Network Infrastructure Security Recommendations

Hardening Red Hat Enterprise Linux
Ensure that file systems with user-writeable directories (ie /home, /tmp, /var/tem) are mounted on separate partitions.

Ensure updates are applied as soon as they become available.

The default version of yum-updatesd does not function reliably. Instead apply updates through a cron job using the following process:

- Disable the service with: /sbin/chkconfig yum-updatesd off
- Create the file yum.cron, make it executable, place it in /etc/cron.daily or /etc/cron.weekly, and ensure that it reads as follows:

  #! /bin/sh
  /usr/bin/yum –R 120 –e 0 –d 0 –y update yum
  /usr/bin/yum –R 10 –e 0 –d 0 –y update

Disable Unnecesary Services

- Review /sbin/chkconfig --list for services configured to start at boot (The default run level is 5). To disable a service, run the following command: /sbin/chkconfig *servicename* off
- Unless they are required, disable the following:

anacron	haldaemon	messagebus
apmd	hidd	microcode_ctl
autofs`	hplip*	pcscd
avahi-daemon*	isdn	readahead_early
bluetooth	kdump	readahead_later
cups*	kudzu	rhnsd*
firstboot	mcstrans	setroubleshoot
gpm	mdmonitor	xfs

Items marked with a * are network services and it is particularly important to disable these. Additionally, if NFS is not in use the following should be disabled; netfs, nfslock, portmap, rpcgssd, and rpcidmapd. Some software relies on haldaemon and messagebus so care should be taken when disabling them. Changes are applied on reboot.

- Disable SUID and SGID Binaries. The following files can have their SUID or SGID bits safely disabled (by using chmod –s filename) unless required for the specific purpose listed:

File:	Required For:
/bin/ping6	IPv6
/sbin/mount.nfs	NFS
/sbin/mount.nfs4	NFS
/sbin/netreport	network control
/sbin/umount.nfs	NFS
/sbin/umount.nfs4	NFS
/usr/bin/chage	passwd
/usr/bin/chfn	account info
/usr/bin/chsh	account info
/usr/bin/crontab	cron
/usr/bin/lockfile	Procmail
/usr/bin/rcp	rsh
/usr/bin/rlogin	rsh
/usr/bin/rsh	rsh
/usr/bin/wall	console messaging
/usr/bin/write	console messaging
/usr/bin/Xorg	Xorg
/usr/kerberos/bin/ksu	Kerberos
/usr/libexec/openssh/ssh-keysign	SSH host-based authentication
/usr/lib/vte/gnome-pty-helper	Gnome, Xorg
/usr/sbin/ccreds_validate	Pam auth caching

/usr/sbin/suexec	Apache, CGI
/usr/sbin/userisdnctl	ISDN
/usr/sbin/usernetctl	network control

Configure and Use Iptables and TCP Wrapper

- The Iptables firewall should be configured to only allow necessary network communication. If running, view the current firewall policy with the following command: /sbin/iptables –L
- By default, the output should correspond to rules stored in the file /etc/sysconfig/iptables . Understand and edit these rules, removing any lines that allow unneccary communications. To activate the updated rules, restart the services.
- Also configure the TCP Wrapper library to protect network daemons that support its use by adding appropriate rules to /etc/hosts.allow and /etc/hosts.deny.

Configure and Use SELinux. The default SELinux policy (targeted) provides protection against compromised or misconfigured system services. Ensure that /etc/selinux/config includes the following lines:

SELINUX=enforcing
SELINUXTYPE=targeted

*Note: stronger policies such as strict and mls can be used if appropriate. However, these require customization to operate successfully for many usage scenarios.

Set Kernel Parameters. Add the following lines to /etc/sysctl.conf to prevent certain kinds of attacks:

- net.ipv4.conf.all.rp_filter=1
- net.ipv4.conf.all.accept_source_route=0
- net.ipv4.icmp_echo_ignote_broadcasts=1
- net.ipv4.icmp_ignore_bogus_error_messages=1
- kernel.exec-shield=1
- kernel.randomize_va_space=1

Configure SSH. Ensure that /etc/ssh/sshd_config includes the following lines:

PermitRootLogin no
Protocol 2

Hardening MySQL Installation

Ensure Source files are removed from the server.

Network Infrastructure Security Recommendations

Create service account for MySQL
groupadd mysql
useradd –d /dev/null –g mysql –s /bin/false mysql

Ensure proper directory ownership and permissions
chown –R root /usr/bin/mysql*
chown –R mysql:root /var/lib/mysql
chmod –R go-rwx /var/lib/mysql
mkdir –p /var/log/mysql
chown –R mysql:root /var/log/mysql

Copy the main config file from the default directory
cp /usr/share/mysql/my-medium.cnf /etc/my.cnf

Remove the default folder
rm –rf /var/lib/mysql/test
rm –f /usr/share/mysql/*.cnf

Set proper ownership and permissions for my.cnf
chown root /etc/my.cnf
chmod 644 /etc/my.cnf

Edit /etc/my.cnf and add the following lines below [mysqld] section:
pid-file = /var/lib/mysql/test
log = /var/log/mysql/mysql.log
bind-address = 127.0.0.1
Add the following line below [safe_mysqld]
err-log = /var/log/mysql/mysql.err

Set a password for the MySQL root user:
/usr/bin/mysqladmin -u root password 'new-password'
/usr/bin/mysqladmin -u root -h hostname password 'new-password'

Note: Specify a complex password (at least 14 characters) and document it.
Replace “hostname” with the server FQDN (DNS name).

Run the command to login to MySQL: /usr/bin/mysql -uroot -pnew-password. Note: Replace the string “new-password” with the actual password for the root account.

Remove ‘test’ database and access
use mysql; DELETE FROM mysql.user WHERE user = '';

```
DELETE FROM mysql.user WHERE user = 'root' AND host = '%';
DELETE FROM mysql.user WHERE User='root' AND Host!='localhost';
DROP DATABASE test;
DELETE FROM mysql.db WHERE Db='test' OR Db='test\\_%';
FLUSH PRIVILEGES;
quit
```

References

Articlesbase:
http://www.articlesbase.com/security-articles/mysql-security-best-practices-and-hardening-guide-5090978.html

MySQL Security:
http://dev.mysql.com/doc/refman/5.0/en/security.html

National Security Administration:
www.**nsa**.gov/ia/_files/os/**redhat**/rhel5-**guide**-i731.pdf

Open Web Application Security Project:
https://www.owasp.org/index.php/OWASP_Backend_Security_Project_MySQL_Hardening

Publication Information

Altius IT is a security audit, security consulting, and risk management firm. We are certified by the Information Systems Audit and Control Association (ISACA) as a Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Controls (CRISC), and Certified in the Governance of Enterprise Wide IT (CGEIT). For more information, please visit www.AltiusIT.com.