Securing Your System:

Security Hardening Techniques for SUSE® Linux Enterprise Server 12

Craig Gardner
Software Engineer
SUSE
Craig.Gardner@suse.com
Overview

What? and Why?

New for SUSE Linux Enterprise Server 12

Architecture Dive: Inspection

Tools
What? and Why?

What Should “Security” Be?
What is Security?

Good software...

...does what you expect it to do, and does it well.

Secure software...

...is good software that does nothing else.
What to Do?

Software contains errors

• Malfunctions
• Crashes
• Downtime
• Security Vulnerabilities

Data loss and disclosure, identity theft, system abuse, privilege transition

Apply Maintenance Updates

Nowhere is this more evident than with POODLE and SHELLSHOCK
A Closer Look

Administration

Purpose, responsibilities, mandates, team play

Infrastructure

Network and network boundaries, services

Security Zones

Assets and protection, domains, domain transitions

Systems

Deployment, installation, configuration (hardening), monitoring, maintenance, auditing
A Closer Look

Administration
- Purpose, responsibilities, mandates, team play

Infrastructure
- Network and network boundaries, services

Security Zones
- Assets and protection, domains, domain transitions

Systems
- Deployment, installation, configuration (hardening), monitoring, maintenance, auditing
Security Considerations for SUSE Linux Enterprise Server 12
Security Standards Compliance

• Upcoming Common Criteria Certification
  - EAL4+ expected ("under evaluation")

• Upcoming FIPS 140-2 validation
  - OpenSSL
  - OpenSSH client and server
  - Strongswan
  - Kernel Crypto API
  - libgcrypt
SUSE Linux Enterprise 12
Changes Related to Security

• SCC Registration
  - 2nd action after accepting the license
  - Important for getting security updates immediately
  - Updates from SCC, SMT, or Manager

• No more Stage 2 installation
  - “Create New User” and root password in stage 1
  - No more blowfish; default is sha512
  - Simplification; Flexibility
SUSE Linux Enterprise 12
Changes Related to Security

• TLS 1.2 support for all services
• Grub2
• UEFI Secure Boot
• SELinux returns
• systemd
• journald and journalctl
  – Tamper resistant local logging
SUSE Linux Enterprise 12
Changes Related to Security

Built Upon Proven SUSE Linux Enterprise 11
Inspection, Configuration, Hardening
Screenshots
Registration

SUSE Linux Enterprise Server 12

Please enter a registration or evaluation code for this product and your User Name/E-mail address from the SUSE Customer Center in the fields below. Access to security and general software updates is only possible on a registered system.

If you skip product registration now, remember to register after installation has completed.

E-mail Address

Registration Code

Local Registration Server...

Skip Registration

16
### Network Settings

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
<th>Device</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet Card 0</td>
<td>DHCP</td>
<td>eth0</td>
<td></td>
</tr>
</tbody>
</table>

**Ethernet Card 0**

- **MAC**: 52:54:00:53:30:63
- **BusID**: virtio0

- Device Name: eth0
- Started automatically at boot
- IP address assigned using DHCP
Create New User

User's Full Name
Username
Password
Confirm Password

☐ Use this password for system administrator
☐ Receive System Mail
☐ Automatic Login

Summary
The authentication method is local /etc/passwd.
The password encryption method is SHA-512.

Change...
Expert Settings

Authentication Method
- Local (/etc/passwd)

Password Encryption Type
- DES
- MD5
- SHA-256
- SHA-512
Password for the System Administrator "root"

Do not forget what you enter here.

Password for root User

Confirm Password

Test Keyboard Layout
Installation Settings

Click a headline to make changes.

**Software**
- Product: SUSE Linux Enterprise Server 12
- Patterns:
  - Help and Support Documentation
  - Base System
  - AppArmor
  - 32-Bit Runtime Environment
  - Minimal System ( Appliances)
  - GNOME Desktop Environment
  - X Window System
- Size of Packages to Install: 2.5 GiB

**Booting**
- Boot Loader Type: GRUB2
- Status Location: /dev/vda2 (""")
- Change Location:
  - Do not install bootcode into MBR (install)
  - Install bootcode into "/" partition (do not install)

**Firewall and SSH**
- Firewall will be enabled (disable)
- SSH port will be blocked (open)
- SSH service will be enabled (disable)

**Kdump**
- Kdump status: disabled

**Default systemd target**
- Graphical mode

**System**
- System and Hardware Settings

Export Configuration

Help | Release Notes... | Abort | Back | Install
Boot Loader Settings

Boot Code Options

Boot Loader
GRUB2

Kernel Parameters

Boot Loader Location
☐ Boot from Master Boot Record
☒ Boot from Root Partition

Bootloader Options

Distributor
SLES12

☒ Set active Flag in Partition Table for Boot Partition

☒ Write generic Boot Code to MBR

Boot Loader Installation Details

Help  Release Notes...  OK  Cancel
## Boot Loader Settings

### Boot Code Options

**Timeout in Seconds**

- 8

**Default Boot Section**

- 0

### Bootloader Options

- **Probe Foreign OS**
- **Hide Menu on Boot**

**Protect Boot Loader with Password**

- **Password**
- **Retype Password**

---

### Buttons

- **Help**
- **Release Notes...**
- **Cancel**
- **OK**

---

24
### Performing Installation

#### Media

<table>
<thead>
<tr>
<th>Type</th>
<th>Remaining</th>
<th>Packages</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>2.257 GB</td>
<td>1387</td>
<td></td>
</tr>
<tr>
<td>SLES12-12-0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium 1</td>
<td>2.257 GB</td>
<td>1387</td>
<td></td>
</tr>
</tbody>
</table>

**Actions performed:**

- Installing libevdev2-1.2-1.7.x86_64.rpm (installed size 99.5 KiB)
- Installing libestr0-0.1-9-1.54.x86_64.rpm (installed size 14 KB)
- Installing libencav0-0.1-1.15-1.65.x86_64.rpm (installed size 203.6 KiB)
- Installing libelfl0-0.1-158-3.200.x86_64.rpm (installed size 86.5 KB)
- Installing libelfl0-0.8.13-18.64.x86_64.rpm (installed size 104.2 KiB)
- Installing libdvm4-1.0-0.172.85-186_64.rpm (installed size 162 KB)
- Installing libdrm2-2.4-52-2.12-x86_64.rpm (installed size 46.5 KiB)
- Installing libdrmconf0-1.3-1.82.x86_64.rpm (installed size 26.6 KB)
- Installing libdm0-2.2.12.1-16.x86_64.rpm (installed size 79.3 KB)
- Installing libdhash1-0.4-3.1-18.15.x86_64.rpm (installed size 14.2 KiB)
- Installing libdbus-1-3.1-8.8-1.12-x86_64.rpm (installed size 283.9 KB)
- Installing libcpupower0-3.13-5.4.x86_64.rpm (installed size 18.4 KB)
- Installing libcom_err2-1.42.11-1.17.x86_64.rpm (installed size 41.0 KiB)

**Installing Packages...** (Remaining: 2.257 GB, 1387 packages)

- 100%

- 18%
SLES12

Advanced options for SLES12

Start bootloader from a read-only snapshot
## Network Settings

### Global Options

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
<th>Device</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet Card 0</td>
<td>DHCP</td>
<td>eth0</td>
<td></td>
</tr>
</tbody>
</table>

**Ethernet Card 0**

**MAC:** 52:54:00:53:30:63  
**BusID:** virtio0  

- Device Name: eth0  
- Started automatically at boot

### Add/Delete/OK/Cancel/Help

- **Add**
- **Edit**
- **Delete**
- **Cancel**
- **OK**
YaST2 - Network Settings

Hostname and Domain Name

Hostname

Domain Name

- Change Hostname via DHCP
- Assign Hostname to Loopback IP

Modify DNS Configuration

- Use Default Policy

Name Servers and Domain Search List

Name Server 1

Name Server 2

Name Server 3

Domain Search

Help

Cancel

OK

MirrorMode

Administration

Applications · Places · [root@li... YaST2 · Administr... YaST2 -... YaST2 -... 1 / 4 Fri 06:18
Network Settings

Global Options

General Network Settings

Network Setup Method

Wicked Service

IPv6 Protocol Settings

Enable IPv6

DHCP Client Options

DHCP Client Identifier

Hostname to Send

AUTO

Change Default Route via DHCP

Help

Cancel

OK
YaST Security Center and Hardening
<table>
<thead>
<tr>
<th>Security Setting</th>
<th>Status</th>
<th>Security Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use magic SysRq keys</td>
<td>Configure</td>
<td>✓</td>
</tr>
<tr>
<td>Use secure file permissions</td>
<td>Configure</td>
<td>✗</td>
</tr>
<tr>
<td>Remote access to the display manager</td>
<td>Disabled</td>
<td>✓</td>
</tr>
<tr>
<td>Write back system time to the hardware clock</td>
<td>Unknown</td>
<td>✗</td>
</tr>
<tr>
<td>Always generate syslog message for cron scripts</td>
<td>Unknown</td>
<td>✗</td>
</tr>
<tr>
<td>Run the DHCP daemon in a chroot</td>
<td>Unknown</td>
<td>✗</td>
</tr>
<tr>
<td>Run the DHCP daemon as dhcp user</td>
<td>Unknown</td>
<td>✗</td>
</tr>
<tr>
<td>Remote root login in the display manager</td>
<td>Disabled</td>
<td>✓</td>
</tr>
<tr>
<td>Remote access to the X server</td>
<td>Disabled</td>
<td>✓</td>
</tr>
</tbody>
</table>
What “Security Center” Does In the Background

- Run another YaST module
- Change settings in files in /etc/sysconfig
- Modify configuration files directly
Architecture and Design
Schematical Overview:

O/S Kernel + Userland

- Human
  - system calls
  - device files
  - proc, sys

- Libraries
  - VFS
  - ext3, reiserfs, vfat, NFS
  - SCSI, sd, sg
  - (mount table)
  - TCP, ICMP, UDP
  - IP
  - eth0, ppp0
  - BT, USB, Serial
  - PCI

- Shell
  - User-land
    - processes
  - Kernel-land
    - drivers, kernel threads
  - KDE
  - UDP, ICMP, TCP
  - eth0, ppp0
  - BT, USB, Serial
  - PCI

- Physics/Electronics
Inspection

Approach your system as if you were an attacker:

network  ports  services  processes  files  kernel
Network

Interface addresses: all interfaces enabled and conn.?
Routing setup: IP-forwarding on/off?
Netfilter rules: active, any?
maintenance ARP table records
Other tweakables:
txqueuelen, mtu
ICMP replies, ICMP redirects
ECN
slow-start
Ports

port scan: Open TCP and UDP sockets
    nmap -sS -v -O ip.address.on.network

Compare to output of
    netstat -anpl

Discrepancies...?
(Not all services are userland process bound! (knfsd))

Watch out for UDP sockets!
Services

Disable all services that are not needed, permanently

Remove the runlevel symlinks (insserv -r <servicename>)

Kill the servers (rcapache2 stop)

Verify if they the services are really dead!

Remove the packages from the system?
Processes

Get to know all processes on your system in person...

```
ps faux

rpm -qfi /usr/sbin/nscd
```

...and deactivate whatever is not needed running.
Files

Permissions: /etc/permissions* from /etc/sysconfig/security
Use chkstat -set <permissions file> or SuSEconfig

find / /usr ... -mount -type f ( -perm +2000
   -o -perm +4000 ) -ls

PolKit and default rules in /etc/polkit-default-privils.*

Integrity measures: AIDE, RPM

   maintain offsite RPM database backup for rpm -Va

   maintain offsite AIDE database backup

   mount options: /etc/fstab, /proc/mounts
Kernel: Use AppArmor!

Example profile: dhcp daemon

```
#include <tunables/global>

/usr/sbin/dhcpd {
    #include <abstractions/base>
    #include <abstractions/nameservice>
    
capability dac_override,
capability net_bind_service,
capability net_raw,
capability setgid,
capability setuid,
capability sys_chroot,
/db/dhcpd.leases* lrw,
/etc/dhcpd.conf r,
/etc/hosts.allow r,
/etc/hosts.deny r,
/usr/sbin/dhcpd rmix,
/var/lib/dhcp/dhcpd.leases* rwl,
/var/lib/dhcp/etc/dhcpd.conf r,
/var/run/dhcpd.pid wl,
}
```
Kernel: We support SELinux (again!)

• Many government contracts require SELinux

• A lot the same, but different

• Starts everything off with high protection settings (MAC = Mandatory Access Control)

SUSE Linux Enterprise 12 brings back the choice
Tools
Tools

The YaST Security Center

The YaST AppArmor profile generator

Integrity: AIDE and RPM

Port Scanner: nmap

Vulnerability scanner: openSCAP + OVAL
More Tools, More Considerations

System Monitoring: Nagios, Ganglia

Syslog Monitoring: logwatch, Sentinel

Vulnerability Scanner: openvas, tripwire

Configuration Management: puppet, chef, cfengine, or SUSE Manager
Unpublished Work of SUSE. All Rights Reserved.
This work is an unpublished work and contains confidential, proprietary and trade secret information of SUSE. Access to this work is restricted to SUSE employees who have a need to know to perform tasks within the scope of their assignments. No part of this work may be practiced, performed, copied, distributed, revised, modified, translated, abridged, condensed, expanded, collected, or adapted without the prior written consent of SUSE. Any use or exploitation of this work without authorization could subject the perpetrator to criminal and civil liability.

General Disclaimer
This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. SUSE makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. The development, release, and timing of features or functionality described for SUSE products remains at the sole discretion of SUSE. Further, SUSE reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All SUSE marks referenced in this presentation are trademarks or registered trademarks of Novell, Inc. in the United States and other countries. All third-party trademarks are the property of their respective owners.