Automate Security Testing and System Compliance
An introduction to SCAP / STIG / SUSE Manager security automation.

Alexander Bergmann
Security Engineer
SUSE/abergmann@suse.com
Automate Security Testing and System Compliance

Agenda

- Introduction to SCAP
- Introduction to STIG
- SUSE STIG Automation
- Demo Time
- What’s next?
Introduction to SCAP
What is SCAP?

The Security Content Automation Protocol is a multi-purpose framework of specifications that supports automated configuration, vulnerability and patch checking, technical control compliance activities, and security measurement.

- Automated
  - vulnerability management and measurement
  - policy compliance evaluation
- OpenSCAP has received a NIST certification for SCAP 1.2.
What is SCAP?

SCAP uses several formats and enumerations

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>XCCDF</td>
<td>Extensible Configuration Checklist Description Format</td>
<td>XML format specifying security checklists, benchmarks and configuration documentation.</td>
</tr>
<tr>
<td>OVAL</td>
<td>Open Vulnerability and Assessment Language</td>
<td>XML format for testing the presence of a specific machine state.</td>
</tr>
<tr>
<td>CVE</td>
<td>Common Vulnerabilities and Exposures</td>
<td>Reference IDs for publicly known security vulnerabilities.</td>
</tr>
<tr>
<td>CVSS</td>
<td>Common Vulnerability Scoring System</td>
<td>Standard for assessing the severity of security vulnerabilities.</td>
</tr>
<tr>
<td>CPE</td>
<td>Common Platform Enumeration</td>
<td>Structured naming scheme for information technology systems, software, and packages.</td>
</tr>
<tr>
<td>CCE</td>
<td>Common Configuration Enumeration</td>
<td>Unique identifiers to security-related system configuration issues.</td>
</tr>
</tbody>
</table>
What is SCAP?

- **Vulnerability Management**
- **Configuration Management**
- **Asset Management**

SCAP

- **CVE**
- **CVSS**
- **OVAL**
- **CPE**
- **CCE**
- **XCCDF**
XCCDF

Extensible Configuration Checklist Description Format

- Development led by NIST
- XML format
- Automated compliance testing and scoring
  - Security checklists
  - Benchmarks
  - Configuration documentation
OVAL

Open Vulnerability and Assessment Language

- Moderated by the Center for Internet Security (CIS)
- XML format
- Representing system information and reporting results
- Reliable and reproducible
Open Vulnerability and Assessment Language

- Platform dependent (Linux, Windows, etc.) and independent tests.

**Independent**
- family_test
- filehash58_test
- ldap57_test
- sql57_test
- textfilecontent54_test
  ...

**Linux**
- partition_test
- rpminfo_test
- selinuxboolean_test
- systemdunitdependency_test
- dpkginfo_test
  ...

- All tests have an _object and _state element.
CPE

Common Platform Enumeration

• Maintained by NIST / NVD
• Updated online CPE dictionary XML file.
• Standardized naming scheme for IT products.
• cpe:/{part}:{vendor}:{product}:{version}:{update}:{edition}:{language}

Examples:
cpe:/o:suse
cpe:/o:suse:linux_enterprise_server:12
cpe:/o:opensuse:leap:15.0
cpe:/a:open-scap:oscap
cpe:/h:hp:laserjet_p4014
SCAP component interaction (simplified)

- SCAP
- XCCDF
- OVAL
- System Settings
XCCDF Tailoring

```xml
<Profile id="stig">
    <select rule="1" ✔>
    <select rule="2" ✔>
    <select rule="3" ✔>
    <select rule="4" ✗>
        <refine-value "logins" selector="3"/>
    </select>
</Profile>

<Tailoring>
    <Profile id="stig_new" extends="stig">
        <select rule="2" ✗>
            <refine-value "logins" selector="2"/>
        </select>
    </Profile>
</Tailoring>
```
DataStreams

- XML format that packs other SCAP components into a single file.
- Useful when distributing SCAP content for example over the web.
Introduction to STIG
What is STIG?

Security Technical Implementation Guide

- **System hardening**
  - prevent system access (physically/network)
  - defined maintenance processes / patching
  - might cover configuration settings

- **Required to be able to connect to DoD networks**

- **Approved and published by the Defense Information Systems Agency (DISA)**

- **Also used in the non government sector**
SLES 12 STIG

- SUSE Linux Enterprise Server (SLES) 12 STIG
  - Version 1, Release 1
  - Officially published September 2018
- 204 Rules
- Available at DISA web page: https://iase.disa.mil/stigs/os/unix-linux/
The SUSE operating system must be a vendor supported release.

A SUSE operating system release is considered "supported" if the vendor continues to provide security patches for the product. With an unsupported release, it will not be possible to resolve security issues discovered in the system software.

Verification:

1. Check the system name and version using the command:
   ```
   # cat /etc/os-release
   NAME="SLES"
   VERSION="12"
   ```

2. Identify the current end of life for SUSE Linux Enterprise SUSE operating system release 12 which is 31 Oct 2024.

   - If the release is not supported by the vendor, this is a finding.

   - Upgrade the SUSE Linux Enterprise SUSE operating system to a version supported by the vendor. If the system is not registered with the SUSE Customer Center, register the system against the correct subscription. If the system requires Long Term Service Pack Support (LTSS) support, obtain the correct LTSS subscription for the system.

   - Severity: CAT I
SLES 12 STIG

- DISA STIG Viewer
SLES 12 STIG

• DISA STIG Viewer
SLES 12 STIG

- DISA STIG Viewer
SLES 12 STIG Automation

- Using “ComplianceAsCode” project framework
- Publicly hosted at github.com
- Project status:
  - ~90% of the rules are implemented with automated remediation.
Demo Time
<table>
<thead>
<tr>
<th>Title</th>
<th>Rule</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure Users Re-Authenticate for Privilege Escalation - sudo !authenticate</td>
<td>xccdf_org.ssgproject.content_rule_sudo_remove_no_authenticate</td>
<td>pass</td>
</tr>
<tr>
<td>Ensure Users Re-Authenticate for Privilege Escalation - sudo NOPASSWD</td>
<td>xccdf_org.ssgproject.content_rule_sudo_remove_nopasswd</td>
<td>pass</td>
</tr>
<tr>
<td>Ensure zypper Removes Previous Package Versions</td>
<td>xccdf_org.ssgproject.content_rule_clear_components_post_updating</td>
<td>fail</td>
</tr>
<tr>
<td>Ensure gpgcheck Enabled In Main zypper Configuration</td>
<td>xccdf_org.ssgproject.content_rule_gpgcheck_globally_activated</td>
<td>pass</td>
</tr>
<tr>
<td>Ensure Software Patches Installed</td>
<td>xccdf_org.ssgproject.content_rule_security_patches_up_to_date</td>
<td>notchecked</td>
</tr>
<tr>
<td>Disable the usb-storage Kernel Module</td>
<td>xccdf_org.ssgproject.content_rule_blacklist_usb-storage</td>
<td>fail</td>
</tr>
</tbody>
</table>
--- Starting Remediation ---

Title Create Warning Banners for All FTP Users
Rule xccdf_org.ssgproject.content_rule_ftp_present_banner
Result fixed

Title Configure System to Forward All Mail For The Root Account
Rule xccdf_org.ssgproject.content_rule_postfix_clientConfigureMailAlias
Result fixed

Title Configure Time Service Maxpoll Interval
Rule xccdf_org.ssgproject.content_rule_chronyd_or_ntpd_set_maxpoll
Result fixed

Title Disable Compression Or Set Compression to delayed
Rule xccdf_org.ssgproject.content_rule_sshd_disable_compression
Result fixed

Title Disable SSH Access via Empty Passwords
Rule xccdf_org.ssgproject.content_rule_sshd_disable_empty_passwords
Result fixed

Title Disable SSH Root Login
Rule xccdf_org.ssgproject.content_rule_sshd_disable_root_login
Result fixed
OpenSCAP: DISA STIG Viewer output

```
#> ls -lh
total 6.2M
-rw-r--r-- 1 root root 6.0M Mar 25 12:05 ssg-sle12-ds.xml
-rw-r--r-- 1 root root 187K Mar 25 18:09 disa.xml
#>
```
OpenSCAP: DISA STIG Viewer output
# Reference Manual

## 7.4.5.2 Systems Audit Page

### 7.4.5.2.1 List Scans

- **P** Number of checks that passed.
- **F** Number of checks that failed.
- **E** Number of errors that occurred during the scan.
- **U** Unknown.
- **N** Not applicable to the machine.
- **K** Not checked.
- **S** Not Selected.
- **I** Informational.
- **X** Fixed.
What’s next?
What’s next?

- **SUSE Linux Enterprise Server STIG**
  - Update and refinement SLES 12 Version
  - Customer ready automated version
  - SUSE Linux Enterprise Server 15 STIG

- **ComplianceAsCode extension**
  - SUSE Security and Hardening Guide
  - Implementation of PCI-DSS rules
What’s next?

YOUR INPUT IS NEEDED!
What’s next?

security@suse.com