;login:

THE MAGAZINE OF USENIX & SAGE

December 2000 • volume 25 • number 8

inside:

SECURITY:

USING TRINUX FOR SECURITY TESTING

USENIX & SAGE

The Advanced Computing Systems Association &
The System Administrators Guild

using trinux for security testing

by Dario Forte

Dario Forte is a security analyst for several Italian governmental offices and teaches information warfare/management and computer forensics at the university and post-university level.

<dario.forte@inwind.it>

Trinux is a light distribution of Linux, which shares a broader realm with other MiniUNIX such as tomsrtbt, LEM, and PicoBSD.

Trinux is booted from a single floppy, loads the rest of its modules from a FAT/Ext2 partition from other floppy disks or from an HTTP/FTP server, and runs completely in RAM. One of its most important features is that it includes a series of precompiled versions of security tools such as nmap, tcpdump, iptraf, and ntop. Furthermore, this distribution works by default with DHCP.

Trinux demands only modest hardware. The operating system will run on a recycled 486 with 32MB of RAM. This is sure to delight hoarders of old equipment. The kernel supports most network cards and is continually being updated.

Obtain GNU-licensed Trinux from *<http://www.trinux.org>*, which shows all the available FTP resources organized by geographic location.

Installation and Configuration

Since Trinux is a floppy-based distribution, the first thing to do is download the raw disk images from the FTP site and copy them onto the boot disk. This will take care of loading the kernel, mounting the first ramdisk, creating the additional ramdisks, configuring the network, and loading the rest of the packages.

The images can be inflated either with gunzip (UNIX) or Winzip. Below are some of the basic steps we used in our test, as recommended by the designers themselves:

1. Check the size of the images. You will need 1.4MB or 1,474,560-byte floppy disks, which will be completely occupied by the Trinux images. Since the files occupy all the space that is normally available on a floppy (a special program is used to transfer the images), it is a good idea to use clean floppies.
2. Linux users need to use the following command: dd if=image-name of=/dev/fd0. Naturally, you have to know which device to use. It should also be mentioned that the entire product was designed to be initially configurable and managed under Windows. Windows users will need a copy of rawrite, which can be obtained from *<ftp://ftp.trinux.org/pub/trinux/rawrite.exe>*. Install the utility in the same directory as the images to prevent wasting time on pathways.

Network Configuration

Since Trinux is a network-centric operating system, it has to be used on the network to justify its existence, so you will have to configure the network card.

The boot floppy contains a script named /init/netcfg and is configured to use DHCP. As things currently stand, the project documentation indicates general compatibility with both UNIX and NT DHCPs. If you do not want to use the file, it can be moved into the directory /conf/disabled on the boot floppy or deleted. I would personally suggest the first option; the dhcp file may be missing for some reason. In this case, netcfg looks for two files in order to obtain information recently saved on the network: /conf/eth0 and /conf/network. These are scripts that act on variables such as the IP address, subnet mask, default gateway, and so on. You should review the attached project documentation very carefully if you want to personalize the information contained in the files.

In general, remember that the Trinux boot floppies are MS-DOS and thus can also be configured by Windows. WordPad may be useful if you need to do some editing.

Useful notes:

- Unless modifications are made to the file /conf/pkgconf, Trinux loads the packages from one or more floppies. To operate otherwise, specify how to proceed. For example, if you want to interact with an HTTP/FTP server, create an empty file called netload in the directory /conf and insert the complete URL of the server from which you will be downloading.
- Likewise, loading the packages from a hard disk (more advisable) requires you to work with the pkgsrc file to indicate on which device Trinux can find the packages. In the case of a DOS/FAT partition, for example, you generally specify /dev/hda1. You must also determine the filesystem and the pathway to the files.

Tools Included in Trinux

Once installed and configured, Trinux is ready to use. One of the advantages for those who use Trinux, apart from being able to reuse the old computer, is the precompiled security tools.

Trinux elements are divided into categories. One part comprises packet sniffers, in particular, tcpdump, ipgrab, and ngrep. Each one has special features to let you get the most out of them. The network monitors in this case are iptraf and ntop, the latter certainly one of the most interesting currently in circulation. Netmapping and vulnerability-scanning tools such as nmap, exscan, saint, queso, hping, firewalk, and cgichk are also included. These are today's standard tools for the kit of any self-respecting security analyst.

Trinux also has firewalls and proxies, including the noted ipchains, redir, and tinyproxy.

Lastly, two tools are included from a chapter in the Tiger Team bible: netcat and hunt. These test eventual vulnerabilities to connection hijacking.

Special attention should be paid to the use of X Windows under Trinux. Given the types of tools included, something like this should not be necessary, partly because the tools (except for ntop, which, in spite of several recent security bugs, is very well respected by the technical community) do not use graphical interfaces in the true sense of the term. Practically speaking, it makes sense to use X only when you intend to deal with a plurality of X term windows contemporaneously. Moreover, at present, a mouse cannot be used; a workaround was adopted for using the keyboard in its place. You will also have to be content with only 16 colors.

The ntop program can be managed remotely from an HTTP console. However, as things currently stand, we do not know of any cryptosystem protection of the connection between ntop and its console.

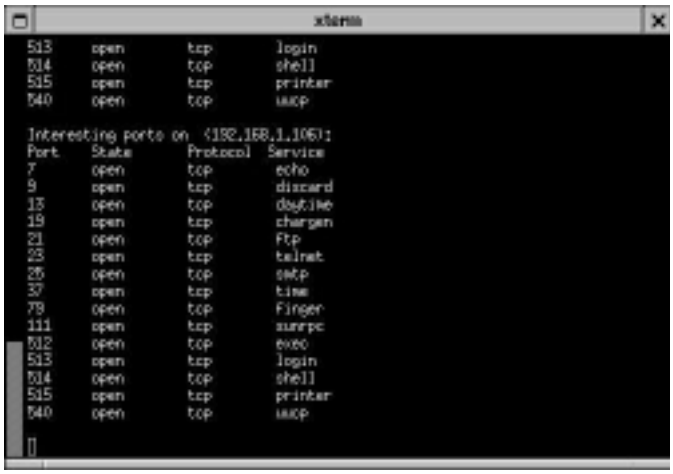
Conclusions

I had my first exposure to Trinux a year ago along with two friends (currently Italian managers of two important American security companies). We had our little laugh about the future prospects of the project. Now, in spite of the fact that my two friends and colleagues see me as laboring under an illusion, Trinux has made it into the top ten free security tools worldwide. I have decided to launch an FTP mirror of trinux.org on my Web site. Matthew Franz, the mind behind the project, will be delighted to receive your comments and requests to participate in the initiative.

[See images on next page.]

Trinux has made it into the top-ten free security tools worldwide.

nmap is Trinux's cutting edge. It is surely the most reliable portscanner, with numerous added features such as OS detection. It is also available under Windows NT, but does not enjoy the same stability.



exscan is an alternative portscanner to nmap that also captures login banners.

ntop can also be run via HTTP. If you use it off the Trinux machine there is no graphical interface.