# **Openscap Local file testing**

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

A screenshot of a computer

Description automatically generated with medium confidence

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

Text

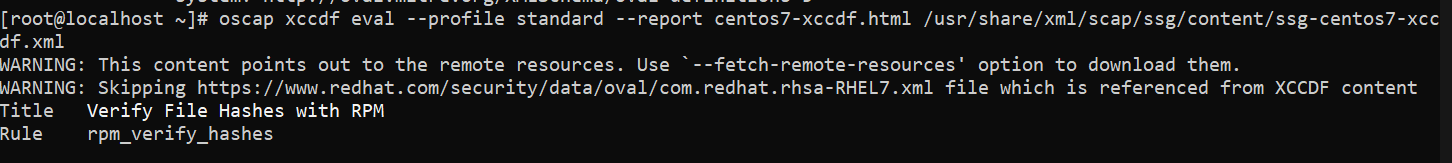
Description automatically generated

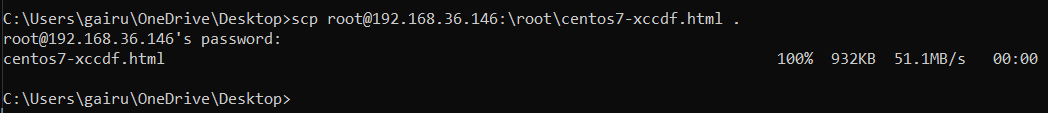
## Display description for each content

Text

Description automatically generated

## 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



Graphical user interface, text, application, email

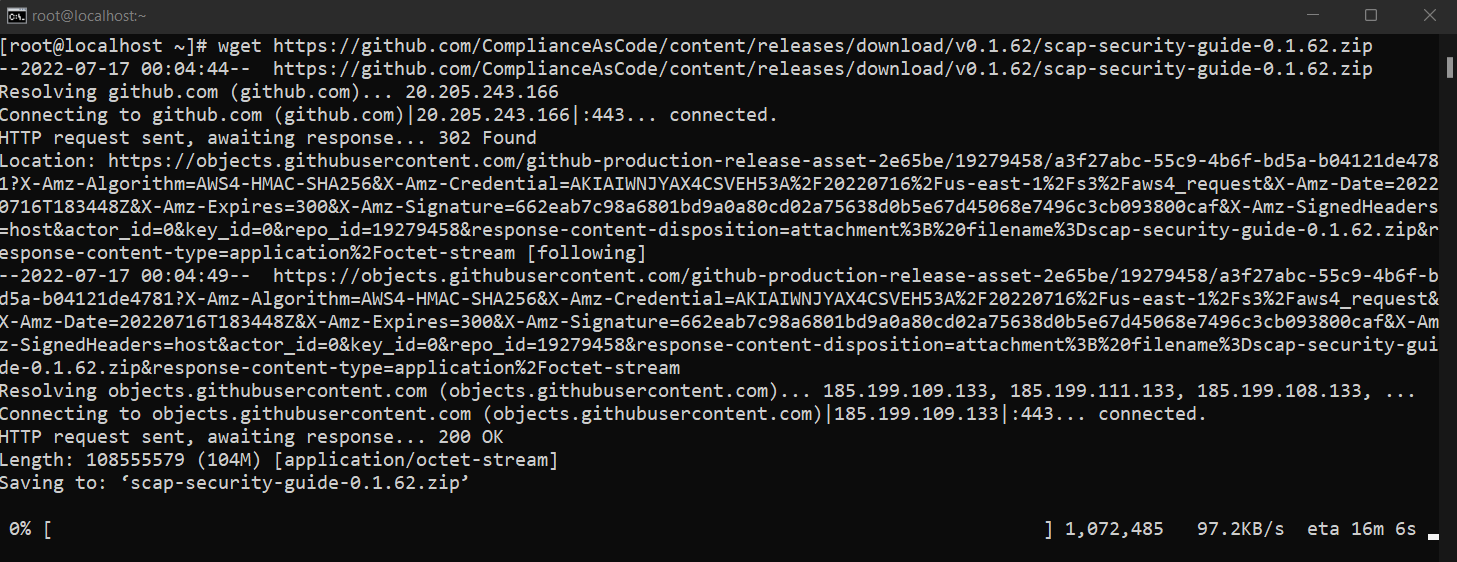
Description automatically generated

# **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>

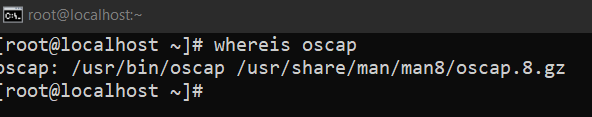


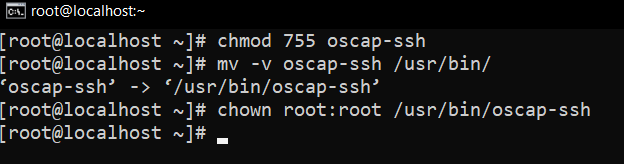
We need to install oscap-ssh which would allow to perform audit on remote hosts. However, this is a part of openscap project, but it’s not included in "openscap-scanner”, we would need to download it from openscap project repository.

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

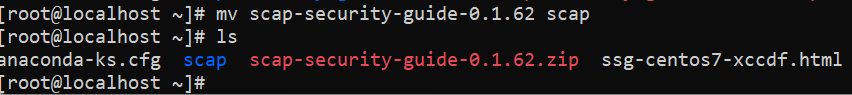


Next Find to oscap Location and move to that location to run the oscap-ssh file in command line









## 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

Graphical user interface, text

Description automatically generated

A picture containing text

Description automatically generated

References:

* [CentOS 7 : OpenSCAP : Security Audit : Server World (server-world.info)](https://www.server-world.info/en/note?os=CentOS_7&p=openscap)
* [How to Audit Linux Systems using OpenSCAP - Knoldus Blogs](https://blog.knoldus.com/openscap/)