Linux Security

Oded Maimon

Linux Security

1. Introduction

This document is intended for linux administrator and security personal. The purpose of this document is to secure linux servers for production use. This document shows how to secure a default installation of Redhat Enterprise Linux but can be adopt for other linux distors as well.

2. Installation process

- The Redhat server "Install Everything" installation, installs more than 1000 RPM's in RHEL5 and more than 1400 RPM's in RHEL4. The best way to install a server is to "Install what you need", Use the "Minimum" installation and after the install add what you need or to use the "Custom" installation and select the packages needed. (NOTE: The minimum installation installs less than 300 packages!)
- Patch the servers to the latest patch available - After the installation, the server should be patched to the latest errata available. Run "up2date –u" to update the system, If there is no internet connection then download the latest patch from Redhat web site.
- Some packages are not recommended for installation on a server:
  - X/Gnome/KDE – The reasons to not install X/Gnome/KDE are performance and security issues
  - Telnet/Ftp/Rsh – SSH is much better solution to for all those tools
- If the OS is already installed then remove unnecessary software
- Partition your disks to:
  - / - 2G
  - /var – 1G (can be smaller)
  - /var/log – 1G
  - /tmp – 2G
  - /usr – 4G (this is the main directory used for tools)
  - /usr/local – 1G (can be smaller)
  - /home – 500M (depends on the space needed by users)
  - /opt – 500M
  - /boot – 100M

3. Run level

The linux machine run level is used to define what system services are operating. There are seven run levels:

- 0: Halt the machine

- 1: Single user mode
- 2-5: Normal operating mode (user defined)
  - 2 – Multiuser, without NFS
  - 3 – Full multiuser mode
  - 4 – Unused
  - 5 – X
- 6: Reboot

The default run level for a server should be 3. Run level 3 will start without X (GNOME/KDE/other). To change the default run level on boot you should edit the file /etc/inittab and change the default run level by editing this line:

```
id:5:initdefault:
```

to:

```
id:3:initdefault:
```

4. Detect open ports

One of the most important things is to close all unneeded network ports and know which ports you leave open. To get the list of open ports run:

```
netstat –tulpn
```

The output of this command will return something like this:

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      2391/portmap
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1966/sshd
udp        0      0 0.0.0.0:68              0.0.0.0:*                           1570/dhclient
udp        0      0 0.0.0.0:111             0.0.0.0:*                           2391/portmap
```

Services/ports that you may not want to leave running/open are:

Tool/Services	Port	Dependencies	Handle service
Sendmail	25	SMTP protocol	If you need the server to act as SMTP server for outgoing emails only then go to "Secure Sendmail" Section in this document. If you don't need to use this server as SMTP server

Tool/Services	Port	Dependencies	Handle service
			in any way you can stop it by running: service sendmail stop chkconfig sendmail off
Portmap (RPC)	111	Handles RPC calls Used by NFS client	service portmap stop chkconfig portmap off
Nfslock	TCP:32700 UDP:32768, 729	Used by NFS client	service nfslock stop chkconfig nfslock off
Cupsd	631	Printing service	service cups stop chkconfig cups off
Hplip/hpiod	2208	HP Linux Imaging and Printing	service hplip stop chkconfig hplip off
avahi-daemon	UDP:1024 , 5353, 1025	MDNS/DNS-SD Multicast DNS service Discovery	service avahi-daemon stop chkconfig avahi-daemon off

5. Stop unneeded services

The default installation starts some services that you may not need or wish to leave running, this list will show most of them. First of all, the way to get the list of running services is:

```
chkcnfig –list | grep ":on"
```

The output for this command will return something like this:

```
acpid           0:off  1:off  2:off  3:on   4:on   5:on   6:off
anacron         0:off  1:off  2:on   3:on   4:on   5:on   6:off
apmd            0:off  1:off  2:on   3:on   4:on   5:on   6:off
atd             0:off  1:off  2:off  3:on   4:on   5:on   6:off
auditd          0:off  1:off  2:on   3:on   4:on   5:on   6:off
autofs          0:off  1:off  2:off  3:on   4:on   5:on   6:off
avahi-daemon    0:off  1:off  2:off  3:off  4:off  5:off  6:off
```

```
avahi-dnsconfd      0:off   1:off   2:off   3:off   4:off   5:off   6:off
bluetooth           0:off   1:off   2:on    3:on    4:on    5:on    6:off
conman              0:off   1:off   2:off   3:off   4:off   5:off   6:off
cpuspeed            0:off   1:on    2:on    3:on    4:on    5:on    6:off
crond               0:off   1:off   2:on    3:on    4:on    5:on    6:off
firstboot           0:off   1:off   2:off   3:on    4:off   5:on    6:off
gpm                 0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

To stop a service from running and start at boot time use:

service <***service name***> stop
chkconfig <***service name***> off

List of services that run by default:

Service name	Description	Needed?
acpid	Handles ACPI event and invokes the command. For example, what happens when the power/sleep button is pressed or AC adapter state is changed.	Y
anacron	Like cron but it will run jobs that didn't run because the server was down.	N
apmd	Monitoring battery status	N
arptables_jf	Automates a packet filtering firewall with arptables	N
atd	The same tool as cron. Needed only if using the at command.	N
auditd	Handles the audit system	Y
autofs	Automount filesystems	If using autofs
avahi-daemon (RHEL5)	MDNS/DNS-SD, Multicast DNS service Discovery	If using MDNS
avahi-dnsconfd (RHEL5)	Daemon which configures unicast DNS servers using server info published via mDNS	If using MDNS

Linux Security

Service name	Description	Needed?
bluetooth	Bluetooth services for service discovery, authentication, Human Interface Devices, etc	If using Bluetooth devices
canna	Japanese Conversion Engine	N
cpuspeed	Monitors the systems idle percentage and reduces or raises the CPUs clock speeds and voltages accordingly to minimize power consumption	Y IBM claims it can be off
crond	Handles corn jobs	Y
cups-config-daemon	configuring printers through D-BUS	N
firstboot	Run the first boot program if this is the first boot or run the reconfiguration program if reconfiguration file exists	Y
gpm	Mouse support for text based mode	N
haldaemon	Daemon for collecting and maintaining information about hardware from several sources.	Y
hidd	Bluetooth Human Interface Device Daemon. Provides keyboard, mouse etc. functionality over Bluetooth.	If using Bluetooth
hpoj	HP OfficeJet Linux driver	N
iiim	Needed if using IM	N
ip6tables	Iptables firewall for IPv6	?
iptables	Iptables firewall for IPv4	?
irqbalance	The irqbalance daemon will distribute interrupts across cpus on a multiprocessor/multithreaded system with the purpose of spreading the load. Can be disabled on a single CPU machines.	Y
isdn	ISDN	N
kudzu	Discover new hardware (can run manually). Run it manually in case of hardware changes.	N
lm_sensors	Monitoring motherboard sensor values	Why not

Service name	Description	Needed?
mcstrans (RHEL5)	SELinux Context Translation System Daemon	If using SELinux
mdmonitor	Software RAID monitor	If using software RAID
messagebus	This is a daemon which broadcasts notifications of system events and other messages.	Y
microcode_ctl	Apply cpu microcode (IA32 Arch)	Y
netfs	Mount network filesystems on boot. This service is needed when using NFS filesystems.	Y
network	Network configuration	Y
openibd	Activates/Deactivates InfiniBand Subnet Manager	If using InfiniBand
pcmcia	Handles pcmcia devices	N
pcscd (RHEL5)	Smart Card support	N
rawdevices	If using rawdevices	If using rawdevices
readahead	Prereads programs required for startup into memory	Why not?
readahead_early	Prereads programs required for startup into memory (/etc/readahead.d/*.early)	Why not?
readahead_later	Prereads programs required for startup into memory (/etc/readahead.d/*.later)	Why not?
restorecond (RHEL5)	Used when using SELinux to restore specific files security context	If using SELinux
rhnsd	Redhat network daemon	If using RHN updates

Service name	Description	Needed?
rpcgssd	manages RPCSEC GSS contexts for the NFSv4 client	If using NFSv4
rpcidmapd	maps user names to UID and GID numbers for NFSv4	If using NFSv4
setroubleshoot (RHEL5)	starts the SELinux Troubleshooting Daemon	If using SELinux
smartd	Self Monitoring and Reporting Technology (SMART) Daemon	Y
sshd	SSH	Y
syslog	Starts syslog	Y
xfs	X font server. You can load it only in run level 5.	N
xinetd	Xinetd service	Y
yum-updatesd (RHEL5)	Provides notification of updates which are available to be applied to your system	If using network updates using yum

To check which xinetd services run by default:

```
chkconfig --list | awk '/xinetd based services/,/""/' | grep on
```

Service name	Description	Needed?
auth	allows remote daemons to query information about users establishing TCP connections on the local server	N

6. Remove unneeded LKM's (Loadable Kernel Modules)

Loadable kernel modules will be loaded when they are needed by the OS/tools, so after disabling all unneeded services we can see that the amount of loaded modules (using lsmod) before is much greater than now.

To disable unneeded LKM's we can use this method:

- lsmod – Displays a list of all loaded modules
- modinfo <module name> - Displays information about a specific module
- rmmod <module name> – Will try to unload a module (if not used)

To prevent a specific LKM from loading at boot time you will need to change the modprobe configuration files:

- RHEL4 – edit /etc/modprobe.conf and add the line:
  alias <driver name> off
  for example: "alias floppy off"
- RHEL5 – edit /etc/modprobe.d/blacklist and add the line:
  blacklist <driver name>

To find the <driver name> you can use modinfo <module name> and get the value in the alias field for example: "modinfo ipv6".

7. Disable CTRL+ALT+DEL

CTRL+ALT+DEL are the default keys defined to reboot the machine, we've seen few cases which cause this defaults to reboot a production server because of a human mistake. To remove this default, edit the file /etc/inittab and comment the line:

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

Or to this line if you whish to echo a message when buttons are pressed:

```
ca::ctrlaltdel:/bin/echo "CTRL+ALT+DEL is disabled."
```

after saving the file run this command to reload the init settings:

```
init q
```

8. Disabling IPv6

To disable IPv6 you need to:

- Add this line to /etc/modprobe.conf:
  alias net-pf-10 off

  NOTE: if the line "alias net-pf-10 ipv6" exists in the file, change it.
- Add this line to /etc/sysconfig/network
  NETWORKING_IPV6=no

  NOTE: If the line "NETWORKING_IPV6=yes" exists in the file, change it.

9. Secure SSHD

SSH is the replacement for telnet, rsh, rcp and rlogin, with SSH you can create an encrypted & secure connection to the machine. The main sshd configuration file is /etc/ssh/sshd_config.

- To restrict direct root login via ssh set:
  ```
  PermitRootLogin no
  ```
- Allow only ssh version 2 connections, set:
  ```
  Protocol 2
  ```
- Ensure that strict mode is enabled to check file permissions and ownerships of important files locate at the user home directory. With this setting set to yes the sshd will fail connection to the user if the files are not set correctly:
  ```
  StrictMode yes
  ```
- Disable all host based authentications via ssh:
  ```
  IgnoreRhosts yes
  HostbasedAuthentication no
  RhostsRSAAuthentication no
  ```
- Set idle session timeout to 15 min:
  ```
  ClientAliveInterval     300
  ClientAliveCountMax   3
  ```
- Allow only specific users to connect via ssh by create a sshgroup and enable it in ssh:
  ```
  AllowGroups sshgroup
  ```
- Disable sftp if not needed, remark the line:
  ```
  Subsystem               sftp      /usr/lib/misc/sftp-server
  ```
- Use privilege separation to separate the ssh daemon into two parts, a small part will run as root and the second part will run in cohort jail environment. To do this set:
  ```
  UsePrivilegeSeparation yes
  ```

10. Kernel Security Tuning

Purpose	Description	Parameter
TCP SYN attack cookie protection	TCP SYN Attack is a DOS attack that consumes all the resources of a machine.	net.ipv4.tcp_syncookies = 1
Disable IP forwarding	Disable ip forwarding. This parameter should be set to 1 when the linux server acts as a router.	net.ipv4.ip_forward = 0

Purpose	Description	Parameter
Disable IP source routing	Source routing is used to specify a path or route through the network from source to destination. This feature can be used by intruders to send a new source route to route traffic to different place and listen to the server network without the server know it happens.	net.ipv4.conf.all.accept_source_route = 0
Disable ICMP Redirect Acceptance	ICMP redirects are used to tell a server the better path to other networks than the one chosen by the server. This feature can be used by intruders.	net.ipv4.conf.all.accept_redirects = 0
Enable IP Spoofing Protection	IP sppofing is when an intruder change the source of an IP packet.	net.ipv4.conf.all.rp_filter = 1
Disable ping	Disable ping requests	net.ipv4.icmp_echo_ignore_all = 1
Disable broadcast requests	Disable broadcast requests	net.ipv4.icmp_echo_ignore_broadcasts = 1
Alert for bad error messages in network		net.ipv4.icmp_ignore_bogus_error_responses = 1
Enable logging	Enable logging of source route packets, spoofed packets and redirect packets	net.ipv4.conf.all.log_martians = 1

11. Lock unused accounts

There are many accounts created with linux installation (more than 40), most of them are locked already locked. We will check the users that are not locked and decide what to do with each account.

To get the list of open account use:

```
cat /etc/passwd | grep -v nologin | grep -v false | grep -v root | grep -v sync | grep -v shutdown | grep -v halt
```

Account	Description	Action

Account	Description	Action
news	Used when using the machine as a news feed server	lock
postgres	Used for postgresql database	lock
mysql	Used for mysql database	lock
netdump	Send oops data and memory dumps over the network	lock
pvm	Parallel processing, used for GRID	lock
cyrus	IMAP server	lock
amanda	Backup tool	lock

12. Configure TCP-Wrapper

To allow access from and to specific networks/servers/services we can use TCPWrapper.

The configuration files for TCP Wrapper are:

- /etc/hosts.allow
- /etc/hosts.deny

The files format is:

```
<daemon list> : <client list> [ : shell command ]
```

Useful man pages for more information:

- hosts_options(5)
- hosts_access(5)

NOTE: hosts.allow file take precedence over hosts.deny.

For example:

- Allowing access via ssh only from specific hosts/subnets:
  sshd: server1 server2 .mydomain.com
- Allowing any type of access to the server only from specific hosts/subnets:
  ALL: server1 server2 .mydomain.com
- To remote logging all connections from server1 use:
  sshd: server1: spawn echo "Login from %c to %s" | mail –s "Login" admin@mydomain.com

NOTE: For more complex filtering we can use iptables.

13. Password policies

13.1. Password Aging

- Edit /etc/login.defs
    - Change the values of: PASS_MAX_DAYS, PASS_MIN_DAYS, PASS_WARN_AGE
- Edit /etc/default/useradd
    - Change the value of: EXPIRE to the number of days the password will live
    - Change the value of: INACTIVE to the number of days that the user will be locked after a password expires
    - Or use chage…
- use passwd –S <user> to get password aging information for a user

13.2. Strong password enforcement

- Edit /etc/pam.d/system-auth and add:

  ```
   minlen=10 lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1 difok=3
  ```

  To the end of the line:

  ```
   /lib/security/$ISA/pam_cracklib.so retry=3
  ```

13.3. Password history

- Edit /etc/pam.d/system-auth and add:

  ```
  remember=20
  ```

  To the end of the line:

  ```
  /lib/security/$ISA/pam_unix.so nullok use_authtok md5 shadow
  ```

13.4. Locking user after too many logins

- Edit /etc/pam.d/system-auth and add:

  ```
  auth        required      /lib/security/$ISA/pam_tally.so onerr=fail no_magic_root
  ```

  after the line:

  ```
  auth        required      /lib/security/$ISA/pam_env.so
  ```

  Also, add the line:

  ```
  account     required      /lib/security/$ISA/pam_tally.so per_user deny=5 no_magic_root reset
  ```

  after the line:

  ```
  account     required      /lib/security/$ISA/pam_unix.so
  ```

14. Set accounts ulimits

To prevent accidental DOS we will set ulimits for all users/groups that we use. This example will show how to set the ulimit for oracle user and for users group. We will use only 2 type of limits (nofile and nproc), but there are more than 10 other types of limits that can be set, like memory, cpu, max logins and more.

- Edit /etc/security/limits.conf, and add:
  - For oracle account:
    ```
    oracle   soft   nofile   4096
    oracle   hard   nofile   63536
    oracle   soft   nproc    2047
    oracle   hard   nproc    16384
    ```
  - For the users group:
    ```
    @users   soft   nofile   500
    @users   hard   nofile   1000
    @users   soft   nproc    250
    @users   hard   nproc    500
    ```

15. Enable auditing

Auditing will log all activities made by users, the drawback of linux auditing system is that we are unable to see the parameters used by a command, for example, if a user will run the command "rm –rf" we will only see rm in the audit trail.

Auditing users commands is available by psacct daemon.

To enable psacct run:

```
/etc/init.d/psacct start
chkconfig psacct on
```

Commands to get information from psacct database are:

- lastcomm – last commands by users
- ac – statistics about users connect time
- ac –p – Total time for each user
- ac –d – Total time for each day
- sa – summarize accounting information
- sa –u – print the user for each command
- sa –m – CPU usage per user
- and more options for each command (sa, ac, lastcomm)…

16. Patch management

There are few patch management solutions, here is a list of a few products:

- Yum (Yellow dog Updater, Modified) – Opensource tool to manage RPM based installations
    - Opensource & Free
    - Simple to use and manage
    - No central management console
- Redhat default up2date solution:
    - No central management console
    - Each server handles it's own updates
    - Each server need access to RHN (can be solved by http proxy server)
- Redhat Satellite server –Implements a solution for patch management by creating a single server that all servers register to get the new patches. This server collects all needed information and packages from Redhat Network for all the registered servers, and can automatically/manually update the registered servers. The satellite server is the only one that needs to have access to the Internet. Redhat Satellite server benefits:
    - Single place to manage all servers
    - Single place with access to the internet. Can be protected by firewalls.
    - Monitoring system – can monitor servers performance
    - Network based server install (Kickstart install solution implemented)
    - Servers cloning (clones software that were installed by RPM's only)
- IBM Tivoli provisioning management
- HP Radia
- Quest configuration management for SMS

17. Enable iptables

Using iptables we can filter/reroute/logging packets and more. For example, if we would like to allow connections log all packets received from a specific ip on a specific port we can do it with iptables.
I will not discuss iptables in this document, but this is a very good way to do this type of jobs.

iptables can be loaded by the services:

- iptables6 – for IPv6
- iptables – for IPv4

If you will use iptables to forward communication you will also need to set the kernel parameter ip_forward to 1.

18. Syslog shipping (Remote Logging)

Syslog can send the log records to a remote host for central monitoring, protecting the data from the administrator and from hackers. To do this all you need to do is:

- On the syslog server side (The server that will log and save the data) edit the file /etc/sysconfig/syslog and add "-r" to the SYSLOGD_OPTIONS variable and restart syslog daemon.
- On each client add the following line to /etc/syslog.conf and restart the syslog daemon:
  ```
  *.*        @syslog-server
  ```
  Where syslog-server is the syslog server name/ip.

NOTE: Running syslog server (The server that will log and save the data) will open UDP:514 port.

19. Apache Hardening

Apache is the default web server for linux and the most common web server on the internet. Because of this, apache is a very secure web server but there are few things to do when configuring apache, the main configuration file of apache is /etc/httpd/conf/http.conf:

- By default apache bounds it self to all networks (Ethernet interfaces) available in the server. Bounding apache to listen to specific interface will minimize the vulnerable of apache, to do that we will need to set the parameter: Listen to smoothing like this:
  ```
  Listen 192.168.0.122:80
  ```
  Where 192.168.0.122 is the ip address that we wish apache to listen on.
- The default configuration of apache is to follow symbolic links and this could be exploited by hackers, to disable this feature remove the "FollowSymLinks" option from apache configuration file.
- Remove SSI (Server-Side Includes) support – SSI is a way to run server side commands before an html is delivered to the client. SSI is usually disabled by default, to check that that it is also true for our installation check if the option "+Includes" exists in apache configuration files.
- Disable CGI support – apache CGI support is a way to run scripts from apache, this could be exploited if the script is not written in a secure way. CGI is enabled for all "ScriptAlias" directories and disabled for all other directories by default. To check that the CGI is disable in our installation we need to check that the "ExecCGI" option is not used.
- Remove unused modules – apache comes with a very big set of loadable modules, we can find the loaded modules in apache configuration files by looking for the directive "LoadModule". It is a good idea to comment the modules that are not used. Here is a list of few modules that are not used commonly, and can be removed probably:

Module Name	Description
ldap_module	LDAP support

Linux Security

Module Name	Description
auth_ldap_module	LDAP authentication with apache
include_module	SSI support
dav_module	WebDAV support
autoindex_module	Needed if using the Index option
info_module	Provides a comprehensive overview of the server configuration
status_module	Provides information on server activity and performance
dav_fs_module	filesystem provider for mod_dav
proxy_module	HTTP proxy server
proxy_ftp_module	FTP support module
proxy_http_module	HTTP support module
cgi_module	Execution of CGI scripts

- Hiding apache version number and other sensitive information by setting:
  ServerSignature Off
  ServerTokens Prod
- Turn off support for .htaccess files, This is done in a Directory tag with the AllowOverride directive. Set it to None:
  AllowOverride None
- Lower the "Timeout" value to 45
- Limiting large requests:
  - Limiting the size of a body requests to 1MB (Do not set this if allowing to upload large files):
    LimitRequestBody 1048576
  - Limiting the size of an XML file (if using webdav):
    LimitXMLRequestBody 10485760
  - You can also check "LimitRequestFields", "LimitRequestFieldSize" and "LimitRequestLine". These directives are set to a reasonable defaults for most servers, but you may want to tweak them to best fit your needs.

- Use SSL communication, apache support SSL and can be very easily configured for ssl.
- The final thing to do, but only if truly needed is to run apache in a chrooted environment. This is very tricky thing to do, but possible, we will not discuss this in here.

20. Sendmail Hardening

Sendmail is the default mail server for linux, it's not very secure and pretty hard to configure, But Sendmail is usually used for local mail delivery and not as an SMTP server, if you need an SMTP server I recommend postfix over Sendmail. To use Sendmail for local mail delivery we don't need it to listen to SMTP port 25, to do that all we need to do is edit the file /etc/sysconfig/Sendmail and change the DAEMON variable from "yes" to "no" like this:

```
DAEMON=no
```

21. NFS Hardening

- Use NFS over TCP
- Restrict use for NFSv3 and v4 only
- Use TCP wrapper on NFS
- Export only to those machines that you really need
- Use fully qualified domain names
- Export only directories you need to export
- Export read-only wherever possible

22. Antivirus

Antivirus for linux are no commonly used unless:

- The server role is a windows file server using samba
- The server role is a mailserver

There are three very well known anti-viruses for linux:

- ClamAV – OpenSource antivirus
- Panda – Commercial antivirus
- McAfee LinuxShield - Commercial antivirus

23. Other tools worth checking

23.1. Nessus

Nessus is a very popular vulnerability scanner used, started as an opensource and now it's a closed source but still available for free download.
http://www.nessus.org

23.2. Bastille Linux

Bastille Linux is a tool that helps protecting the operating system by setting a large amount of parameters. It's a good thing to run this tool after implementing this document.
http://www.bastille-linux.org/

23.3. DenyHosts

DenyHosts is a script intended to be run by Linux system administrators to help thwart SSH server attacks (also known as dictionary based attacks and brute force attacks)
http://denyhosts.sourceforge.net/

23.4. Checking for rootkits

Rootkits - (Wikipedia) a set of software tools intended to conceal running processes, files or system data from the operating system. Rootkits have their origin in benign applications, but in recent years have been used increasingly by malware to help intruders maintain access to systems while avoiding detection. chkrootkit is one of the most commonly used for rookits checking.
http://www.chkrootkit.org/

23.5. Nikto

Nikto is an Open Source web server scanner which performs comprehensive tests against web servers.
http://www.cirt.net/code/nikto.shtml

23.6. Tripwire

Tripwire is a file and directory integrity checker. Tripwire is a tool that aids system administrators and users in monitoring a designated set of files for any changes.
http://www.tripwire.com/

23.7. Ntop

ntop is a network traffic probe that shows the network usage, similar to what the popular top Unix command does.
http://www.ntop.org