Global Information Assurance Certification Paper

The Webmin Unix Administration Tool
Timothy Grovac
February 11, 2001

Introduction to Webmin

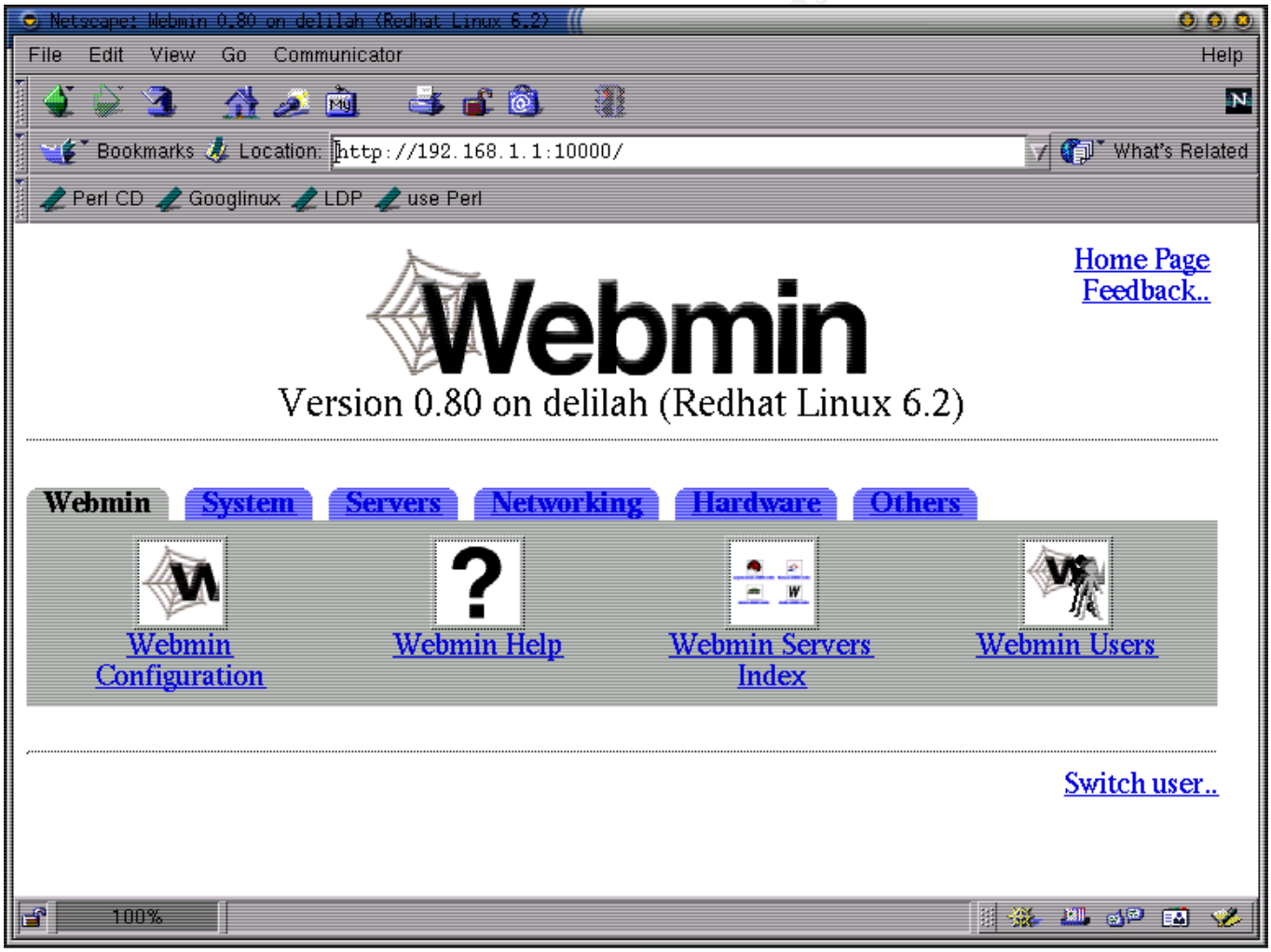
Webmin is a powerful, browser-based interface for UNIX system administration. Using any browser that supports forms and tables, Webmin can perform routine system administration tasks. Webmin does all the proper editing of configuration files for tasks such as adding users or groups, manipulating file systems, or adding and deleting software packages. It can also control many server programs such as Apache, DHCP, PPP, Sendmail, and FTP. When using this program the system administrator doesn't have to remember the location of all configuration files and the syntax of each, Webmin knows the right way. Webmin is written to support many UNIX operating systems. Below is the list of supported systems:

Operating System	Supported versions
Sun Solaris	2.5, 2.51, 2.6, 7, 8
Caldera Open Linux eServer	2.3, 3.1
Caldera Open Linux	2.3, 2.4, 2.5
Redhat Linux	4.0, 4.1, 4.2, 5.0, 5.1, 5.2, 6.0, 6.1, 6.2, 7.0
Slackware Linux	3.2, 3.3, 3.4, 3.5, 3.6, 4.0, 7.0, 7.1
Debian Linux	1.3, 2.0, 2.1, 2.2
SuSE Linux	5.1, 5.2, 5.3, 6.0-4, 7.0
Corel Linux	1.0-2
TurboLinux	4.0, 6.0
Cobalt Linux	2.2, 5.0
Mandrake Linux	5.3, 6.0, 6.1, 7.0-2
Delix DLD Linux	5.2, 5.3, 6.0
Convectiva Linux	3.0, 4.0-2, 5.0-1, 6.0
MkLinux	2.1, 3
LinuxPPC	2000
Xlinux	1.0
LinuxPL	1.0
Linux from Scratch	2.2
Trustix	1.1
Ute Linux	1.0
FreeBSD	2.1-2, 3.0-5, 4.0, 5.0
OpenBSD	2.5-7
BSDI	3.0-1, 4.0
HP-UX	10.01, 10.10-30, 11
SGI Irix	6.0-5
DEC/Compaq OSF/1	4.0
IBM AIX	4.3

SCO UnixWare	7, 2
SCO OpenServer	5
MacOS Server X	1.0, 1.2

Webmin consists of a web server and a number of Common Gateway Interface (GCI) programs. All GCI programs are written in Perl version 5. You access the program with a browser pointing to the web server address port 10000 (this port can be changed if desired).

The Initial Webmin Screen:



Webmin Modules

It would take too many screens to graphically show all the Webmin functionality so the following table shows each Webmin module and a brief description of its functionality:

Module	Description
Webmin Configuration	Configures settings affecting Webmin's operations
Webmin Help	Searchable index of Webmin's help system
Webmin Servers Index	Locates and lists all Webmin servers on the LAN
Webmin Users	Manages Webmin users and their privileges
Bootup and Shutdown	Controls system startup and shutdown processes
Disk and Network Filesystems	Lists and manipulates locally mounted filesystems
NFS Exports	Add, delete, and edit NFS exported filesystems
Running Processes	Lists detailed information about running processes
Scheduled Cron Jobs	Shows and controls cron jobs
Software Packages	Graphical interface to the RPM system
Users and Groups	Manage users and groups
Apache Webserver	Configures the Apache Webserver
BIND 8 DNS Server	Configures the BIND 8 domain nameserver
DHCP Server	Configures the DHCP server (not the client)
FTP Server	Configures the WU-FTP daemon
Internet Services and Protocols	Manages internet services
Majordomo List Manager	Graphically manages the majordomo listserver
PPP Usernames and Passwords	Controls the PPP server
Samba Windows File Sharing	Manipulates the SAMBA server/client
Sendmail Configuration	Edits the sendmail configuration file
Squid Proxy Server	Configures the Squid proxy/caching server
Linux Bootup Configuration	Edits the LILO configuration file
Network Configuration	Controls NIC and network configuration
Partitions on Local Disks	Adds, edits, and deletes disk partitions
Printer Administration	Manages local and remote printers and queues
System Time	Sets system and hardware clocks
Custom Commands	Creates custom commands to execute from Webmin

File Manager	Java-based file manager
Telnet Login	Java-based telnet applet

Security Considerations

It is easy to see why a system administration would enjoy working with Webmin. Many complex jobs can be easily performed using this tool. But what threats to security does this tool pose?

1. Get the Latest Version

Security Advisory CSSA-2001-004.0, was issued on January 17, 2001, which stated "On several occasions, webmin creates temporary files insecurely. This can be exploited by a local attacker to overwrite or create arbitrary files and possibly grain root privilege." Webmin issued a new version on January 23rd to fix this problem, version webmin-0.84. Installing this package is a mandatory first step in using the tool.

2. Consider SSL Implementation

Because Webmin uses a standard web server all the client/server vulnerabilities regarding browser issues prevail. For initial login you go to address: http://your.machine.whatever:1000 and the Webmin server presents you with a username and password prompt. The initial setup of the software sets the username to root and the password to your system root password. Your first note of caution on this screen is that all passwords typed at this prompt are passed as plain text between the client and the server. If you are worried about a sniffer between you and your Webmin server you should consider using Secure Socket Layers (SSL) with Webmin. SSL implementation software is not included with the Webmin distribution and requires the Perl Net::SSLeay module and the OpenSSL C libraries. If you install SSL with the Webmin server you must also be sure your browser supports SSL. Also consider the proxy or firewall issues when trying to connect using SSL. You may have to let SSL requests pass through the firewall if not already enabled.

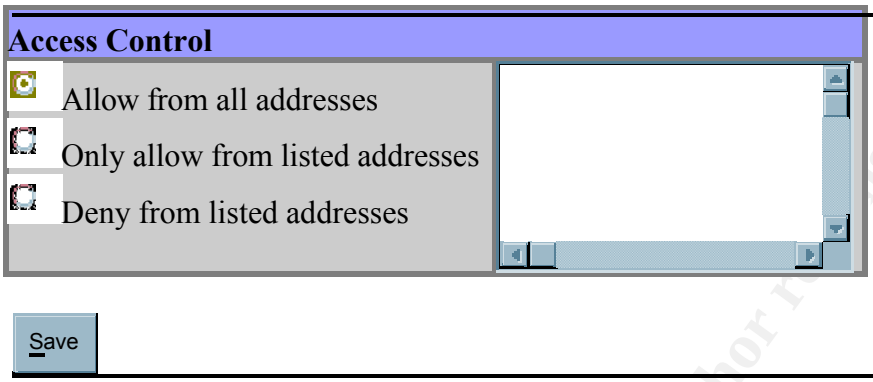
3. Restricting Access by IP Address

Webmin has some built-in tools that help secure the application. You can easily determine which IP addresses can access Webmin by following the configuration tab to IP access. The following screen then appears:

Webmin Index
Module Index

IP Access Control

The Webmin server can be configured to deny or allow access only from certain IP addresses using this form. Hostnames (like foo.bar.com) and IP networks (like 10.254.3.0 or 10.254.1.0/255.255.255.128) can also be entered. You should limit access to your server to trusted addresses, especially if it is accessible from the Internet. Otherwise, anyone who guesses your password will have complete control of your system.

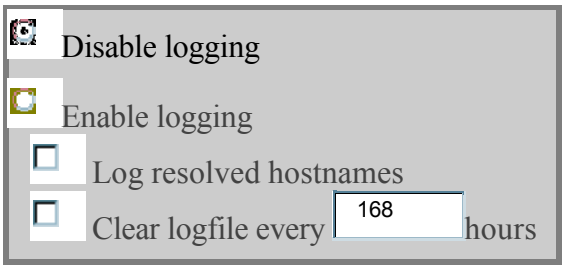


As you can see the default configuration is to allow all addresses. This should be changed to only allow trusted IP addresses. Be sure to add address 127.0.0.1 for the localhost.

4. Activate Logging

Logging is disabled by default and should be enabled.

Webmin can be configured to write a log of web server hits, in the standard CLF log file format. If logging is enabled, you can also choose whether IP addresses or hostnames are recorded, and how often the log file is cleared. When enabled, logs are written to the file `/var/log/webmin/miniserv.log`.



Summary

Webmin is an excellent tool for Unix system administrators. It makes most routine tasks quick and easy. By following a few simple security precautions you can make the tool secure without compromising functionality.

References

[1] "Using SSL with Webmin." URL:
http://www.webmin.com/webmin/ssl.html

[2] "One-Stop Linux Administration with Webmin" 6 April 2000. URL:
http://www.devshed.com/Server_Side/Administration/Webmin/Page3.html

[3] Caldera Systems, Inc. Security Advisory. "Security problems in webmin" 17 January 2001. URL:
http://www.calderasystems.com/support/security/advisories/CSSA-2001-004.0.txt

[4] The Webmin Users Guide. URL:
http://www.calderasystems.com/products/edesktop/usersguide/ch10.html

[5] Sans.org Security Alert Consensus. Cross platform Alerts. "{00.57.024} Cross - Webmin insecure temp file handling" URL:
http://www.sans.org/newlook/digests/SAC/cross.htm

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS