Automated implementation of PCI DSS compliant solution using open-source tools

•••

Meet business (PCI DSS) requirements instantly

Ján Lieskovský

January 2016

Payment Card Industry Data Security Standard (PCI DSS)

- Applies to all entities (somehow) associated with (credit / debit) payment cards (merchants, financial institutions, card issuers, gateways...)

Payment Card Industry Data Security Standard (PCI DSS)

- Applies to all entities (somehow) associated with (credit / debit) payment cards (merchants, financial institutions, card issuers, gateways...)

It's clear why the organizations care!!!

- Mandatory
- Want protect security of payment systems

Payment Card Industry Data Security Standard (PCI DSS)

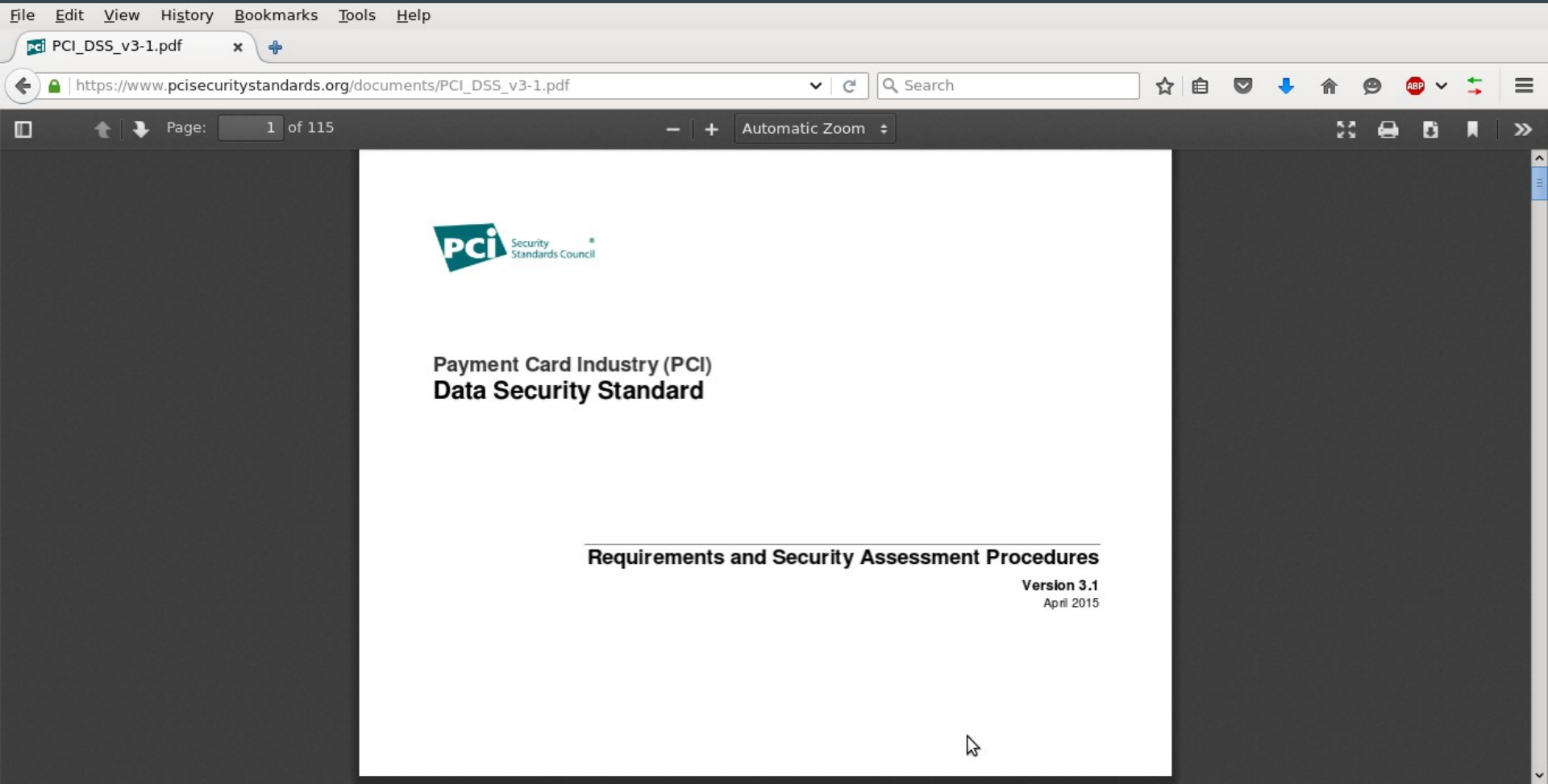
- Applies to all entities (somehow) associated with (credit / debit) payment cards (merchants, financial institutions, card issuers, gateways...)

It's clear why the organizations care!!!

But why I should care?

- Distributions are multi-purpose (not insecure, but also not secure)
- Rules from PCI DSS standard can improve security of **any** system (=> creation of derived own security policy)

Payment Card Industry Data Security Standard (PCI DSS)



Payment Card Industry Data Security Standard (PCI DSS)

- Rules are universal:

PCI DSS Requirements	Testing Procedures	Guidance
8.2.3 Passwords/phrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.	**8.2.3a** For a sample of system components, inspect system configuration settings to verify that user password parameters are set to require at least the following strength/complexity: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. **8.2.3.b** ***Additional testing procedure for service provider assessments only*:** Review internal processes and customer/user documentation to verify that non-consumer customer passwords are required to meet at least the following strength/complexity: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters.	Strong passwords/phrases are the first line of defense into a network since a malicious individual will often first try to find accounts with weak or non-existent passwords. If passwords are short or simple to guess, it is relatively easy for a malicious individual to find these weak accounts and compromise a network under the guise of a valid user ID. This requirement specifies that a minimum of seven characters and both numeric and alphabetic characters should be used for passwords/phrases. For cases where this minimum cannot be met due to technical limitations, entities can use “equivalent strength” to evaluate their alternative. NIST SP 800-

- Gap between the official requirements of the standard and implementation details of the concrete OS / product

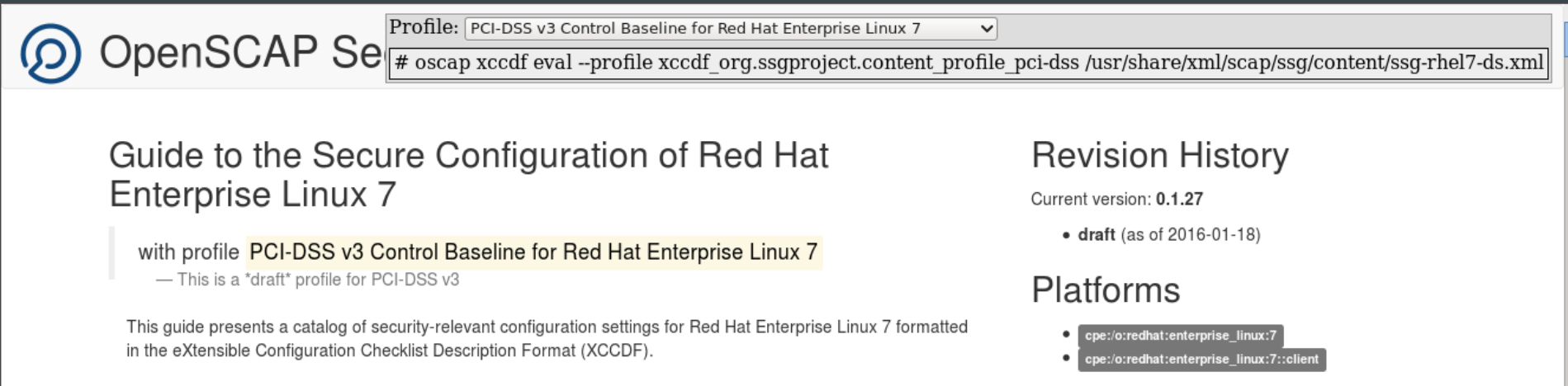
Inspecting policy status of a single computer / host

- Components
  - Security policies
  - Security scanners
- Phases
  - Original assessment
  - Subsequent correction – remediation

Inspecting policy status of a single computer / host

SCAP Security Guide (SSG)

- Represents security policies components
- Provides policies for many standards (not just PCI DSS)
- Policies shipped in both forms:
  - XML files suitable for automated processing
  - **HTML guides**



Inspecting policy status of a single computer / host

SCAP Security Guide (SSG)

- Bridges the gap !!!

SCAP
SECURITY GUIDE

For example Requirement 8.2.3 of PCI DSS maps to the following SSG rules:

no_empty_passwords

accounts_password_pam_dcredit

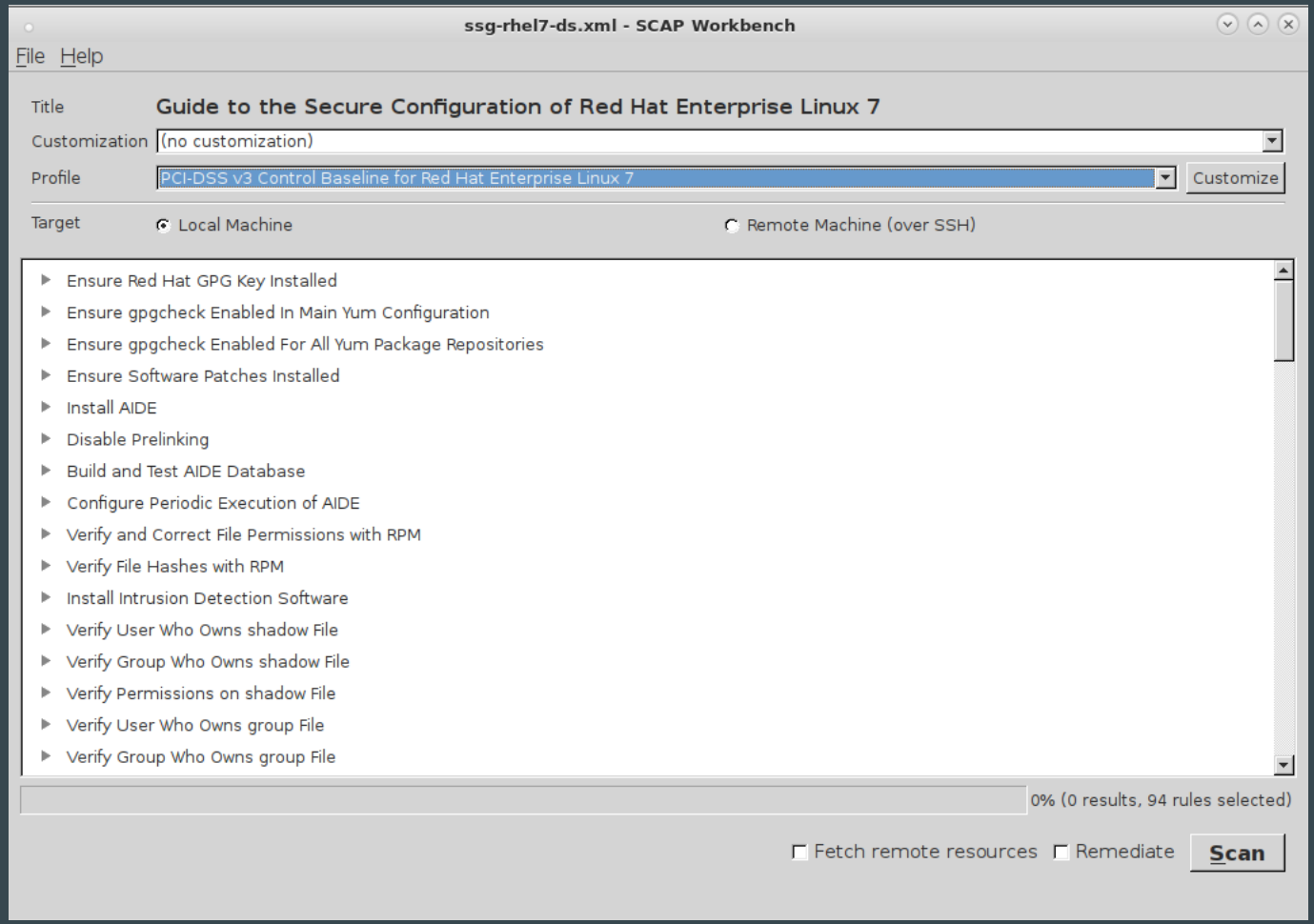
accounts_password_pam_minlen

accounts_password_pam_ucredit

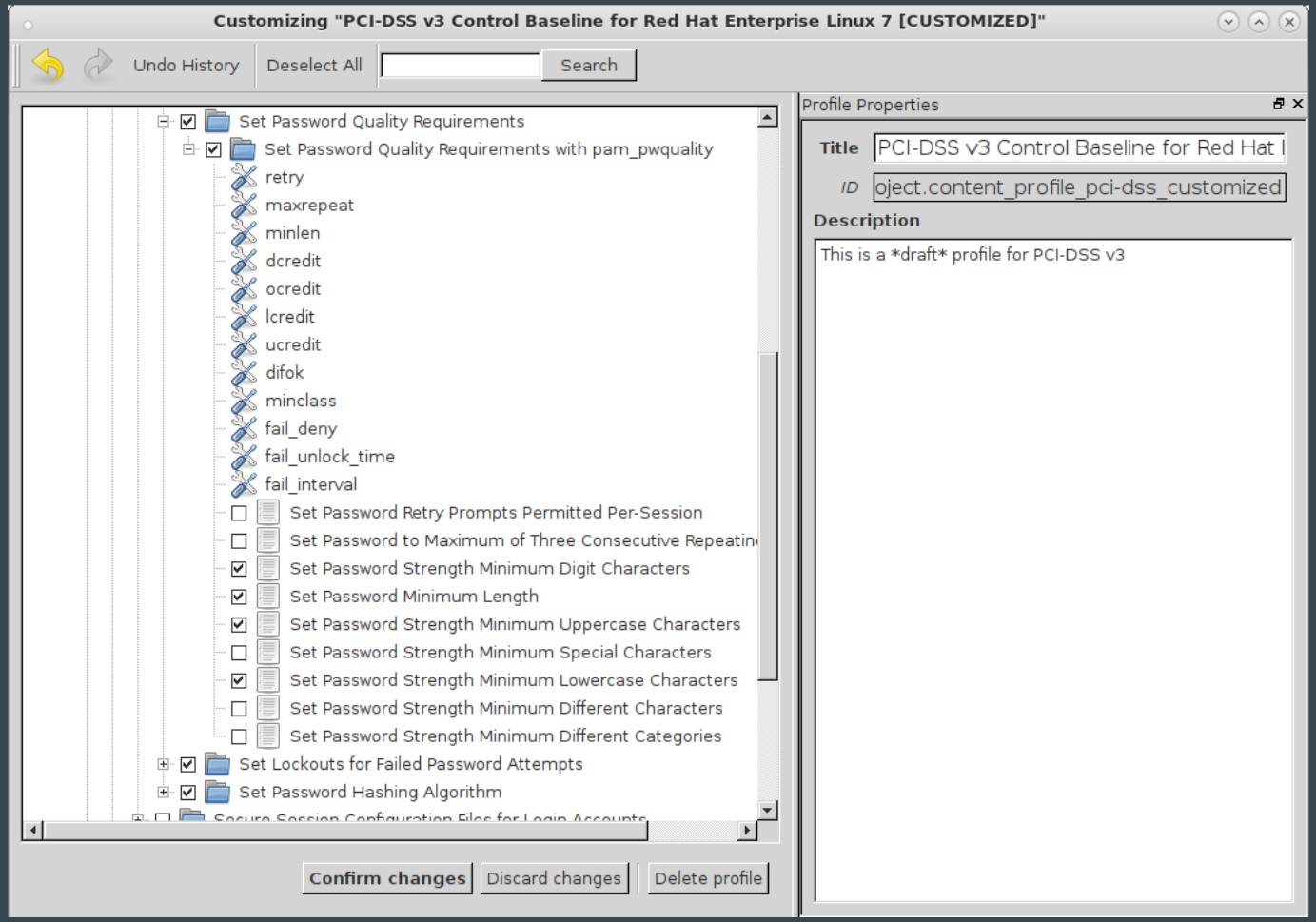
accounts_password_pam_lcredit

Inspecting policy status of a single computer / host

SCAP Workbench



SCAP Workbench – Customizing security policy



Why to customize policy?

To improve security of the system!!!

Inspecting policy status of a single computer / host

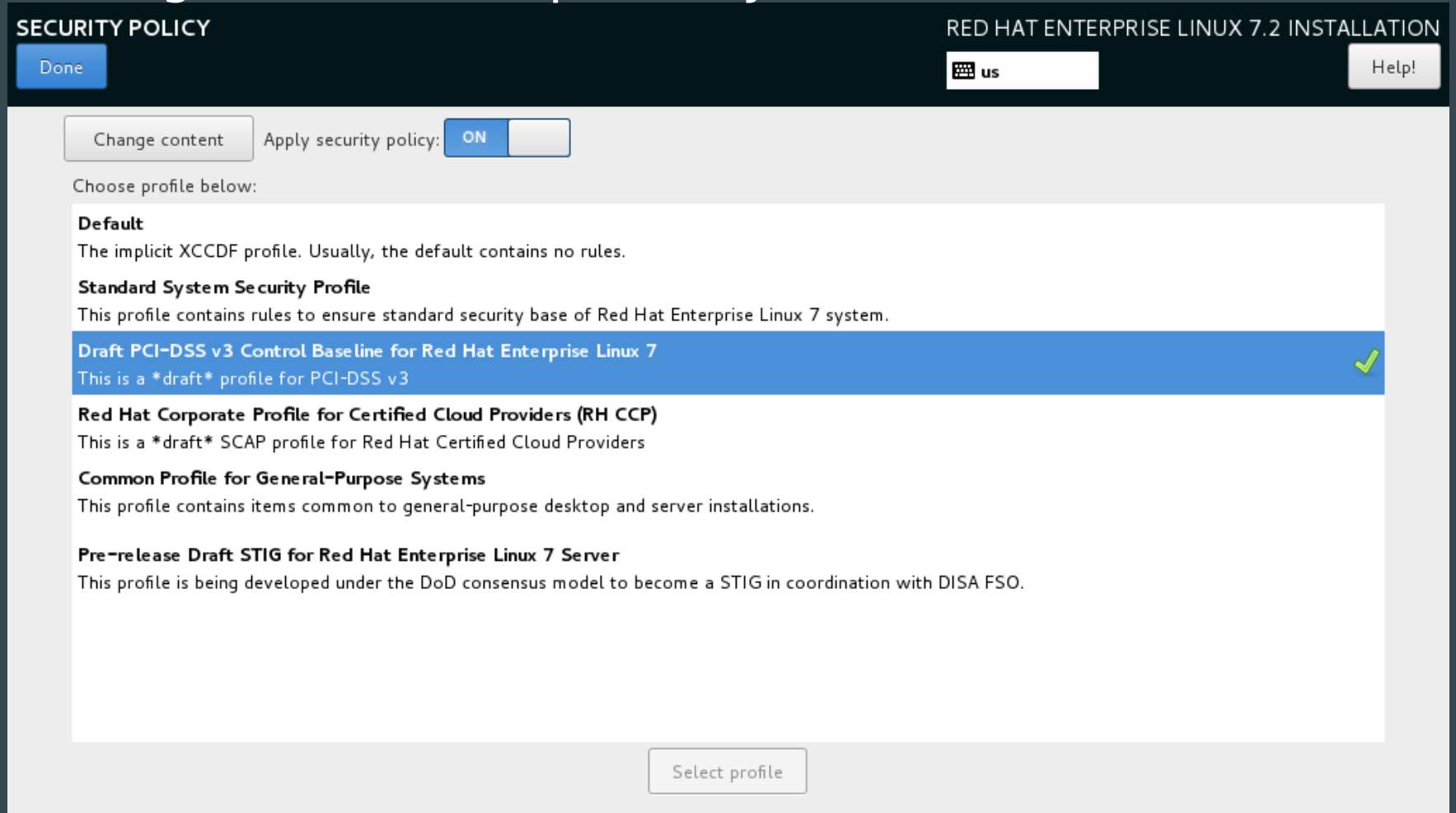
OpenSCAP Base:

- Represents security scanner component
- CLI tool suitable for script engines / playbooks
- Feature highlights:
  - Original host assessment
  - Remediation
  - ..

OpenSCAP BASE

```
File  Edit  View  Search  Terminal  Help
[root@localhost ~]# grep '<Profile' /usr/share/xml/scap/ssg/content/ssg-rhel7-xccdf.xml
  <Profile id="standard">
  <Profile id="pci-dss">
  <Profile id="C2S">
  <Profile id="rht-ccp">
  <Profile id="common">
  <Profile id="stig-rhel7-server-upstream">
  <Profile id="ospp-rhel7-server">
[root@localhost ~]# oscap xccdf eval --profile pci-dss --report /tmp/ssg-rhel7-report.html /usr/share/xml/scap/ssg/content/ssg-rhel7-xccdf.xml
```

Installing PCI DSS compliant system – OSCAP Anaconda Addon:



Installing PCI DSS compliant system – **OSCAP Anaconda Addon:**

Caution:

- Will the system be truly compliant once the installation is complete?

Inspecting multiple systems

OpenSCAP Daemon:

- Supports scans on various assets (local, remote, virtual machines, containers)
- CLI suitable for script engines / playbooks
- Feature highlights:
  - Regular (daily, weekly, ..) or custom evaluation
  - Evaluation on demand
  - Parallel task processing
  - Results history
  - ..

```
# interactively create a new task
oscapd-cli task-create -i
Creating new task in interactive mode
Title: Daily USGCB
Target (empty for localhost):
Found the following SCAP Security Guide content:
        1:  /usr/share/xml/scap/ssg/content/ssg-fedora-ds.xml
        2:  /usr/share/xml/scap/ssg/content/ssg-firefox-ds.xml
        3:  /usr/share/xml/scap/ssg/content/ssg-java-ds.xml
        4:  /usr/share/xml/scap/ssg/content/ssg-rhel6-ds.xml
        5:  /usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
Choose SSG content by number (empty for custom content): 4
Tailoring file (absolute path, empty for no tailoring):
Found the following possible profiles:
        1:  CSCF RHEL6 MLS Core Baseline (id='xccdf_org.ssgproject.content_profile_CSCF-RHEL6-MLS')
        2:  United States Government Configuration Baseline (USGCB) (id='xccdf_org.ssgproject.content_profile
        3:  Common Profile for General-Purpose Systems (id='xccdf_org.ssgproject.content_profile_common')
        4:  PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 6 (id='xccdf_org.ssgproject.content_prof
        5:  Example Server Profile (id='xccdf_org.ssgproject.content_profile_CS2')
        6:  C2S for Red Hat Enterprise Linux 6 (id='xccdf_org.ssgproject.content_profile_C2S')
        7:  Common Profile for General-Purpose SystemsUpstream STIG for RHEL 6 Server (id='xccdf_org.ssgproje
        8:  Common Profile for General-Purpose SystemsServer Baseline (id='xccdf_org.ssgproject.content_profi
        9:  Red Hat Corporate Profile for Certified Cloud Providers (RH CCP) (id='xccdf_org.ssgproject.conten
Choose profile by number (empty for (default) profile): 2
Online remediation (1, y or Y for yes, else no):
Schedule:
 - not before (YYYY-MM-DD HH:MM in UTC, empty for NOW): 2014-07-30 01:00
 - repeat after (hours or @daily, @weekly, @monthly, empty or 0 for no repeat): @daily
Task created with ID '1'. It is currently set as disabled. You can enable it with `oscapd-cli task 1 enable`.
```

Thanks!

Additional information:

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

http://www.open-scap.org/security-policies/scap-security-guide/

http://www.open-scap.org/tools/

Contact us:

https://www.redhat.com/mailman/listinfo/open-scap-list

https://lists.fedorahosted.org/mailman/listinfo/scap-security-guide