Nessus Setup For Windows Users

This document describes how to install and configure the Nessus network security auditing tool on RedHat/Fedora Linux. The purpose is to provide safe step-by-step procedures to Windows system administrators and auditors as a compliment to the original instructions provided by Nessus.org.

- **Check For Dependencies (via shell console)**
  - rpm –qa | grep gtk -- result must show version 1.2 or 2.2 installed for GUI
    - ☐ gtk and/or gtk2
    - ☐ gtk-devel packages belonging to appropriate version
  - rpm –qa | grep openssl
    - ☐ openssl
  - you will also need to have installed gcc development tools and libraries to compile Nessus (beyond the scope of this document)
- **Install**
  - Download the following compressed tarballs
    - ☐ nessus-libraries-x.x.tar.gz
    - ☐ libnasl-x.x.tar.gz
    - ☐ nessus-core.x.x.tar.gz
    - ☐ nessus-plugins.x.x.tar.gz
  - Inflate compressed files
    - ☐ tar –zxvf nessus-libraries-x.x.tar.gz
    - ☐ tar –zxvf libnasl-x.x.tar.gz
    - ☐ tar –zxvf nessus-core.x.x.tar.gz
    - ☐ tar –zxvf nessus-plugins.x.x.tar.gz
  - Make the following modifications:
    - ☐ Edit profiles to reflect library PATH
      - `export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/local/lib`
        - ☐ `located in user profile folder as .bash_profile`
        - ☐ `-or- system wide profile - /etc/profile`
    - ☐ Edit /etc/ld.so.conf
      - Add usr/local/lib
      - Type ldconfig at shell console
  - Build && Install
    - ☐ nessus-libraries
      - cd nessus-libraries
      - ./configure && make && make install
    - ☐ libnasl
      - cd libnasl
      - ./configure && make && make install
    - ☐ nessus-core – NOTE: if you wish to use this machine only as a remote server and are not utilizing X-windows or the nessus client GUI locally, use the optional line for installation
      - cd nessus-core
      - ./configure && make && make install
      - Option (sans GUI) - ./configure --disable-gtk && make && make install
    - ☐ nessus-plugins
      - cd nessus-plugins
      - ./configure && make && make install
- **Configure**
  - Edit /usr/local/sbin nessus-update-plugins if you have a proxy

- ☐ Copy, uncomment and modify proxy lines under “Proxy users” section. Do not forget to add proxy port (e.g., proxy="myproxy.mydomain:8080")
- ☐ -or- (for a multi-user system) copy and add those lines in ~/.nessus-update-pluginsrc

- Make server certificate - ./nessus-mkcert
- Add users – ./nessus-adduser
  - ☐ Decide if you want users to login manually with username and password or if you would rather have them use a certificate
  - ☐ Define what users are allowed to scan in the ruleset (ACL style entry)
    - allow mydomain.com
    - allow 10.1.1.0/24
    - default deny
  - ☐ If a user certificate is used, it can be found in /tmp (e.g., /tmp/nessus-mkcert.#####), and must be copied manually to the destination machine.
- nessusd (the daemon)
  - ☐ Edit /usr/local/etc/nessus/nessusd.conf if you want to specify non-default parameters for the nessus daemon
  - ☐ A startup script can be written or obtained to start this service automatically at boot-up. As Linux rarely requires reboots, it is just easier to start this service by typing the following at the shell console once a user have been added:
    - /usr/local/sbin/nessusd –D

- **Maintenance**
  - To run updates to local vulnerability knowledgebase
    - ☐ ./usr/local/sbin/nessus-update-plugins
  - Add/remove users, change certificates – follow steps outlined in “Configure” section above
  - Uninstall nessus completely
    - ☐ ./usr/local/sbin/uninstall-nessus