Security Audit with Spacewalk & OpenSCAP

Šimon Lukašík

Milan Zázrivec

Martin Preisler

Fudcon 2012, Paris

Agenda

- Introduction of SCAP, OpenSCAP and Spacewalk.
- Spacewalk and OpenSCAP Integration.
- Demo.
- How to apply SCAP on GNU/Linux?

What is SCAP?

- Security Content Automation Protocol.
- Provides vendor neutral way of expressing security policy.
- U.S. Government Standard (NIST, MITRE).
- Encompasses several underlying standards.
  - OVAL: Open Vulnerability and Assessment Language – a language for vulnerability assessment.
  - XCCDF: Extensible Configuration Configuration Checklist Description Format – a language to express, organize, and manage checklists (your security guidance).
- What do I need to implement SCAP in my organization?
  - A security guidance in form of SCAP.
    (There are public guidances for GNU/Linux)
  - A scanner which implements SCAP.

OpenSCAP

- http://www.open-scap.org/
- Open-source implementation of SCAP.
- Encompasses:
  - libopenscap library
  - `oscap` command-line tool (the scanner)
  - Example SCAP content.
- Script Check Engine (SCE)
  - Similar to OVAL in its purpose.
  - Enables users to use scripting languages instead of OVAL for writing checks.
  - Non-standardized extension.

Evaluating SCAP content

- Scanning a single machine:
  - oscap - command line tool.
  - scap-workbench - GUI tool.
  - openscap API
- Doesn’t scale with increasing number of machines.
- No aggregation of results.

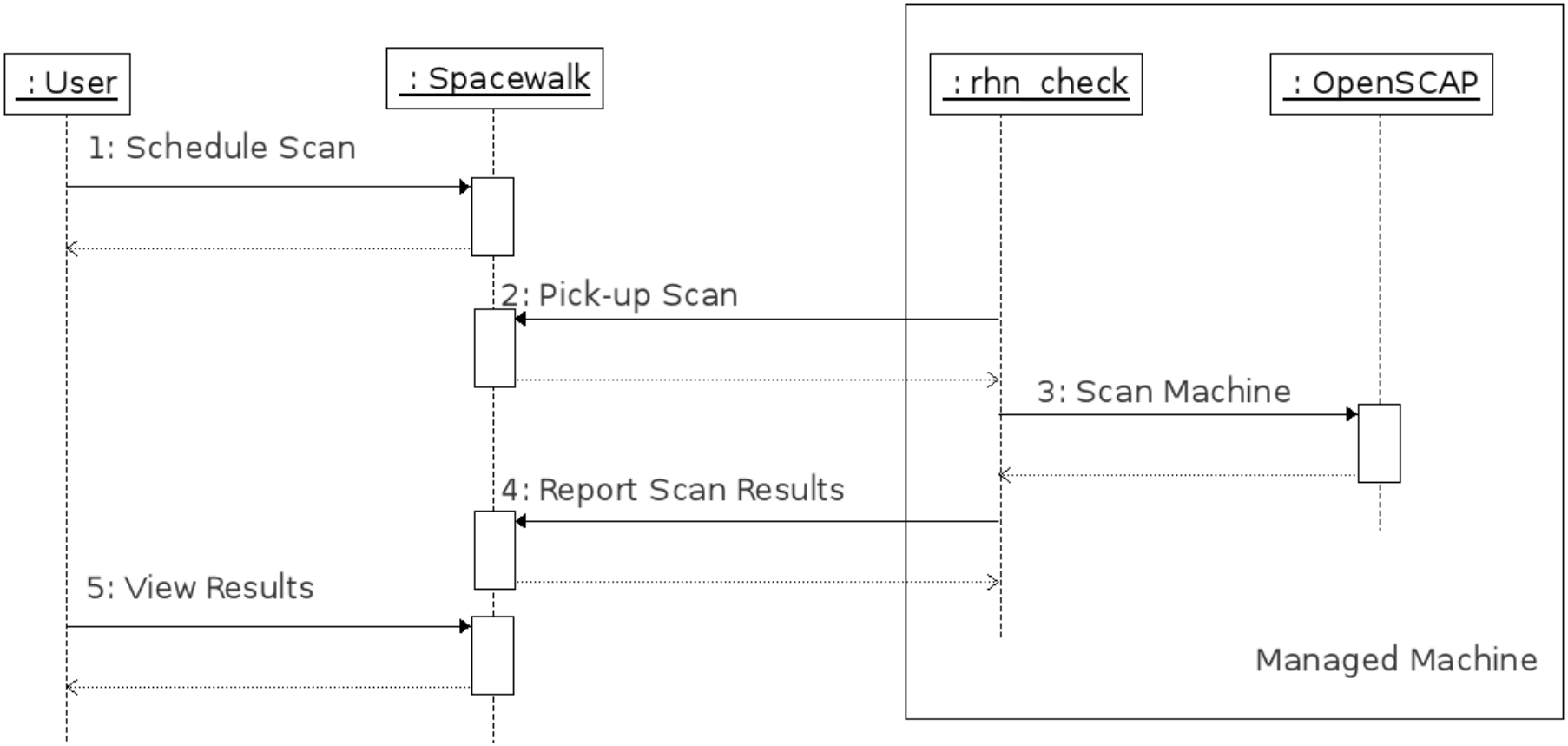
Existing content

- USGCB – Official Government Guidance for Red Hat Enterprise Linux 5.
- SCAP Security Guide – Community Guidance for Red Hat Enterprise Linux 6.
- DISA STIG

What is Spacewalk?

- http://spacewalk.redhat.com/
- Open-source enterprise-class system management system.
- Web based, running on either PostgreSQL or Oracle DB.
- Manages complete system life-cycle.
- Supports Fedora, Debian and OpenSuSE clients and their derivates.
- Provisioning, Package and Patch Management, Configuration, Monitoring, Virtual Guests Management, Hardware Inventory.
- Recently added Security Audit.

SCAP Scan through Spacewalk



- Demo.

Thank You.