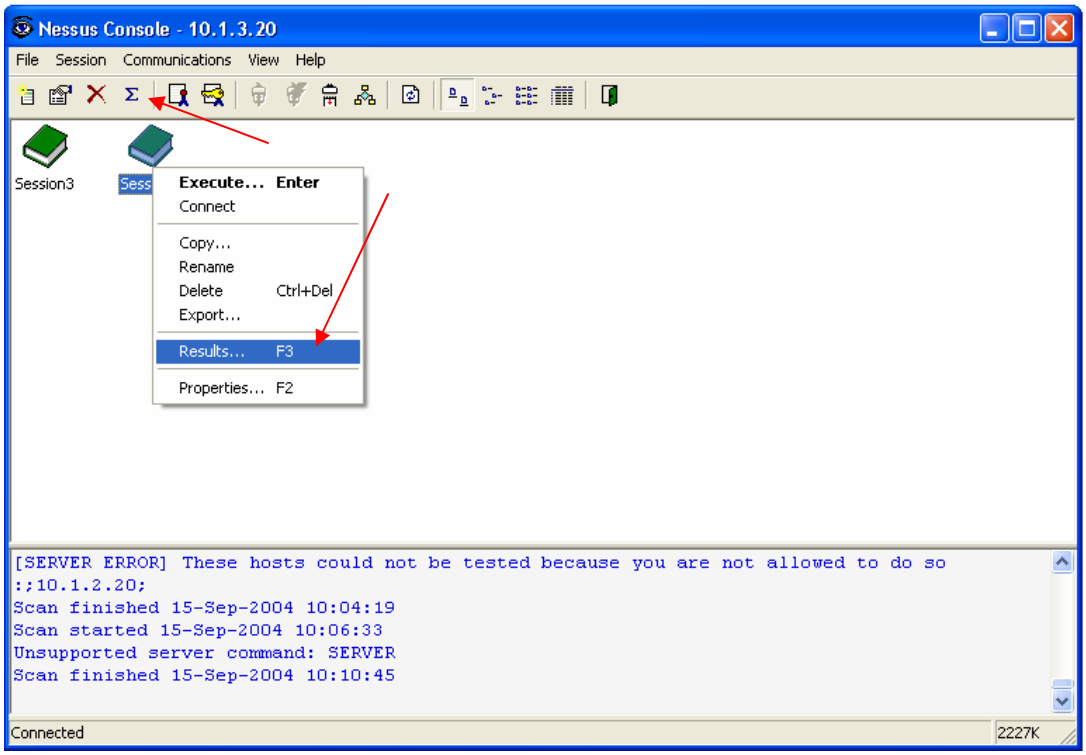
14. The scanning process will start. Later you can create a scan report and save it in the desired directory.



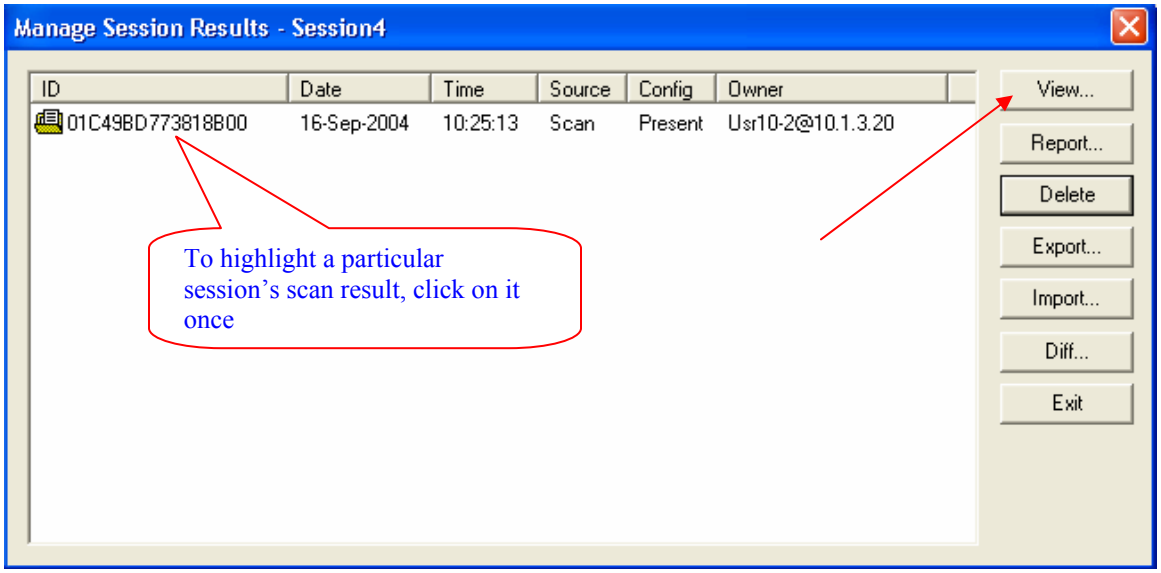
15. When scanning is complete, click **Close**.



16. To view the outcome of the scanning process, highlight the session you want to view and click the "∑" item form the menu bar, or right click the session icon and click **Results**.

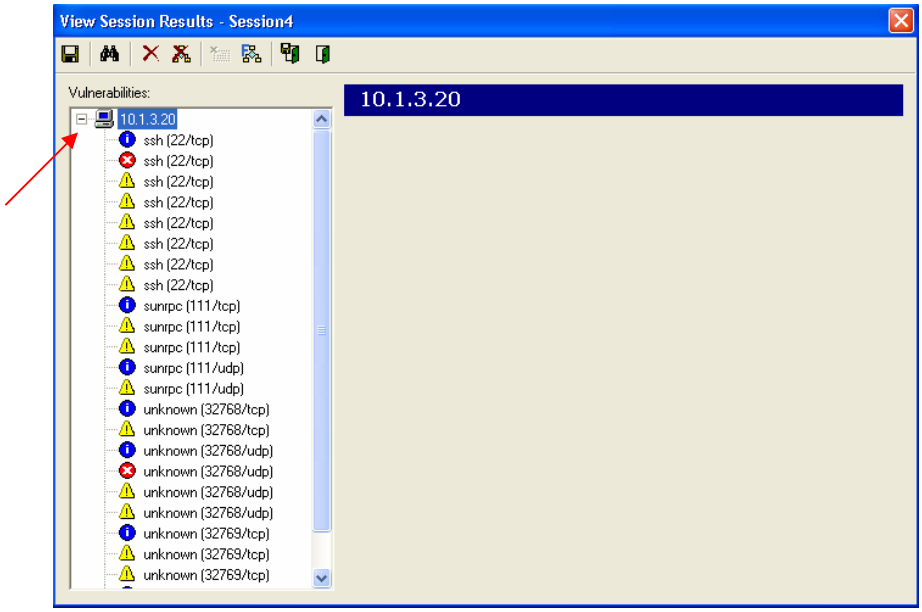


17. When the **Manage Session Results** window appears, highlight the particular scan you want to view, and click **View** form the right hand menu.



18. Next the **View Session Results** window will appear. To view the vulnerabilities of any of the scanned hosts, click on the maximize box next to that host and you will be able to see all the vulnerabilities of that hot.

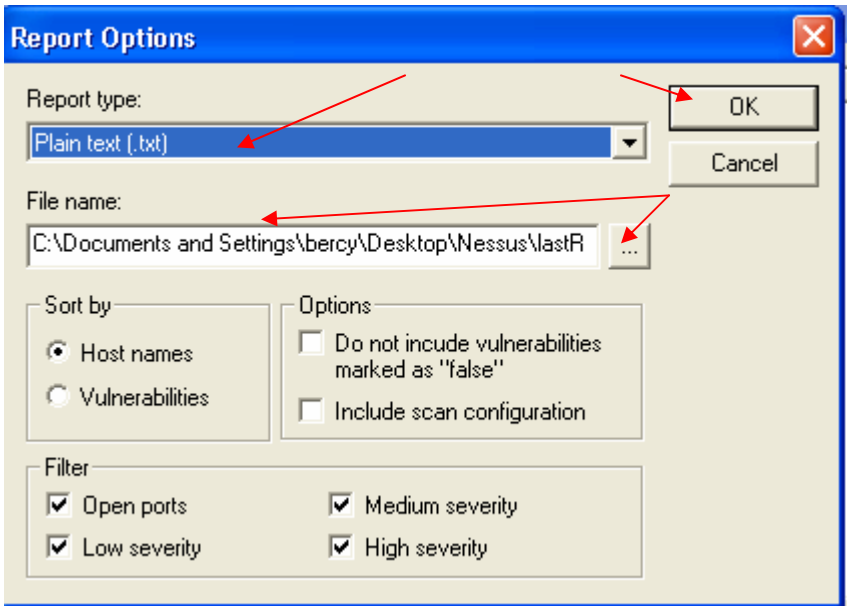
    Note: *There are three levels of severity, low, medium, and high. To view more details about each vulnerability, click on it once.*



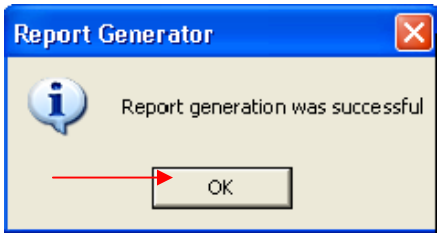
19. To get a complete report of the scanning outcome, close the **View Session Results** window. Once that window is closed, you will automatically go back to the **Management Session Results** window, where you can highlight the scan you want to get a report for. Then, click the **Report** button on the right menu.

20. When you click the **Report** button, the **Report Options** screen will appear. Form the **Report type** dropdown menu, choose the format of the report as a plain text, html, or pdf document. In this case the plain text format option is used. In the **File name** text box, specify the path of the location where you want to save the generated report. You can also select a path by clicking the three doted box. To control the way the report will be sorted, select one of the options in the **Sort by** section. You can also filter the scan report according to the vulnerability severity, or the port (open/closed) status, by selecting the desired options from the **Filter** section.

    Note: *To generate a more organized report, choose the pdf format option.*



21. After you select the desired report options, click **OK**. The **Report Generator** screen will appear indicating the report was generated successfully. If the report was successfully created, click **OK**, and look for the report in the location you specified in the earlier step.



22. The report will include valuable information that can be very useful in improving network security. In the introductory part of the report, there are information such as the date and time (start and finish) the report was created, the total number of security holes, the severity level of each security hole, and a list of all the open ports on the host. In the body of the report, each vulnerability is addressed in more details, and suggested solutions and/or help full links are listed.

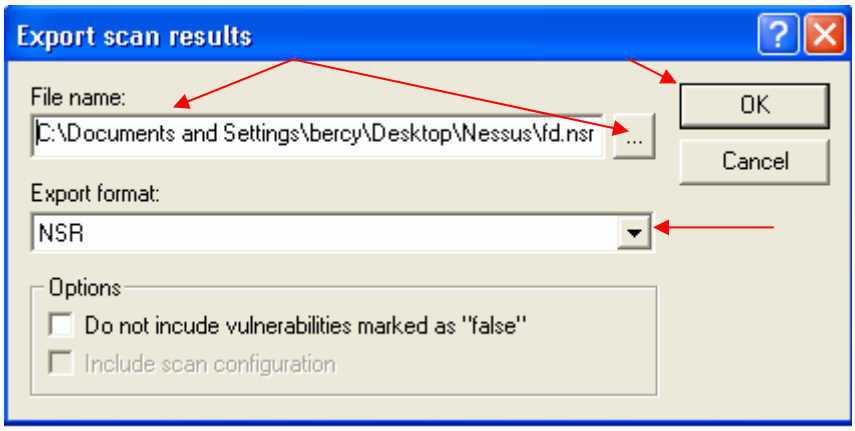
```
Created 16.09.2004                Sorted by host names

Session Name : Session4
Start Time   : 16.09.2004 10:25:13
Finish Time  : 16.09.2004 10:30:46
Elapsed Time : 0 day(s) 00:05:32

Total security holes found : 24
             high severity : 2
              low severity : 15
             informational : 7

Scanned hosts:

Name                              High  Low   Info
-----------------------------------------------
10.1.3.20                         2     15    7

Host: 10.1.3.20

Open ports:

   unknown (32768/udp)
   sunrpc (111/tcp)
   ssh (22/tcp)
   x11 (6000/tcp)
   unknown (32768/tcp)
   sunrpc (111/udp)
   unknown (32769/tcp)

Service: unknown (32768/udp)
Severity: High

The remote statd service may be vulnerable to a format string attack.
This means that an attacker may execute arbitrary code thanks to a bug in
this daemon.

Only older versions of statd under Linux are affected by this problem.

*** Nessus reports this vulnerability using only information that was gathered.
*** Use caution when testing without safe checks enabled.

Solution : upgrade to the latest version of rpc.statd
```

Scrawl down to see the rest of the report

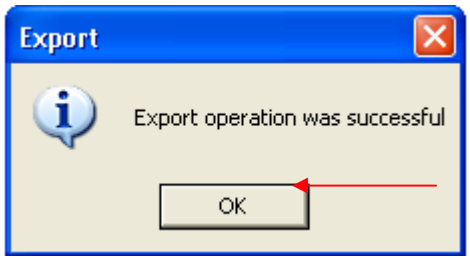
23. To delete a host scan result session, in the **Manage Session Results** window, highlight the session you want to delete and click **Delete** from the right menu.

24. To export a host scan result session to a particular file or location on you computer, highlight the session result you want to export from the **Manage Session Results** screen, and click **Export** form the right menu.

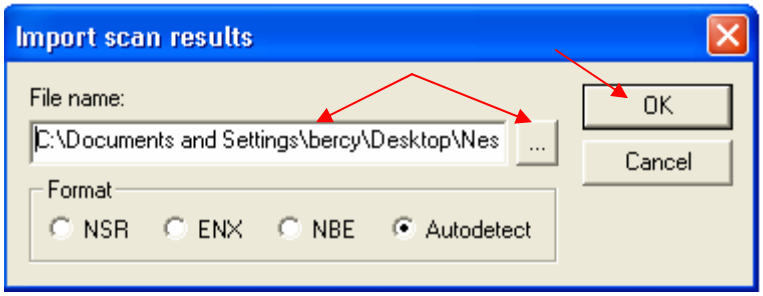
25. When you click **Export**, the **Export scan results** screen will appear. Type the file path, to which you want to export the scan results, in the **File name** text box, or brows for the file by clicking the three doted box. From the **Export format** dropdown menu, select the format you want to export the scan result as, and click **OK**.



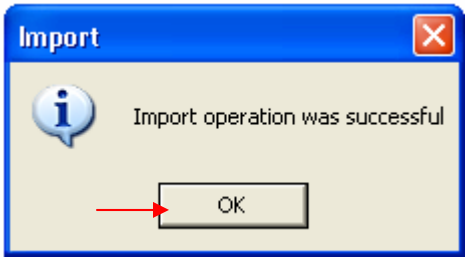
26. When you click **OK**, the **Export** screen will appear indicating the export was successful. Click **OK**, and the scan results will be exported to the indicated file.



27. To import a specific scan result session form any file on you computer, click the **Import** button form the right menu. The **Import scan results** screen will appear. Type the path to the file you want to import the scan result session from in the **File name** text box, or browse for it by click the three doted box. Select the session format or **Autodetect,** to automatically detect the session format, form the **Format** section. Click **OK**.

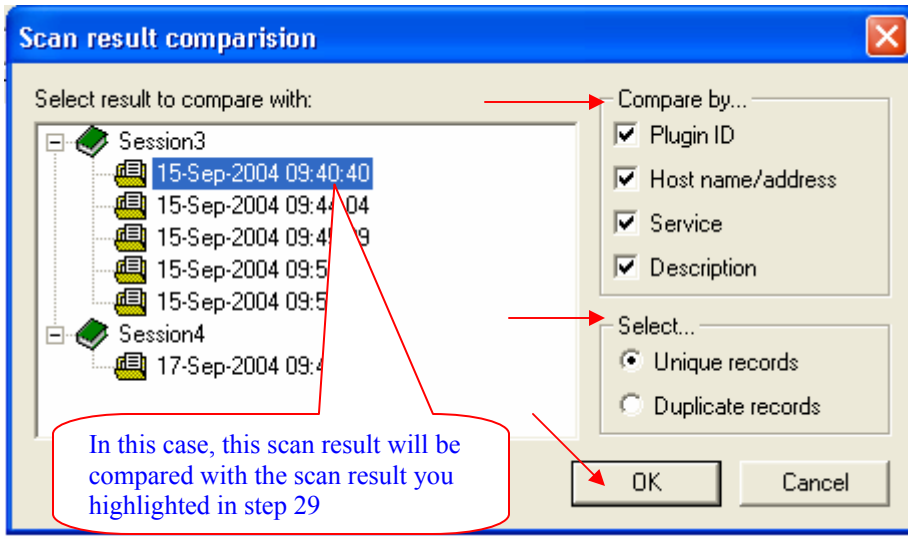


28. Next the **Import** screen will appear indicating the import was a success. Click **OK**, and the imported session will appear in the **Manage Session Results** window.

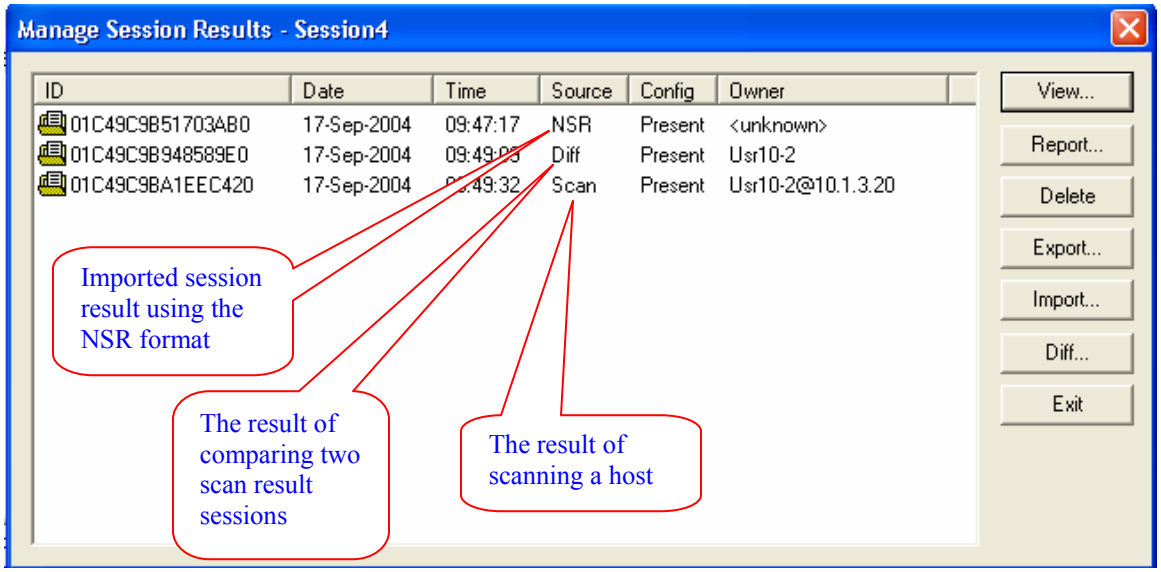


29. To find the differences between two different scan sessions, form the **Manage Session Results** window highlight the session you want to compare and click **Diff** form the right side menu.

30. The **Scan result comparison** screen will appear. From the **Select result to compare with** box, select the session you want to compare with, by highlighting it. You can specify the comparison between the two sessions by selecting the items you want to compare them by from the **Compare by** section. You can also specify if you want the comparison to be between unique or duplicate records form the **Select** section. Click **OK** when done, and the difference result will appear in the **Manage Session Results** window.

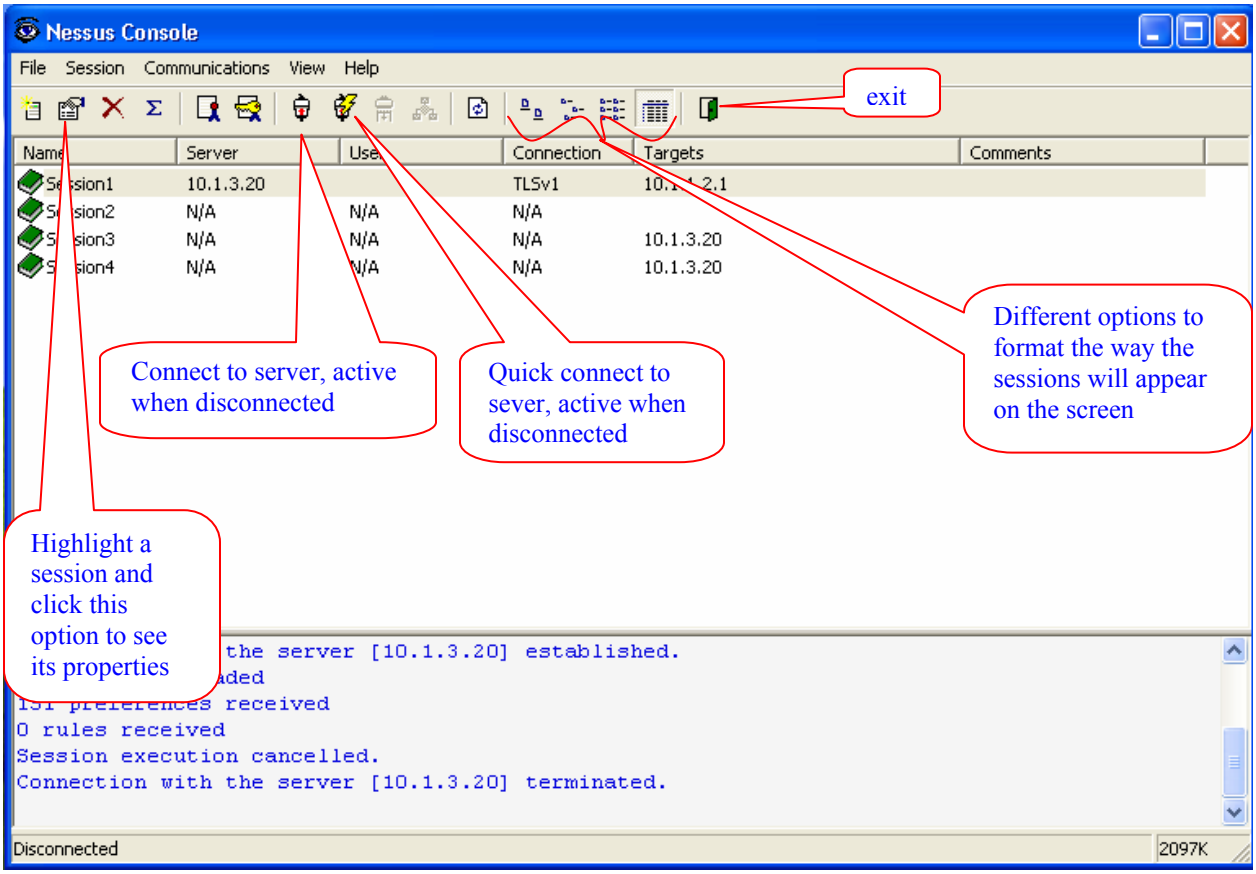


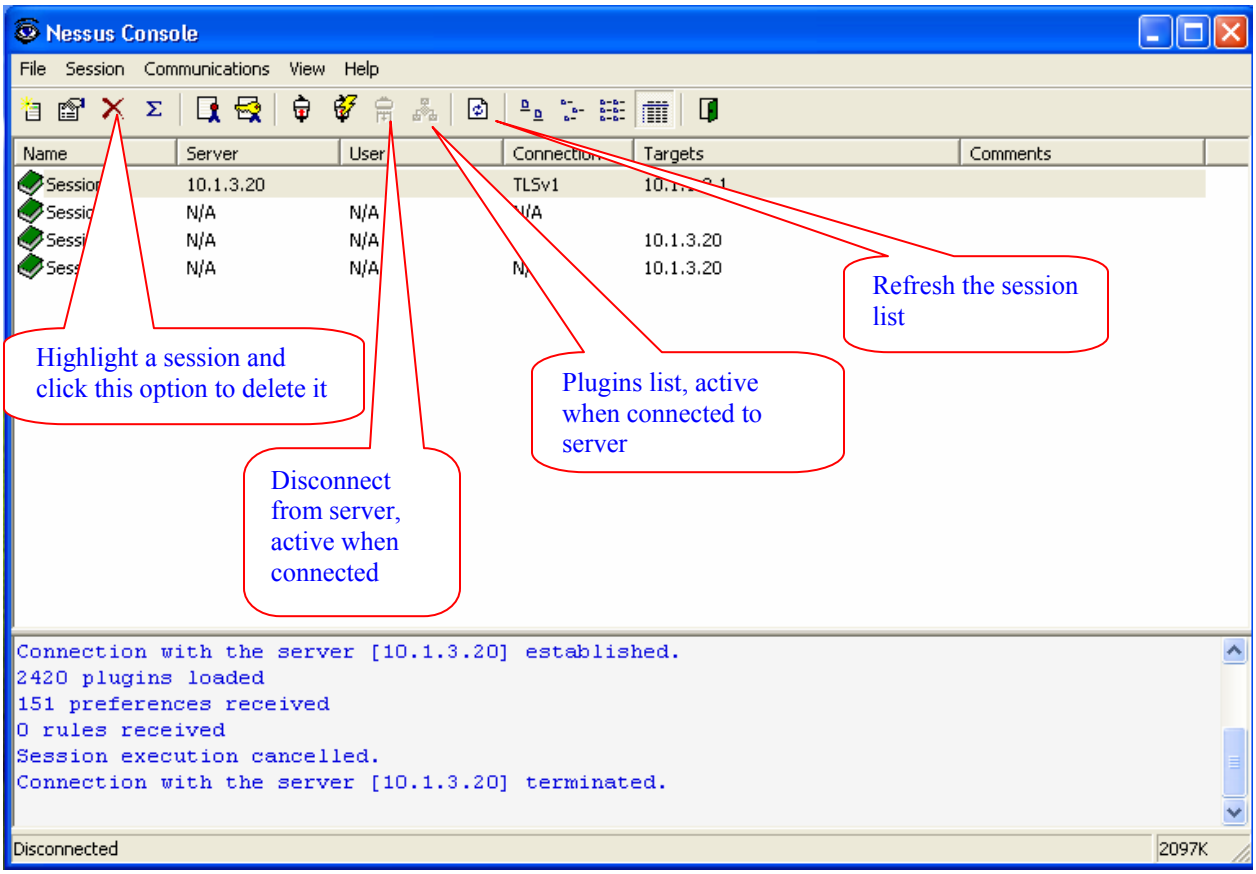
31. To find out if a result session is the outcome of a scan, importation, or comparison, check the **Source** column in the **Manage Session Results** window. To exit the **Manage Session Result** window, click **Exit** from the right side menu.



Other helpful menu bar options

The following two figures will show some of the helpful options at the menu bar:




Nessus Console
File Session Communications View Help
Name Server User Connection Targets Comments
10.1.3.20 TLSv1
N/A N/A
N/A N/A 10.1.3.20
N/A N/A 10.1.3.20
Connection with the server [10.1.3.20] established.
2420 plugins loaded
151 preferences received
0 rules received
Session execution cancelled.
Connection with the server [10.1.3.20] terminated.
Disconnected
2097K
Highlight a session and click this option to delete it
Disconnect from server, active when connected
Plugins list, active when connected to server
Refresh the session list