

# Installing and Configuring Nessus

by Nitesh Dhanjani

Unless you've been living under a rock for the past few years, it is quite evident that software vulnerabilities are being found and announced quicker than ever before. Every time a security advisory goes public, organizations that use the affected software must rush to install vendor-issued patches before their networks are compromised. The ease of finding exploits on the Internet today has enabled a casual user with little skills to launch attacks and compromise the networks of major corporations. It is therefore vital for anyone who has any hosts connected to the Internet to perform routine audits to detect unpatched remote vulnerabilities.

Network security assessment tools such as Nessus can perform automated detection of vulnerabilities. A vulnerability detection assessment usually involves three distinct phases.

## Scanning

In this phase, the software probes a range of addresses on a network to determine which hosts are alive. One type of probing sends ICMP echo requests to find active hosts, but does not discount hosts that do not respond -- they might be behind a firewall. Port-scanning can determine which hosts are alive and what ports they have open. This creates a target set of hosts for use in the next step.

## Enumeration

In this phase, the software probes network services on each host to obtain banners that contain software and OS version information. Depending on what is being enumerated, username and password brute-forcing can also take place here.

## Vulnerability Detection

The software probes remote services according a list of known vulnerabilities such as input validation, buffer-overflows, improper configuration, and so on.

## Why Nessus?

You just can't beat free. There are commercial vulnerability scanners available and they may be useful in their own right, but consider that Nessus is comparable to some commercial scanners that can cost hundreds of thousands of dollars. In addition Nessus is open source, and its source is published under the GPL. As we will see in Part 2 of this article, you can write custom plugins for Nessus with NASL or C.

Nessus uses a client-server architecture. The Nessus server, `nessusd`, listens for incoming connections from the clients that can configure the server to launch specific attacks. In addition, `nessusd` authenticates the clients, allowing for each user to have individual access to specific functionality. Also, the communication between the client and the server is encrypted.

Therefore, the Nessus architecture and its free and open source nature are good reasons to award it high points. If you haven't already, give Nessus a try. Here's how to install it.

## Installing Nessus

Brave users may attempt the following method that performs an automated installation:

```
[notroot]$ lynx -source http://install.nessus.org | sh
```

The rest of us need to download the latest version of Nessus. First, install `nessus-libraries`:

```
[notroot]$ tar zxvf nessus-libraries-x.y.z.tar.gz
[notroot]$ cd nessus-libraries
[notroot]$ ./configure
```

# Installing and Configuring Nessus

by Nitesh Dhanjani

```
[notroot] make
[root]# make install
Next, install libnasl:
[notroot]$ tar zxvf libnasl-x.y.z.tar.gz
[notroot]$ cd libnasl
[notroot]$ ./configure
[notroot]$ make
[root]# make install
[root]# ldconfig
```

Then, install nessus-core:

```
[notroot]$ tar zxvf nessus-core.x.y.z.tar.gz
[notroot]$ cd nessus-core [notroot]$ ./configure
[notroot]$ make
[root]# make install
```

If you are installing nessus-core on a server that does not have the GTK libraries and you don't need the Nessus GUI client, run `./configure` with the `--disable-gtk` option.

If all went well, you are all set with the installation!

**Note:** if you want to update your Nessus installation with the latest plugins, run `nessus-update-plugins` as root.

## Running Nessus

Start the Nessus server:

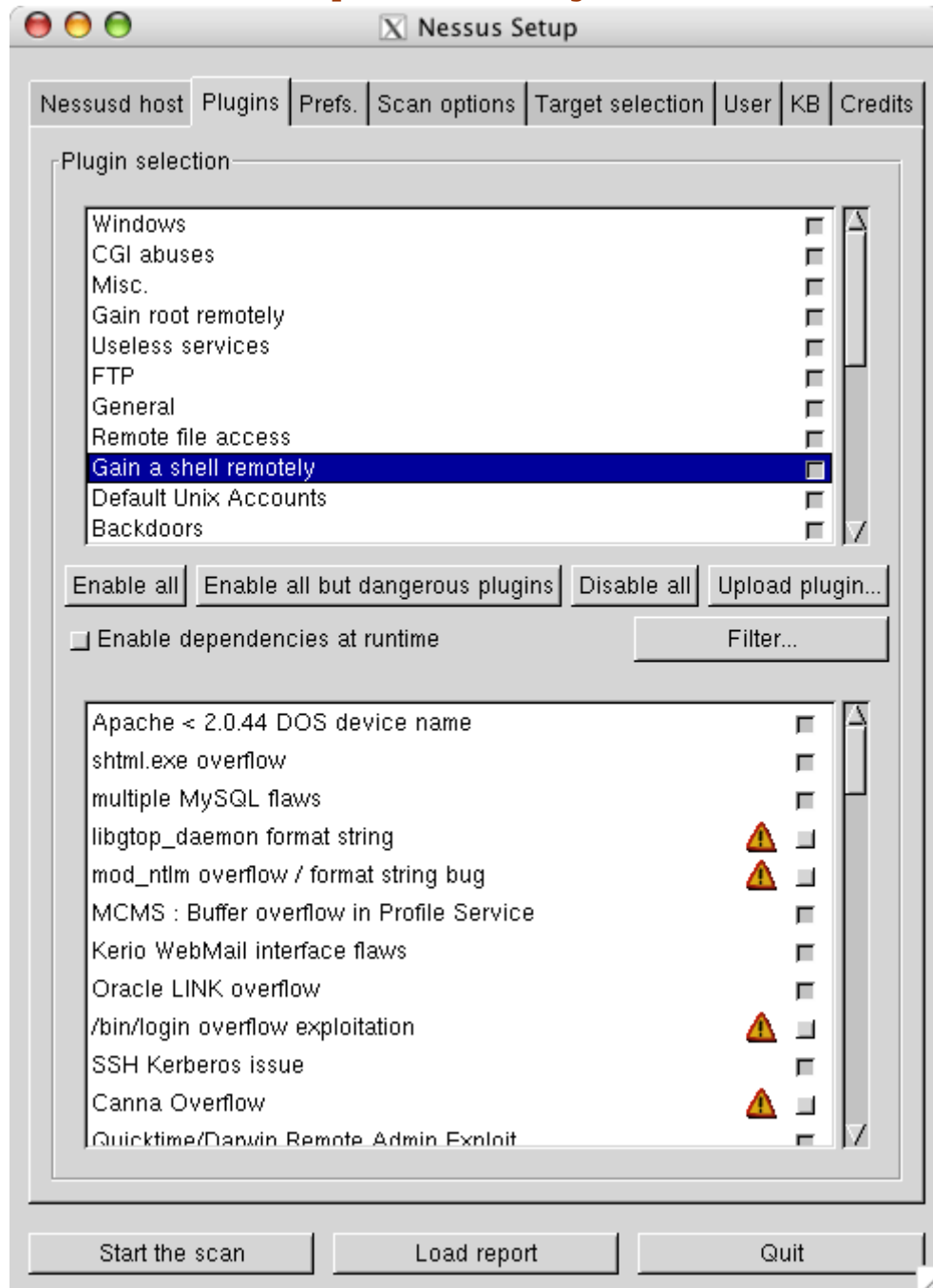
```
[root]# nessusd -D
```

Before you can connect to the server, you must first add a Nessus user, using the `nessus-adduser` command.

Now, run `nessus` to launch the Nessus client and login as the user you just created. Next, take a look at the different plugins you can select from the Plugins tab.

# Installing and Configuring Nessus

by Nitesh Dhanjani



**Figure 1**  
**Selecting Nessus plugins**

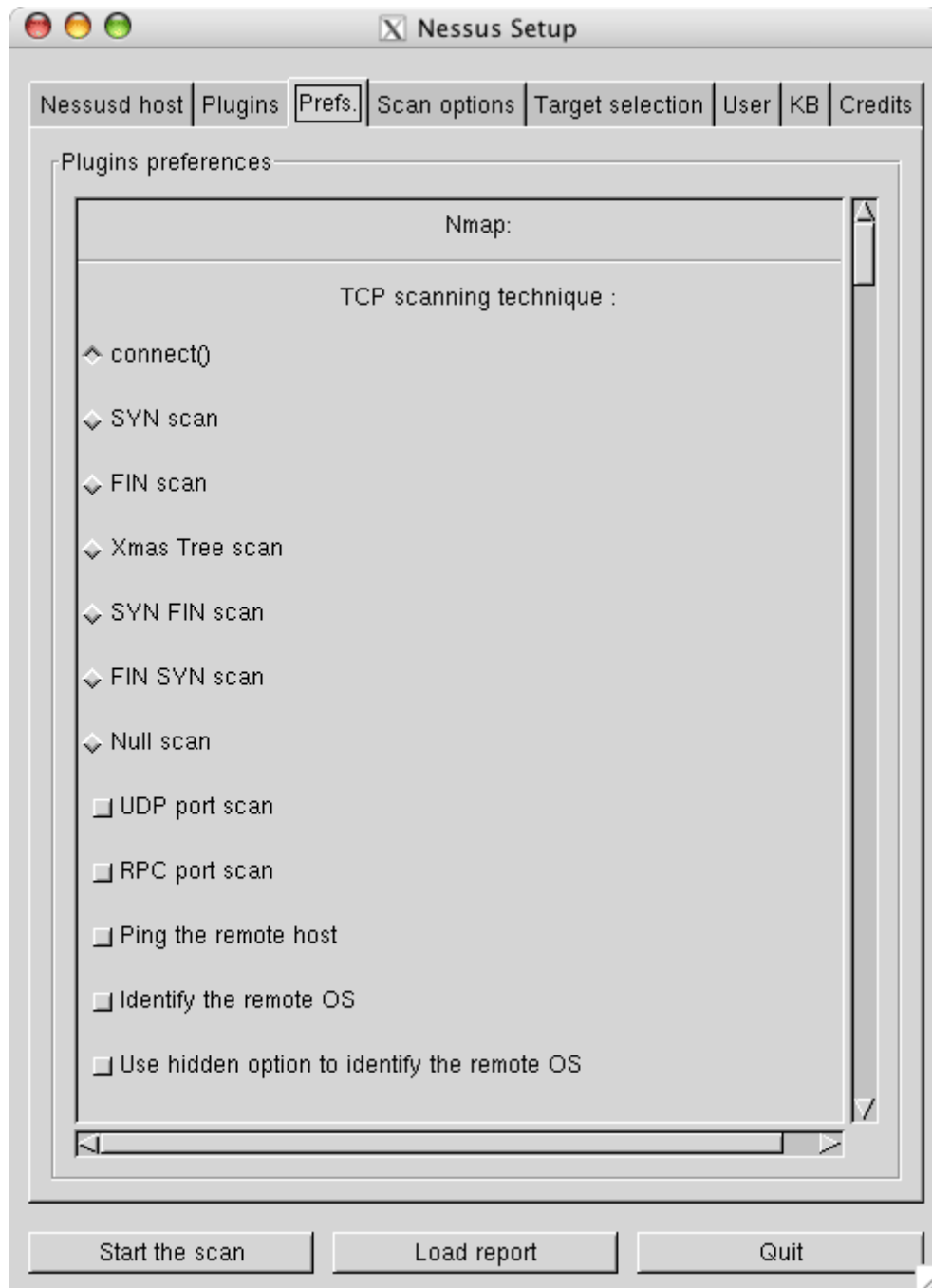
The Enable all but dangerous plugins button will disable plugins that are known to crash the remote services being scanned. Also take a look at the scans listed under the Denial of Service category. It is a good idea to disable these checks when scanning hosts that provide critical services.

Use the Filter button to search for specific plugin scripts. For example, it is possible to search for vulnerability checks that have a certain word in their description or by the CVE name of a specific vulnerability. It is up to the author of each specific vulnerability check to make sure he provides all appropriate information and places his script under the proper category. As you will note by looking at

# Installing and Configuring Nessus

by Nitesh Dhanjani

the descriptions of some of the vulnerability checks, some authors do not do a good job of filling in this information, so be careful.



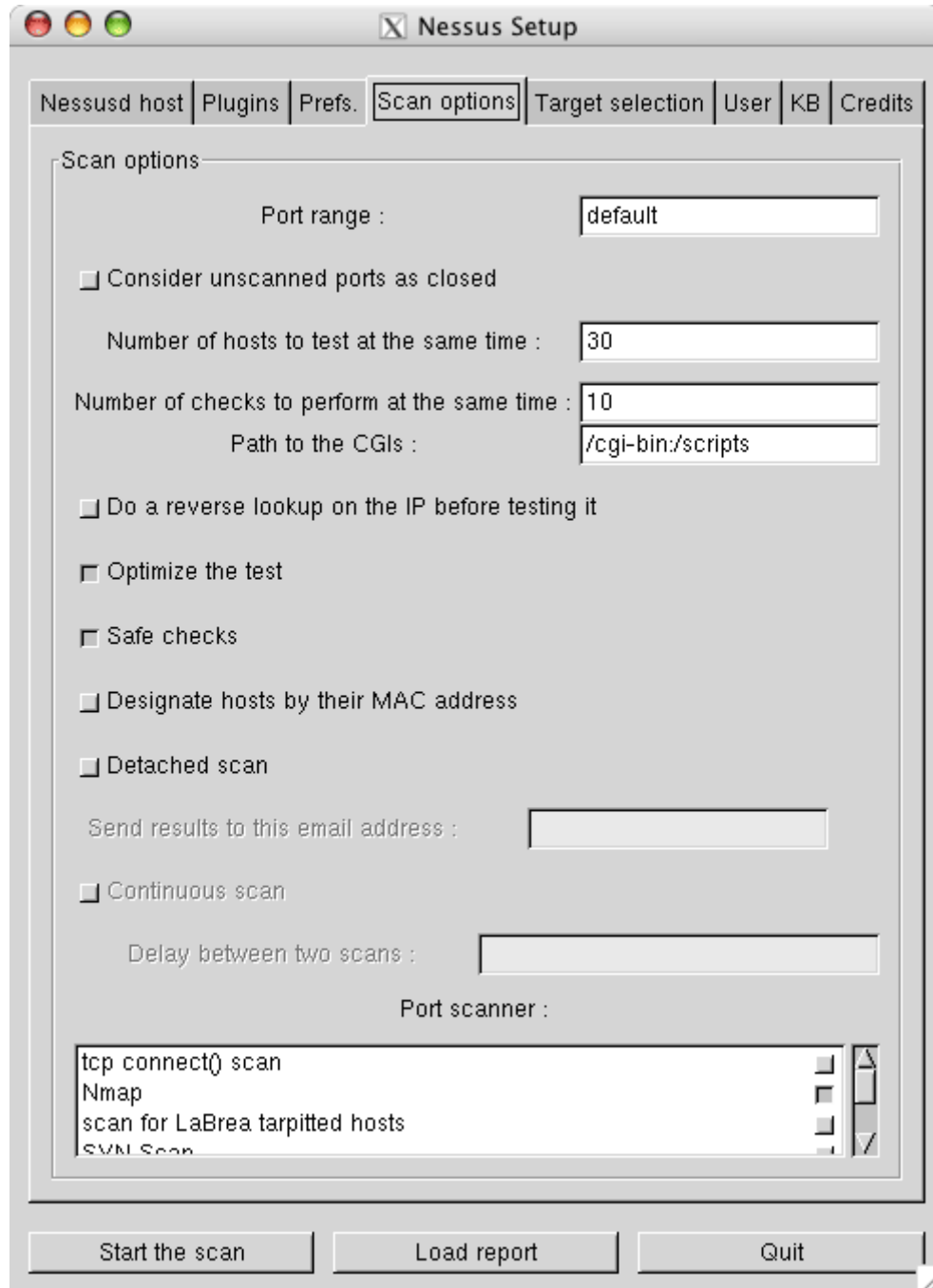
**Figure 2**  
**Nessus preferences**

Next, click on the Preferences tab. Under this section, you can set various options that will affect the way Nessus will perform its scans. Most of the options are self-explanatory. One important preference is that of Nmap options. Nmap is one of the best port-scanners available today, and Nessus can use it to port scan target hosts (make sure to select Nmap in the Scan Options tab). The connection() technique completes the 3-way TCP handshake in order to identify open ports. This means that

# Installing and Configuring Nessus

by Nitesh Dhanjani

services running on the remote host will likely log your connection attempts. The SYN scan does not complete the TCP handshake. It merely sends a TCP packet with the SYN flag set and waits for a response. Receiving a RST packet in response indicates that the host is alive and the port is closed. Receiving a TCP packet with the SYN+ACK flags set that the target is listening on the port. Since this method does not complete the TCP handshake, it is usually stealthier, so services that listen on that port will not detect it. An IDS may detect this. See the nmap man page for more information on other Nmap scanning options and techniques.



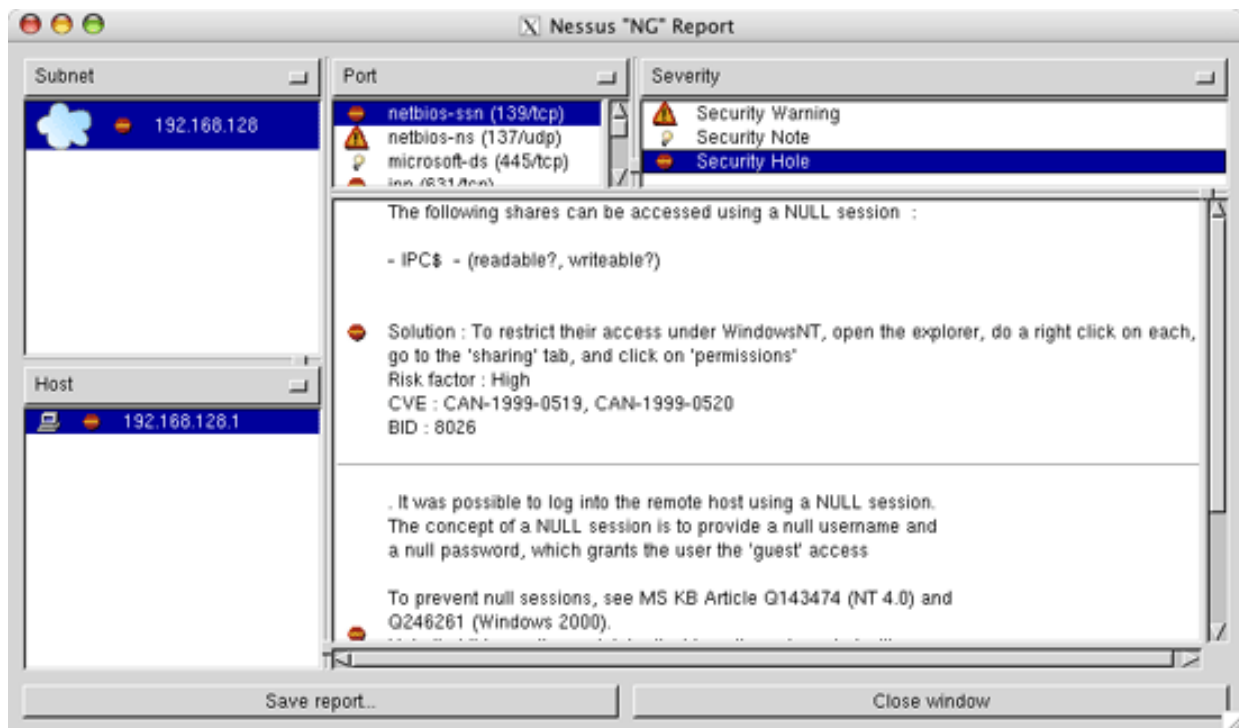
**Figure 3**  
**Nessus scan options**

# Installing and Configuring Nessus

by Nitesh Dhanjani

The Scan options tab allows you to specify the port range that you want Nessus to port-scan. TCP and UDP ports range from 1 to 65535. Use default for the port range to scan the ports listed in the nessus-services text file. Although Nessus is smart enough to recognize services running on non-standard ports, it will not target ports that it does not know are open. So make sure you configure your port ranges appropriately. The Safe checks option will cause Nessus to rely on version information from network service banners to determine if they are vulnerable. This may cause false positives, but it may be useful to scan hosts whose uptime is critical. The Port scanner section in this tab allows you to select the type of port scan you want Nessus to perform. If most of your hosts are behind firewalls or do not respond to ICMP echo requests, you might want to disable the Ping the remote host option.

In the Target Selection tab, enter the IP addresses of hosts you want to scan. Enter more than one IP address by separating each with a comma. You can also enter a range of IP addresses using a hyphen, for example, 192.168.1.1-10. Tell Nessus to read target host IPs from a text file by choosing the Read file... button. Once you are done entering the target IP addresses, and are sure that you are ready to go, click on the Start the scan button to have Nessus begin scanning.



**Figure 4**  
**A Nessus report**

When Nessus finishes its scan, it will present you with a report. You can save it in a variety of formats: HTML (with or without graphics), XML, LaTeX, ASCII, and NBE (Nessus BackEnd). The items with a light bulb next to them are mere notes or tips that provide information about a service or suggest best practices to help you better secure your hosts. The items with an exclamation next to them are findings that suggest a security warning when a mild flaw is detected. Items that have the no-entry symbol next to them suggest a severe security hole. In case you are wondering, the authors of the individual scripts used by the Nessus plugins decide how to categorize the findings.

## Conclusion

Although Nessus is a great tool to perform automated vulnerability scanning, its results can and often do provide false positives. To see how a particular vulnerability scan works, take a look at its

# Installing and Configuring Nessus

by Nitesh Dhanjani

corresponding .nasl script file located in /usr/local/lib/nessus/plugins. Part 2 of this article will cover NASL and that will help you better understand how these work, and this will allow you to manually ensure if a finding is a false positive or not. It is highly recommended that you do not solely rely on automated vulnerability scanning tools, but also perform manual attack and penetration reviews for a better understanding of your organization's network security posture.