Server Hardening:

Table of Contents

1. SecuringLinuxServer

SecurityPatches

InstallthelatestrpmpackagesforLinux.CheckforlatestRPMsatRedHatLinux website.

http://updates.redhat.com/enterprise/3WS/en/os/SRPMS/

http://updates.redhat.com/enterprise/3AS/en/os/SRPMS/

Else goto http://updates.redhat.com/enterprise/ and select the enterpriseversion running and install all patches from the link

Download the current RPMs from Red Hat's Website and install them using the followingcommand.

Rpm –ivh file_name.rpm

2. Filesystemsecurity

Partitionsecurity

Description:

When mounting a partition you can provide various options in the/etc/fstab file that increase the security of your system manifold. The various options that can be used are:

nosuid: Do not set SUID/SGID access on this partition.

noexec: Do not allow execution of any binaries on this partition.

ro: Allow read-only access to the partition.

rw: Allow read-write access to the partition.

Impact:

Without the nosuid value any user can access those file systems with privilege of file system owner or root. Without the rw options any user can write to those file systems.

Solution:

Edit the/etc/fstab file using texteditor.

```
vi/etc/fstab
```

Atypical*/etc/fstab*filewithpartitions*/*,*/tmp*,*/home*and*/var*shouldreadas shownbelow:

```
/dev/hda1   /                    ext3defaults,ro02

/dev/hda4   /usr ext3defaults,ro02

/dev/hda2   /home                ext3defaults,nosuid02

/dev/hda3  /tmp ext3defaults,nosuid02
```

The *nosuid* will result in no user being able to execute a setuidfile in/home and /tmp.

The *noexec* bit will ensure no executable can be run in those partitions.

Also once the system is installed, users probably won't be writing to the / and the */usr* filesystems. Hence those partitions can be mounted read-only.

3. Temporaryfolderpermission

Description:

Ensure that sticky bit is set for /tmp,/utmpand/utmpxfolders. If the sticky bit set then only owner of a file in this folder can delete that file and other users can only read the file but cannot delete it, even they have write permission on the folder.

Impact:

Any user can delete other users files in temporary folders, because by default all users have write permission on those folders.

Solution:

Set the sticky bit on temporary folder(*/tmp*):

```
ls–al (See if sticky bit is set or not)
cd/
chmod1777tmp
```

4.0 Passwd,shadowandgroupfilepermission

Description:

In Linux OS /etc/passwd, /etc/shadow and/etc/group files are most important files. The permission on these files should be secured.

Impact:

If an attacker has access to `passwd` file, he can create user in that file. Attacker can alter the MD5 hash of the root password with a known hash in the `shadow` file to get into the system or he can add a newly created user under root group in the `group` file.

Solution:

Change the owner of these files to root and also change the permission using the following commands:

```
Cd /etc
```

Chown root:root passwd shadow group

chmod644passwdgroup

chmod400shadow

5.0 UserAccountsandPolicies

PasswordPolicy

Description:

Passwords are used to securely log into users' account. The security of the users' passwords can be implemented system wide by enabling MD5 and shadow passwords.

Impact:

All accounts are vulnerable to attacks and hence the passwords should be a stored in a secure fashion. Passwords can be retrieved if they are stored in weak encryption format.

Solution:

Increasepasswordsecurity,byenablingthefollowing:

Type'setup'ontheshellprompt.

ChooseAuthenticationconfiguration.

Clicknext,andconfigure

MD5Passwords *[Allowspasswordsupto256characters]*

Password Shadowing*[Prevents users from obtaining the encrypted passwords]*

Edit/etc/login.defs file and set the following password configuration: Set minimum password length to

PASS_MIN_LEN=8

Setpasswordexpiryto

PASS_MAX_DAYS=45

PASS_MIN_DAYS=1

```
PASS_WARN=15
```

6.0 Disable non-essential accounts

Description:

Unnecessary user accounts should be tracked and be deleted from the system.

Impact:

Attackers can use these accounts to harm the system.

Solution:

Use the following command to delete non-essential accounts.

```
                    cat /etc/passwd|cut–d: -f1

   userdel <unnecessaryUsername>
```

Non-essentialaccounts		
Lp	uucp	ftp
Sync	operator	**nobody**
shutdown	games	nscd
Halt	gopher	nfsnobody
news	adm	

7.0 Disableremoterootlogin

Description:

Root user must not be able to log in from a remote console. The login command is part of the authentication process to access a local Linux Operating Environment account. Any action requiring direct login to the system using 'root' should be restricted to the local console.

Impact:

Logintothe systemthroughtelnetsessioncanrevealthecleartextpasswordof rootuser.Allowingremoteloginforrootalso enablesa malicioususertoattempt accessto thesystemleadingtosystemcompromise.

Solution:

Ensure that/etc/securetty file contains the list of all terminals from where root is not allowed to remotely login. The available terminals are:

[root@localhostroot]#less/etc/securetty			
vc/1	tty0	tty11	tty22
vc/2	tty1	tty12	tty23
vc/3	tty2	tty13	tty24
vc/4	tty3	tty14	tty25
vc/5	tty4	tty15	tty26
vc/6	tty5	tty16	tty27
vc/7	tty6	tty17	tty28
vc/8	tty7	tty18	tty29

vc/9	tty8	tty19	tty30

8.0 LoginBanner

Description:

An appropriateloginmessagemustbedisplayedto theuserwhenhe/shetriesto login to thesystem.Thisfileshouldcontainwarningsaboutinappropriateand unauthorizeduseof thesystem.Itshouldalsowarnusersthattheirsessionsand accountsmaybemonitoredforillegalorinappropriateuse.

Impact:

Displayingappropriatewarningmessageswhenusersaccessasystemwillassist inprocessingcomputercrimecasesandwillalsoactas aneffectivedeterrent.

Create or modify the /etc/issue, /etc/issue.net, /etc/motd files with appropriate statutory warning.

vi/etc/issue

“This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all their activities on this system monitored and recorded by system personnel."

Sameprocessforeditingthefiles

/etc/issue.net

/etc/motd

9.0 AuditingandLogging

Enable user authentication auditing

Description:

Syslog facility is used to log system activities. Syslog daemon receives log messages from several sources and directs them to the appropriate location based on the configured facility and priority. It can be used to capture all successful and failed logins.

Impact:

Malicious login attempts cannot be monitored.

Solution:

Add the following entry to */etc/syslog.conf* for capturing syslog events sent to LOG_AUTH. This contains information on unsuccessful login attempts, successful and failed su (switchuser) attempts.

```
vi/etc/syslog.conf
```

```
authpriv.*                    /var/log/secure
```

Use TAB key to separate auth.info from / `var/log/secure` and notspace.

Create`/var/log/secure` by executing the following commands

```
touch/var/log/secure

chownroot/var/log/secure

        chmod600/var/log/secure
```

10 SystemSecurityoptions

Crtl-Alt-DelSetting

Description:

By default CTRL-ATL-DEL to reboot the machine functionality is enabled in the system. This allows any user to reboot the machine.

Impact:

This function allows an attacker to reboot the server.

Solution:

Edit/etc/inittab file comment the following line:

```
vi/etc/inittab

ca:: ctrlaltdel:/sbin/shutdown–t3–r–now
```

Save the change and restart init service for the change to take effect:

```
/sbin/initq
```