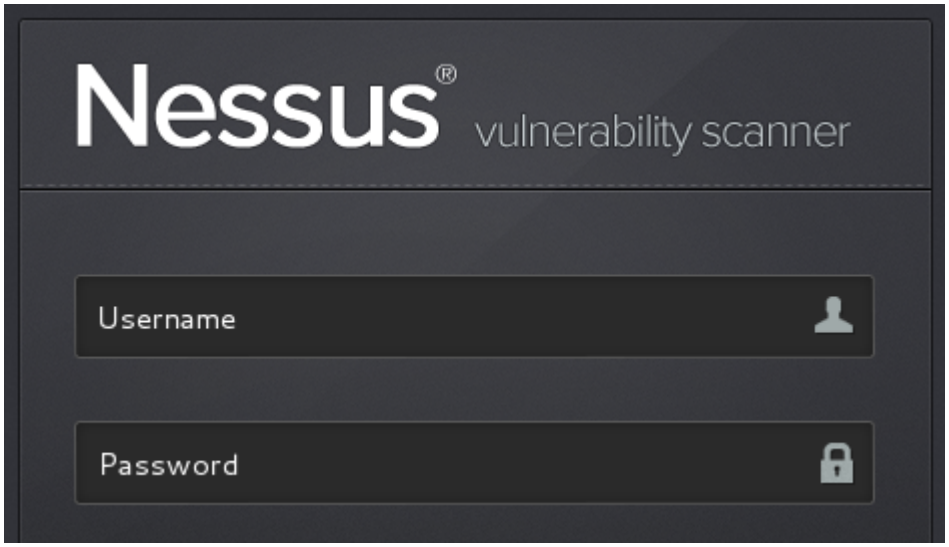
How to Install, Setup and Use Nessus on Kali



Author: Philip Straatsma | October 16, 2013 | 8 Comments

Security How-to, Kali, Nessus

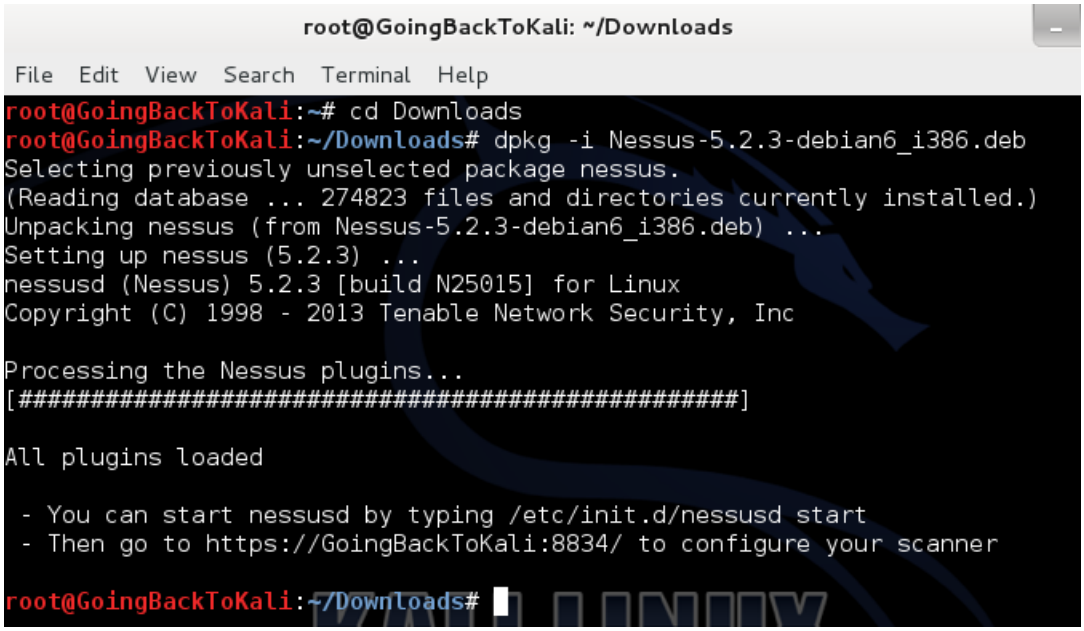
One of the best tools for host vulnerability analysis is Nessus and sadly because of its licensing structure is not included in the Kali Linux distro. But that doesn't mean that you can't install it! Thankfully Tenable offers a free home use license for uh, home use only. Below is our step by step install, setup and basic usage guide for Nessus on Kali 1.0.

The Download:

1. First things first, download Nessus from: http://www.tenable.com/products/nessus/select-your-operating-system Select Linux -> Debian 6.0 (32-bit) or (64-bit) based on the architecture version of your Kali install.

The Install:

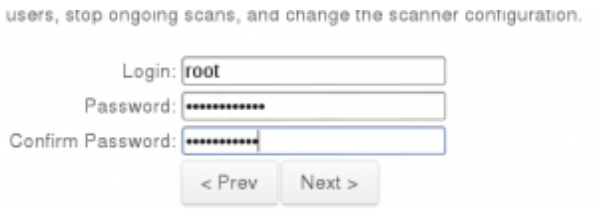
2. Open terminal and change directory to the location you downloaded Nessus to, in my case the Downloads directory. From there execute the dpkg -i Nessus-5.2.3-debian6_i386.deb command to start the Nessus install (swapping in the name of your downloaded file as needed).



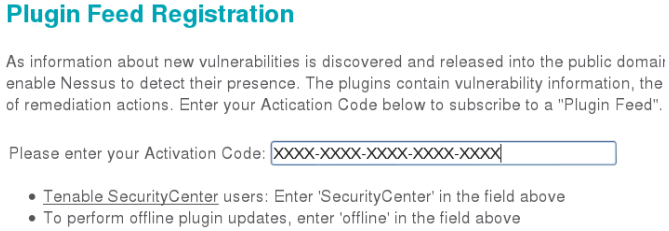
3. Once the install is complete you will need to start Nessus back-end server. To do so enter /etc/init.d/nessusd start. You will need to enter this command each time you reboot Kali which can get tedious and for the forgetful amongst us just plan annoying. In the Ease of Use section of this article you will learn how to streamline this manual process.

The Setup:

4. Once you have started the Nessus Server (Step 3) browse out to https://127.0.0.1:8834 (accepting the risk for the self-signed cert) hit 'Get Started' and you will be prompted to create a Login ID. Make sure you either memorize this username and password combo on the spot or enter it into your favorite encrypted password protected file of passwords as you will need it later to log in to Nessus on your local machine.

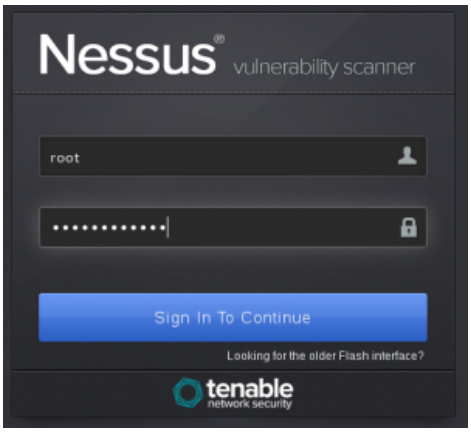


5. Continuing on you will be prompted to enter an Activation Code. A home-use code can be retrieved from Tenable's website for the low low cost of your email address and completely legit first and last name. http://www.tenable.com/products/nessus-home



6. Once you enter your secret decoder Activation Code and hit next Nessus will automagically connect back home to download updates and the latest plug-ins, whether you like it or not. At this point I would get up and take a potty break, stretch and get a bevvie, you are going to be waiting a while.

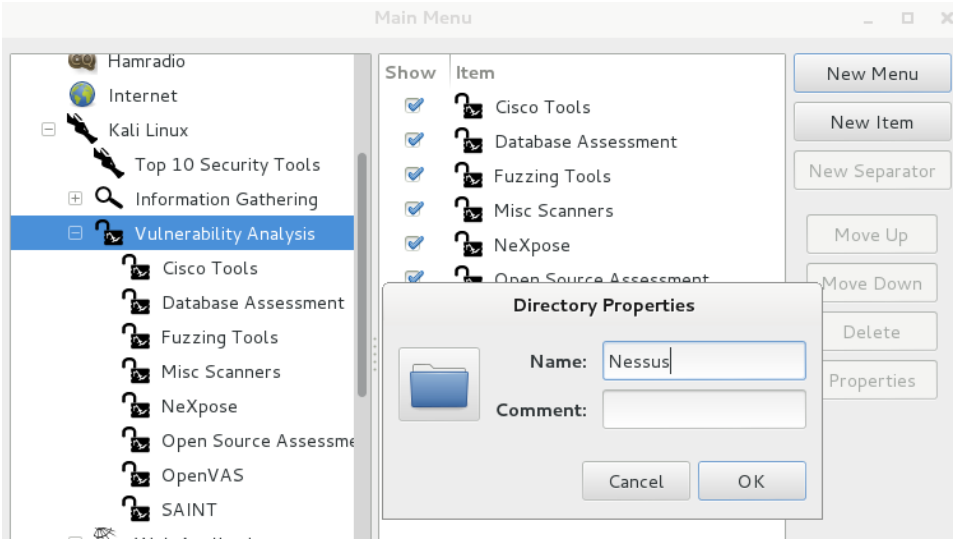
7. When complete you are prompted for the credentials you entered earlier. Before you log in I would recommend bookmarking this page for easy access later.



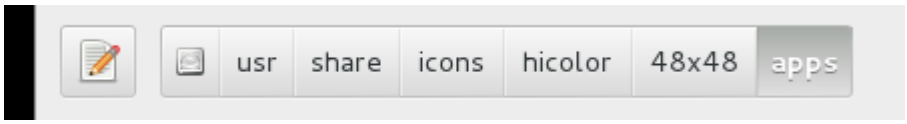
Ease of Use:

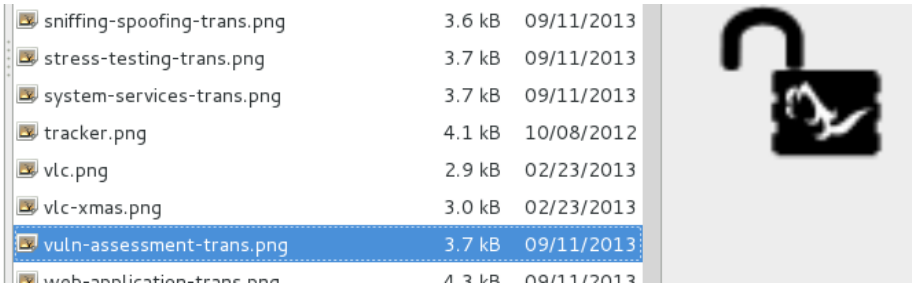
8. As I mentioned earlier, each time you reboot Kali you have to restart the Nessus server back-end by entering /etc/init.d/nessusd start into Terminal. This can be a very tedious process and for those of us who are forgetful, downright frustrating. To make this process a bit easier yet still allow you to load the the server portion of Nessus only when you want to I suggest creating a shortcut in the Applications Menu. To create the shortcut right click on the Applications menu in the upper right hand corner of Kali and click 'Edit Menus'.

On the left side of the Main Menu screen drill down to Vulnerability Analysis under the Kali Linux menu and click 'New Menu'.

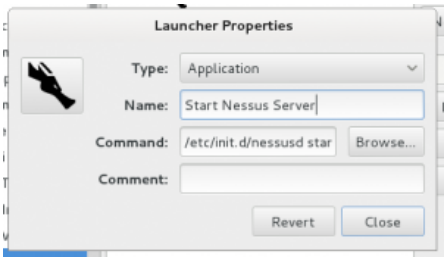


Name this new menu Nessus and click on the folder icon. Navigate to the usr -> share -> icons -> hicolor -> 48×48 -> apps folder and select vuln-assessment-trans.png and hit ‘Open’ and then ‘OK’ on the Dicectory Properties window. This will change the icon for the Nessus menu item that we just created to match the rest of the items in the Vulnerability Analysis menu.

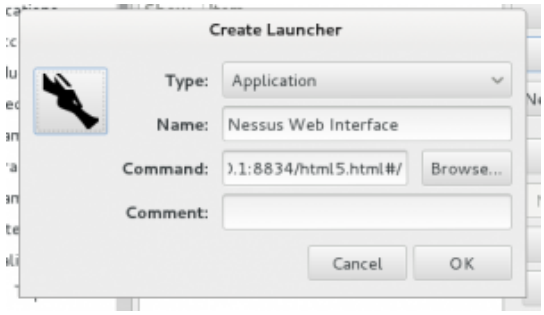




Now to create the actual Nessus server Launcher in the Nessus menu we just created select the Nessus menu on the left and click ‘New Item’. In the Name: field enter Start Nessus Server in the Command: field enter /etc/init.d/nessusd start.
Lastly to match the launcher icon to the reset of the launchers in Kali click on the spring-board icon to the left of the Create launcher window and navigate back to the usr -> share -> icons -> hicolor -> 48×48 -> apps folder, this time you will select the Kali-menu.png icon, hit Open and OK on the Create Launcher window.



Next we will create the launcher to load the Nessus web interface in Iceweasel. Following the exact steps as we did for the Start Nessus Server launcher create the new menu item, but this time enter Nessus Web Interface for the name and iceweasel %u https://127.0.0.1:8834/html5.html#/ in the Command: field.

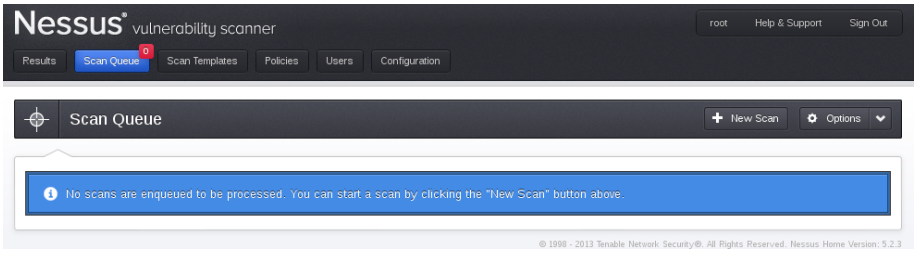


Using the two new menu items we created we can now launch the server and then the web interface from one menu all while following the Kali menu structure standard. Magnificent!

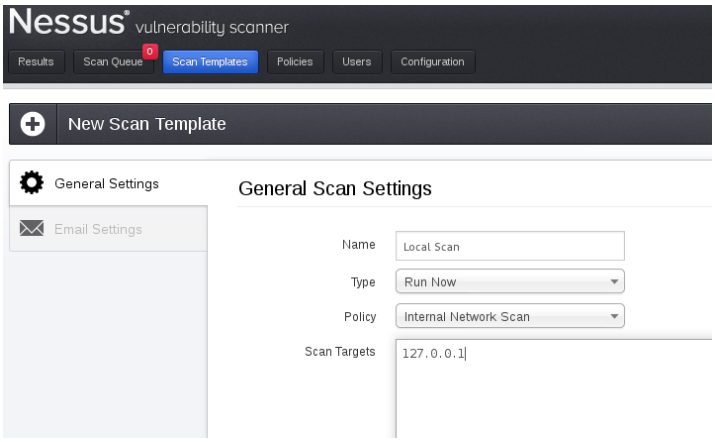
Using Nessus:

9. If you haven't already, launch the Nessus web server from our newly created Start Nessus Server launcher and load the web interface from its corresponding launcher. If your launchers both worked correctly you will be presented with the Nessus login screen, enter the credentials you created earlier to continue.

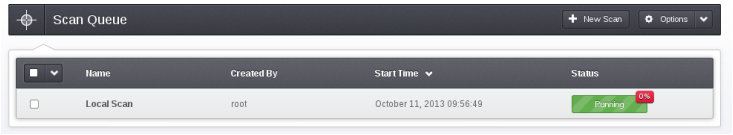
10. By default after you log in your are taken directly to the Scane Queue. Nessus is an extremely straight forward and easy to use vulnerability scanner right out of the box, almost everything you need can be found in the top menu.



11. On the Scan Queue page select New Scan from the sub-menu on the right side of the page. This takes you to the New Scan Template page where you can setup your scan target(s). Name the scan whatever you want, the type should be set to Run Now and select Internal Network Scan for Policy. As for Scan Target you can either a single host IP address, 192.168.1.1, or multiple addresses, 192.168.1.1,192.168.1.4,192.168.1.22, an address range, 192.168.1.1-10, or an entire subnet, 192.168.1.0/24. When done, simply hit Run Scan at the bottom of the screen. ***Pro Tip:** While Nessus does not actually run exploits against the targets you pointed it at, it is possible that if you scan a highly vulnerable target, Nessus may actually crash it. My advice would be to run the scan after hours and make sure you have everything saved on the target box and that it has recently been restarted. ***Pro Tip #2:** Only scan targets that you own or targets that you have secured the permission to scan.

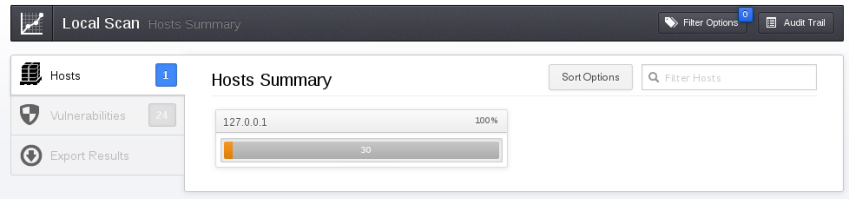


12. Once you start the scan you will be taken back to the Scan Queue page where you can watch the progress of the scan against your poor defenseless target. If you wish you can click on the scan to take you to the Hosts Summary page, or simply wait until it is complete.

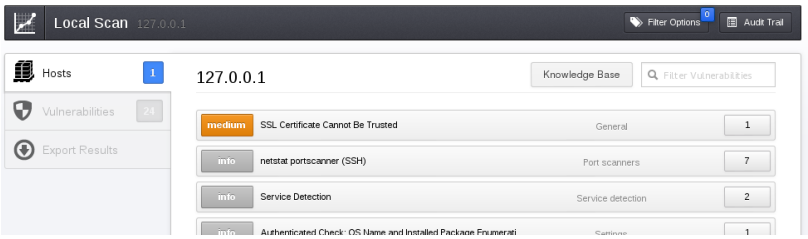


13. Once the scan is complete click on the scan in question to take you to the Hosts Summary page. I have seen in the past where Scan Queue page will not automatically refresh, so feel free to refresh the page as you see fit. Additionally any previous scan can be reviewed later by clicking on the Results tab at the top.

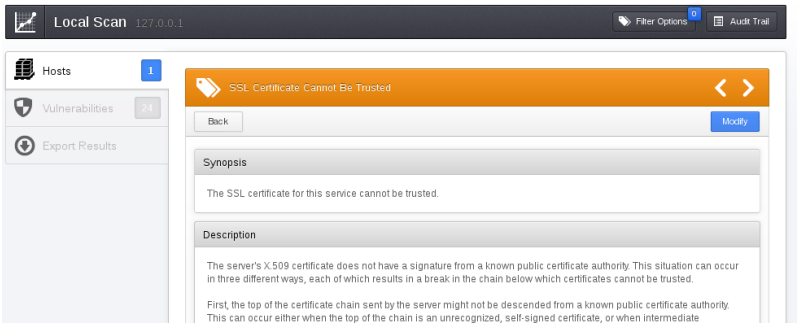
14. The Hosts Summary page will list all of the hosts you included in the Scan Target field individually. In this example I only used one target, the local host, so only one summary shows up. This host summary also includes a count of all the vulnerabilities for for that individual target as well as in information it has gathered.



15. If you click on the host you are presented with a more specific listing of all the potential vulnerabilities it has found along with brief description of any information gathered.



16. Clicking on a vulnerability or information item will take you to the specific page describing the vulnerability in greater detail. **Pro Tip #3:** Nessus will often list Windows specific vulnerabilities by their Security Bulletin number, everyone's favorite MS08-067, for example. This number often corresponds with a known vulnerability within Metasploit allow you to easily transition from vulnerability analysis to exploitation execution.



I hope you find this tutorial useful in your future networking adventures! To receive updates each time we release a new article, feel free to follow us on Twitter via @HackAndTinker.

-Philip Straatsma

← Previous post Next post →

8 Comments

Michał November 9, 2013 at 9:00 am

Hello,
I had install Nessus in Kali like You. But after installation I have empty policy list. Can You help me?

Philip Straatsma (Post author) November 11, 2013 at 8:50 am

I have not run into this before but, you can try and Update the Plugins under Configuration > Feed Settings > Update Plugins. Let me know if this corrects the issue you are having.

Michał November 11, 2013 at 12:14 pm

I installed 5.2.4 version. I have different interface. I try 5.2.3 and is another interface too. I have try reinstall, update from script in /opt/… and it do nothing 🙁

I have something like this on screen:
http://imageshack.us/photo/my-images/801/wcba.png/

…and no default policies. I fight with it 2 weeks and I can not win with it 🙁

Peter Johnson February 2, 2017 at 8:48 am

Hi guys. Firstly I am a complete noob when it comes to Linux and hacking but I am wanting to learn both.

Now. I have Kali Linux installed on VM and I have also installed Nessus and have started it from within console but when I type any of the following into Iceweezel I get an error. I have typed “https://kali:8834” “https://localhost:8834” “https://127.0.0.1:8834” and all come up with an error saying

“Secure Connection Failed

An error occurred during a connection to 127.0.0.1:8834.

SSL received a record that exceeded the maximum permissible length.

(Error code: ssl_error_rx_record_too_long)

The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.

Please contact the website owners to inform them of this problem. Alternatively, use the command found in the help menu to report this broken site.”

with a button labled “try again”

I get no SSL warning just the error page.

What have I done wrong??

Thanks.

P.S. I have an internet connection (which I guess shouldn’t matter)

SadSack8 February 13, 2017 at 9:53 am

you have an “advanced” button that you can click on. you will have to confirm that the certificate is secure and you’ll be able to continue

Ben February 13, 2017 at 12:22 pm

Im having the same problem. iceweasel wants to connect because it takes a minute or so of trying to connect before it fails. if i shut down nessus then it fails automatically, as it should.

Mira April 26, 2018 at 7:30 pm

Was this ever resolved? I ask because I am having the same issue. It know this was a year ago but I can’t find anything on this.

Mira April 26, 2018 at 7:31 pm

The SSL error code is what I mean’t to post the reply to.