Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Trinux - A Digital Tool Belt

As evidenced by the release of Linux, nmap, and nessus under the terms of the GNU General Public License, the popularity and pervasiveness of open source code has placed professional grade operating systems and security utilities within browser's grasp of any Internet connected user. Trinux continues in the same tradition. Accordingly, an aspiring security professional, hoping to understand the foe's mindset and capabilities, will do well to use the same resources that the common system cracker has access to. The purpo...

Copyright SANS Institute

Author Retains Full Rights

AD

Trinux – A Digital Tool Belt

Brad Showalter
GSEC Certification
Version 1.2f

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Trinux – A Digital Tool Belt

Pluralitas non est ponenda sine necessitate
Entities should not be multiplied unnecessarily
- William of Ockham

Tools of a trade are simple, concise, and focused, assembled by the artisan over time and based on experience. The collection of tools and experience, however, begins at the apprentice stage. Thusly, it is an astute pupil that begins the journey by first strapping on a tool belt – Trinux in this case.

Trinux is a minimized Linux distribution, which boots from either a single floppy disk or CD-ROM, and resides completely within system RAM. It's purpose is succinctly stated on its home web page – "Trinux gives you the power of Linux security tools without requiring a full-blown Linux install or the need to download, compile, install, and update a complete suite of security tools that are typically not found in mainstream distributions." (Franz).

As evidenced by the release of Linux, nmap, and nessus under the terms of the GNU General Public License, the popularity and pervasiveness of open source code has placed professional grade operating systems and security utilities within browser's grasp of any Internet connected user. Trinux continues in the same tradition. Accordingly, an aspiring security professional, hoping to understand the foe's mindset and capabilities, will do well to use the same resources that the common system cracker has access to. The purpose of this paper is to outline the installation of Trinux via floppy diskettes, along with several security packages, and detail two scenarios of its usage by the paper's author.

Which Tool Belt?

The first Trinux installation step is downloading an image from http://trinux.org/boot. One will find four different images available, each intended for a specific environment:

- Network – standard floppy disk image, supports common Ethernet NICs, supports FAT and minix file systems, does not support IDE devices (i.e., CD-ROM)
- IDE – standard floppy disk image with the addition of IDE and NTFS (read only) file system support
- PCMCIA – standard laptop, floppy disk image with support for several PCMCIA NICs
- ISO – standard CD-ROM bootable image

Once the proper image has been determined, it must be downloaded to the hard drive. One cannot download the image directly to a floppy disk, a second utility is required for this step. If the operating system on which the downloaded image resides is a Windows system, one must use rawrite, available at http://www.tux.org/pub/dos/rawrite/, or rawrite for Windows, available at http://uranus.it.swin.edu.au/~jn/linux/rawwrite.htm, to copy the downloaded image to floppy disk. If the operating system is a UNIX flavor, one can use the following command, noted in a

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Linux Journal article on Trinux, to do a low level image copy to disk – "dd if=downloaded_image of=/dev/fd0" (Gagne).

Which Tools?

Prior to selecting the security packages one intends to load, knowledge of how Trinux handles the loading process is required. The order of loading and details behind each are as follows:

- Fixed Disk Package Loading – available under the IDE and ISO images, desired packages are downloaded to a *trinux* directory at the root level prior to booting of Trinux; during booting, Trinux scans for the *trinux* directory and installs all present packages.
- Network Package Loading – available under the Network and PCMCIA images; Trinux boots, obtains an IP address through DHCP or initial manual configuration, and downloads and installs packages from a centralized HTTP/FTP server. The latest release (0.80rc2) attempts to connect to three IP addresses, each being listed in the configuration file – /tux/config/server. Packages desired by the user for downloaded should be listed in the configuration file – /tux/config/pkglist.
- Floppy Disk Package Loading – desired packages are downloaded directly to floppies by the user prior to booting of Trinux; during booting, if a network connection is unavailable and a *trinux* directory has not been found, Trinux prompts for floppies containing accessory packages.

Now, on to the package selection, itself. The packaged utilities are far ranging, falling under the following general categories – network analyzers; intrusion detection tools; packet generators; proxy and tunneling tools; encryption tools; miscellaneous security tools; web tools; network tools; scripting languages; text editors; disk and file system tools; debug tools; and system monitoring tools. Helpful descriptions of many of the packages and the depth to which they have been tested in Trinux can be found at http://trinux.sourceforge.net/tools.html. Also found on the just mentioned web site is a collection of mandatory files that will need to be loaded prior to running any of the security packages; this collection consists of:

- system.tgz – network daemon utilities for SMTP and CDP (usually on the boot floppy)
- baselib.tgz – essential libraries needed for most trinux apps, includes ldconfig and the full-blown kernel module utilities
- dnslibs.tgz – libresolv, libnsl, libnss libraries (needed for DNS)
- bash.tgz – shell utility which replaces the limited ash shell
- term.tgz – ncurses and terminal routines
- pthread.tgz – GNU thread libraries, needed for many tools

Once decisions have been made on which packages to download, navigate to the web site http://www.ibiblio.org/pub/Linux/distributions/trinux/latest/pkg/ or to the web site http://trinux.sourceforge.net/pkg/ and begin downloading the files to either the hard drive or the floppy disk. Regarding the floppy disk, neither rawwrite nor dd is necessary, simply save the files directly to the disk.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

First Day on the Job

If successful to this point, it's time to boot up. Insert the floppy disk with the proper image into the disk drive and boot the system. From this point on, Trinux takes over probing hardware and initializing the OS. The only prompting of the user for input will occur when/if the operating system determines that fixed disk and network package loading options are not being utilized; the system will ask for floppies containing extra packages. If the user has more packages, remove the boot disk from the drive, insert the package disk into the drive, and respond to the screen prompt with a 'y <return>'. The OS will load all of the packages on disk and continue to prompt for disks until the user enters a 'n <return>' on the screen. At this point, Trinux will complete loading and then prompt the user to hit <enter> to activate the console. Upon so doing, the user is granted a command line prompt '#' as user 'root', no form of log in is required.

Learning the Ropes

Please note, only during the boot phase is it possible to pop disks in and out of the drive in a Windows like manner. Within Trinux (and all UNIX flavors) it is necessary to mount and umount floppy disks to access the data contained therein. To mount and umount MS-DOS formatted floppy disks, the **fmount** and **fumount** utilities have been provided within Trinux. As an example of reading a text file on an MS-DOS formatted floppy disk:

Insert the floppy into the disk drive
fmount
cd /floppy (change directory to the just mounted floppy)
more some_file.txt (read the text file)
cd / (it is required to change directory from /floppy prior to running the fumount command)
fumount
Remove the floppy from the disk drive

An example of mounting a floppy disk which has been formatted with the Linux based (ext2) file system (Fox):

Insert the floppy into the disk drive
mount –t ext2 /dev/fd0 /floppy
cd /floppy
more some_file.txt
cd /
umount /floppy
Remove the floppy from the disk drive

To shut down the Trinux OS, simply type '**halt <return>**'. Be forewarned, any work that one creates within Trinux must be saved to an external media prior to halting the system. Due to the fact that Trinux is a wholly RAM based OS, all work will be lost otherwise. The utilities **savehome** and **gethome** are provided for the user to facilitate saving work to external systems via ssh or ftp. Alternatively, one can copy (**cp**) or move (**mv**) work to a floppy disk prior to system shut down. Finally, the command **man** followed by the name of a loaded package will

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

display the help page for that particular package, detailing options and proper syntax to run the utility.

Tool Safety

Trinux is safe. Trinux in not safe. The outcome is based upon the nature of the person using it. Granted physical access to a Windows 2000 workstation, the IDE image of Trinux (NTFS file system support already included) has the utilities at hand for a user to extract the SAM database. (The SAM database contains user accounts and associated passwords.) The rather simple steps to do so:

- boot Trinux
- remove the boot disk and insert a second disk
- **fmount**
- **cp /hda1/winnt/system32/config/sam /floppy**
- **fumount**
- feed the results from the floppy into the latest version of L0phtCrack – LC3 (available at http://www.atstake.com/research/lc3)

Whether the above steps are taken by a system administrator to recover the lost Administrator account's password or by a system cracker who has found an unsecured workstation and has nefarious intentions, the results are the same regardless of the mindset.

Earning One's Keep

Though Trinux's base utilities are useful, they are limited. The true beauty of Trinux lies in the packages. One of the available packages is ettercap. Described by the tool's authors as "a multipurpose sniffer/interceptor/logger for switched LANs. It supports active and passive dissection of many protocols (even ciphered ones) and includes many feature for network and host analysis. a packet sniffer." (Ornaghi and Valleri) This author installed ettercap during the boot up phase of Trinux from floppy disk. After verifying that the file existed in the /usr/bin directory, he typed "man ettercap" at the command prompt to gain insight on how to run ettercap. After a few minutes of perusing the details, he typed "/usr/bin/ettercap –a" to attempt ARP based sniffing; the utility correctly identified the four IP addresses in the network it was attached to, however, it appeared to hang when it attempted to resolve each IP address. The author returned to the man page for ettercap for guidance, noting the "-d" option which prevents resolving of IP addresses during start up. The option worked and the author was rewarded with a multi-colored screen similar to the following:

Ettercap 0.5.4

4 hosts in this LAN (192.168.123.151 : 255.255.255.0

1) 192.168.123.151	1) 192.168.123.151
2) 192.168.123.113	2) 192.168.123.113
3) 192.168.123.167	3) 192.168.123.167
4) 192.168.123.254	4) 192.168.123.254

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Before sniffing select AT LEAST source OR destination!!

Your IP: 192.168.123.151 MAC: 00:BF:BF:BF:BF:BF Iface: eth0 Link: SWITCH
Host: Unknown host (192.168.123.151) : 00:BF:BF:BF:BF:BF

By hitting the ESC button, the "Before sniffing…" statement was removed. Using the arrow keys then permitted the author to highlight an IP address for the source, pressing the enter button designated it accordingly. A destination IP address was chosen in the same fashion. The designated IP addresses were written to the screen, just below the "ettercap 0.5.4" banner.

Next, the author pressed the F1 key and was greeted with an options window. The ARP poisoning option looked interesting, so he hit ESC and then punched the "A" button on the keyboard to begin the packet capture. (ARP poisoning is a sniffing method in which computer A poisons the switch's ARP cache and acts as a man-in-the-middle, passing back and forth communications between two IP addresses with neither being aware that an imposter is in their midst.) The Packets and details began to appear on the screen accordingly:

Ettercap 0.5.4

SOURCE: 192.168.123.113 <-- Filter: OFF
--doppleganger – illithid (ARP Based) – ettercap
DEST : 192.168.123.167 <-- Active Dissector: ON

4 hosts in this LAN (192.168.123.151 : 255.255.255.0
1) 192.168.123.113:1561 <--> 192.168.123.167:137 | UDP | netbios-ns
2) 169.254.185.219:137 <--> 192.168.123.167:137 | UDP | netbios-ns
3) 192.168.123.113:137 <--> 192.168.123.167:137 | UDP | netbios-ns
4) 192.168.123.167:33145 <--> 192.168.123.113:23 | OPENING | telnet
5) 192.168.123.113:2106 <--> 192.168.123.167:23 | CLOSED | telnet
6) 192.168.123.113:2111 <--> 192.168.123.167:21 | OPENING | ftp

Your IP: 192.168.123.151 MAC: 00:BF:BF:BF:BF:BF Iface: eth0 Link: SWITCH
Host: Unknown host (192.168.123.151) : 00:BF:BF:BF:BF:BF

As evidenced from the above screen rendition, ettercap is able to glean numerous details of the transactions between the two IP addresses – port numbers, packet type (UDP, TCP), TCP state (opening, closed), service type (netbios, telnet, ftp, etc.). Furthermore, ettercap has options to create filters to limit what types of data are captured, capture passwords to log files, and inject characters into the connections to actually manipulate the data in transit; this is a limited sample of ettercap's many capabilities.

One may view the above scenario and think that only bad things could come of such software. Consider, however, the case of using non-commercial software downloaded from the Internet in a switched LAN environment. It never hurts to slip ettercap between the PC with the untested

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

software and, perhaps, one's Internet gateway to ensure that the software is behaving properly and as documented.

Summary

"Trinux introduces the Linux-shy to the world of security tools with compassion and ease." (McClure and Scambray) It is difficult to conceive a better description of Trinux. In a similar manner, it would be difficult to conceive acquiring the status of computer security guru without advancing into the world of Linux and the numerous security tools created within its domain. Trinux affords an easy transition into both.

© SANS Institute 2001, Author retains full rights.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

References

Franz, Matthew. Trinux home page.
URL: http://trinux.org or
URL: http://trinux.sourceforge.net

Fox, Tammy. "Using Your Floppy Drive." Linux Headquarters. 22 April 2001
URL: http://www.linuxheadquarters.com/howto/basic/floppy.shtml

Gagne, Marcel. "Getting Small with Linux, Part 2." Linux Journal. 7 April 2000.
URL: http://www2.linuxjournal.com/articles/sysadmin/028.html

McClure, Stuart. Scambray, Joel. "Security Watch" Infoworld. 22 February 1999
URL: http://www.infoworld.com/cgi-bin/displayArchive.pl?/99/08/o03-08.52.htm

Ornaghi, Alberto. Valleri, Marco. Ettercap home page.
URL: http://ettercap.sourceforge.net/index.php?s=home

© SANS Institute 2001, Author retains full rights

Last Updated: May 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced