Exercises: Nessus Install and use under FreeBSD: SANOG VI IP Services Workshop

July 16, 2005

The Nessus website is http://www.nessus.org/

Note: The "#" and "$" characters before commands represents your system prompt and is not part of the command itself. "#" indicates a command issued as root while "$" indicates a command issued as a normal user.

Note 2: If you install software, update your environment as root and the change is not immediately available try typing `rehash` at the root shell prompt. This is only necessary when running a C shell (e.g., like /bin/csh).

Nessus installation using ports

You need to be root to do this. If you install the Nessus package you'll find that it doesn't come with a GUI. You want a GUI with Nessus, so we instal from ports. The Nessus website has good documentation on setting up Nessus post installation starting here:

> http://www.nessus.org/demo/index.php?step=1

Now to install do this:

```
# cd /usr/ports/security/nessus
# make install
```

Nessus will compile for quite some time. While it's doing this we'll take this chance to talk about what Nessus does and, possibly show it in action from your instructor's machine.

Now that the main Nessus program has compiled we still need to compile the plugins for Nessus. We do this separately by typing:

```
# cd /usr/ports/security/nessus-plugins
# make install
```

This, also, takes some time. You should see an indication that over 2,000 plugins were compiled! Don't forget to type:

```
# rehash
```

if you are using a C-shell.

Before you can run the Nessus daemon you need to make a local ssl certificate. To do this type:

```
# nessus-mkcert
```

You will be presented with several questions to answer. Here are the screens and the responses you should give:

```
-------------------------------------------------------------------------------
                        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 yourNessus daemon will be able to retrieve this information.


CA certificate life time in days [1460]: RETURN
Server certificate life time in days [365]: RETURN
Your country (two letter code) [FR]: bt
Your state or province name [none]:
Your location (e.g. town) [Paris]: Thimphu
Your organization [Nessus Users United]: SANOG VI Workshop
```

If certficate generation works you should get a screen that looks like this:

```
-------------------------------------------------------------------------------
                        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/CA/cacert.pem
   Private key = /usr/local/var/CA/cakey.pem

. Nessus Server :
    Certificate = /usr/local/com/CA/servercert.pem
    Private key = /usr/local/var/CA/serverkey.pem

Press [ENTER] to exit
```

Now we need to create a Nessus userid that we can use when connecting to the Nessus server. This userid is *separate* from any system userid you may have. To do this type:

```
# nessus-adduser
```

Now you'll be presented with multiple choices to fill in. Follow the example below to create the Nessus userid *sanog* with appropriate network filtering for our local network.

```
Login : sanog
Authentication (pass/cert) [pass] : RETURN
Login password :
Login password (again) :
```

```
User rules
----------
nessusd has a rules system which allows you to restrict the hosts
that sanog has the right to test. For instance, you may want
them to be able to scan their own host only. Note the "nnn.nnn.nnn.0"
prefix should be substituted with our class IP prefix. The "xx" should
be our class allocation, which in this case is a /27. So, our class network is
202.144.151.0/27, and we want to only allow the user sanog to scan in
our network. This looksl ike this:

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 202.144.151.0/27
default deny

Login             : sanog
Password          : ***********
DN                :
Rules             :
accept 202.144.151.0/27
default deny


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

You could enable Nessus to boot every time you start your machine by adding the following line to your */etc/rc.conf* file:

```
nessusd_enable="YES"
```

but, I would recommend against this unless you plan on using this machine heavily as a Nessus scanner.

Now you can start the Nessus daemon:

```
# nessusd -D
```

Now as a user *other than root* connect to the Nessus server on your local machine using the Nessus program:

```
$ nessus &
```

In the opening screen enter in the *Nessus* Login name you created (not your account name) and password, then press the "Log in" button.

At this point you could read in detail about configuring Nessus to be used exactly as you want here:

> http://www.nessus.org/demo/index.php?step=2

Or, you can follow these quick steps to run an initial scan using Nessus:

- Press "OK" on the initial SSL dialogue that appears.
- Press "YES" to accept the local SSL certificate you have generated.
- By default you'll be dumped to the "Plugins" tab screen. And, by default all plugins are enabled. Either make no changes and continue to start scanning, or pick some subset of plugins that you think might be interesting. Do this by pressing "Disable all" and then choosing the plugins you want. A scan with all plugins may take so long that we won't have time to complete it during class.
- Click on the "Target" tab.
- In the "Target(s):" box enter in the IP address of the machine to your right. If no one is to your right, then enter in the IP address of the machine to your left.
- Press the "Start the scan" button. A new window opens.
- Scanning may take quite some time since we have enabled all plugins.
- If you had chosen to scan an entire network this can take quite some time and can generate a lot of traffic.
- Be *very careful* about using this tool as it can set off all sorts of security alarms. You should always let the recipient of a Nessus scan know ahead of time that you are going to be scanning their machine for potential security holes.
- Once scanning completes click on the "Subnet" icon, then the "Host" icon, and then on the individual "Port" icons to get more information.
- If you click on "Save report..." and then choose a "Report file format" of "HTML with Pies and Graphs", then you can save your report to a folder and view it in a web browser immediately. Maybe use the IP address of the scanned machine as the report name.
- Open the folder that is created and then open the "index.html" file that should exist.
- Click around in the report, particularly the IP address at the bottom of the first page, to see a *large* amount of information.

If you scan on a subnet, then Nessus will give you meaninful aggregate results on the initial report page.

As you may note as you read through your report, Nessus has up-to-date security vulnerabilities listed via their web site.

You can configure Nessus using cron and by going to:

> http://www.nessus.org/register/

to get a "full plugin feed" and to stay up-to-date at all times if you wish. You will receive an activation code via email for plugins if you register your Nessus installation at the site above.

Hervey Allen

Last modified: Fri Jul 8 01:32:32 CLT 2005