

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.

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

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.]

```
Port 109 Open; Post Office Protocol 2 Service Running,
Data Returned:
+ POP2 localhost v4,46 server ready

Port 110 Open; Post Office Protocol 3 Service Running,
Data Returned:
+ OK POP3 localhost v6,50 server ready

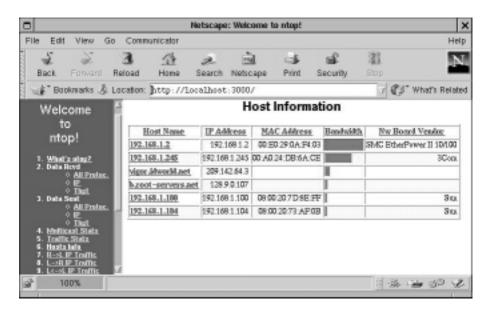
Port 111 Open; SumPPC Service Running,
Port 113 Open; Buttentication Service Running,
Port 129 Open; Buttentication Service Running,
Port 130 Open; Buttenti Secution Service Running,
Port 145 Open; Interia Hail Access Protocol 2 Service Running,
Data Returned;
• OK localhost IMMPérevi vii.261 server ready

Port 513 Open; login Service Running,
Port 514 Open; ond Service Running,
Port 515 Open; NFS Mount Service Running,
Scan Completed Successfully,
Croot@localhost /tapl* []
```

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.

| 513 open top login 514 open top shell 515 open top printer 540 open top sacp Interesting porto on (182,158,1,106): Port State Protocol Service 7 open top echo 9 open top discard 13 open top discard 13 open top discard 19 open top top sacp 21 open top there 22 open top tell 23 open top tell 24 open top ftp 25 open top sacp 37 open top sacp 37 open top size 38 open top sacp 39 open top sacp 311 open top size 512 open top size 513 open top size 514 open top open 515 open top open 516 open top open 517 open top size 518 open top open 519 open top open 510 open top open 510 open top open 511 open top open 512 open top open 513 open top open 514 open top open 515 open top open 516 open top open 517 open top open 518 open top open 519 open top open 510 open top open 510 open top open 511 open top open 512 open top open 513 open top open 514 open top open 515 open top open 515 open top open 516 open top open 517 open 518 open top open 519 open 510 open 510 open 511 open 511 open 512 open 513 open 514 open 515 open 516 open 517 open 518 open 519 open 510 open 510 open 511 open 511 open 512 open 513 open 514 open 515 open 516 open 517 open 518 open 519 open 510 open 510 open 510 open 511 open 511 open 512 open 513 open 514 open 515 open 515 open 516 open 517 open 517 open 518 op | | | | xterm | × |
|--|--------|------------|--------------|-----------|---|
| 515 spen top printer 540 open top satep Interesting ports on (192,158,1,106); Port State Protocol Service 7 open top echo 9 open top discard 13 open top discard 12 open top stargen 21 open top frp 23 open top satep 25 open top satep 37 open top satep 38 open top satep 59 open top satep 510 open top site 511 open top finger 511 open top surryce 512 open top surryce 513 open top satep 514 open top open 515 open top open 516 open top open 517 open top surryce 518 open top surryce 519 open top open 519 open top open 510 open top open 510 open top open 511 open top open 512 open top open 513 open top open 514 open top open 515 open top open 515 open top open 516 open top open 517 open top open 518 open top open 519 open | 513 | open | tep | login | |
| 515 spen top printer 540 open top satep Interesting ports on (192,158,1,106): Port State Protocol Service 7 open top echo 9 open top discard 13 open top discard 12 open top discard 12 open top ships 21 open top there 22 open top site 25 open top site 37 open top site 37 open top site 38 open top site 191 open top site 510 open top site 511 open top finger 111 open top surryc 112 open top surryc 113 open top site 114 open top site 115 open top open 116 open top open 117 open top site 118 open top site 119 open top site 119 open top site 119 open top site 110 open top open 111 open top site 112 open top open 113 open top site 114 open top open 115 open top open 115 open top open 116 open top open 117 open top open 118 open top open 119 open | 51.4 | open | top | shell | |
| Interesting ports on (182.168.1.106): Port State Protocol Service 7 open top cho 13 open top discard 13 open top discard 19 open top deptime 19 open top there of the protocol 21 open top the protocol 25 open top talrat 25 open top setp 37 open top sitp 178 open top sitp 179 open top sitp 171 open top finger 171 open top surryc 172 open top surryc 173 open top sitp 174 open top sitp 175 open top sitp 177 open top sitp 178 open top sitp 179 open top sitp 170 open top sitp 170 open top sitp 170 open top sitp 171 open top sitp 172 open top sitp 173 open top sitp 175 o | 515 | | | printer | |
| Port. State Protocol Service 9 open top echo 13 open top discard 13 open top destile 19 open top chargen 21 open top chargen 25 open top selp 37 open top sine 79 open top finger 111 open top evec 512 open top evec 513 open top login 514 open top shell 515 open top printer | 540 | open | top | шер | |
| Port State Protocol Service 9 open top echo 13 open top daytile 19 open top daytile 21 open top ftp 23 open top ftp 25 open top outp 37 open top sine 79 open top finger 111 open top evec 512 open top evec 513 open top evec 514 open top open 515 open top printer | Intere | etina port | o on <152,16 | 8,1,106); | |
| 13 | Port. | State | Protocol | Service | |
| 13 open top daytime 19 open top chargen 21 open top ftp 23 open top satp 25 open top satp 37 open top time 79 open top fingen 111 open top sampe 512 open top eveo 513 open top eveo 513 open top ingen 514 open top open 515 open | | open | top | echo | |
| 13 | 9 | | | discard | |
| 19 span top chargen 21 span top ftp 23 span top sate 25 span top sate 37 span top sate 79 span top finger 111 span top sampe 512 span top sampe 513 span top sampe 514 span top span 515 span top span top span 515 span top span to | 13 | | | daytine | |
| 25 open top setp 37 open top time 79 open top time 111 open top sumpe 512 open top exec 513 open top exec 514 open top similar 514 open top shell 515 open top printer | 19 | open | | | |
| 25 open top setp 37 open top time 78 open top finger 111 open top sumrpc 512 open top evec 513 open top evec 514 open top shell 515 open top shell 515 open top printer | 21. | open | top | Ftp | |
| 25 open top setp 37 open top time 78 open top finger 111 open top sumrpc 512 open top evec 513 open top evec 514 open top shell 515 open top shell 515 open top printer | 23 | open | | telret | |
| 79 | 25 | | | setp | |
| 79 | 37 | | | | |
| 111 open top sumpo 512 open top eveo 513 open top login 514 open top shell 515 open top printer | 79 | open | top | Finger | |
| 512 open top exec 513 open top login 514 open top shell 515 open top printer | 111 | | | | |
| 513 span tep login 514 open top shell 515 span tep printer | 512 | open | | | |
| 515 open top printer | 513 | | | login | |
| 515 open top printer | 51.4 | open | top | shell | |
| | 515 | | | printer | |
| | 540 | | | | |
| | П | | | | |

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.

