Installing Nessus 2.0 on SuSE 9.0 Pro with KDE 3.1

By Lew Newlin

Installing Nessus 2.0 on SuSE 9.0 Pro with KDE 3.1 by Lew Newlin

Installing Nessus 2.0 on SuSE 9.0 Pro with KDE 3.1

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"
Select Language
Select "New Installation"
(Screen may not appear depending on installation)
"Installation Settings" change anything needed then
YaST2 "Start installation"
(Screen may not appear depending on installation)
System Reboots...

Insert Disk 2 as requested, select
Click "Expert Options" button and change Encryption type to MD5
Enter root user password
"Network Configuration" − change as needed
"Test Internet Connection"
"User Authentication Method"

"Add a New Local User" − uncheck "Auto Login, enter data as desired
"Release Notes"
"Hardware Configuration"
"Installation Completed"
System boots to KDE interface
Login as root
"Welcome to SuSE Linux 9.0"
Click "Control Center" on task bar
Click "Desktop"
Click "Size & Orientation"
Select desired screen resolution, check "Apply settings on KDE startup"
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
Click "Start online update"
"Welcome to YaST Online Update"

Take desired actions when prompted.
When completed, check "Remove Source Packages after Update", click

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

.

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 "/"
Right click and Create New directory titled "nessus−installer", close window
Using browser go to

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"
Accept defaults by pressing
(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 to quit.

Nessus Server Setup

Type "nessus−mkcert" to make a server certificate

Accept default for "CA certificate life"
Accept default for "Server certificate life"
Enter your 2 letter country code
Enter your state or province code
Enter your location
Enter your organization name
Certificate process completed message

Type "nessus−adduser" to create a user account

Enter login name
Accept default for authentication
Enter password
Press ctrl−D to end user creation process
"Is that ok?" message

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
"Nessus" windows asking to accept this certificate, click
"Warning" message about plugins crashing remote systems will appear, click
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 button, then
Close "Kalarm" window (Kalarm by default is automatically stated 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"
"Firewall configuration − deactivate firewall", click
"The firewall is now turned off"

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.

is CTO of Information Solutions, Inc. that operates SiteRecon.com.

specializes

in security, email monitoring, and web site monitoring for Internet service providers and businesses.

Know Linux

By Pawan Bangar

Linux

Linux essentials:

Its free for download but you have to pay a tiny bit to mail order it or buy it from a company. If youre getting Linux for more than 2−3 PCs, you can also get training and support at a small free, if you choose to have it. Else its the Linux community on the Net to your rescue.

If you want to get comfortable with Linux, you dont have to let go of windows. Get Linux installed on a seprate partition and you can switch between Windows and Linux. There are some Linux versions that run off CDs too−xandross and Knoppix.

You dont have to be a geek to work with Linux. There are Desktop environments that let you work in Linux as you work in Linux as you would in Windows.

Linux hand in decreasing PC prices.

The PCs bundle the operating system. Linux being an open source operating system, means that the code that runs is open for everyone to see, work with, modify and develop their own innovative apps for it. The deal with this experimentation is that you have to share the knowledge you gained and the software you created with the public domain. So the operating system comes to you for free, or if there are some copyrighted application on it, you play up a bit. But this is nothing compared to the fortune people spend on OSs like windows. And a company bundles Linux and applications based on it with a computer, quite a bit of the software cost comes down.

Linux came into being about 11 years ago− it was developed by Linux Tornados of Finland along with a group of programmers from the open source software movement. Linux was mostly something only the geeks worked with. And yes, it was mostly about commands and programming. But over the years with so many Linux enthusiasts (about 50 million of them) working on it and sharing knowledge about it, quite a few versions have come up which are as easy to use as windows. And developers are still free to work with code and enhance it.

Linux is growing steadily year after year. With a passionate community backing it, with big companies Like IBM and HP pledging their support for it, its no wonder Linux− the wonder operating system for servers of the past, has also made it to the desktops of today. Not in a sweeping way yet, but in ways that will help you the user. PC prices are already on their way down. And you get more choice with operating systems and applications. From being an OS only computer professionals had heard about, Linux, in a short time, has made a transition into the lucrative and high profile home PC segment. Most of the decision to switchover sounds very economical. From a measly base of a few thousand users, Linux now boasts of close to 50 million users, cracking the monolith of Microsofts monopoly. Companies like IBM, HP and Dell have also taken to Linux in a big way. Microsoft doesnt agree with

the free concept at all−the software is free but the support isn't Windows code to outsiders so they could build on to it. Very recently though, the company has allowed part of the code to be opened up to some US government are vying with each other to get tech−savvy and help the citizens through e−governance, the opening up of the OS code is important, countries like India need a variety of regional language fonts and content to be created which cant done without Microsofts help, if the choice is Windows. Since this isnt happening much, they have gone ahead with adopting Linux.

Linux is based on the commercial OS, UNIX. All the OSs tries to pack in command line management of systems. System administrators of companies use command lines all the times as their lifeline, but its not really meant for regulars users. But UNIX and Linux are not all about just command line stuff. UNIX has had a graphical user interface for 30 years. In its 11 years Linux has always had always had a GUI too−in fact a choice of GUIs.

Linux Versions:

If there are so many people working on it. Theres likely to be many Linux versions too. Many companies working on Linux have come up with what are called Linux distributions. There are Linux versions that are compiled and packaged and released with various additional software.

The popular distributions or destroys include Red Hat Linux Mandrake Linux, Corel Linux SUSE Linux and Debian . its just like having different flavors of ice cream. True to the spirit of open source, if you download the distro from the companys Website, it is free for use. But the distros are usally quite huge. If you are getting the distorts from the company, be ready to pay up a tiny bit. Companies compile the packages, make installation hassle free, bundle applications, add a manual, and extend any support you need. So they charge a fee for all this.

One note here though: the free in Linux stands for freedom of choice, to redistribute, to install a feature, freedom to modify the source code. Thats the spirit of Linux being free.

Linux better than other OS

Linux users wont even bat an eyelid before they say an emphasis comes from a deep dislike of Microsofts practice of changing the earth for software. But a lot of it comes from the fact they are ready to swear upon−that Linux is more stable. There are no blue screens and no viruses to speak of. Linux has a better security support for multi−users, lets you set up a stable server, internet gateways etc, and still lets it−self to be used as a desktop workstation. Add to that it being free, and they argue that you dont lose anything by giving it a try. You get free support on the Net quickly on any query you may have. And you dont even have to wipe out your Windows. Just get Linux on a different hard disk partition and free to switch between the OSs as you please .

Myths about Linux

Installation:

Linux is hard to install, isnt it? Not really. Most people havent ever installed Windows on their computers either−since it comes preloaded. Linux is as easy−some say easier−to install compared to

Windows. You can install it through a graphical user interface like Windows. But what really stumps most people in installing Linux on a second partition on their hard disk, when they want to be able to use both operating systems.

A partition is a way of organizing space on your hard disk by creating virtual sections that are separate from each other. Most computers that are running Windows or MS DOS have one large chunk of space holding the OS. This space is the C drive. If you have a large hard disk, its likely that it has been divided up into smaller bits called partitions to help you organize your data better. These partitions are usually called D:\, E:\ etc. you could have Linux on any of these.

Windows 98 creates a file system called FAT32 on the entire hard disk, DOS and Win95 use FAT16. Linux has many file systems−on the most popular is ext3. But you could have Linux installed on Fat32 partitions also.

Linux is geeky and based on text command

Linux has come a long way from being the system of geeks. It has an extremely advanced X Windows systems that has a complete graphical user interface−you know, like Windows. It also has a large number of window manager that let you work with different levels of customization of your desktop.

Linux has a robust character−cell interface where commands need to be typed in. x Windows is a free program that runs with Linux to provide a GUI where the mouse and keyboard can be used extensively. But the X system itself is quite primitive and needs a window manager, or a desktop environment− like GNOME or KDE− to be really usable. Window managers are programs that let you interact with the underlying X system and LinuxOS by relaying commands. The popular window managers are Sawfish, Enlightenment, Black box, after step and Window maker.

As for desktop managers, they have their own window manager and other tools that make you feel that you are working in Window! GNOME and KDE are the most popular of these. GNOME stands for GNU Network Model Environment and KDE for K desktop Environment. They have tools that allow drag and drop, have panels and taskbar− almost like clones of windows.

Hardware compatibility problem and few applications that run on Linux

Well, most new distributions will detect and configure your hardware in a jiffy, unless you have some really old or exotic piece of hardware. Only Win modems (internal modems driven by Window drivers) face problems.

As for software, theres plenty. And most of it comes free−free for you to use, modify and configure according to your needs. Other packages are commercial and you have to buy the software−but this is mostly for the software and training you need, and not for the support and training you need, and not for the software itself. Sometimes, if you have the Windows version (as a doom) you can download a small program that will allow you to play the game in Linux. Here whats available?

Office suites: Star Office, Open Office, Applixware, Corel WordPerfect

Graphics: GIMP, Corel Photo paint

Music: XMMS, Free amp, Real Player

Video: MTV, Xine

Games: FreeCiv, Tux racer, Doom, Quake, Heretic, Unreal

And the list is growing.

Linux varieties:

Debian : One of the oldest and still most popular distros is Debian. This Project is a voluntary effort of a team of programmers who developed the GNU system. Debian is not very easy to install, and that has been its problem, Debian also has its own software comes with a. DEB extension. Updating and installing new software is very easy. The applications bundled with Debian are great for even a power user.

RedHat: Probably the most popular and in many ways the leading distro. Its currently in version 8. The installation and configuration is easy. A blue curve file manager and the default GNOME desktop make it look simply stunning. It comes with a host of tools that allow usage as a server and as a workstation. The Red Hat Package Manger(RPM) format developed by Red Hat has almost become the defector for software distribution in Linux world. Installing new software is a breeze. It also has an advanced and easy font management system that makes fonts in X Windows look cool. But being the leader comes at a price. Red Hat charges a little more than others for its istro.

Mandrake: Mandrake Linux is now in its 9 version. This distro can be installed on a native Windows Partition using the Lin4Win tool, but this may slow the machine down. It also lets you do a traditional Linux install into its own dedicated partition. Mandrakes configuration and software installation is painless. It follows a slightly modified RPM architecture called mdk.rpm but most Red Hat software can also be used for Mandrake. The outstanding feature in this distro is the collection of window managers−eye−candy freaks will have a great time.

SUSE : From Germany comes the Chameleon Distro, SUSE. Now in its 8.1 avatar, it has one of the most extensive software packages compiled, and getting them installed is easy with yast (Yet another Software Tool) which gives a centralized interface from where you can pick and choose the software to be installed. Among other things, SUSE comes with some stunning 3D games that showcase Linuxs gamming prowess.

Corel/Xandross : Corel entered the Linux distro market with Corel Linux a few years ago. Now it has merged into Xandross OS, which is based on Corel Linux. This is a Debian−type distro, and can be installed without much fuss after resizing the Windows partition. Xandross contains Crossover office, which is a refined retail version of WINE that lets you install and run many Microsoft apps.

Windows applications in Linux

Some applications have been ported over to Linux, other run with a program called WINE (Wine is Not an Emulator). Crossover, commercially available software also lets you use your Windows programs Linux. VMWare is another program that lets you run Windows under Linux.

Bottom Line:

The cool thing about Linux is that most software is free, and you can legitimately use them without worrying about piracy. If youre worried that Linux wont look as pretty as windows can, all you have to do is check out some of the cool Linux interfaces and Window managers. But you dont find a lot of multimedia titles for Linux. And if youre into a lot of these, Windows in the way to go. So if you have a PC that runs both, you can easily switch between the two, and get the best of both worlds.

Pawan Bangar, technical Director, Birbals, India.