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 ~]#
```

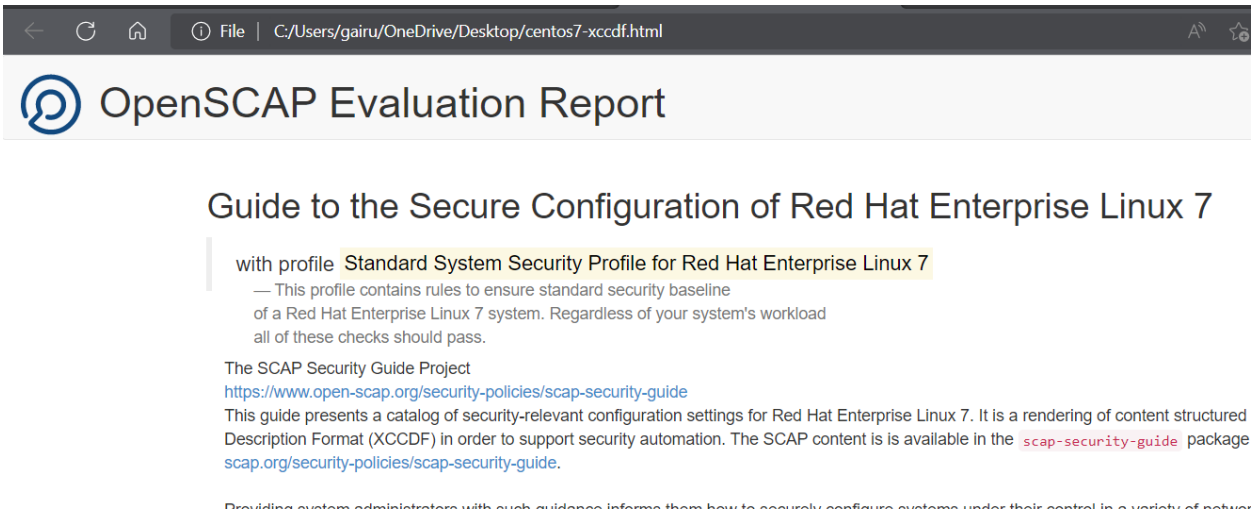
Scan System with [oscap] command. Usage is like follows.

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-xcc
df.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>
```

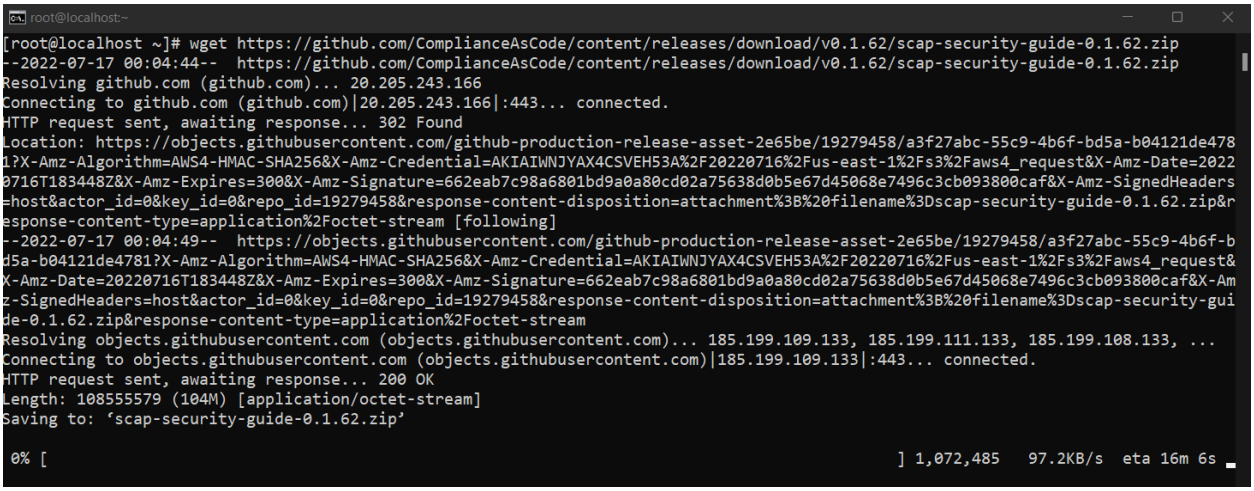


Remote CIS Benchmark Testing

Environment Setting

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

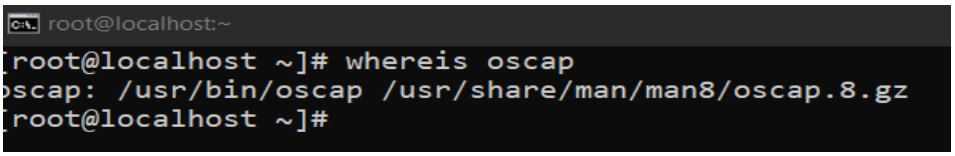
wget https://github.com/ComplianceAsCode/content/releases/download/v0.1.62/scap-security-guide-0.1.62.zip

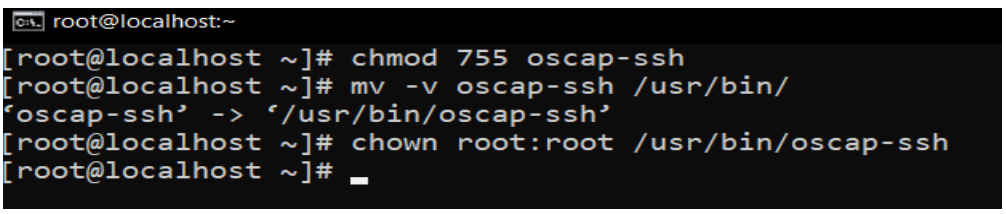


We need to install oscap-ssh which would allow to perform audit on remote hosts. However, this is a part of openscap project, but it's not included in "openscap-scanner", we would need to download it from openscap project repository.

wget https://raw.githubusercontent.com/OpenSCAP/openscap/maint-1.3/utils/oscap-ssh

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





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

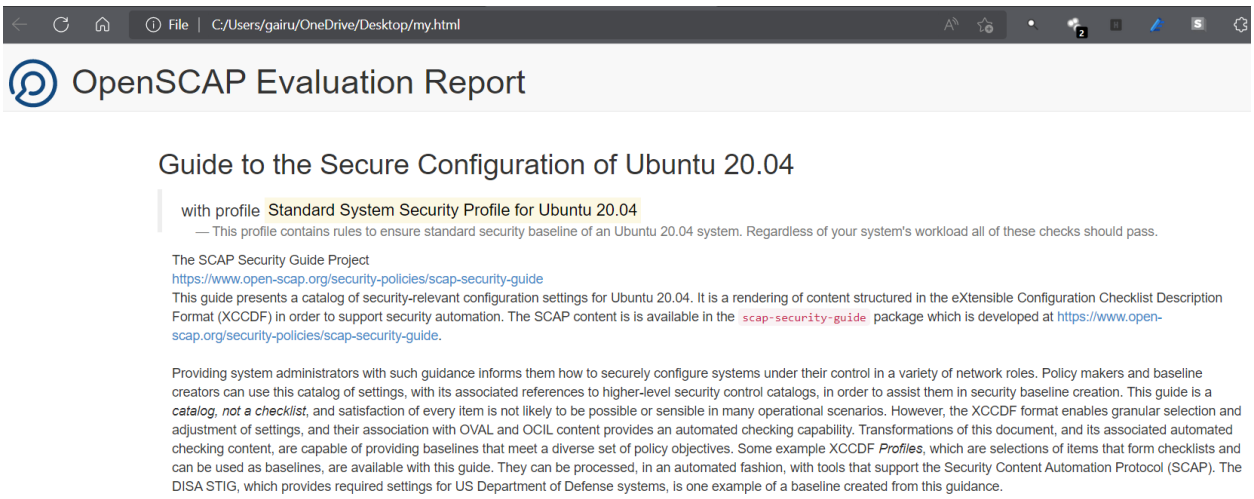
```
[root@localhost ~]# mv scap-security-guide-0.1.62 scap
[root@localhost ~]# ls
anaconda-ks.cfg  scap  scap-security-guide-0.1.62.zip  ssg-centos7-xccdf.html
[root@localhost ~]#
```

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+YX2yAZoPKQkGx2VrGuWOZmwdnRfk.
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'...
ssg-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
```



References:

- CentOS 7 : OpenSCAP : Security Audit : Server World (server-world.info)
- How to Audit Linux Systems using OpenSCAP - Knoldus Blogs