

OpenScap Local file testing

Install OpenSCAP command line tool and SCAP Security Guide for Linux.

```
root@localhost:~  
[root@localhost ~]# yum -y install openscap-scanner scap-security-guide
```

SCAP Security Guide is installed under the [/usr/share/xml/scap/ssg/content] directory.

```
[root@localhost ~]# ll /usr/share/xml/scap/ssg/content/  
total 328524  
-rw-r--r--. 1 root root 35382862 May 18 21:26 ssg-centos7-ds-1.2.xml  
-rw-r--r--. 1 root root 35383333 May 18 21:26 ssg-centos7-ds.xml  
-rw-r--r--. 1 root root 11421839 May 18 21:26 ssg-centos7-xccdf.xml  
-rw-r--r--. 1 root root 18347667 May 18 21:26 ssg-centos8-ds-1.2.xml  
-rw-r--r--. 1 root root 18347993 May 18 21:26 ssg-centos8-ds.xml  
-rw-r--r--. 1 root root 11859245 May 18 21:26 ssg-centos8-xccdf.xml  
-rw-r--r--. 1 root root      591 May 18 21:24 ssg-firefox-cpe-dictionary.xml  
-rw-r--r--. 1 root root     3885 May 18 21:24 ssg-firefox-cpe-oval.xml  
-rw-r--r--. 1 root root  286324 May 18 21:24 ssg-firefox-ds-1.2.xml  
-rw-r--r--. 1 root root  286324 May 18 21:24 ssg-firefox-ds.xml  
-rw-r--r--. 1 root root   39209 May 18 21:24 ssg-firefox-ocil.xml  
-rw-r--r--. 1 root root   53469 May 18 21:24 ssg-firefox-oval.xml
```

Display description for each content

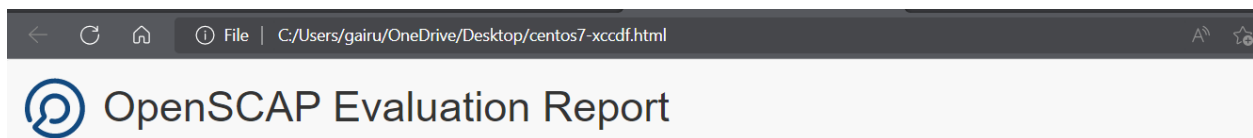
```
[root@localhost ~]# oscap info /usr/share/xml/scap/ssg/content/ssg-centos7-xccdf.xml  
Document type: XCCDF Checklist  
Checklist version: 1.1  
Imported: 2022-05-18T21:26:11  
Status: draft  
Generated: 2022-05-18  
Resolved: true  
Profiles:  
  Title: PCI-DSS v3.2.1 Control Baseline for Red Hat Enterprise Linux 7  
  Id: pci-dss  
  Title: Standard System Security Profile for Red Hat Enterprise Linux 7  
  Id: standard  
Referenced check files:  
  ssg-rhel7-oval.xml  
  system: http://oval.mitre.org/XMLSchema/oval-definitions-5  
  ssg-rhel7-ocil.xml  
  system: http://scap.nist.gov/schema/ocil/2  
  https://www.redhat.com/security/data/oval/com.redhat.rhsa-RHEL7.xml  
  system: http://oval.mitre.org/XMLSchema/oval-definitions-5  
[root@localhost ~]#
```

Scan System with [oscap] command. Usage is like follows.

```
oscap xccdf eval --profile standard --report centos7-xccdf.html /usr/share/xml/scap/ssg/content/ssg-centos7-xccdf.xml
```

```
[root@localhost ~]# oscap xccdf eval --profile standard --report centos7-xccdf.html /usr/share/xml/scap/ssg/content/ssg-centos7-xccdf.xml
WARNING: This content points out to the remote resources. Use '--fetch-remote-resources' option to download them.
WARNING: Skipping https://www.redhat.com/security/data/oval/com.redhat.rhsa-RHEL7.xml file which is referenced from XCCDF content
Title  Verify File Hashes with RPM
Rule   rpm_verify_hashes
```

```
C:\Users\gairu\OneDrive\Desktop>scp root@192.168.36.146:\root\centos7-xccdf.html .
root@192.168.36.146's password:
centos7-xccdf.html                                100% 932KB 51.1MB/s 00:00
C:\Users\gairu\OneDrive\Desktop>
```



Guide to the Secure Configuration of Red Hat Enterprise Linux 7

with profile **Standard System Security Profile for Red Hat Enterprise Linux 7**

— This profile contains rules to ensure standard security baseline of a Red Hat Enterprise Linux 7 system. Regardless of your system's workload all of these checks should pass.

The SCAP Security Guide Project

<https://www.open-scap.org/security-policies/scap-security-guide>

This guide presents a catalog of security-relevant configuration settings for Red Hat Enterprise Linux 7. It is a rendering of content structured Description Format (XCCDF) in order to support security automation. The SCAP content is available in the [scap-security-guide](#) package [scap.org/security-policies/scap-security-guide](#).

Providing system administrators with such guidance informs them how to securely configure systems under their control in a variety of nature

Remote CIS Benchmark Testing

Environment Setting

Download latest scap security guide from scap project repo and extract it.

wget <https://github.com/ComplianceAsCode/content/releases/download/v0.1.62/scap-security-guide-0.1.62.zip>

```
root@localhost:~# wget https://github.com/ComplianceAsCode/content/releases/download/v0.1.62/scap-security-guide-0.1.62.zip
--2022-07-17 00:04:44-- https://github.com/ComplianceAsCode/content/releases/download/v0.1.62/scap-security-guide-0.1.62.zip
Resolving github.com (github.com)... 20.205.243.166
Connecting to github.com (github.com)|20.205.243.166|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/19279458/a3f27abc-55c9-4b6f-bd5a-b04121de4781?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWVNJYAX4CSVEH53A%2F20220716%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20220716T183448Z&X-Amz-Expires=300&X-Amz-Signature=662eab7c98a6801bd9a0a80cd02a75638d0b5e67d45068e7496c3cb093800caf&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=19279458&response-content-disposition=attachment%3B%20filename%3Dscap-security-guide-0.1.62.zip&response-content-type=application%2Foctet-stream [following]
--2022-07-17 00:04:49-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/19279458/a3f27abc-55c9-4b6f-bd5a-b04121de4781?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWVNJYAX4CSVEH53A%2F20220716%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20220716T183448Z&X-Amz-Expires=300&X-Amz-Signature=662eab7c98a6801bd9a0a80cd02a75638d0b5e67d45068e7496c3cb093800caf&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=19279458&response-content-disposition=attachment%3B%20filename%3Dscap-security-guide-0.1.62.zip&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.109.133, 185.199.111.133, 185.199.108.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.109.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 108555579 (104M) [application/octet-stream]
Saving to: 'scap-security-guide-0.1.62.zip'

0% [ ] 1,072,485 97.2KB/s eta 16m 6s
```

We need to install oscap-ssh which would allow to perform audit on remote hosts. However, this is a part of openscap project, but it's not included in "openscap-scanner", we would need to download it from openscap project repository.

wget <https://raw.githubusercontent.com/OpenSCAP/openscap/maint-1.3/utlis/oscap-ssh>

```
root@localhost:~# wget https://raw.githubusercontent.com/OpenSCAP/openscap/maint-1.3/utlis/oscap-ssh
--2022-07-17 00:12:02-- https://raw.githubusercontent.com/OpenSCAP/openscap/maint-1.3/utlis/oscap-ssh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.109.133, 185.199.111.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.109.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 13110 (13K) [text/plain]
Saving to: 'oscap-ssh'

100%[=====>] 13,110 --.-K/s in 0.1s

2022-07-17 00:12:08 (114 KB/s) - 'oscap-ssh' saved [13110/13110]

root@localhost:~#
```

Next Find to oscap Location and move to that location to run the oscap-ssh file in command line

```
root@localhost:~# whereis oscap
oscap: /usr/bin/oscap /usr/share/man/man8/oscap.8.gz
root@localhost:~#
```

```
root@localhost:~# chmod 755 oscap-ssh
root@localhost:~# mv -v oscap-ssh /usr/bin/
'oscap-ssh' -> '/usr/bin/oscap-ssh'
root@localhost:~# chown root:root /usr/bin/oscap-ssh
root@localhost:~#
```

```
inflating: scap-security-guide-0.1.62/ssg-ocp4-ds.xml
[root@localhost ~]# unzip scap-security-guide-0.1.62.zip
```

```
[root@localhost ~]# mv scap-security-guide-0.1.62 scap
[root@localhost ~]# ls
anaconda-ks.cfg  scap  scap-security-guide-0.1.62.zip  ssg-centos7-xccdf.html
[root@localhost ~]#
```

Launching compliance test

Now we will perform vulnerability check with the collaboration of openscap and scap security guide content in another ubuntu host which has IP 192.168.36.147

```
oscap-ssh cis@192.168.36.147 22 xccdf eval --profile standard --report my.html scap/ssg-ubuntu2004-ds-1.2.xml
```

```
[root@localhost ~]# oscap-ssh cis@192.168.36.147 22 xccdf eval --profile standard --report my.html scap/ssg-ubuntu2004-ds-1.2.xml
Connecting to 'cis@192.168.36.147' on port '22'...
The authenticity of host '192.168.36.147 (192.168.36.147)' can't be established.
ECDSA key fingerprint is SHA256:0nLixNXo/5a5IZ+YX2yAZoPKQkGx2VrGuW0ZmwdnRfk.
ECDSA key fingerprint is MD5:3b:eb:39:ab:b9:a2:ed:0e:39:e1:e3:0b:8b:33:1a:03.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.36.147' (ECDSA) to the list of known hosts.
cis@192.168.36.147's password:
Connected!
Copying input file 'scap/ssg-ubuntu2004-ds-1.2.xml' to remote working directory '/tmp/tmp.6S2aUoip9j'...
scap-ubuntu2004-ds-1.2.xml
Starting the evaluation...
Title  Ensure /home Located On Separate Partition
Rule   xccdf_org.ssgproject.content_rule_partition_for_home
Result fail
```

```
< > File | C:/Users/gairu/OneDrive/Desktop/my.html
```

OpenSCAP Evaluation Report

Guide to the Secure Configuration of Ubuntu 20.04

with profile **Standard System Security Profile for Ubuntu 20.04**

— This profile contains rules to ensure standard security baseline of an Ubuntu 20.04 system. Regardless of your system's workload all of these checks should pass.

The SCAP Security Guide Project

<https://www.open-scap.org/security-policies/scap-security-guide>

This guide presents a catalog of security-relevant configuration settings for Ubuntu 20.04. It is a rendering of content structured in the eXtensible Configuration Checklist Description Format (XCCDF) in order to support security automation. The SCAP content is available in the `scap-security-guide` package which is developed at <https://www.open-scap.org/security-policies/scap-security-guide>.

Providing system administrators with such guidance informs them how to securely configure systems under their control in a variety of network roles. Policy makers and baseline creators can use this catalog of settings, with its associated references to higher-level security control catalogs, in order to assist them in security baseline creation. This guide is a *catalog*, not a *checklist*, and satisfaction of every item is not likely to be possible or sensible in many operational scenarios. However, the XCCDF format enables granular selection and adjustment of settings, and their association with OVAL and OCIL content provides an automated checking capability. Transformations of this document, and its associated automated checking content, are capable of providing baselines that meet a diverse set of policy objectives. Some example XCCDF *Profiles*, which are selections of items that form checklists and can be used as baselines, are available with this guide. They can be processed, in an automated fashion, with tools that support the Security Content Automation Protocol (SCAP). The DISA STIG, which provides required settings for US Department of Defense systems, is one example of a baseline created from this guidance.

References:

- [CentOS 7 : OpenSCAP : Security Audit : Server World \(server-world.info\)](https://server-world.info)
- [How to Audit Linux Systems using OpenSCAP - Knoldus Blogs](#)