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..............................................................................................................4

2 AUTHENTICATION ..........................................................................................................5
  2.1 Minimal Number of Users With Group root .................................................................5
  2.2 Check all Passwords are Shadowed..............................................................................5
  2.3 Use Strong Hashing Algorithm ..................................................................................5
  2.4 Implement Secure Password Policy ............................................................................5
  2.5 Ensure the Presence of one root User .........................................................................6
  2.6 Implement Account Lockout Policy .............................................................................6
  2.7 Implement Password Aging .......................................................................................6
  2.8 Do not use rlogin, rsh and rcp ..................................................................................6
  2.9 Do not use telnet ........................................................................................................6
  2.10 Secure SSH .............................................................................................................7
  2.11 Secure use of the X Window System .......................................................................7

3 SYSTEM SECURITY ........................................................................................................8
  3.1 Install Updates on a Regular Basis .............................................................................8
  3.2 Check for Unused Services .........................................................................................8
  3.3 Disable Default Services Accounts ............................................................................8
  3.4 Avoid Sensitive Data ..................................................................................................9
  3.5 Secure Cron Jobs ......................................................................................................9
  3.6 Check for Global Writable Paths in Path Environment Variables ...............................9
  3.7 Restrict Mount ..........................................................................................................9
  3.8 File System Types ......................................................................................................9
  3.9 Session Timeout .........................................................................................................10
  3.10 Find SUID/GUID Files ..............................................................................................10
  3.11 Disable Core Dumps ..................................................................................................10
  3.12 Enforce Strict Permissions for /root .........................................................................10
  3.13 Enforce Strict Permissions for /home .......................................................................10
  3.14 Location of Home Directories ..................................................................................11
  3.15 Ensure Mail Distribution to Live Mail Accounts ......................................................11
  3.16 Remove Unnecessary Software Package ..................................................................11
3.17  REGULAR CHECK FOR WORLD READABLE DIRECTORIES AND FILES .......................... 11
3.18  REGULAR CHECK FOR WORLD WRITABLE DIRECTORIES AND FILES .................. 11
3.19  SETUMASK GLOBALLY .................................................................................. 11
3.20  SET UP LOG FILES ...................................................................................... 12
3.21  AUDIT LOG FILES REGULARLY .................................................................... 12
4  NETWORK SECURITY .......................................................................................... 13
  4.1  DISABLE NFS ......................................................................................... 13
  4.2  DISABLE SMB ......................................................................................... 13
  4.3  SMB SHARES AND PERMISSIONS ............................................................ 13
  4.4  BIND SSH TO MANAGEMENT VLAN ....................................................... 13
  4.5  PACKET FILTERING .............................................................................. 13
5  APPENDIX: LIST OF SERVICES ....................................................................... 14
6  APPENDIX: LIST OF DEFAULT SUID FILES .................................................. 15
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:  

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.

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

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
### 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.

### 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).

### 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).

### 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
  ```

### 2.9 Do not use telnet

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

  ```
  zypper rm telnet-server
  ```
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
  ```

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
  ```
# 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.

## 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.

## 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.
### 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 czf 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.

### 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
```

### 3.6 Check for GlobalWritable 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 writable or writable by users that are not in the administrative group.

### 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.

### 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.
### 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
     ```

### 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
  ```

### 3.11 Disable Core Dumps

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

### 3.12 Enforce Strict Permissions for `/root`

- Use the following command:
  ```
  chmod -R 700 /root
  ```

### 3.13 Enforce Strict Permissions for `/home`

- Use the following commands:
  ```
  chmod -R 700 /home
  chmod a+x /home
  ```
### 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.  

### 3.15 Ensure Mail Distribution to Live Mail Accounts

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

### 3.16 Remove Unnecessary 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`

### 3.17 Regularly Check for World Readable Directories and Files

- Use the following commands:
  
  ```bash
  find / -perm -0004 -type d -print
  find / -perm -0004 -type f -print
  ```

### 3.18 Regularly Check for World Writable Directories and Files

- Use the following commands:
  
  ```bash
  find / -perm -0002 -type d -print
  find / -perm -0002 -type f -print
  ```

### 3.19 Set umask Globally

- Edit the files `/etc/login.defs` and `/etc/profile` and set the umask to 077.
### 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* samba/*
  /bin/chmod g-rwx boot.log* mail* messages* samba/*
  /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):
  ```plaintext
  *.warn;*.err    /var/log/syslog
  kern.*          /var/log/kernel
  ```

### 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` with the command:
  ```
  last -f wtmp
  ```
- 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.
4 NETWORK SECURITY

4.1 Disable NFS

- If NFS is not needed, disable this service with the following command:
  
  ```
  chkconfig nfs off
  ```

4.2 Disable SMB

- If SMB is not needed, disable this service with the following commands:
  
  ```
  chkconfig smb off
  chkconfig nmb off
  ```

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
  ```

4.4 Bind SSH to Management VLAN

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

4.5 Packet Filtering

- Allow incoming traffic only on necessary ports
- 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.
### Appendix: 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.

<table>
<thead>
<tr>
<th>Service</th>
<th>Service Description</th>
<th>Recommendation</th>
<th>Potential Functional Implication</th>
</tr>
</thead>
<tbody>
<tr>
<td>anacron</td>
<td>Anachronistic cron.</td>
<td>disable</td>
<td>When using cron instead, none.</td>
</tr>
<tr>
<td>atd</td>
<td>Schedule commands.</td>
<td>disable</td>
<td>When using cron instead, none.</td>
</tr>
<tr>
<td>auditd</td>
<td>Saves audit records generated by the kernel.</td>
<td>enable</td>
<td>Missing logs when disabled.</td>
</tr>
<tr>
<td>autos</td>
<td>Controls the operation of the automount(8) daemons.</td>
<td>disable</td>
<td>Will break automount.</td>
</tr>
<tr>
<td>avahi-daemon</td>
<td>Implements networking services.</td>
<td>disable</td>
<td>Will break functionality like bonjour and zeroconf.</td>
</tr>
<tr>
<td>bluetooth</td>
<td>Provide Bluetooth.</td>
<td>disable</td>
<td>Will break Bluetooth functionality.</td>
</tr>
<tr>
<td>cron</td>
<td>Scheduled tasks.</td>
<td>enable</td>
<td>Will break scheduled tasks.</td>
</tr>
<tr>
<td>cups</td>
<td>Provides printing capabilities.</td>
<td>disable</td>
<td>Will break printing.</td>
</tr>
<tr>
<td>GPM</td>
<td>Provides support for mouse devices.</td>
<td>disable</td>
<td>Will break mouse usage.</td>
</tr>
<tr>
<td>haldaemon</td>
<td>Device database.</td>
<td>disable</td>
<td>Discovery and monitoring of devices may break.</td>
</tr>
<tr>
<td>hidd</td>
<td>Bluetooth HID.</td>
<td>disable</td>
<td>Will break usage of HID via Bluetooth.</td>
</tr>
<tr>
<td>hlp</td>
<td>Printing interface.</td>
<td>disable</td>
<td>Will break printing capabilities.</td>
</tr>
<tr>
<td>iptables</td>
<td>Packet filtering.</td>
<td>enable</td>
<td>If disabled, no packet filtering on the machine is possible.</td>
</tr>
<tr>
<td>kudzu</td>
<td>Device detection on boot.</td>
<td>disable</td>
<td>Will break device discovery during boot. Disable after first boot when all devices are known.</td>
</tr>
<tr>
<td>netfs</td>
<td>Network configuration through the file system.</td>
<td>disable</td>
<td>None.</td>
</tr>
<tr>
<td>nfs</td>
<td>Network file system.</td>
<td>disable</td>
<td>Will break NFS capabilities. Enable only if needed.</td>
</tr>
<tr>
<td>nfslock</td>
<td>NFS file locking.</td>
<td>disable</td>
<td>Will break locking of NFS.</td>
</tr>
<tr>
<td>ntpd</td>
<td>Network time.</td>
<td>enable</td>
<td>Time synchronization will break.</td>
</tr>
<tr>
<td>pcsd</td>
<td>Smart Card daemon.</td>
<td>disable</td>
<td>Will break the usage of smart cards.</td>
</tr>
<tr>
<td>Portmap / rpcbind</td>
<td>Provides RPC support.</td>
<td>disable</td>
<td>Disabling will break use of NFS.</td>
</tr>
<tr>
<td>rpcgssd</td>
<td>Used for NFS.</td>
<td>disable</td>
<td>Disabling will break use of NFS.</td>
</tr>
<tr>
<td>rpclnmapd</td>
<td>Used for NFS.</td>
<td>disable</td>
<td>Disabling will break use of NFS.</td>
</tr>
<tr>
<td>sendmail</td>
<td>Mail transport agent</td>
<td>enable</td>
<td>Disabling breaks mail forwarding.</td>
</tr>
<tr>
<td>syslog</td>
<td>System Logging.</td>
<td>enable</td>
<td>Disabling will break system logging.</td>
</tr>
<tr>
<td>xfs</td>
<td>X Font Server.</td>
<td>disable</td>
<td>Will break displaying of fonts.</td>
</tr>
</tbody>
</table>
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/policykit-1/policykit-1
- /lib64/dbus-1/dbus-daemon-launch-helper