ERNW
providing security.

SLES Hardening

SUSE Linux Enterprise 11

Version:	1.00
Date:	8/14/2013
Classification:	Public
Author(s):	Florian Grunow, Matthias Luft

TABLE OF CONTENT

1 Introduction

ERNW has compiled the most relevant settings for SLES 11 into this checklist. While there is a significant amount of controls that can be applied, this document is supposed to provide a solid base of hardening measures. Settings which might have severe impact on the functionality of the operating system and need a lot of further testing are not part of this checklist.

We have marked each recommended setting in this checklist either with "mandatory" or "optional" to make a clear statement, which setting is a MUST (mandatory) or a SHOULD (optional) from our point of view. "Optional" also means that we recommend to apply this setting, but there may be required functionality on the system that will become unavailable once the setting is applied.

2 AUTHENTICATION

2.1 Minimal Number of Users With Group root

- Review the file `/etc/group`. It should contain the following line, without specifying any user names:

```
root:x:0:
```

Mandatory

2.2 Check all Passwords are Shadowed

- The following command can be used to verify this:

```
awk -F: '($2 != "x") {print}' /etc/passwd
```

The command should produce NO output if there are only shadowed passwords.

Mandatory

2.3 Use Strong Hashing Algorithm

- Ensure that PAM is using a strong hashing mechanism. The following is an example configuration for files in `/etc/pam.d/` that specifies blowfish:

```
password required       /lib/security/pam_pwcheck.so
          nullok blowfish

  password required       /lib/security/pam_unix2.so
          nullok blowfish use_first_pass use_authtok
```

Mandatory

2.4 Implement Secure Password Policy

- Make use of the PAM modules `pam_cracklib`, `pam_pwhistory`, and `pam_unix2`. The following password policy is an example:

```
min length = 10
lower case = 1
upper case =1
number = 1
passwords to remember (password history) = 5
```

- To enforce this policy, edit the file `/etc/pam.d/common-password` and add the following lines:

```
password  required    pam_cracklib.so dcredit=-1 ucredit=-1
  lcredit=-1 minlen=8 retry=5

password  required    pam_pwhistory.so use_authtok
  remember=3 retry=5
password  required    pam_pwcheck.so remember=5

password  required    pam_unix2.so use_authtok
```

Mandatory

2.5 Ensure the Presence of one root User

- Review the file `/etc/passwd` for users that are in the group root other than the user root. To ensure that there is only one user with UID and GUID 0, run the following command:

```
awk -F: '($3 == "0") {print}' /etc/passwd
  awk -F: '($4 == "0") {print}' /etc/passwd
```

This command should only return the root user.

Mandatory

2.6 Implement Account Lockout Policy

- Add the following two lines to the `/etc/pam.d/common-auth`:

```
auth required pam_tally.so onerr=fail no_magic_root unlock_time=1800
account required pam_tally.so per_user deny=5 no_magic_root reset
```

The first added line counts failed logins and su attempts per user and sets an account lock of 30 minutes. The second added line specifies to lock accounts automatically after 5 failed login or su attempts (deny=5).

Mandatory

2.7 Implement Password Aging

- This can be done using the YaST tool or using system-wide configuration files. For YaST go to *User and Group Management*. When adding new users, the password expiration can be configured on a per-user basis.
- When using configuration files, the following options are available:
  1. In the file `/etc/login.defs` specify PASS_MAX_DAYS (maximum number of password validity, set this to 180), PASS_MIN_DAYS (minimum days a password cannot be changed by the user, set this to 1) and PASS_WARN_AGE (when to start the password reminder).
  2. In the file `/etc/default/useradd` specify INACTIVE (when to disable an account after password is expired) and EXPIRE (the date the user account expires).

Mandatory

2.8 Do not use rlogin, rsh and rcp

- Check if the rsh-server package is installed. The package can be removed with:

```
zypper rm rsh-server
```

Mandatory

2.9 Do not use telnet

- Check if the telnet-server package is installed. It can be removed with:

```
zypper rm telnet-server
```

Mandatory

2.10 Secure SSH

- Edit the file `/etc/ssh/sshd_config` and set the following options:

```
# Disable root login.
PermitRootLogin no
# Let SSH listen on the management VLAN interface only.
ListenAddress MGMT_VLAN_IP
# Enable privilege separation. This will only let a small part of the
# daemon run with root privileges.
UsePrivilegeSeparation yes
# Only use the more secure SSHv2 protocol.
Protocol 2
# No TCP forwarding and no X11 forwarding.
AllowTcpForwarding no
X11Forwarding no
# Check permissions of configuration files related to SSH on login.
# If this fails, the user won't be able to login.
StrictModes yes
# Disable host-based authentications.
IgnoreRhosts yes
HostbasedAuthentication no
RhostsRSAAuthentication no
# Ensure that the following line is commented out to disable sftp.
#Subsystem sftp /usr/lib/misc/sftp-server
# Set log level to be verbose.
LogLevel INFO
# Ensure usage of PAM
UsePAM yes
```

Mandatory

2.11 Secure use of the X Window System

- Remove the X Window System from the server if it is not needed. If it is needed, disable the use of host based or cookie based use of the X Window System. If X must be accessible from remote systems, use SSH to tunnel the session:

```
ssh -X remotehost
```

Mandatory

3 System Security

3.1 Install Updates on a Regular Basis

- To list all available patches, run the command:

```
zypper list-patches
```

- To apply patches on a SLES11 system, run the command:

```
zypper patch
```

- Configure a daily or weekly automatic online update:
    - Start YaST, go to *Software+Online Update Configuration* and activate *Automatic Online Update*.
    - Configure the update time to be *Daily* or *Weekly*. YaST has additional options to accept licenses automatically and to skip patches that require user interaction.

Mandatory

3.2 Check for Unused Services

- To review the installed services, list the services with the following command:

```
chkconfig --list | less
```

- To stop a service and then deactivate it, use the following commands:

```
rpcbind stop
chkconfig off rpcbind
```

The table in Section 4.5 lists common services of a SLES11 installation.
You can manually review the file `/etc/inittab` and the folder `/etc/init.d` for services that get started and are not needed.

Mandatory

3.3 Disable Default Services Accounts

- To lock accounts on the system, use the following command:

```
passwd <username> -l
```

- To replace the shell of a user, run the following command:

```
chsh -s /bin/false <username>
```

This has to be done for all service users.

Mandatory

3.4 Avoid Sensitive Data

Sensitive data that is not in productive use (e.g. copies of configuration files) must not be stored on the system. If sensitive data must be stored temporary, do not store this data in plaintext. Use a cryptographic storage.

1) Use zip and set a password to encrypt the zip file:

```
zip -e target.zip sources
```

2) Create an archive file and encrypt the contents with openssl. This can be done with the following command:

```
tar cz folder_to_encrypt | openssl enc -aes-256-cbc -e >
   out.tar.gz.enc
```

Decryption can be done with the following command:

```
cat out.tar.gz.enc  | openssl enc -aes-256-cbc -d
```

3) Create an archive file and encrypt it with PGP.

```
gpg --encrypt out.tar.gz
```

Delete the sources afterwards, so that only the encrypted container holds the archived files.

Optional

3.5 Secure Cron Jobs

- To allow the access to the configuration to root only, run the following commands:

```
rm -f /etc/cron.deny /etc/at.deny
echo root > /etc/cron.allow
echo root > /etc/at.allow
```

Mandatory

3.6 Check for Global Writable Paths in Path Environment Variables

- Check the files `/etc/bashrc` and `/etc/profile` for the following entries and delete them if they are found:

```
“.” and “..”
“;” not at the beginning or end
directories, that are world writeable or writable by users that
  are not in the administrative group.
```

Mandatory

3.7 Restrict mount

- Make sure that the file `/etc/fstab` includes no `user` attribute for all configured devices.
- Additionally add the options `nosuid` and `nodev` for removable media.

Optional

3.8 File System Types

- For partitioning use only file system types that allow access controls such as Ext2, Ext3 or ReiserFS. Do not use FAT32 as it is not possible to enforce access controls.

Mandatory

3.9 Session Timeout

- Configuration of automatic logout depends on the shell used. The following examples are valid for bash and csh:
  1. When using bash edit the file `/etc/bashrc` and add the following lines:
     ```
     TMOUT=900
     readonly TMOUT
     export TMOUT
     ```
  2. When using csh edit the file `/etc/csh.cshrc` and add the configuration option:
     ```
     set autologout=15
     ```

Optional

3.10 Find SUID/GUID Files

- To find all SUID and GUID files on the system that are owned by anyone, use the following command:

```
find / -perm -4000 -o -perm -2000 -print
```

- Review these files. A list of default files that carry the SUID bit after an installation can be found in Section 6. If the file does not need the SUID bit, remove it from the file with the following command:

```
chmod -s /path/file
```

Mandatory

3.11 Disable Core Dumps

- In the file `/etc/security/limits.conf` insert the following options:
  ```
  * soft core 0
  * hard core 0
  ```

Optional

3.12 Enforce Strict Permissions for /root

- Use the following command:

```
chmod -R 700 /root
```

Mandatory

3.13 Enforce Strict Permissions for /home

- Use the following commands:

```
chmod -R 700 /home
chmod a+x /home
```

Mandatory

3.14 Location of Home Directories

- Home directories should not be located on NFS shares they should be kept locally on the disk of the system.

Optional

3.15 Ensure Mail Distribution to Live Mail Accounts

- Edit the file `/etc/aliases` and set a forward rule for root.

Mandatory

3.16 Remove Unecessary Software Package

- Get a list of installed software packages by using one of the following commands:

```
zypper search -is
yast2 --install and export the list to a file
rpm -qa --last
```

- Find out dependencies for the:

```
rpm -e --test package_name
```

- If there are no dependencies and the package is not used, remove it:

```
rpm -e package_name
```

Mandatory

3.17 Regulary Check for World Readable Directories and Files

- Use the following commands:

```
find / -perm -0004 -type d -print
find / -perm -0004 -type f -print
```

Mandatory

3.18 Regulary Check for World Writable Directories and Files

- Use the following commands:

```
find / -perm -0002 -type d -print
find / -perm -0002 -type f -print
```

Mandatory

3.19 Set umask Globally

- Edit the files `/etc/login.defs` and `/etc/profile` and set the umask to 077.

Mandatory

3.20 Set up Log Files

- Use the following commands to set strict permissions on log files:

```
cd /var/log
/bin/chmod o-w boot.log* httpd/* mail* messages* news/* samba/*
/bin/chmod o-w wtmp
/bin/chmod o-rx boot.log* mail* messages*
/bin/chmod g-w boot.log* httpd/* mail* messages* samba/*
/bin/chmod g-rx boot.log* mail* messages*
/bin/chmod o-w httpd/ news/ samba/
/bin/chmod o-rx httpd/ samba/
```

- Edit the file `/etc/syslog.conf` and add the following two lines (use tabs as a separator):

```
*.warn;*.err          /var/log/syslog
kern.*        /var/log/kernel
```

Mandatory

3.21 Audit Log Files Regularly

- To find information on all kinds of problems, use `/var/log/messages`.
- For failed login attempts, successful login attempts and reboots check `/var/log/wtmp.1` with the command:

```
   last -f wtmp.1
```

- For additional login information use the file `/var/log/auth.log` and the command:

```
   lastlog
```

- The file `/var/log/zypp/history` holds information on the installation of additional software packages.

Mandatory

4 Network Security

4.1 Disable NFS

- If NFS is not needed, disable this service with the following command:

```
chkconfig nfs off
```

Mandatory

4.2 Disable SMB

- If SMB is not needed, disable this service with the following commands:

```
chkconfig smb off
 chkconfig nmb off
```

Mandatory

4.3 SMB Shares and Permissions

- Ensure no default shares are enabled on the system (e.g. root export for NFS or administrative shares for SMB). Additionally make sure that all shares have a minimal permission set on a need-to-know basis. To find available shares on a system, use the following commands:

```
smbclient -L <hostname>
showmount -a
```

Mandatory

4.4 Bind SSH to Management VLAN

- This can be achieved by using the SSH configuration specified in Section 2.10.

Optional

4.5 Packet Filtering

1) Allow incoming traffic only on necessary ports
2) Outgoing traffic only
   - For established connections
   - NTP
   - SLES updates
   - Mails
   - Connected subsystems required for service (e.g. database, file shares)
   - No global permit of outgoing traffic

- Start YaST and go to *Security and Users* and then *Firewall*. You can open the firewall for services under the category *Allowed Services* or you can manually configure the firewall under *Custom rules*.

Optional

5 APENDIX: LIST OF SERVICES

The next table gives a short overview of the functionality of the services and if it is recommended to activate it on start up or not. However, this list might be incomplete as your system might be customized to fit your needs. It is important to review the individual list of services on the system on a regular basis.

Service	Service Description	Recommendation	Potential Functional Implication
anacron	Anachronistic cron.	disable	When using cron instead, none.
atd	Schedule commands.	disable	When using cron instead, none.
auditd	Saves audit records generated by the kernel.	enable	Missing logs when disabled.
autofs	Controls the operation of the automount(8) daemons.	disable	Will break automount.
avahi-daemon	Implements networking services.	disable	Will break functionality like bonjour and zeroconf.
bluetooth	Provide Bluetooth.	disable	Will break Bluetooth functionality.
cron	Scheduled tasks.	enable	Will break scheduled tasks.
cups	Provides printing capabilities.	disable	Will break printing.
GPM	Provides support for mouse devices.	disable	Will break mouse usage.
haldaemon	Device database.	disable	Discovery and monitoring of devices may break.
hidd	Bluetooth HID.	disable	Will break usage of HID via Bluetooth.
hplip	Printing interface.	disable	Will break printing capabilities.
iptables	Packet filtering.	enable	If disabled, no packet filtering on the machine is possible.
kudzu	Device detection on boot.	disable	Will break device discovery during boot. Disable after first boot when all devices are known.
netfs	Network configuration through the file system.	disable	None.
nfs	Network file system.	disable	Will break NFS capabilities. Enable only if needed.
nfslock	NFS file locking.	disable	Will break locking of NFS.
ntpd	Network time.	enable	Time synchronization will break.
pcscd	Smart Card daemon.	disable	Will break the usage of smart cards.
Portmap / rpcbind	Provides RPC support.	disable	Disabling will break use of NFS.
rpcgssd	Used for NFS.	disable	Disabling will break use of NFS.
rpcidmapd	Used for NFS.	disable	Disabling will break use of NFS.
sendmail	Mail transport agent	enable	Disabling breaks mail forwarding.
syslog	System Logging.	enable	Disabling will break system logging.
xfs	X Font Server.	disable	Will break displaying of fonts.

6 APENDIX: LIST OF DEFAULT SUID FILES

Default SUID files:

- /bin/su
- /bin/eject
- /bin/umount
- /bin/mount
- /bin/ping6
- /bin/ping
- /sbin/unix2_chkpwd
- /sbin/mount.nfs
- /sbin/unix_chkpwd
- /proc
- /usr/bin/rcp
- /usr/bin/chsh
- /usr/bin/chfn
- /usr/bin/passwd
- /usr/bin/crontab
- /usr/bin/gpasswd
- /usr/bin/wall
- /usr/bin/at
- /usr/bin/rsh
- /usr/bin/chage
- /usr/bin/rlogin
- /usr/bin/get_printing_ticket
- /usr/bin/vlock
- /usr/bin/lppasswd
- /usr/bin/newgrp
- /usr/bin/write
- /usr/bin/sudo
- /usr/bin/fusermount
- /usr/bin/opiepasswd
- /usr/bin/opiesu
- /usr/bin/expiry
- /usr/sbin/utempter
- /usr/sbin/zypp-refresh-wrapper
- /usr/sbin/postqueue
- /usr/sbin/uuidd
- /usr/sbin/postdrop
- /usr/lib/PolicyKit/polkit-set-default-helper
- /usr/lib/PolicyKit/polkit-explicit-grant-helper
- /usr/lib/PolicyKit/polkit-read-auth-helper
- /usr/lib/PolicyKit/polkit-revoke-helper
- /usr/lib/PolicyKit/polkit-grant-helper
- /usr/lib/PolicyKit/polkit-grant-helper-pam
- /usr/lib64/pt_chown
- /lib64/dbus-1/dbus-daemon-launch-helper