Module 10 Lab Securing Network Infrastructure with Nessus

Background: This Lab reinforces the concepts of vulnerability scanning as discussed in the lecture.

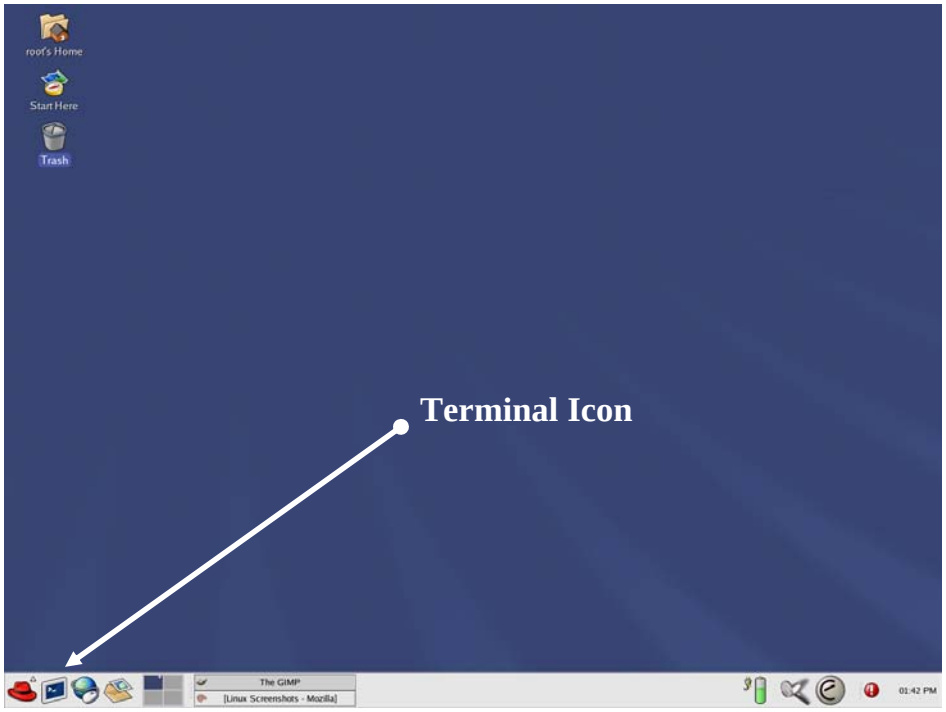
Requirements/assumptions:

- Workstation with Linux Red Hat 8.0 preloaded with Nessus
- Local administrative (root) privileges
- Internet connection

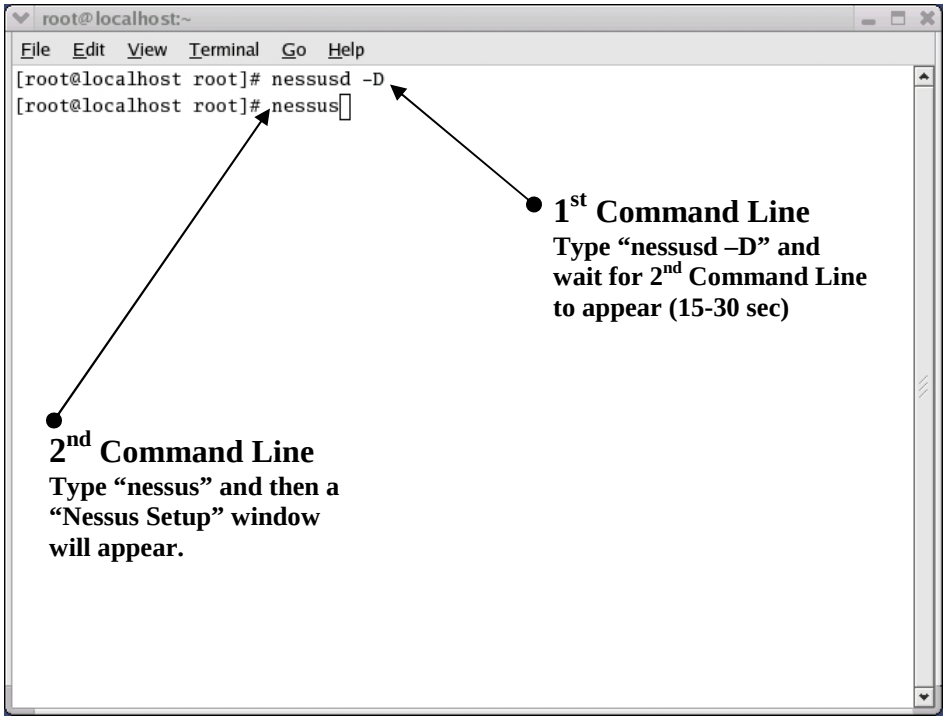
Exercise 1: Red Hat (Linux) Installation and Scanning

1. Using an ISFTS Student Laptop Computer, power on the computer. During start-up you will be presented with a window to choose an Operating System, select "**Red Hat Linux (2.14 18-14)**". The loading process for Red Hat Linux may take several minutes. Once Red Hat Linux has completely loaded a desktop interface will appear requesting a Username: "**root**" and Password: "**tartans**".

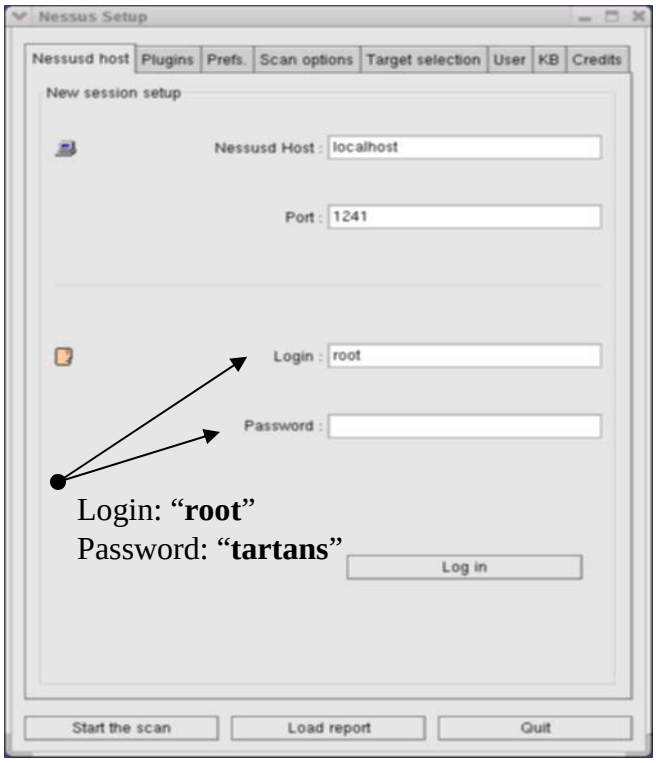
2. Once log-on is complete, a Red Hat Desktop interface will appear. In order to begin utilizing Nessus, you must first launch the program from a Terminal window. A Terminal window can be opened by clicking on the flat screen icon located at the bottom left of the screen, between the Red Hat Icon and Globe w/Mouse Icon.



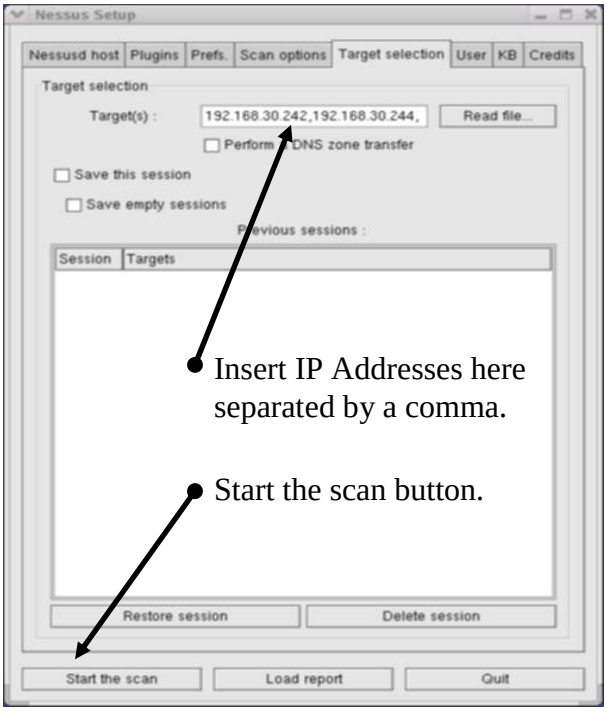
3. Once you have opened a Terminal window, a command line window will appear: **"[root@localhost root]"**. Type "**nessusd –D**" then press the enter key. After a few seconds (15-30 sec) another command line will appear beneath the command line that was just entered. At this second command line type "**nessus**".



4. From the Nessus Setup window, you will need to enter a Login: "**root**" and Password: "**tartans**" to start using Nessus. Failure to complete this step will result in Nessus not working. After Login is complete you will be able to click through the various "tabbed" options. Look at the "**Plugins**" tab. This is a very nice feature of Nessus. Nessus comes with several pre-loaded scanning filters. It is not recommended to attempt to use all the filters at once during this lab; therefore select only a few for experimentation. Next you will need to provide Nessus with the IP Addresses that are to be scanned. To do this you must click on the tab "**Target selection**".



5. Once the “Target selection” tabbed window is open, you will need to insert the IP Addresses that are to be scanned by Nessus. For the purpose of this exercise the follow IP Addresses are to be used: 192.168.30.242, 192.168.30.244, 192.168.30.249, 192.168.30.251, and 192.168.30.252. These IP Addresses need to be typed in separated with a comma.



6. After you have inserted the IP Addresses in the **“Target(s)”** window you can now click the “**Start the scan**” button. Once you click on the “**Start the scan**” button a secondary report screen will appear providing the information resulting from the scan.

7. Take the time and scan the IP Addresses using a variety of the “Plugins” pre-loaded with Nessus. Try and identify the Operation Systems and any vulnerabilities present. What could be done given the vulnerabilities present?

