Encryption and Security

LUKS for NBDE

SCAP Customization and Remediation

Environment Setup

- Workstation (Graphical Workstation/SCAP Workbench/Ansible System)
- servera (Clevis/LUKS encrypted drive Server)
- serverb (Tang Server 1)
- serverc (Tang Server 2 and SCAP Target System)
- serverd (Tang Server 3)

Terminology

LUKS (Linux Unified Key Setup): LUKS is the standard for Linux hard disk encryption. By providing a standard on-disk-format, it does not only facilitate compatibility among distributions, but also provides secure management of multiple user passwords. LUKS stores all necessary setup information in the partition header, enabling to transport or migrate data seamlessly.

https://gitlab.com/cryptsetup/cryptsetup/blob/master/README.md

NBDE (Network Bound Disk Encryption): Allows the user to encrypt root volumes without requiring you to manually enter a password when the operating system is restarted

https://blog.cloudpassage.com/2017/12/21/network-bound-disk-encryption-red-hat-linux-7/

Terminology

Clevis: Clevis is a plugable framework for automated decryption. It can be used to provide automated decryption of data or even automated unlocking of LUKS volumes.

Tang: Server side service that Clevis connects to in order to receive a decryption key and allow the NBDE service connection.

https://rhelblog.redhat.com/2018/04/13/an-easier-way-to-manage-disk-decryption-at-boot-with-red-hat-enterprise-linux-7-5-using-nbde/#more-4351

Terminology

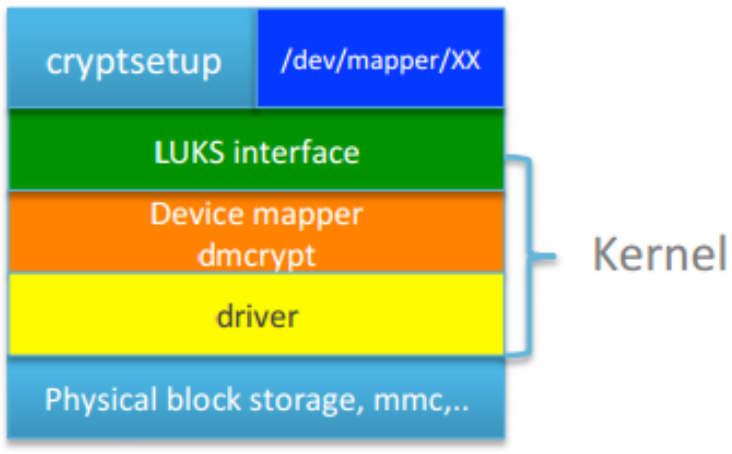
SCAP: The Security Content Automation Protocol (SCAP) is a method for using specific standards to enable the automated vulnerability management, measurement, and policy compliance evaluation of systems deployed in an organization, including e.g., FISMA compliance. The National Vulnerability Database (NVD) is the U.S. government content repository for SCAP. An example of an implementation of SCAP is OpenSCAP

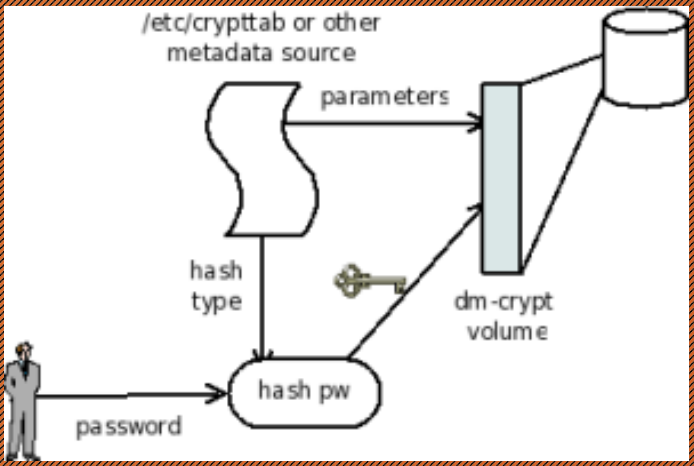
https://csrc.nist.gov/projects/security-content-automation-protocol

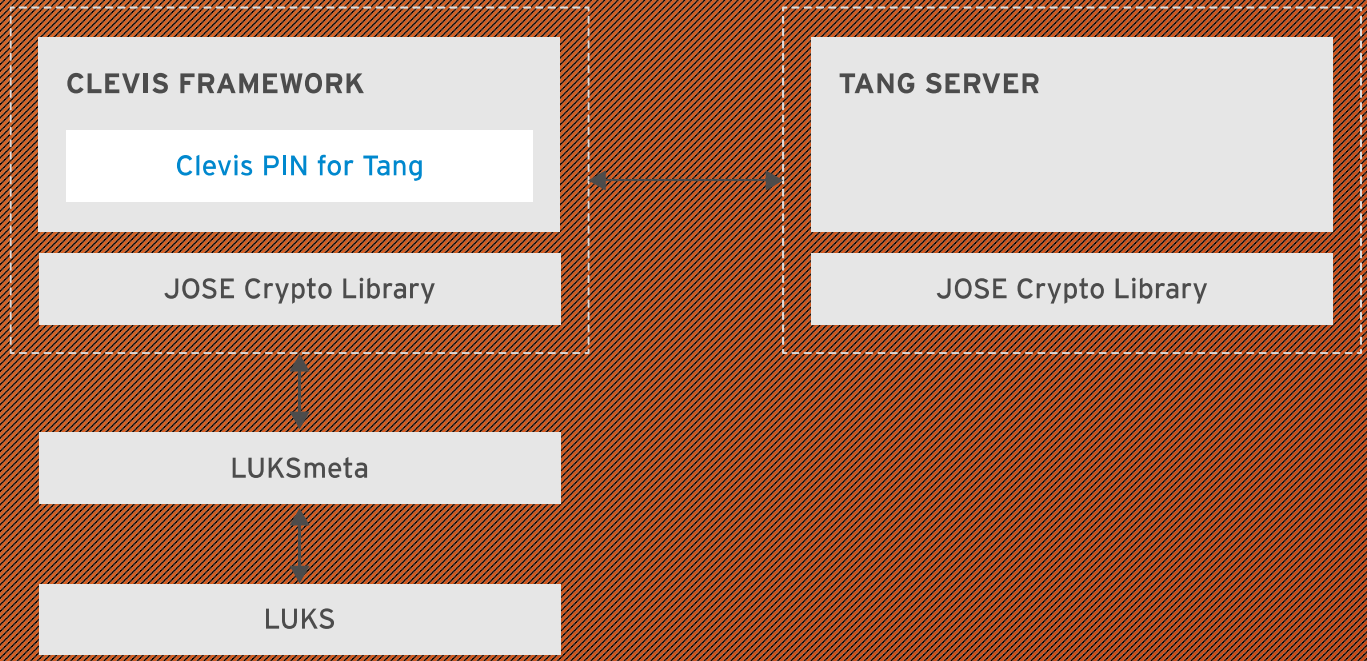
OpenSCAP: An auditing tool that utilizes the Extensible Configuration Checklist Description Format (XCCDF). XCCDF is a standard way of expressing checklist content and defines security checklists

https://www.open-scap.org/

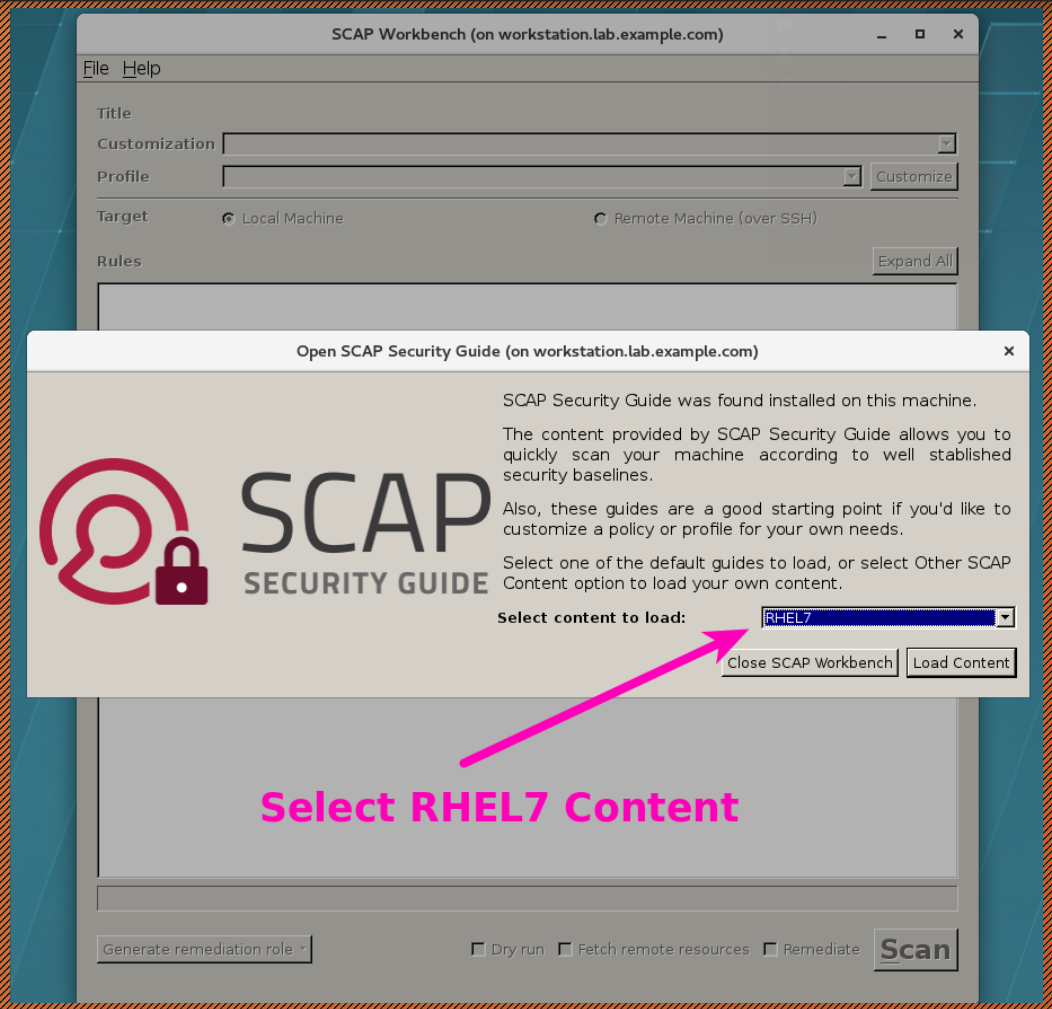
LUKS and NBDE

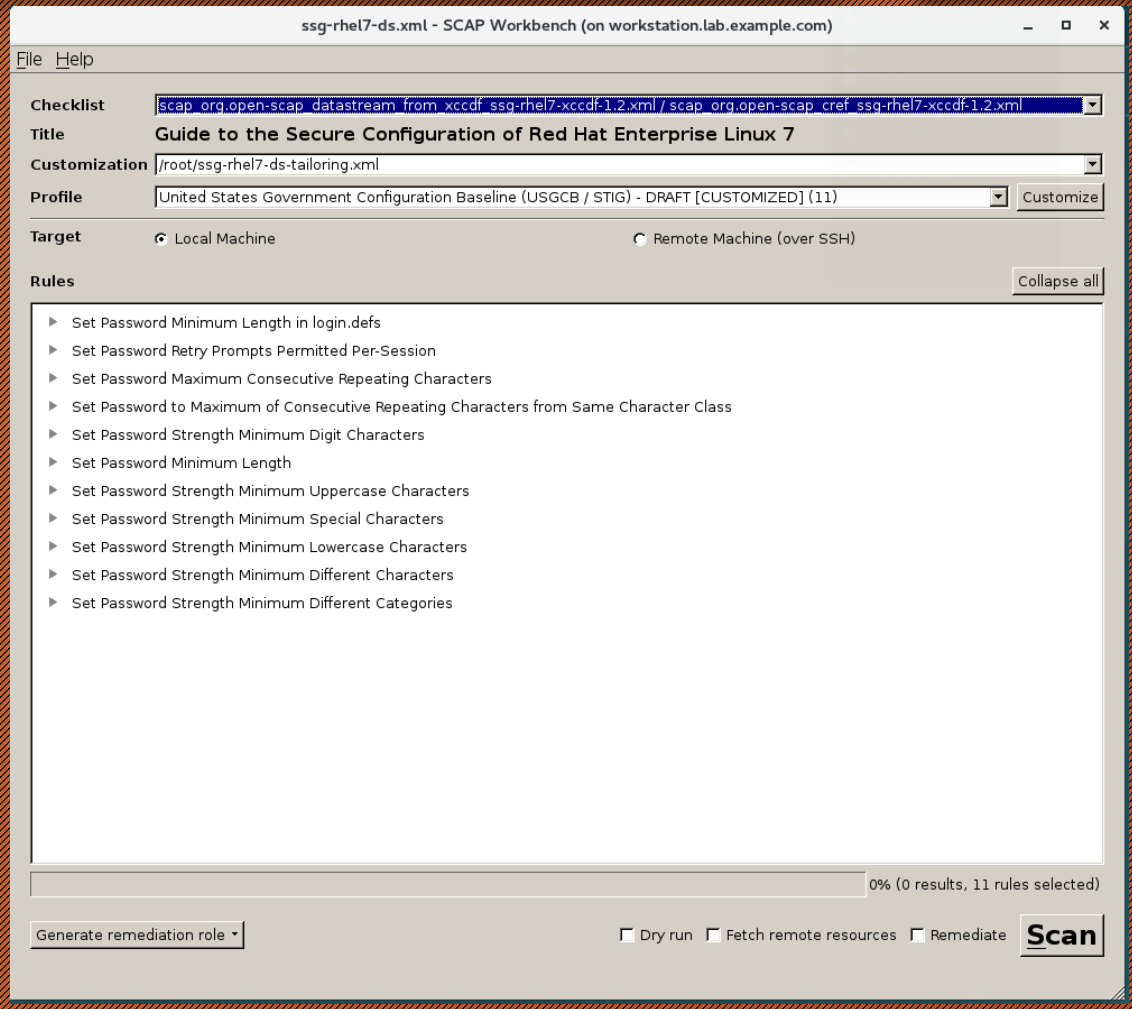




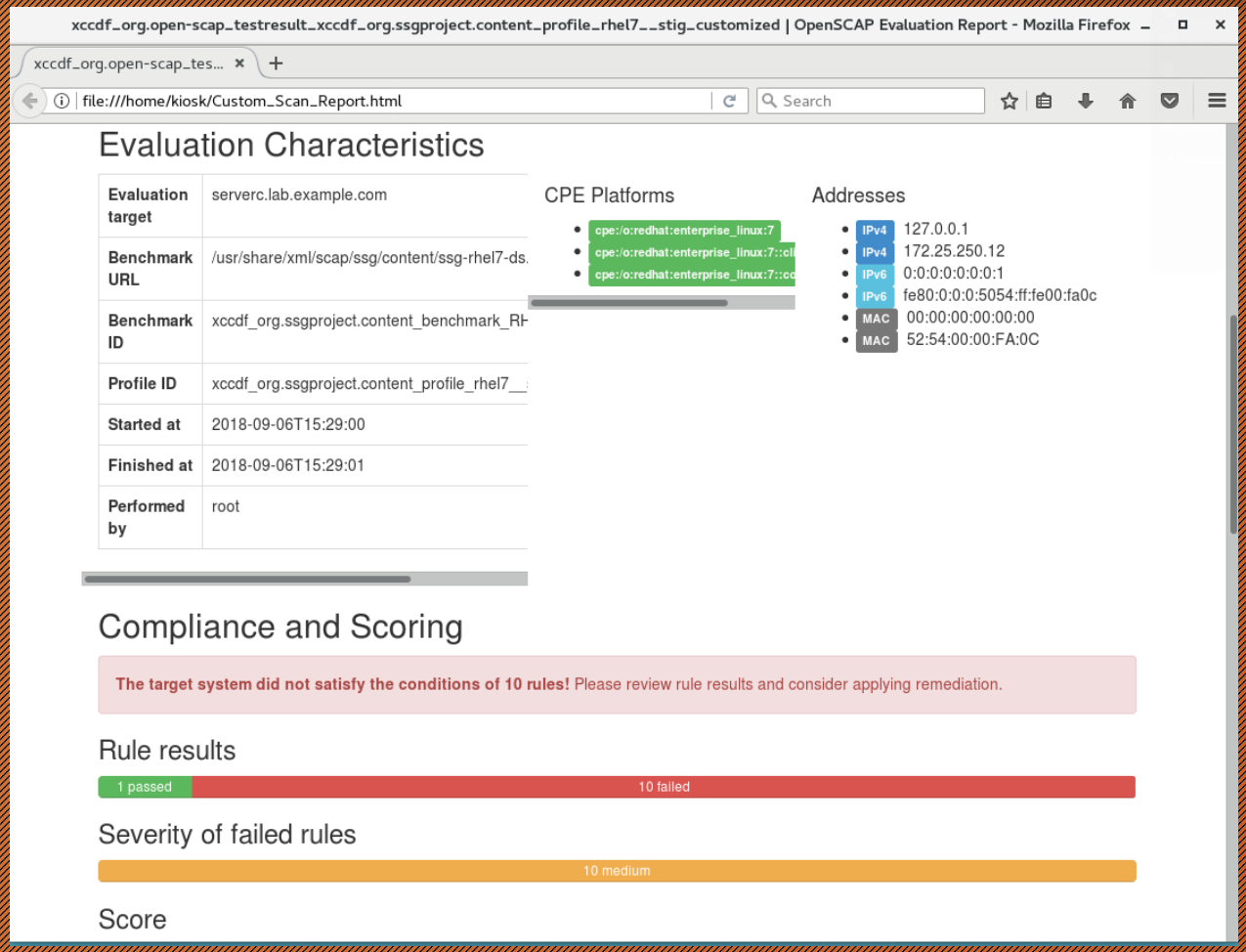


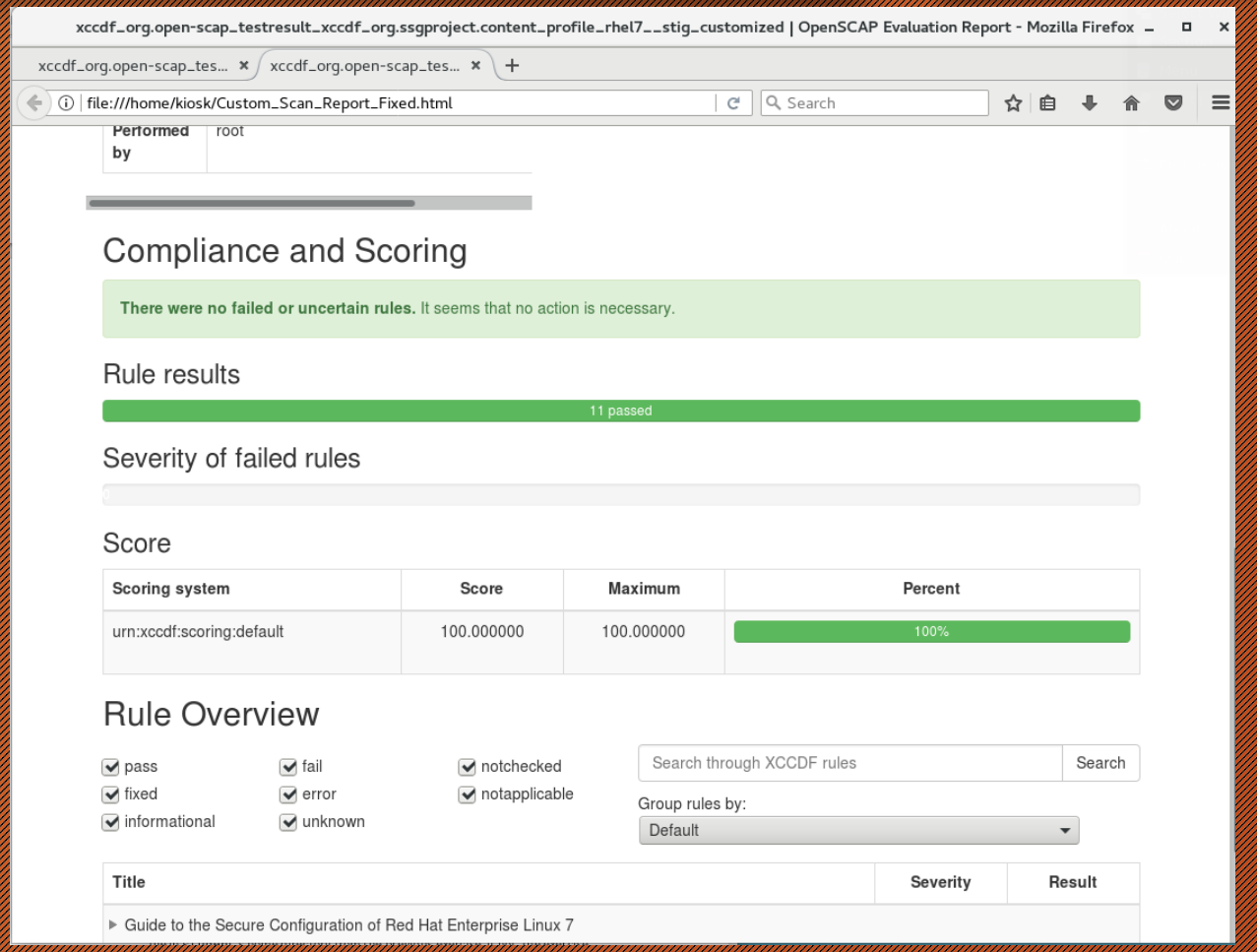
SCAP Workbench





SCAP Scan Results





Hands-On Lab

- NBDE
  - Creating a LUKS Encrypted Disk
  - Setting up and Configuring Clevis/Tang
  - Using Clevis/Tang to Unencrypt Disk at Bootup
- SCAP Scanning
  - Using SCAP Workbench to Customize Content
  - Scanning with Custom Content
  - Remediating Systems Based on Scan Results
  - Verifying System Remediation

Questions