

Nessus Scanning

Let's face it: Networks are dynamic environments, and it can be a daunting task to keep up with system, application, hardware, and OS changes. As a result, securing this environment is not a one-time deal but an ongoing task.

Although there's no single panacea for dealing with this dynamic security challenge, a variety of tools can help ensure that we know what systems are on our networks and can verify that those systems are secure. One must-have tool is a good network scanner, such as Nessus. Using a scanner can help you identify security problems before hackers do. In addition, data gathered from scanning can be used to justify business cases for security changes, additional security equipment such as firewalls, or additional resources such as personnel or training. You can also use Nessus to establish a baseline to tangibly show security improvements over time.

The Word on Nessus

Nessus is a scanner that not only will tell you what systems are on your network and what ports are open, but it will also tell you about those systems' security vulnerabilities. And although scanners and outsourced scanning services can run in the thousands of dollars per IP address, Nessus is free. But don't let the price fool you. Nessus is a powerful resource, backed by a dedicated team, and it's constantly updated with new vulnerability signatures. In fact, the security checks database is updated on a daily basis. Nessus is also easy to install and use.

Nessus is modular, having two parts: a server and a client. The server, `nessusd`, runs on a UNIX-like system, such as Linux, and performs the actual scans. The client, `nessus`, can run on UNIX or Windows systems. This modular approach allows the server to support multiple clients running multiple scans at the same time. Clients securely log in to the server with usernames and passwords and can be limited to scan only certain hosts or network ranges.

The security tests are written as external plug-ins in a C-like script language called NASL (Nessus Attack Scripting Language), which is designed for easily writing additional custom scripts. You can also write your own scripts using C. As of this writing, the database includes 1,515 plug-ins that cover 1,020 Common Vulnerabilities and Exposures (CVEs) and 963 Bugtraq IDs.

What makes Nessus different from a common port scanner such as NMAP is that in addition to finding open ports, Nessus does not make assumptions about those ports. For each open port, Nessus runs a variety of checks to see what services are running there (HTTP, SMTP, FTP, Subseven, etc.). This means that a Web server answering on something other than the normal port 80 will still be found. Once a service has been identified, Nessus checks it for the relevant vulnerabilities.

Server Installation

Nessus will run on any POSIX system, such as Linux, FreeBSD, NetBSD, and Solaris. I'm running my Nessus server on Red Hat Linux 8.0 using an old PIII with only 256 MB, and it still does an awesome job. It's quite fast, but that's also a factor of the size of the network segment you're scanning.

The latest version of Nessus is 2.0.4 and is best installed as a stand-alone package that automatically installs itself. You can find it here. You'll also need to install the GTK, (The Gimp Toolkit), which has a link on the same page. Simply type `sh nessus-installer.sh` to use the auto-install feature.

If you prefer to work directly with the tarballs, you can download and compile these four files instead:

`Nessus-libraries-x.x.tar.gz`
`Libnasl-x.x.tar.gz`
`Nessus-core.x.x.tar.gz`
`Nessus-plugins.x.x.tar.gz`

Nessus Scanning

Compile them in this order:

```
nessus-libraries
libnasl
nessus-core
nessus-plugins
```

To compile nessus-libraries, type:

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

After this, execute as root:

```
make install
```

To compile libnasl, type:

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

Then, execute as root:

```
make install
```

To compile nessus-core, type:

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

Next, execute as root:

```
make install
```

To compile nessus-plugins, type:

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

After this, execute as root:

```
make install
```

If you're using Linux, make sure that `/usr/local/lib` is listed in the `/etc/ld.so.conf` file and then execute the `ldconfig` command.

Setting up Usernames and Privileges

Once you have the server installed, you need to create the user database. Here, I'm creating the new user named `eyeopener`, with the password `findtheholes`. Start by running the following command:

```
# nessus-adduser
```

This will result in the prompts for information shown in Listing A.

After you've created your user accounts, you can tweak the configuration file parameters, if you want. The changelogs and readme files are a great place to find optimization tips.

Nessus Scanning

To start the Nessus server, simply run the following command:

```
nessusd -D
```

Getting the latest scan plug-ins

Once you've installed the server, you'll need to get the latest plug-ins from the Nessus site. From the Linux/UNIX system, you can do this directly (as the root user). Just type `nessus-update-plugins`. Your server will automatically download them for you. I recommend doing this at least once a week if you're scanning frequently. If you scan only now and then, just remember to update your plug-ins before each use.

Client Installation

You'll find the Windows GUI client here, along with other Windows-related download information. It is self-extracting and extremely easy to install and use.

Remember to always get permission before scanning any hosts or networks. Anyone running scans without prior notice and permission will be seen as a hacker, no matter how good the intentions are. Learn how to scan for security flaws with Nessus

Nessus is a powerful tool for scanning your network and pinpointing security issues such as missing patches and flaws that could be targeted by attackers. In my previous article, I introduced Nessus and explained how it can be a valuable asset. Now, I'm going to show you the specifics of how to use it.

First Things First

Before you start scanning your hosts or network, you need to get permission. Anyone running scans without prior notice and permission will be seen as a hacker—no matter how good your intentions are. Scanning can freeze host systems and is visible to IDS devices and sniffers. I strongly suggest that you start scanning in a lab environment before trying this on a live production network. When you are ready to scan production systems, run the scans during nonworking hours (or at least, during less hectic times) and have fellow administrators ready to restart systems or applications if necessary.

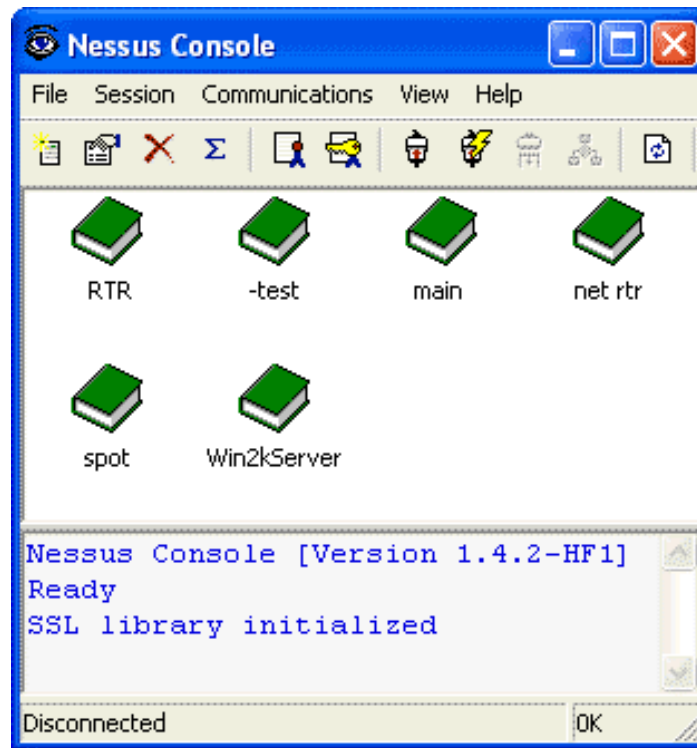
Defining Your Scan

Nessus is highly configurable, as you will see. It's impossible to cover all variations and options in the short span of this article; however, I'll give you an overview that will help you get started. You'll need time and experimentation to really discover what you can do with this tool.

Now on to the fun part. Figure A shows the Nessus Windows client.

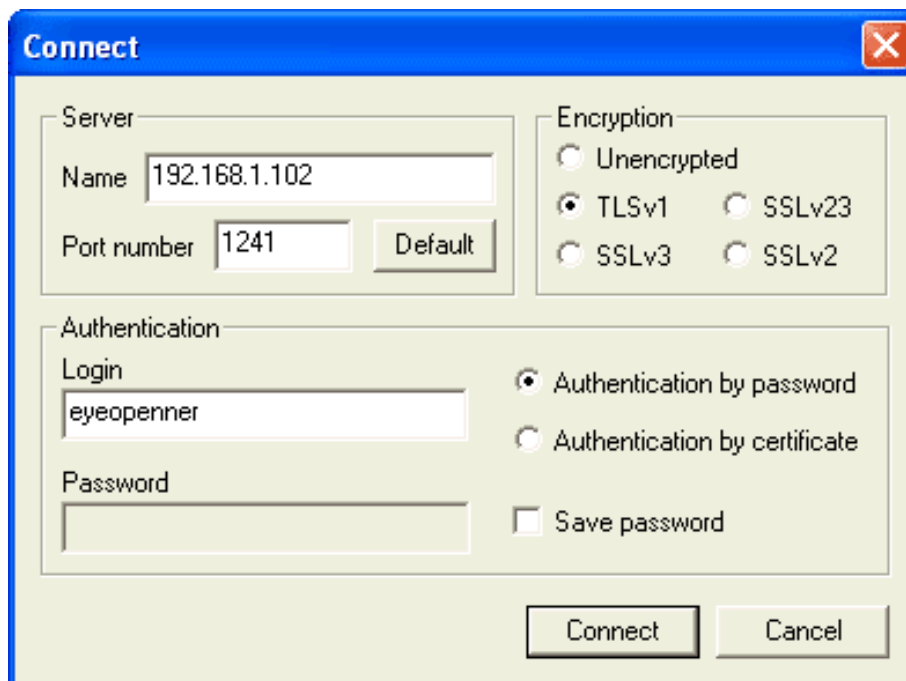
Nessus Scanning

Figure A



The first thing you need to do is establish a connection from the client to the server. You'll find two connection options on the Communications menu. Select Connect to open the Connect dialog box (Figure B), where you can enter your username in the Login text box. This is what you'll use if you have more than one user configured on the server. You can choose Quick Connect if you do not want to use individual usernames.

Figure B



Nessus Scanning

You can connect using either the DNS name of your server or the IP address. The default port is 1241, but this is changeable through your server configuration file. Click Connect, and the server will prompt you for your password and authenticate you. You will then see how many plug-ins have been loaded for the client to use during scans.

Now, you need to start a scanning session by selecting from the Session menu. You'll be asked to create a session name when creating a new scan file. Then, you can define the parameters you want to use for this scan in the Session Properties dialog box (Figure C). Click Add to define the host, network, or IP address range you want to scan (Figure D).

Figure C

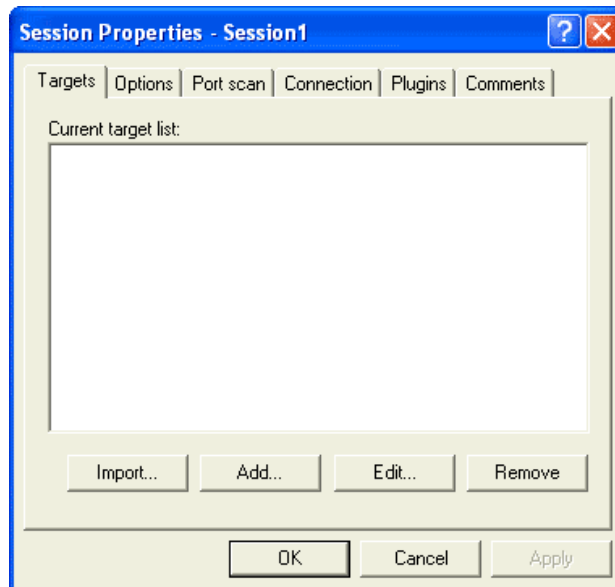
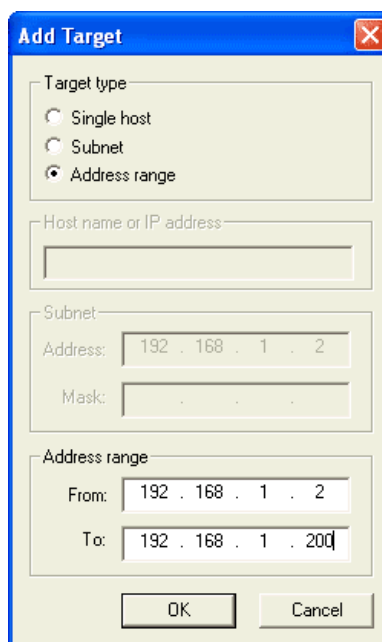


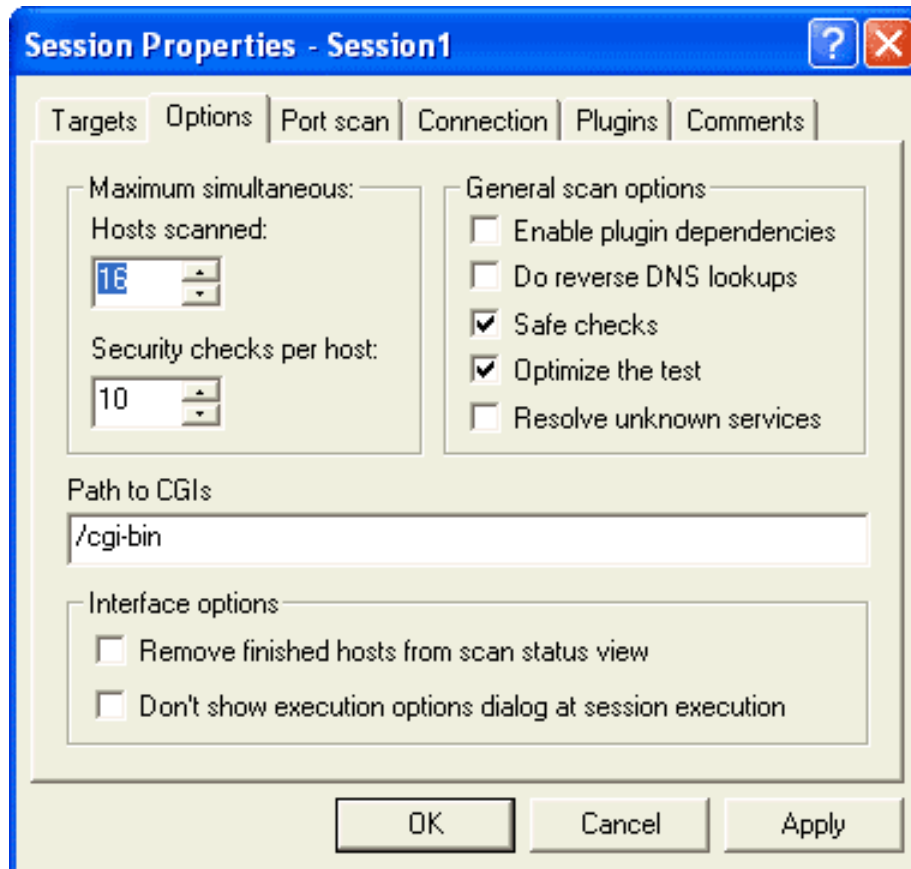
Figure D



Nessus Scanning

After you define the target, select the Options tab (Figure E).

Figure E

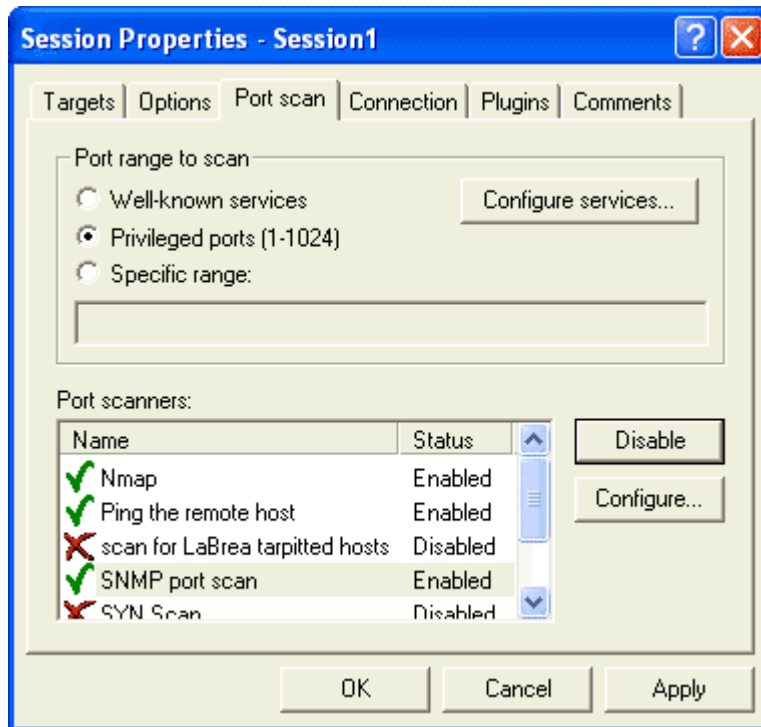


At first, make sure you have the Safe Checks option selected—unless you want to bring the wrath of some poor administrator upon yourself. With this option selected, Nessus relies on using banners to report vulnerabilities instead of actually trying to use the suspected vulnerability to see how far it can be exploited.

The Port Scan tab (Figure F) allows you to define specific ports or ranges of ports. If you wanted to run a scan on your network or host to find out whether or where a particular service is running—such as SMTP servers—you would click the Configure Services button. This is also where you select specific scanners to use. All port scanners are off by default. To activate them, just highlight and enable them.

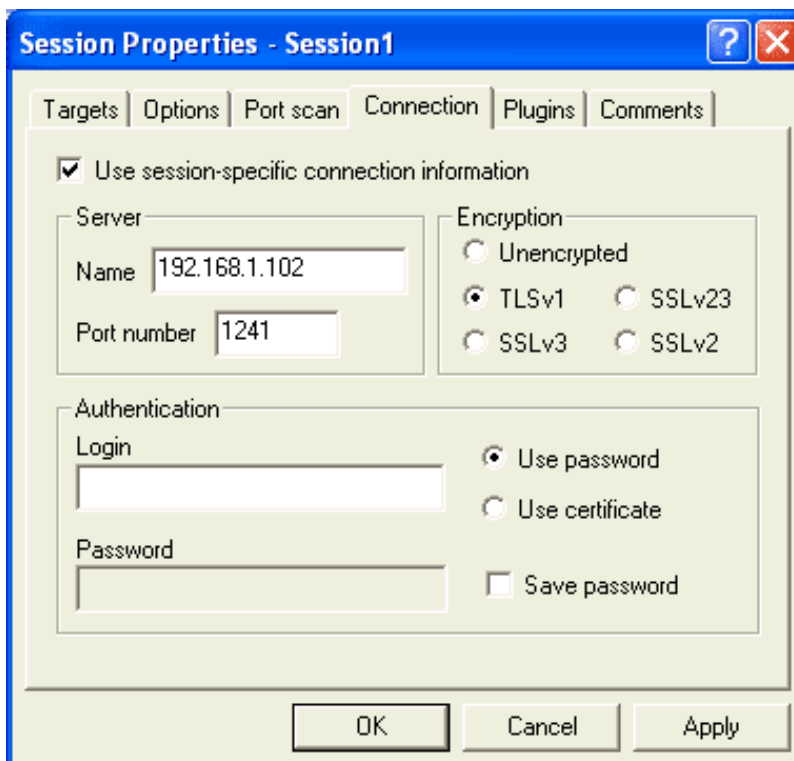
Nessus Scanning

Figure F



The Connection tab (Figure G) allows you to use logins and passwords for your scan parameters, as well as to specify encryption methods for your session.

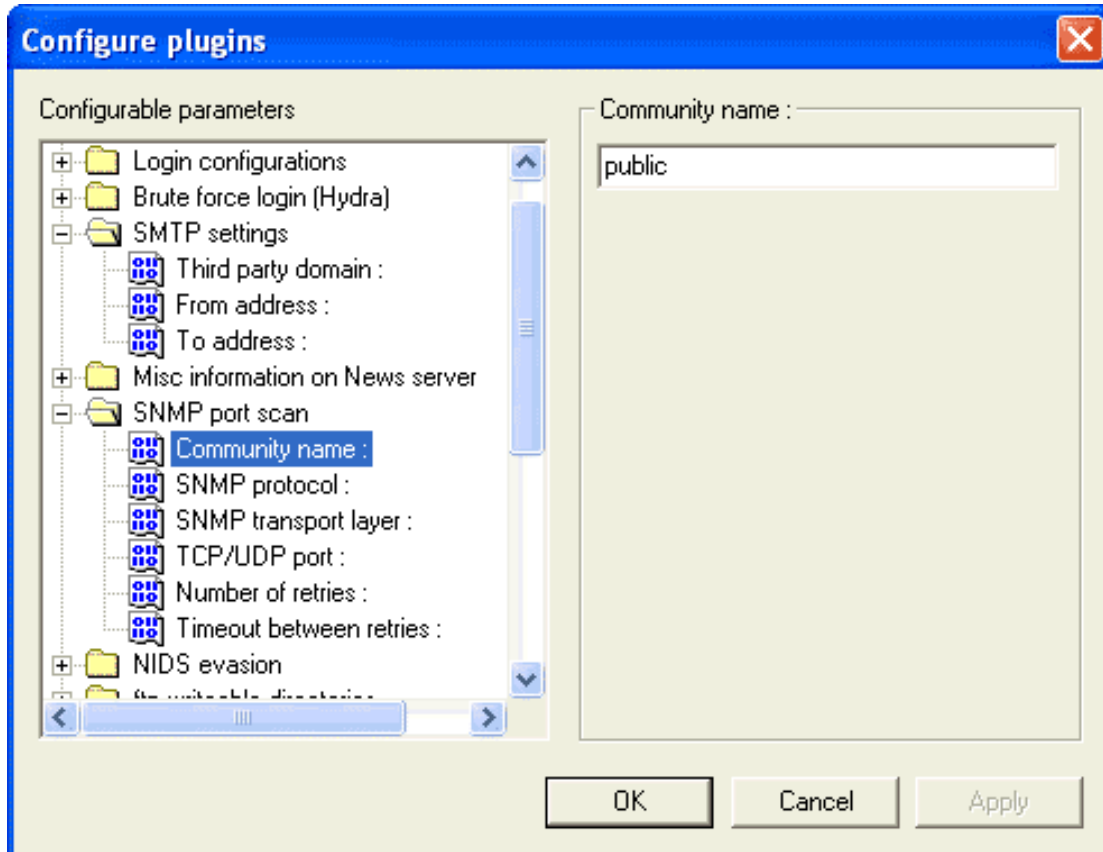
Figure G



Nessus Scanning

In the Plugins tab, click the Configure Plugins button to see how incredibly configurable Nessus can really be. Each plug-in has a default setting that can be changed, and you can use the Configure Plugins dialog box (Figure H) to select the desired plug-ins to fine-tune your scan. For instance, if you know you're scanning a UNIX host, you can disable the Cisco and Windows plug-ins.

Figure H



Executing Your Scan

Once you've defined your scan, simply double-click its icon to execute it. The scans are saved as part of the database that Nessus creates, called NessusDB. You can view reports at the end of a scan or save them as text files or HTML files. Reports are saved in the NessusWX folder.

Additional report options, such as pie charts, are handy for pitching cases to management-type folks. You can also import the results to a spreadsheet if you want to track results for large scans.

Figure I shows part of the results of a sample scan. The offending service and the severity level are reported, as well as information about the vulnerability. Web links for more in-depth information are often supplied in the Description section.

Nessus Scanning

Figure I

The screenshot shows a web browser window displaying a Nessus report. The title is "Network Vulnerability Assessment Report" with a date of "05.04.2003". It is sorted by host names. The report details a session named "Scan A" that started at 19:00:41 and finished at 19:06:21 on 05.04.2003, lasting 00:05:39. It generated 32 records: 10 high severity, 16 low severity, and 6 informational. A summary table for host 192.168.103.31 shows 10 holes, 16 warnings, 6 open ports, and a state of "Finished". A detailed view for host 192.168.103.31 lists several services as "Info" (ssh, general/udp, ftp, https, smtp, http) and one as "High" severity: smtp (25/tcp). The high severity finding is described as a buffer overflow in Sendmail's DNS handling code, with a solution to upgrade to Sendmail 8.12.5. The risk factor is high, with CVE: CAN-2002-0906 and BID: 5122.

Host	Holes	Warnings	Open ports	State
192.168.103.31	10	16	6	Finished

Service	Severity	Description
ssh (22/tcp)	Info	Port is open
general/udp	Info	Port is open
ftp (21/tcp)	Info	Port is open
https (443/tcp)	Info	Port is open
smtp (25/tcp)	Info	Port is open
http (80/tcp)	Info	Port is open
smtp (25/tcp)	High	The remote sendmail server, according to its version number, may be vulnerable to a buffer overflow its DNS handling code. The owner of a malicious name server could use this flaw to execute arbitrary code on this host. Solution : Upgrade to Sendmail 8.12.5 Risk factor : High CVE : CAN-2002-0906 BID : 5122

An Impressive Solution

Worried about running these scans on your network? You shouldn't be, as long as you use common sense, get permission, and work closely with system owners. After all, hackers may have already run the same scans against your network. Just remember, these scans are a snapshot of time. Systems that look secure today may not be secure tomorrow or next week. Security is an ongoing process, not a one-shot deal.

Once you've used Nessus, you can easily see how administrators can put this valuable tool to work. You can pay a lot of money for a commercial product, you can pay someone a lot of money to do it for you, or you can take control and get an excellent picture of vulnerabilities on your own. Nessus is an easy to use, up-to-date tool that enables you to find vulnerabilities and check them on a routine basis, and it often points you to resources for fixes. That's pretty impressive for a free tool.