System Hardening

From concepts into details

Marcus Meissner
Technical Project Manager Security
meissner@suse.com

Craig Gardner
Engineering Lead Storage
cgardner@suse.com

Hardening – Top Down

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.

Hardening – Ensuring this for your operating system

Hardening at different levels

High

- Purpose
- Lifetime
- Capabilities

Midrange

- Network location
- Compute location
- Virtual / Physical / Container
- HA / Cloud / GEO

Lowlevel

- Checklists

Hardening starting points

Building new installations

Auditing existing installations

Contributing Decision Factors

Administration

- Purpose, Responsibilities, Mandates, Team Play

Infrastructure

- Network and network boundaries, services

Security Zones

- Assets and protection, domains, domain transitions

Systems

- Deployments, Installation, Configuration (hardening), Monitoring, Maintenance, Decomissioning

System Deployment Philosophies

Manual Installation

- Install once and keep running

Automated Deployments

- Install and redeploy at need

Containers

- Running third party supplied operating system parts

System Lifetime Philosophies

- Static
  - Single tasks for fixed service lifetime
- Dynamic
  - add / remove software / users over machine lifetime

Installation and Setup

Installation

Packages

- Services & administrative
- From which vendor (SUSE, third party)

Users

- Service and administrative users

Network Interfaces

- Match designed network location

Data

- Only data needed by the services
- No unneeded mounts of company wide shares etc.

Document decisions

Packages

Start with minimal set

Add only required packages on top

Manual

- zypper, yast2, ...

Salt

- salt.pkg module

Docker

- docker scripts

System Settings

Manual

- Editors
- Yast2 modules, including yast2 security module
- Management software

Automated Deployments / Containers

- Codify rules into the manifests / docker scripts

Secure setup

Maintenance

Lifetime concerns

Apply Maintenance Updates

- Actually single most important
- Not just the SUSE Updates, but for all third party software

Monitoring

- Not just for full disks or dieing processes
- Logfile monitoring for security incidents
  - Logwatch

Backup and Recovery strategies

  - Rear backup tool

Auditing – more structured logging

Linux Audit Framework (LAF)

Ability to monitor

- User management
- User access
- File / Directory access
- Systemcalls

Local storage or delivery to remote agents

Lifetime changes

Cryptographic changes

- Phasing out protocols
  - RC4, Triple DES, Blowfish
- SSL certificate management
- SSH key management

Protocol changes

- Disabling SSH protocol 1, SSL v2 , v3

Documented in SUSE TIDs, external guidelines, by auditor rules

Shipped in SUSE package default configuration files

Lifetime purpose changes

Static systems

- Not applicable

Dynamic Systems

- Document change choices same as install choices
- Service Phase-In and Phase-Out processes
- Same for Users and Data on machines

User Management

Adding users

Removing users

Password policies

- Acceptable password rules
- Change times
- Failed logins

Centralized user management

Two Factor Auth

Account hardening

PAM - the Linux Authentication Module standard

- /etc/pam.d/<service> configuration files
- /etc/pam.d/common-* as common includes for services

Tools

- Yast Users module
- Useradd / userdel / usermod
  - Creation / modification of users
- pam-config
  - tool to edit the SUSE PAM configurations
  - Enable / disable / configure PAM modules

Account hardening

- User Creation defaults & Password Aging
  - /etc/login.defs
- Failed login handling
  - pam_tally2
- Password strength checking
  - pam_pwcheck

Decomissioning

Confidential data on harddisks

Check pointers to the machine from the outside

- IP address ACLs

Mark in documentation as “decomissioned”

The attacker look – Auditing installations

Inspection

Approach your system as if you were an outside attacker

- Network
- Ports
- Services
- Processes
- Files
- Kernel

Network

Port scan from outside:

- nmap -sS -v -O ip.address.on.network
- Wireshark / tcpdump

Looking at system ports inside

- Netstat -anpl

Services

SUSE enables only a minimal set of services by default

Listing, Enabling and Disabling services:

- Chkconfig (works for sysvinit and systemd)
- systemctl (status, enable, disable) service.name
- yast2 services module

Processes

Not all processes are covered by service files.

- ps aufx

Check processes that sound unknown where they belong

- rpm -qf /usr/sbin/nscd

Files

- setuid and setroot binaries are tracked and recorded in the permissions framework
  - /etc/permissions.*
- “chkstat –system” to restore the recorded settings
- Use seccheck to find non-tracked ones

Integrity checking using AIDE and RPM

- RPM for installed packages (rpm -V)
- AIDE for other files
  - Keep database offline

Protect using AppArmor

AppArmor gives application confinement

Perfect for services with limited variability

Easy learning curve

Generate profiles either using commandline or yast2

Checklists

Hardening Guides

Hardening Guide in SLES Documentation

Hardening Guide specific to PCI-DSS requirements

DISA STIG for SUSE Linux Enterprise Server

- US Military approved hardening guidelines

And more …

SCAP (Security Content Automation Protocol)

Components:

- XCCDF: Extensible Configuration Checklist Description Format
- OVAL: Open Vulnerability and Assessment Language

Automated testing and optional fixing

Currently work in progress at SUSE

Recommended Sessions

BOV92129 - SUSE Security Certifications

TUT91122 - SUSE Linux Security Essentials

BOV89033 - Using SUSE Manager's Audit capabilities to improve efficiency and security

TUT83954 - Improve security using 2 Factor Authentication with SSSD via LDAP, OAuth, Centralized SSH Keys and Sudoers