

Publication Date: 4/18/2004

Installing Nessus 2.0 on SuSE 9.0 Professional with KDE 3.1

Author

Lew Newlin is CTO of [SiteRecon](#), a provider of internet [email monitoring](#) and [web site monitoring](#) services for business.

Guide

The following is a simple how-to guide for installing the Nessus vulnerability scanner, server daemon, and client on SuSE Linux. The instructions do not include in depth explanations as it is assumed that you are familiar with features and benefits of Nessus and have a general working knowledge of Linux.

As with any software installation, your results may vary depending on the machine. The installation steps were conducted using the commercial version of SuSE 9.0 Professional steps were tested on a notebook, workstation, and server to insure accuracy. The one difference that may occur during your installation is that of the network card and/or Internet connection. At SiteRecon we do not use DHCP and each installation required manual setup of NIC and IP information. If you use DHCP, the network and Internet setup will differ from the instructions below.

The installation process should be conducted using the "root" account. It is strongly suggested that your install take place on a safe non-routable network that does not have hostile traffic. Your system will be vulnerable and could easily become infected with a virus, worm, bomb, or hacked.

Install SuSE 9.0 Professional

- Insert Disk 1 and boot system
- Press F2 – select screen resolution
- Use up/down arrows to select "Installation" <enter>
- Select Language <accept>
- Select "New Installation" <ok>
 - (Screen may not appear depending on installation)
- "Installation Settings" change anything needed then <accept>
- YaST2 – Start installation" <Yes, install>
 - (Screen may not appear depending on installation)
- System Reboots....
- Insert Disk 2 as requested, select <ok>
- Click "Expert Options" button and change Encryption type to MD5 <ok>
- Enter root user password <next>
- "Network Configuration" – change as needed <next>
- "Test Internet Connection" <next>
- "User Authentication Method" <next>
- "Add a New Local User" – uncheck "Auto Login, enter data as desired <next>
- "Release Notes" <next>
- "Hardware Configuration" <next>
- "Installation Completed" <finish>
- System boots to KDE interface
- Login as root <go!>
- "Welcome to SuSE Linux 9.0" <close>
- Click "Control Center" on task bar
- Click "Desktop"
- Click "Size & Orientation"
- Select desired screen resolution, check "Apply settings on KDE startup" <apply>
- Click "Accept Configuration"
- Close "Size & Orientation" window

Network Card Setup (if needed)

- Click “Control Center” on task bar
- Click “YaST2 modules”
- Click “Network Devices”
- Click “Network card” and setup you NIC

SuSE Watcher

- Click “SuSE Watcher” on task bar (round green or red icon on right)
- Click <yes>
- Click “Start online update...”
- “Welcome to YaST Online Update” <next>
- <Accept>
- Take desired actions when prompted....
- When completed, check “Remove Source Packages after Update”, click <finish>

If you wish to automatically install patches upon release:

- Click “SuSE Watcher” on task bar
- Click “Start online update...”
- Click “Configure Fully Automatic Update....”

You now have a fully functioning and patched installation of SuSE and are ready to install the applications required for Nessus. It should be noted that by installing the programs below, you are also setting up an environment to compile GCC C programs. Additional information on GCC can be found at <http://gcc.gnu.org/>.

Nessus Application Requirements

- Click “Control Center” on task bar
- Click “YaST2 modules”
- Click “Software”
- Click “Install and Remove Software” and install the following programs:
 - Bison
 - Flex
 - Gcc
 - Gcc-c++
 - GTK2
 - GTK2-devel
 - GTK-devel
 - kdepim3-time-management package
 - libnet
 - Make
 - OpenSSL
 - OpenSSL-devel
 - Perl
 - sharutils
 - xfree86
 - xfree86-compat-libs
 - xfree86-devel
- Run YaST Online Update to patch all installed programs

Download Nessus

- Click “Local Network”
- Change location to “/” <enter>
- Right click and Create New directory titled “nessus-installer”, close window
- Using browser go to <http://www.nessus.org>
- From “The easy and less dangerous way” section download “nessus-installer.sh” file saving to the “nessus-installer” directory.

Compile Nessus

- Click “Konsole” on task bar and change directories to “nessus-installer”
- Type “sh nessus-installer.sh” <enter>
- Accept defaults by pressing <enter>
(During the compiling process you may receive warning messages for “nessus_popen”, “insert_nasl_func”, and “extra tokens”. These are warning messages and the compiling process should complete successfully.)
- When compiling process is complete you will be prompted to press <enter> to quit.

Nessus Server Setup

- Type “nessus-mkcert” to make a server certificate
 - Accept default for “CA certificate life” <enter>
 - Accept default for “Server certificate life” <enter>
 - Enter your 2 letter country code <enter>
 - Enter your state or province code <enter>
 - Enter your location <enter>
 - Enter your organization name <enter>
 - Certificate process completed message <enter to exit>
- Type “nessus-adduser” to create a user account
 - Enter login name <enter>
 - Accept default for authentication <enter>
 - Enter password <enter>
 - Press ctrl-D to end user creation process
 - “Is that ok?” message <enter>
- Type “nessusd -D” to start the Nessus server service
(It may take several seconds for Nessus to finish initializing. The command prompt will return once the Nessus daemon is started. If you wish to have the Nessus Server daemon automatically started when the system is booted, edit the “etc/init.d/boot.local” file and append “nessusd -D”).)

Nessus Setup

- Type “nessus”
- Enter login
- Enter password
- Click “Log in” button
- “SSL Setup” window will appear, click <ok> button
- “Nessus” windows asking to accept this certificate, click <yes> button
- “Warning” message about plugins crashing remote systems will appear, click <ok> button
- Close “Konsole” window

KAlarm

- Click “Start Applications” on task bar and select “Utilities”, “Time”, then “KAlarm”
- In the KAlarm window click “Actions”, then New
- Check “Command” and enter “nessus-update-plugins” as the command line
- Check “Any time” check box
- Check “Recur” for Repetition, then select the “Recurrence” Tab
- Enter “01:00” for “Recurr every” field
- Select <Try> button, then <ok>
- Close “Kalarm” window (Kalarm by default is automatically started upon boot.)

Firewall

KDE provides built-in firewall protection. Vulnerability scanners such as Nessus do not normally function well with software firewalls in place. To remove the firewall:

- Click “Control Center” on task bar
- Click “YaST2 modules”
- Click “Security and Users”
- Click “Firewall”

- Check “Stop Firewall and Remove from Boot Process” <next>
- “Firewall configuration – deactivate firewall”, click <next>
- “The firewall is now turned off” <ok>

General Information

Uninstall executable: “/usr/local/sbin/uninstall-nessus”

Configuration file: “/usr/local/etc/nessus/nessusd.conf”

Certificate Authority: “/usr/local/com/nessus/CA/cacert.pem”

Certificate Authority – Private: “/usr/local/var/nessus/CA/cakey.pem”

Nessus Server Certificate file: “/usr/local/com/nessus/CA/servercert.pem”

Nessus Server – Private Key file: “/usr/local/var/nessus/CA/serverkey.pem”

Nessus uses port 1241 to communicate

You now have a fully functioning Nessus server daemon and client installed on SuSE using the KDE desktop environment. Kalarm is setup to automatically update Nessus plugins once per hour to insure you have the latest vulnerability tests. Nessus is now fully operational to help with your security needs.

Copyright 2004, Information Solutions, Inc., All rights reserved.