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 modes

Unfortunately Linux machines are broken almost every day. This happens not because it is an in

Our goal in this article is to list the most critical situations, and how to prevent an invasi

1- Weak passwords ˘ By far the first and most used method used by hackers to try penetr
A- use ˆpassword˜ 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 passwo

Limit which terminals root may log in from. If the root account is allowed to log in only in c

2- Open Network Ports

Any Linux default installation will provide the Operating System with tons of software and ser

3- Old Software Versions

Everyday vulnerabilities are found in programs, and most of them are fixed constantly. It is i
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

4- Insecure and Badly Configured Programs

There are some programs that have a history of security problems. To name a few IMAP, POP, FTP

It is important that, before deploying any service, the administrator investigate its securi

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
- Make sure the privileged data that a user supplies on a form does not show up as a def
    - 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 sta

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/

This is a demo version of txt2pdf v.10.1
Developed by SANFACE Software http://www.sanface.com/
Available at http://www.sanface.com/txt2pdf.html