Installing additional weapons

Although the latest version of Kali Linux always comes with many security tools, sometimes you need to add additional software tools due to the following reasons:

- The latest version of the tool has not been included in Kali Linux yet
- You want to have the latest version of the software that is not available in the Kali Linux repository

Our suggestion is to try to search for the software package in the repository first. If you can find the package in the repository, just use that package. However, if you can't find it in the repository, you may want to get the software package from the author's website and install it yourself.

Based on our experience, we suggest that you use the software in the repository as much as you can to ease the package management process.

There are several package management tools that can be used to help you manage the software package in your system, such as `dpkg` , `apt` , and `aptitude` . Kali Linux comes with `dpkg` and `apt` installed by default.

Note

If you want to find out more about the `apt` and `dpkg` command, you can go through the following references: https://help.ubuntu.com/community/AptGet/Howto/ and http://www.debian.org/doc/manuals/debian-reference/ch02.en.html.

In this section, we will briefly discuss the `apt` command in a practical way that is related to the software package installation process.

To search for a package name in the repository, you can use the following command:

```
apt-cache search <package_name>
```

This command will display the entire software package that has the name `package_name` . For example, let's search for a software package called `nessus` ; the following is the command to do that:

```
apt-cache search nessus
```

To display more detailed information about a software package such as its description, size, and version, you can use the following command:

```
apt-cache show <package_name>
```

If you want install the package or upgrade an individual software package, you can use the `apt-get` command to install the package. The following is the basic syntax for `apt-get` to do that:

```
apt-get install <package_name>
```

If you can't find the package in the Kali Linux repository and are sure that the package will not cause any problems in the future, you can install the package manually.

Download the software package only from trusted sources such as the software developer's site. If the developer provides the `.deb` (the Debian package format) packages, you can use the `dpkg` command to install the additional software. If the `.deb` package is not provided, you can install the software from the source code. The actual process may vary but the general steps are usually similar to the following:

1. Extract the software package using archiver programs such as Tar and 7-Zip.
2. Change to the extracted directory.
3. Run the following commands:

```
 ./configure
make
```

```
make installh
```

In this section, we will provide you with examples on how to install several additional security tools that are not available from the Kali Linux repository. We will give various mechanisms that can be used to install the software:

- Downloading the Debian package and installing it
- Downloading from the source package and installing it

Installing the Nessus vulnerability scanner

As an example, we want to install the latest Nessus vulnerability scanner (Version 5) for the first installation mechanism. We have searched the Kali Linux repository but are unable to find Nessus.

Nessus Version 5 has many new features as compared to Nessus Version 4, such as more flexible results filtering and report creation and simplified policy creation; we chose to use this version instead of Nessus Version 4.

Note

You can find more information about the features and enhancement in Nessus Version 5 from http://www.tenable.com/products/nessus/nessus-product-overview/why-upgrade-to-nessus-5.

We can download the latest Nessus package generated for Debian 6 Linux distribution from the Nessus website (http://www.nessus.org/products/nessus/nessus-download-agreement). To install this package, we issue the following command:

```
dpkg -i Nessus-x.y.z-debian6_i386.deb
```

Note

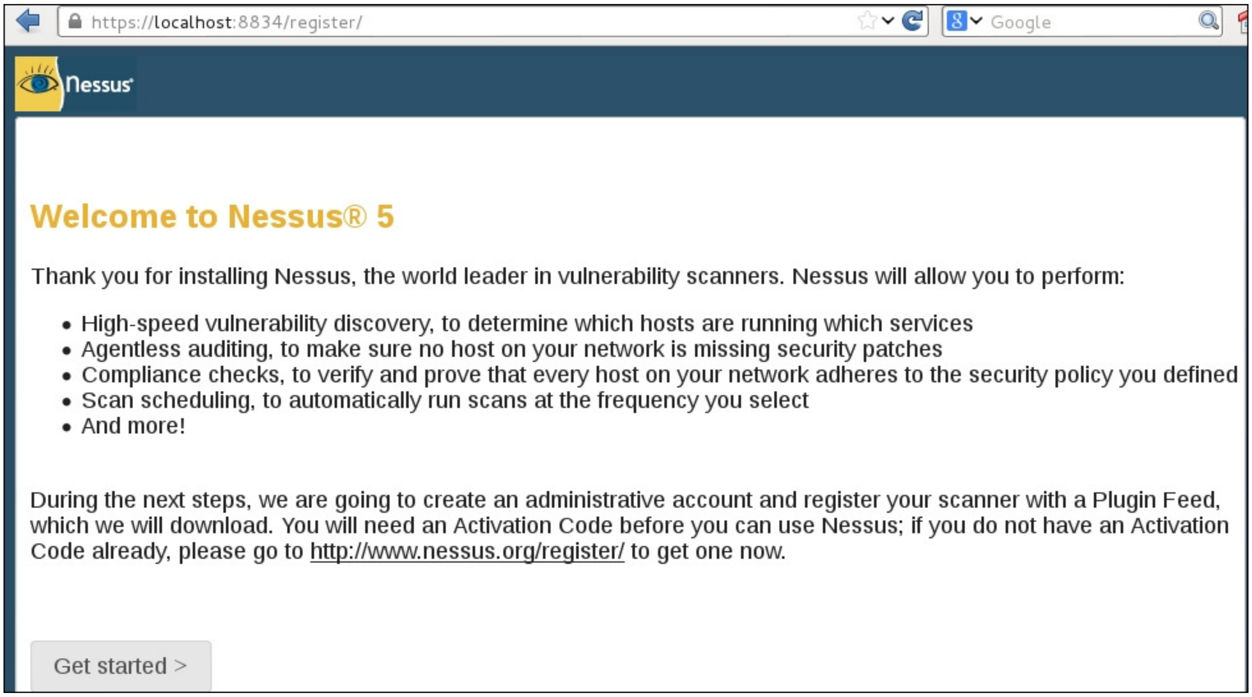
We used `x.y.z` in the previous command to denote the Nessus version number. You need to change those numbers to the Nessus version that you just downloaded successfully.

You can then follow the instructions given on the screen to configure your Nessus server:

1. Start the Nessus server by typing the following if it has not started yet:

```
/etc/init.d/nessusd start
```

2. Open your browser and connect to `https://localhost:8834`. You will then be prompted with a warning about an invalid SSL certificate used by Nessus. You need to check the SSL certificate and then store the exception for that SSL certificate. The following is the Nessus page that will be shown after you have stored the SSL certificate exception:



https://localhost:8834/register/

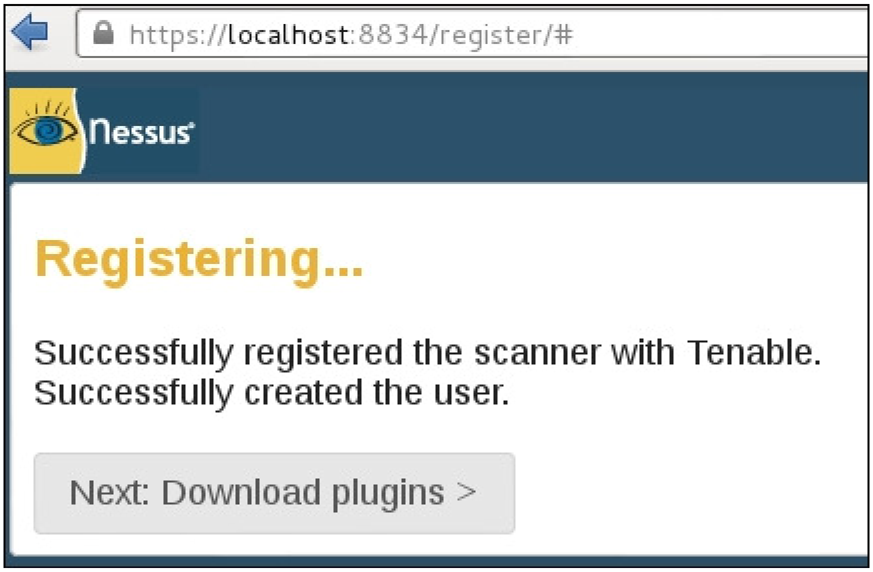
Welcome to Nessus® 5

Thank you for installing Nessus, the world leader in vulnerability scanners. Nessus will allow you to perform:

- High-speed vulnerability discovery, to determine which hosts are running which services
- Agentless auditing, to make sure no host on your network is missing security patches
- Compliance checks, to verify and prove that every host on your network adheres to the security policy you defined
- Scan scheduling, to automatically run scans at the frequency you select
- And more!

During the next steps, we are going to create an administrative account and register your scanner with a Plugin Feed, which we will download. You will need an Activation Code before you can use Nessus; if you do not have an Activation Code already, please go to http://www.nessus.org/register/ to get one now.

3. After that, you will be guided to create a Nessus admin credential. Next, you will be asked to enter your activation code to register the Nessus scanner to Tenable. You need to register at http://www.nessus.org/register/ to obtain the activation code:



Registering...

Successfully registered the scanner with Tenable.
Successfully created the user.

4. After you have registered successfully, you will be able to download the newest Nessus plugins. The plugins download process will take some time to complete; you can do something else while waiting for the download process to finish.

Installing the Cisco password cracker

For the second example, we will use a simple program called `cisco_crack` (http://insecure.org/sploits/cisco.passwords.html). This tool is used to crack the Cisco type 7 password.

> **Note**
>
> Cisco type 7 password is a very weak password, so it should not be used anymore. However, for penetration testing, we see that it is still being used, although it's not widespread anymore. This tool will be a help for this occasion.

After downloading the source code, the next step is to compile it. Before you can compile the source code cleanly, you need to add the following `include` statements:

```
#include <string.h>
#include <stdlib.h>
```

Now, you have four `include` statements in the source code.

To compile the code, you can just give the following command:

```
gcc cisco_crack.c -o cisco_crack
```

If there is no error, an executable file with the name of `cisco_crack` will be created. The following is the help screen of `cisco_crack` :

```
# ./cisco_crack  -h
Usage: ./cisco_crack -p <encrypted password>
       ./cisco_crack <router config file> <output file>
```