Title:
Check List for Linux Security

Word Count:
1006

Summary:
It describes the most common actions one can take to keep the Linux Operating System secure.

Keywords:
Linux, Security

Article Body:
Check List for Linux Security

Linux is an amazing operating system considering how it was originally created. It was a modest program written for one person as a hobby – Linus Torvald of Finland. It has grown into a full-fledge 32-bit operating system. It is solid, stable and provides support for an incredible number of applications. It has very powerful capabilities and runs very fast and rarely crashes.

Unfortunately Linux machines are broken almost every day. This happens not because it is an insecure operating system. It contains all the necessary tools to make it very secure. But the truth is. It hasn't become significantly more secure with the increase in popularity. On the other hand, our understanding of the hackers methods and the wide variety of tools and techniques available contributed to help system administrators to secure their Linux computers.

Our goal in this article is to list the most critical situations, and how to prevent an invasion with simple measures.

1- Weak passwords – By far the first and most used method used by hackers to try penetrating a Linux system is cracking a password, preferently of the user root. Usually they will target a common user first, and then, using his/her access to the operating system, try to get a privileged access cracking the root password. Good password policy, and good passwords are absolutely critical to the security on any computer. Some common mistakes when selecting a password:
A- use "password" as password.
B- use the name of the computer.

C- a well-know name from science, sports or politics.
D- reference to movies.
E- anything that is part of the user web site.
F- references associated with the account.

The latest version of Linux offer shadowed passwords. If a cracker can see an encrypted password, crack it would a simple task. So, instead of storing the password in the passwd file, they are now stored in the shadow file which is readable only for root. Before a hacker can crack a password he needs to figure out an account name. So, simple accounts names must be avoided as well. Another security measure is to apply a "no login" to the account in the passwd file. This must be done to all the accounts that don't need to log in to the system. Examples are: apache, mysql, ftp and other.

Limit which terminals root may log in from. If the root account is allowed to log in only in certain terminals that are considered secure, it will be almost impossible for a hacker to penetrate the system. This can be done listing the allowed terminals on /etc/security. The login program will consider insecure any terminal that is not listed on this file, which is readable, only by root.

2- Open Network Ports

Any Linux default installation will provide the Operating System with tons of software and services. Several of them are not necessary or even wanted by the administrator. Removing these software and services will close the path to several attacks and improve security. The /sbin/chkconfig program can be used to stop services from automatically starting at run levels 3, 4 and 5. Log in as root and type /sbin/chkconfig --list to view all the services set to start automatically. Select the ones you don't need and type /sbin/chkconfig 345 name_of_service off. You must do that to all services you don't want to keep running. Also, the xinetd server can be used to disable other services as well.

3- Old Software Versions

Everyday vulnerabilities are found in programs, and most of them are fixed constantly. It is important, and sometimes critical, to keep up with the changes. There are mailing lists for every Linux distribution where one can have security related information's, and the latest vulnerabilities found.
Some place to watch for security holes are:

- http://www.redhat.com/mailman/listinfo/redhat-announce-list

· http://www.debian.org/MailingLists/
· http://www.mandrakesecure.net/en/mlist.php
· http://www.suse.com/us/private/support/security/index.html
· http://www.freebsd.org/security/index.html
· http://www.linuxtoday.com/
· http://www.lwn.net/

It is crucial to insure that the security released patches are applied to the programs as soon as they area available. The hacker community will be aware of the discovered holes and will try to explore them before the fixes are applied.

4- Insecure and Badly Configured Programs

There are some programs that have a history of security problems. To name a few IMAP, POP, FTP, port map and NFS, are the most known. The good thing is that most of these programs can be replaced by a secure version like spop, sftp or scp.

It is important that, before deploying any service, the administrator investigate its security history. Sometimes simple configuration measures can prevent serious headaches in the future.

Some advices regarding a web server configuration are well worth to mention:

- Never run the web server as a privileged user;
- Do not keep clients' confidential data on the web server – Credit card numbers, phone numbers, mailing addresses, must be recorded on a different machine.
- Make sure the privileged data that a user supplies on a form does not show up as a default for the next person to use the form;
- Establish acceptable values for data that is supplied by web clients.
- Check vulnerabilities on CGI programs.

5- Stale and Unnecessary Accounts

When a user no longer uses his /her account, make sure it is removed from the system. This stale account won't have this password changed periodically leaving a hole. Publicly readable or writable files owned by that account must be removed. When you remove an unnecessary service make sure you remove or disable

the correspondent account.

Security Resources in the web

Bugtraq – Includes detailed discussions of Unix security holes
http://www.securityfocus.com/

Firewalls – Discuss the design, construction, operation, and maintenance of firewall systems.

http://www.isc.org/services/public/lists/firewalls.html

RISKS Discuss risks to society from computers

http://www.risks.org/

Insecure.org

http://www.insecure.org/