How to Secure RHEL/CentOS 7.x with OpenSCAP (STIGing the server)

Motivation

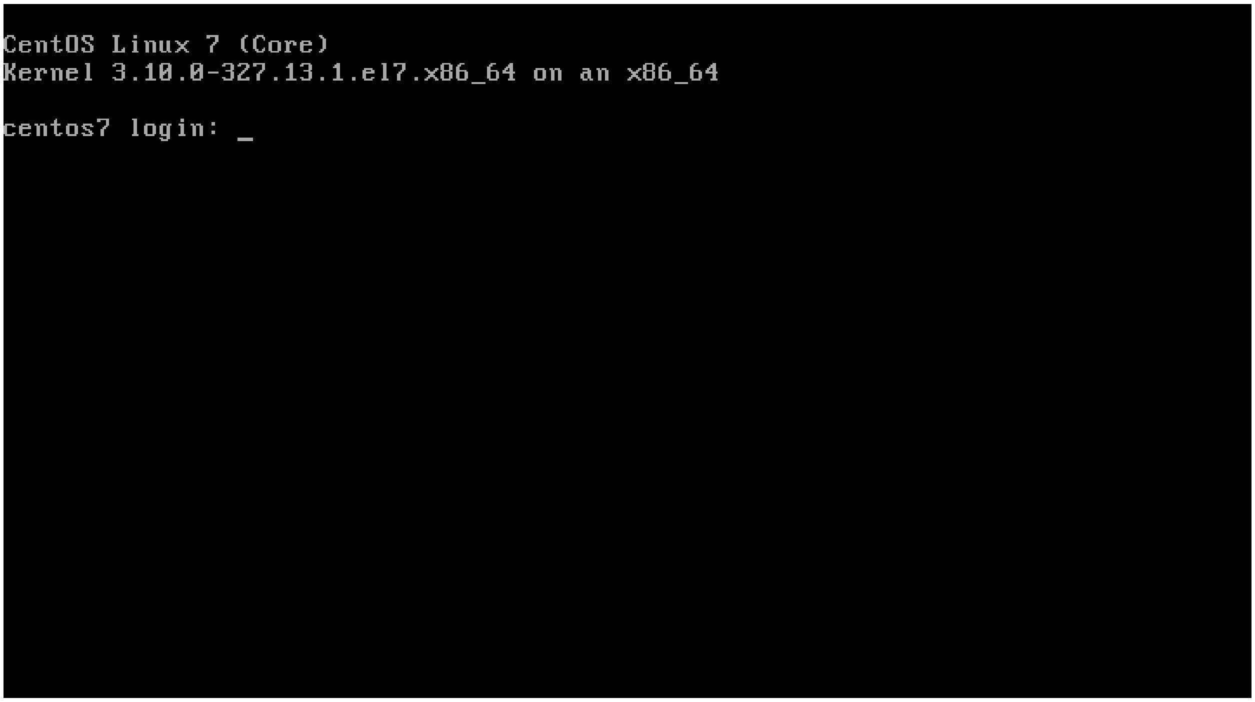
If you have ever had the miserable, unfortunate task of STIG'ing a computer system, you will know the horrific, soul evaporating hell that no human should ever have to deal with. Somehow, DISA has stacked feces, layer upon layer, until the bottom layer is beginning to be pushed out of the way from the weight of the top pushing down. OpenSCAP is the better path in order to harden an operating system. This guide is the quick and dirty way to lock down a system, fast with openscap. You will need internet access to down the software and the rules.

Test environment layout

My workstation is running Ubuntu 16.10.
I am first installing VirtualBox 5.1.6 for Ubuntu, using method 2 below.
Testing with CentOS 7.2 inside of a virtualbox.
  With 2 network interfaces.
  One on NAT-139 → 192.168.139.0/24 network.
  One on Host-only → 172.20.0.0/24 network.

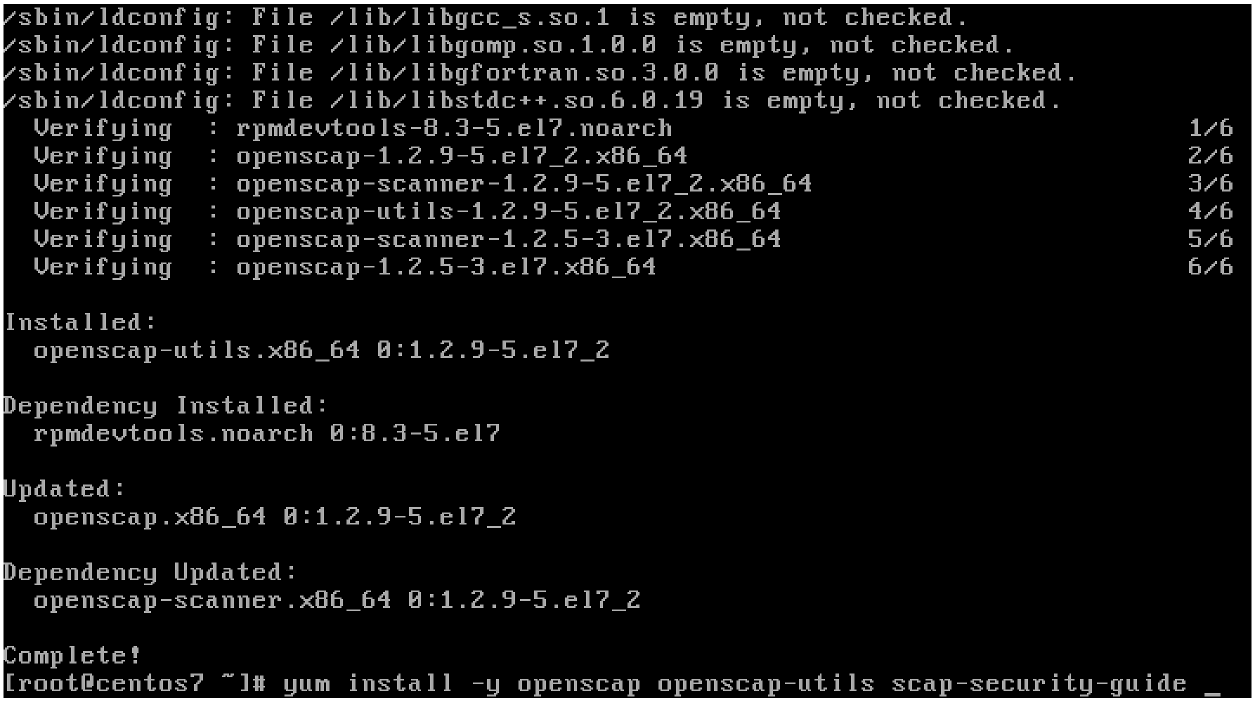
Execution

After installing a clean install of CentOS 7.x, perform the following steps to secure the system. You will have some post actions, such as reading the report and following any failed items to secure said.



```
CentOS Linux 7 (Core)
Kernel 3.10.0-327.13.1.el7.x86_64 on an x86_64

centos7 login: _
```

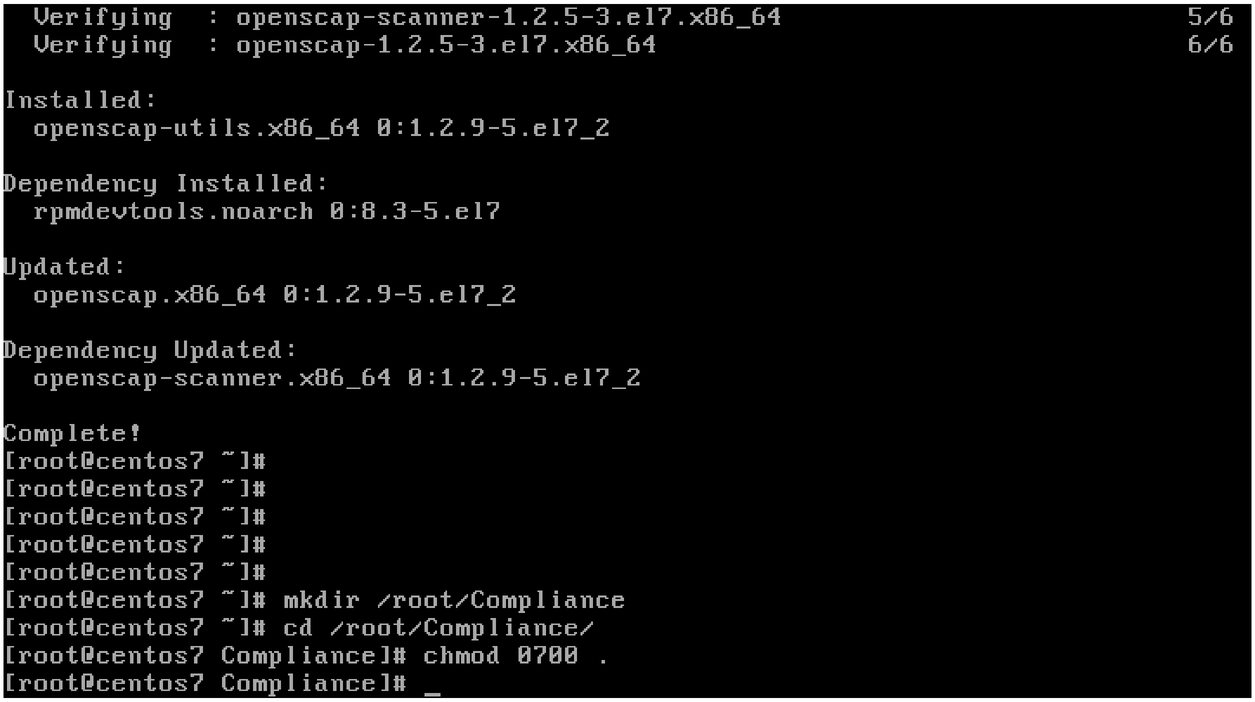
Initial Login screen. You will need to log in as the root user id to perform the lock down.



```
/sbin/ldconfig: File /lib/libgcc_s.so.1 is empty, not checked.
/sbin/ldconfig: File /lib/libgomp.so.1.0.0 is empty, not checked.
/sbin/ldconfig: File /lib/libgfortran.so.3.0.0 is empty, not checked.
/sbin/ldconfig: File /lib/libstdc++.so.6.0.19 is empty, not checked.
  Verifying  : rpmdevtools-8.3-5.el7.noarch                              1/6
  Verifying  : openscap-1.2.9-5.el7_2.x86_64                             2/6
  Verifying  : openscap-scanner-1.2.9-5.el7_2.x86_64                     3/6
  Verifying  : openscap-utils-1.2.9-5.el7_2.x86_64                       4/6
  Verifying  : openscap-scanner-1.2.5-3.el7.x86_64                       5/6
  Verifying  : openscap-1.2.5-3.el7.x86_64                               6/6

Installed:
  openscap-utils.x86_64 0:1.2.9-5.el7_2

Dependency Installed:
  rpmdevtools.noarch 0:8.3-5.el7

Updated:
  openscap.x86_64 0:1.2.9-5.el7_2

Dependency Updated:
  openscap-scanner.x86_64 0:1.2.9-5.el7_2

Complete!
[root@centos7 ~]# yum install -y openscap openscap-utils scap-security-guide _
```

Execute:

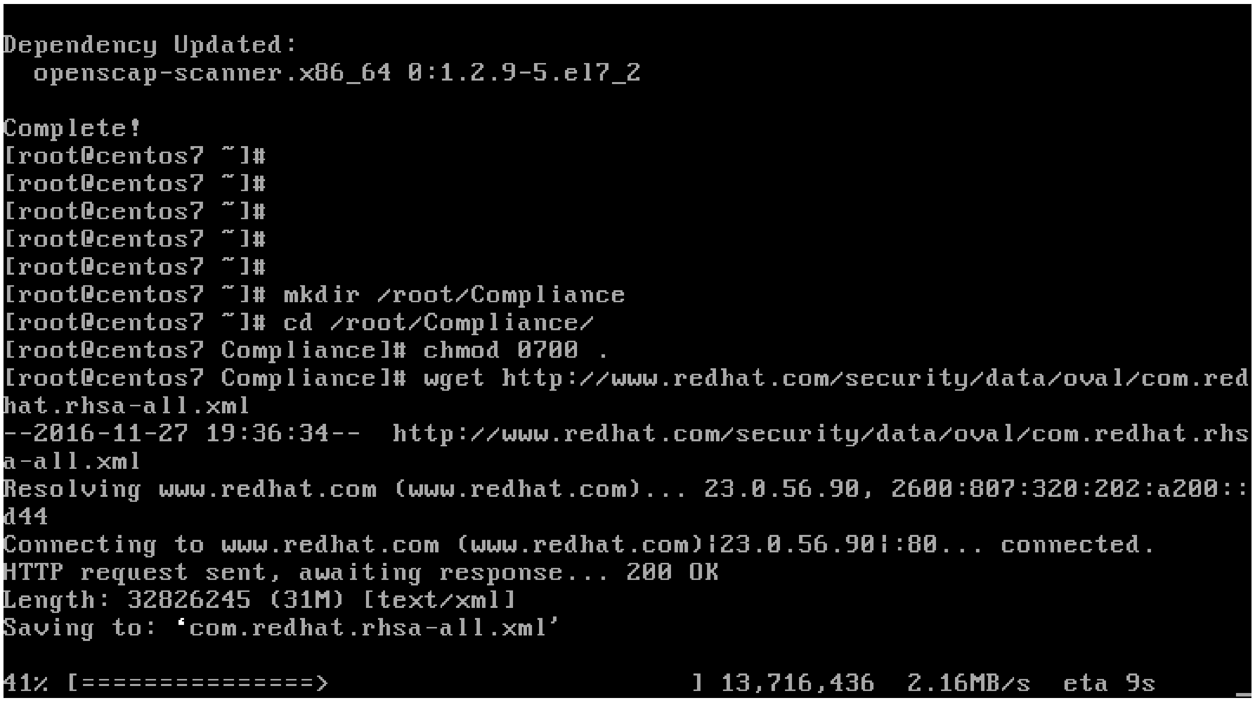
```
yum install -y openscap openscap-utils scap-security-guide
```



```
  Verifying  : openscap-scanner-1.2.5-3.el7.x86_64                              5/6
  Verifying  : openscap-1.2.5-3.el7.x86_64                                      6/6

Installed:
  openscap-utils.x86_64 0:1.2.9-5.el7_2

Dependency Installed:
  rpmdevtools.noarch 0:8.3-5.el7

Updated:
  openscap.x86_64 0:1.2.9-5.el7_2

Dependency Updated:
  openscap-scanner.x86_64 0:1.2.9-5.el7_2

Complete!
[root@centos7 ~]#
[root@centos7 ~]#
[root@centos7 ~]#
[root@centos7 ~]#
[root@centos7 ~]#
[root@centos7 ~]# mkdir /root/Compliance
[root@centos7 ~]# cd /root/Compliance/
[root@centos7 Compliance]# chmod 0700 .
[root@centos7 Compliance]# _
```

Execute:

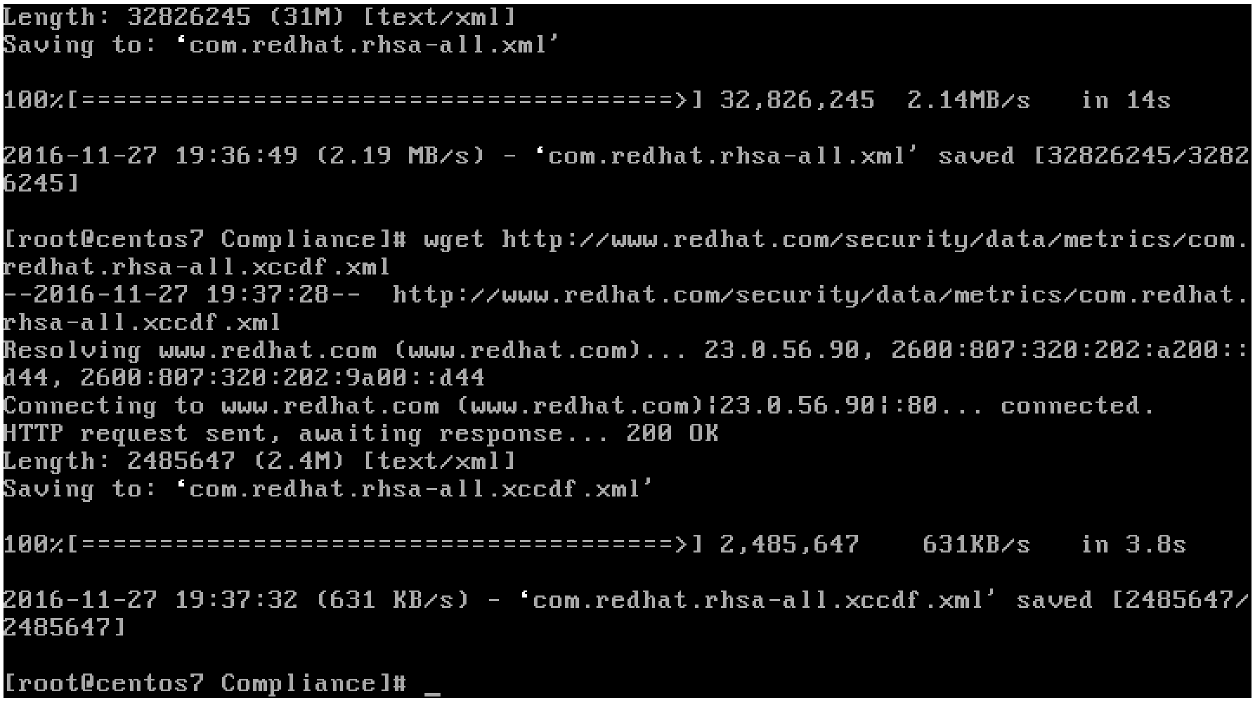
```
mkdir /root/Compliance
chmod 0700 /root/Compliance
cd /root/Compliance
```



```
Dependency Updated:
  openscap-scanner.x86_64 0:1.2.9-5.el7_2

Complete!
[root@centos7 ~]#
[root@centos7 ~]#
[root@centos7 ~]#
[root@centos7 ~]#
[root@centos7 ~]#
[root@centos7 ~]# mkdir /root/Compliance
[root@centos7 ~]# cd /root/Compliance/
[root@centos7 Compliance]# chmod 0700 .
[root@centos7 Compliance]# wget http://www.redhat.com/security/data/oval/com.red
hat.rhsa-all.xml
--2016-11-27 19:36:34--  http://www.redhat.com/security/data/oval/com.redhat.rhs
a-all.xml
Resolving www.redhat.com (www.redhat.com)... 23.0.56.90, 2600:807:320:202:a200::
d44
Connecting to www.redhat.com (www.redhat.com)|23.0.56.90|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 32826245 (31M) [text/xml]
Saving to: ‘com.redhat.rhsa-all.xml’

41% [===============>                        ] 13,716,436  2.16MB/s  eta 9s     _
```

Execute:

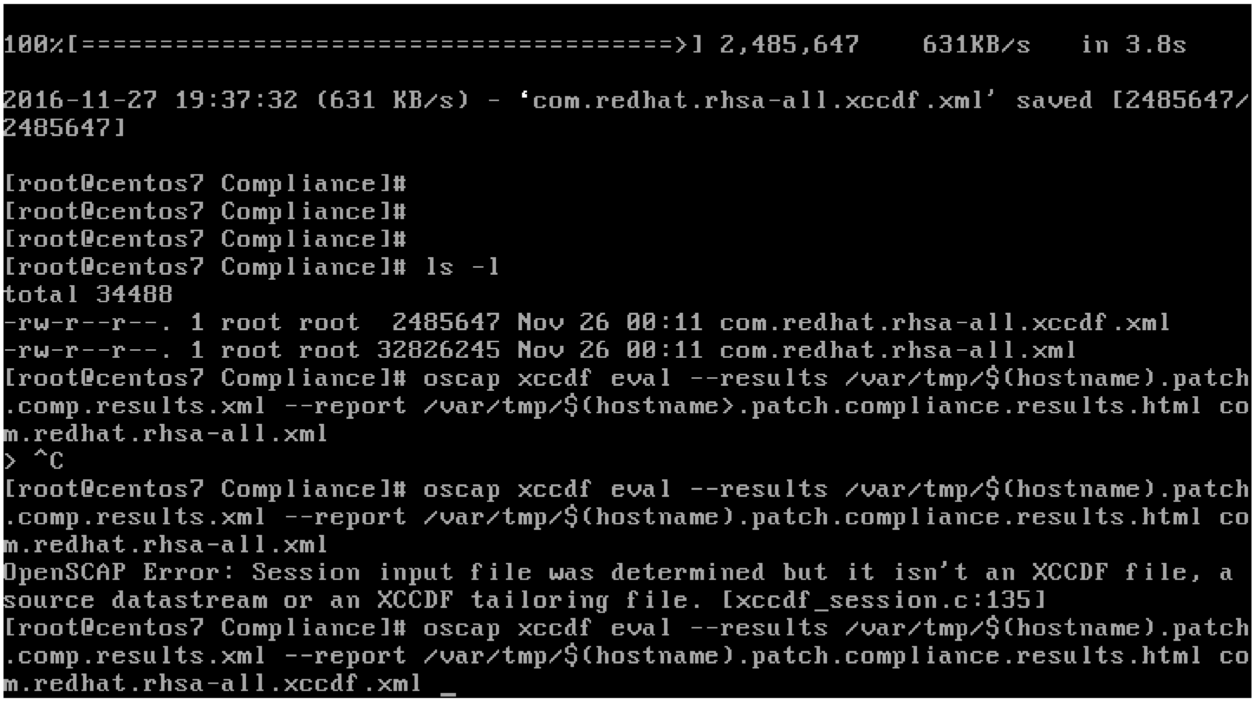
```
wget http://www.redhat.com/security/data/oval/com.redhat.rhsa-all.xml
```



```
Length: 32826245 (31M) [text/xml]
Saving to: ‘com.redhat.rhsa-all.xml’

100%[=======================================>] 32,826,245  2.14MB/s    in 14s

2016-11-27 19:36:49 (2.19 MB/s) - ‘com.redhat.rhsa-all.xml’ saved [32826245/3282
6245]

[root@centos7 Compliance]# wget http://www.redhat.com/security/data/metrics/com.
redhat.rhsa-all.xccdf.xml
--2016-11-27 19:37:28--  http://www.redhat.com/security/data/metrics/com.redhat.
rhsa-all.xccdf.xml
Resolving www.redhat.com (www.redhat.com)... 23.0.56.90, 2600:807:320:202:a200::
d44, 2600:807:320:202:9a00::d44
Connecting to www.redhat.com (www.redhat.com)|23.0.56.90|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2485647 (2.4M) [text/xml]
Saving to: ‘com.redhat.rhsa-all.xccdf.xml’

100%[=======================================>] 2,485,647    631KB/s    in 3.8s

2016-11-27 19:37:32 (631 KB/s) - ‘com.redhat.rhsa-all.xccdf.xml’ saved [2485647/
2485647]

[root@centos7 Compliance]# _
```

Execute:

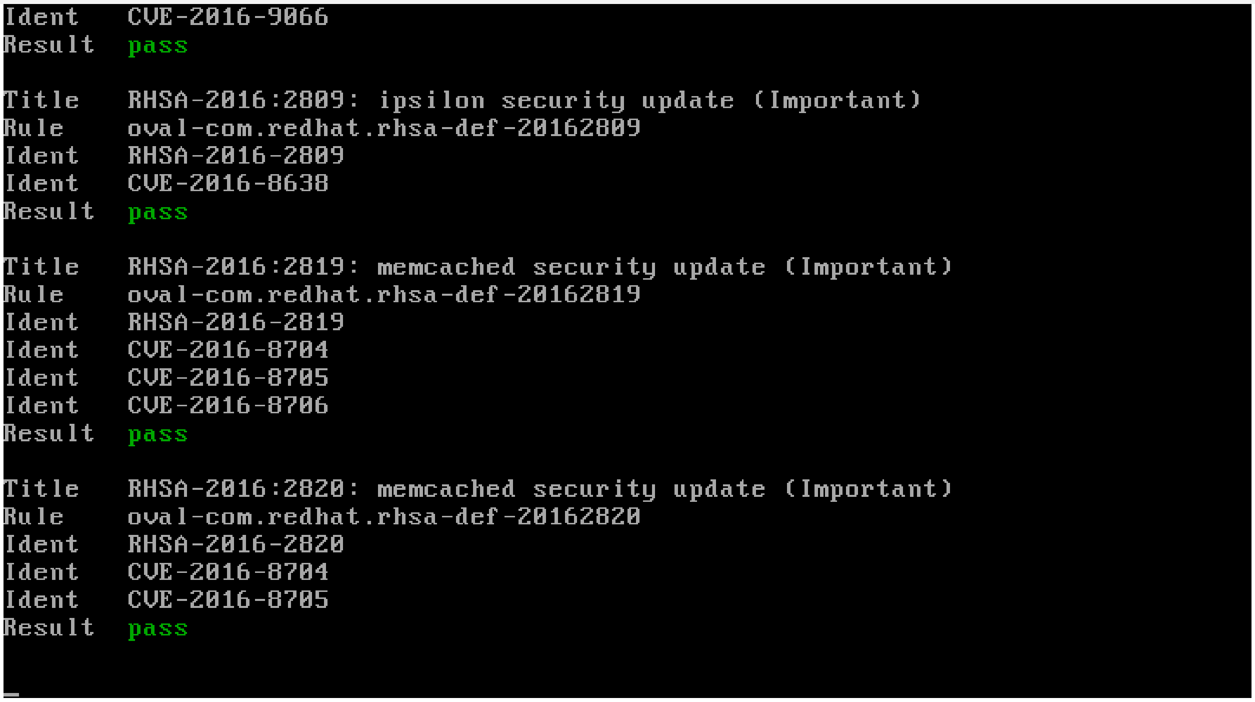
```
wget http://www.redhat.com/security/data/metrics/com.redhat.rhsa-
all.xccdf.xml
```



```
100%[======================================>] 2,485,647    631KB/s    in 3.8s

2016-11-27 19:37:32 (631 KB/s) - ‘com.redhat.rhsa-all.xccdf.xml’ saved [2485647/
2485647]

[root@centos7 Compliance]#
[root@centos7 Compliance]#
[root@centos7 Compliance]#
[root@centos7 Compliance]# ls -l
total 34488
-rw-r--r--. 1 root root  2485647 Nov 26 00:11 com.redhat.rhsa-all.xccdf.xml
-rw-r--r--. 1 root root 32826245 Nov 26 00:11 com.redhat.rhsa-all.xml
[root@centos7 Compliance]# oscap xccdf eval --results /var/tmp/$(hostname).patch
.comp.results.xml --report /var/tmp/$(hostname>.patch.compliance.results.html co
m.redhat.rhsa-all.xml
> ^C
[root@centos7 Compliance]# oscap xccdf eval --results /var/tmp/$(hostname).patch
.comp.results.xml --report /var/tmp/$(hostname).patch.compliance.results.html co
m.redhat.rhsa-all.xml
OpenSCAP Error: Session input file was determined but it isn’t an XCCDF file, a
source datastream or an XCCDF tailoring file. [xccdf_session.c:135]
[root@centos7 Compliance]# oscap xccdf eval --results /var/tmp/$(hostname).patch
.comp.results.xml --report /var/tmp/$(hostname).patch.compliance.results.html co
m.redhat.rhsa-all.xccdf.xml _
```

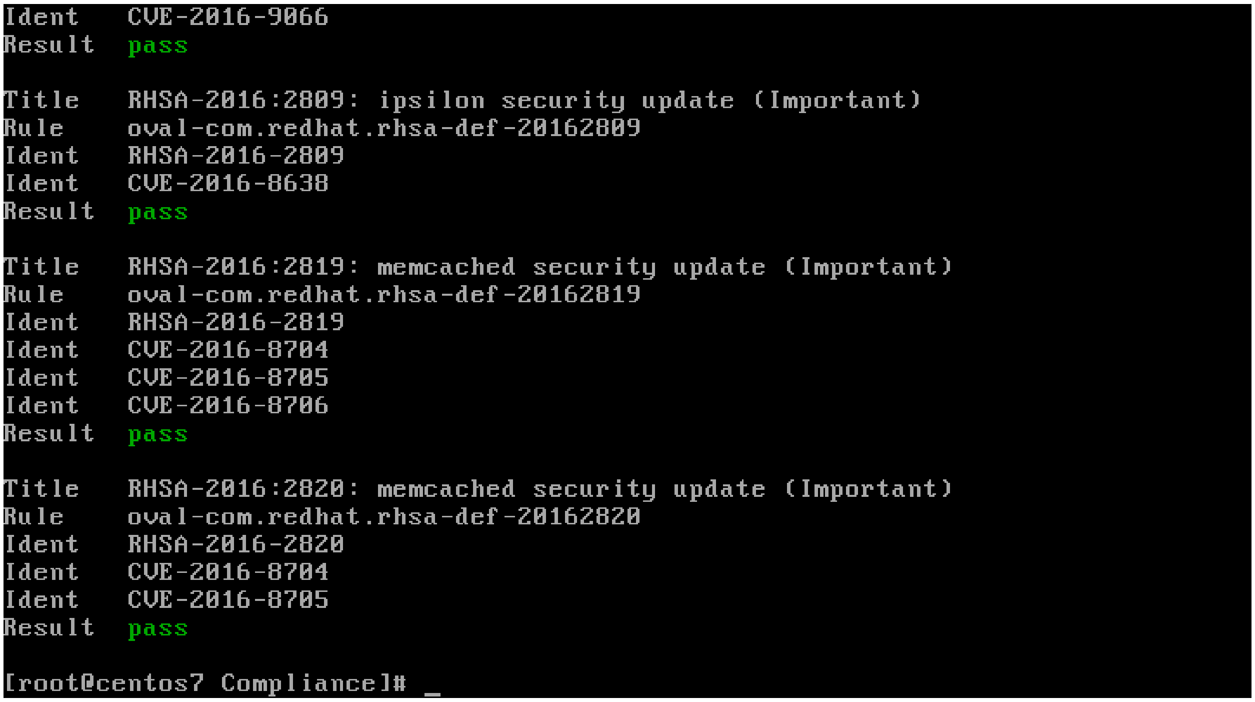
Execute:

```
oscap xccdf eval --results /var/tmp/$(hostname).patch.comp.results.xml \
  --report /var/tmp/$(hostname).patch.compliance.results.html \
  com.redhat.rhsa-all.xccdf.xml
```



```
Ident   CVE-2016-9066
Result  pass

Title   RHSA-2016:2809: ipsilon security update (Important)
Rule    oval-com.redhat.rhsa-def-20162809
Ident   RHSA-2016-2809
Ident   CVE-2016-8638
Result  pass

Title   RHSA-2016:2819: memcached security update (Important)
Rule    oval-com.redhat.rhsa-def-20162819
Ident   RHSA-2016-2819
Ident   CVE-2016-8704
Ident   CVE-2016-8705
Ident   CVE-2016-8706
Result  pass

Title   RHSA-2016:2820: memcached security update (Important)
Rule    oval-com.redhat.rhsa-def-20162820
Ident   RHSA-2016-2820
Ident   CVE-2016-8704
Ident   CVE-2016-8705
Result  pass

_
```

Output from previous command.

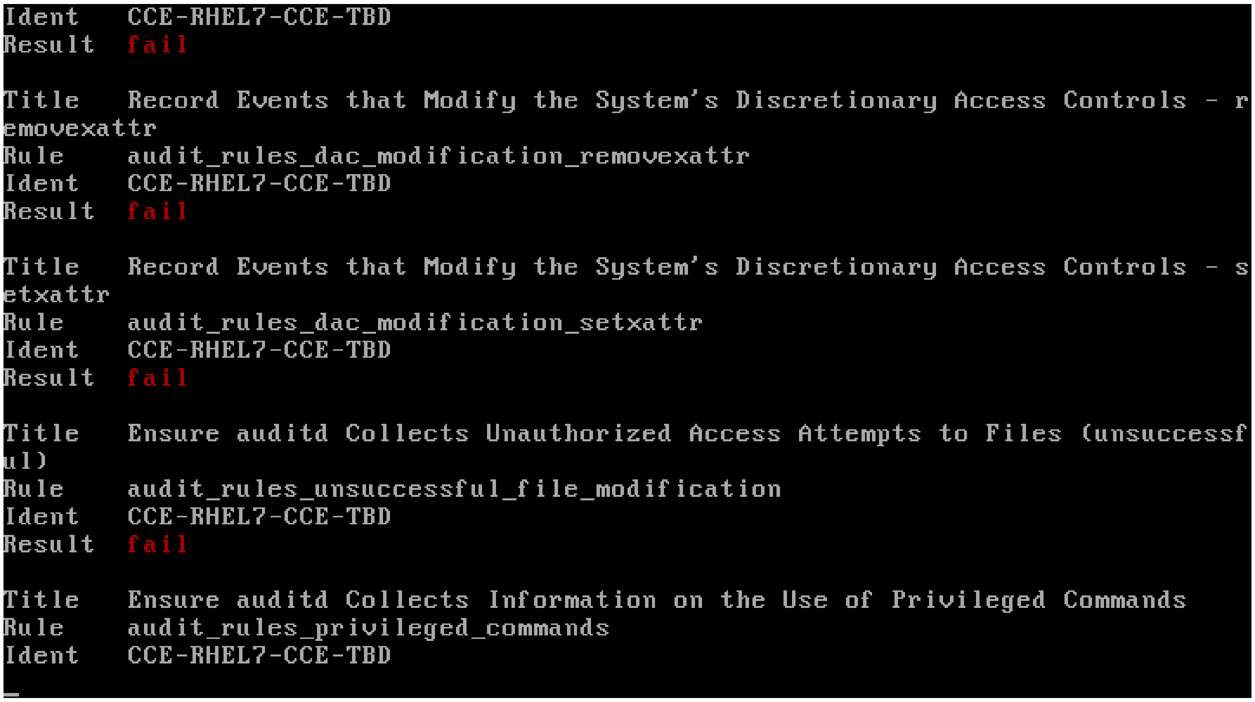


```
Ident    CVE-2016-9066
Result   pass

Title    RHSA-2016:2809: ipsilon security update (Important)
Rule     oval-com.redhat.rhsa-def-20162809
Ident    RHSA-2016-2809
Ident    CVE-2016-8638
Result   pass

Title    RHSA-2016:2819: memcached security update (Important)
Rule     oval-com.redhat.rhsa-def-20162819
Ident    RHSA-2016-2819
Ident    CVE-2016-8704
Ident    CVE-2016-8705
Ident    CVE-2016-8706
Result   pass

Title    RHSA-2016:2820: memcached security update (Important)
Rule     oval-com.redhat.rhsa-def-20162820
Ident    RHSA-2016-2820
Ident    CVE-2016-8704
Ident    CVE-2016-8705
Result   pass

[root@centos7 Compliance]# _
```

Complete.

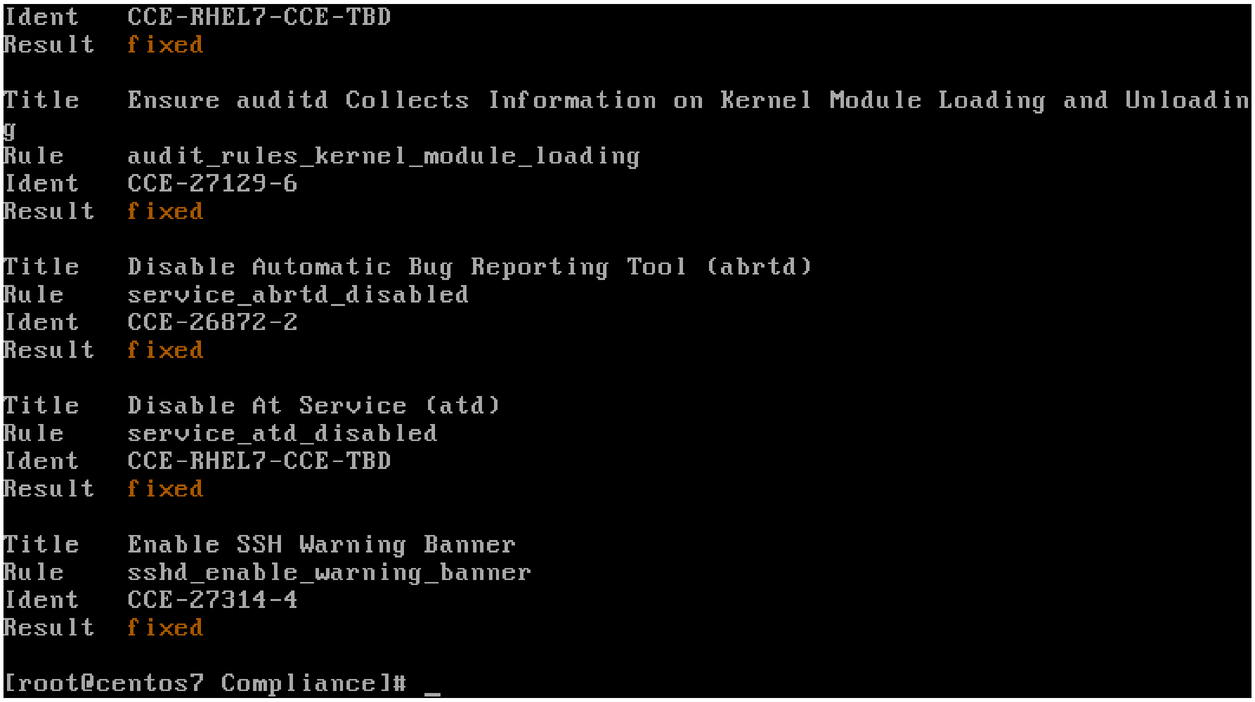
Execute:

```
oscap xccdf eval --profile stig-rhel7-server-upstream --remediate \
  --results /var/tmp/$(hostname).SSG.lockdown.xml \
  --cpe /usr/share/xml/scap/ssg/content/ssg-rhel7-cpe-dictionary.xml \
  /usr/share/xml/scap/ssg/content/ssg-centos7-xccdf.xml
```



```
Ident    CCE-RHEL7-CCE-TBD
Result   fail

Title    Record Events that Modify the System's Discretionary Access Controls - r
emovexattr
Rule     audit_rules_dac_modification_removexattr
Ident    CCE-RHEL7-CCE-TBD
Result   fail

Title    Record Events that Modify the System's Discretionary Access Controls - s
etxattr
Rule     audit_rules_dac_modification_setxattr
Ident    CCE-RHEL7-CCE-TBD
Result   fail

Title    Ensure auditd Collects Unauthorized Access Attempts to Files (unsuccessf
ul)
Rule     audit_rules_unsuccessful_file_modification
Ident    CCE-RHEL7-CCE-TBD
Result   fail

Title    Ensure auditd Collects Information on the Use of Privileged Commands
Rule     audit_rules_privileged_commands
Ident    CCE-RHEL7-CCE-TBD
_
```

Running.

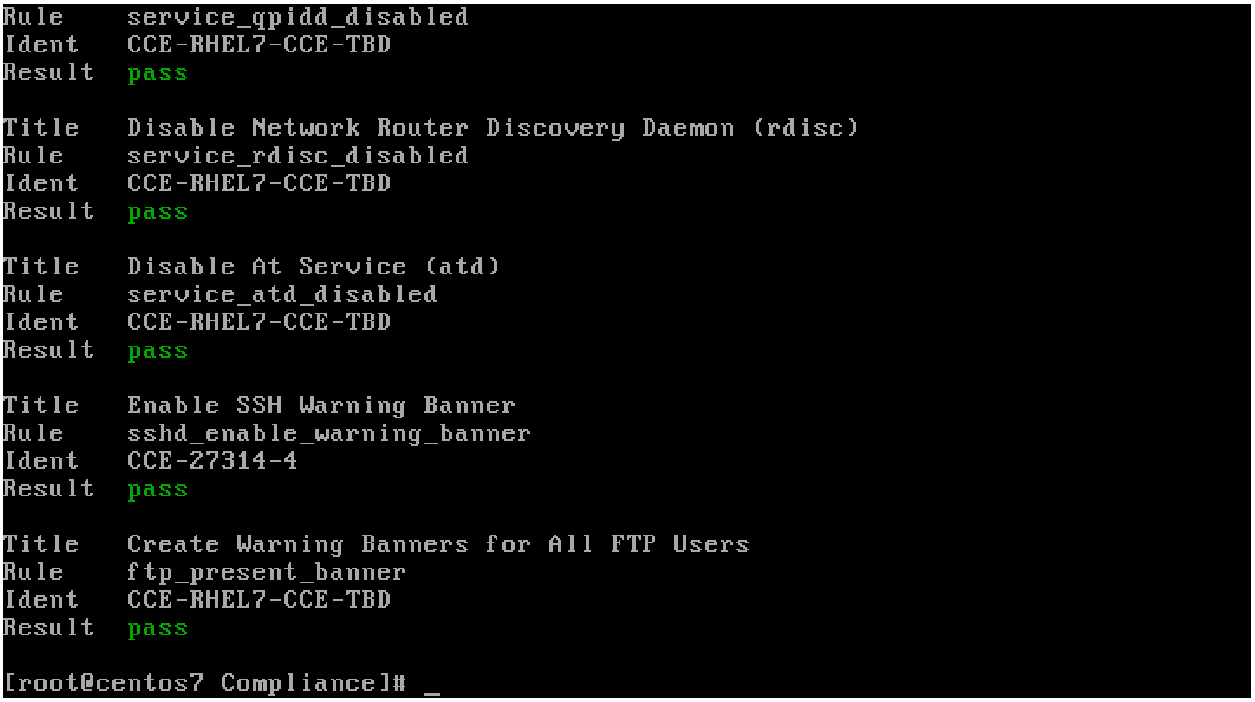


```
Ident    CCE-RHEL7-CCE-TBD
Result   fixed

Title    Ensure auditd Collects Information on Kernel Module Loading and Unloadin
g
Rule     audit_rules_kernel_module_loading
Ident    CCE-27129-6
Result   fixed

Title    Disable Automatic Bug Reporting Tool (abrtd)
Rule     service_abrtd_disabled
Ident    CCE-26872-2
Result   fixed

Title    Disable At Service (atd)
Rule     service_atd_disabled
Ident    CCE-RHEL7-CCE-TBD
Result   fixed

Title    Enable SSH Warning Banner
Rule     sshd_enable_warning_banner
Ident    CCE-27314-4
Result   fixed

[root@centos7 Compliance]# _
```

Complete.

Execute:

```
oscap xccdf eval --profile stig-rhel7-server-upstream \
  --results /var/tmp/$(hostname).compliance.results.xml \
  --report /var/tmp/$(hostname).compliance.report.html \
  --cpe /usr/share/xml/scap/ssg/content/ssg-rhel7-cpe-dictionary.xml \
  /usr/share/xml/scap/ssg/content/ssg-centos7-xccdf.xml
```



```
Rule    service_qpidd_disabled
Ident   CCE-RHEL7-CCE-TBD
Result  pass

Title   Disable Network Router Discovery Daemon (rdisc)
Rule    service_rdisc_disabled
Ident   CCE-RHEL7-CCE-TBD
Result  pass

Title   Disable At Service (atd)
Rule    service_atd_disabled
Ident   CCE-RHEL7-CCE-TBD
Result  pass

Title   Enable SSH Warning Banner
Rule    sshd_enable_warning_banner
Ident   CCE-27314-4
Result  pass

Title   Create Warning Banners for All FTP Users
Rule    ftp_present_banner
Ident   CCE-RHEL7-CCE-TBD
Result  pass

[root@centos7 Compliance]# _
```

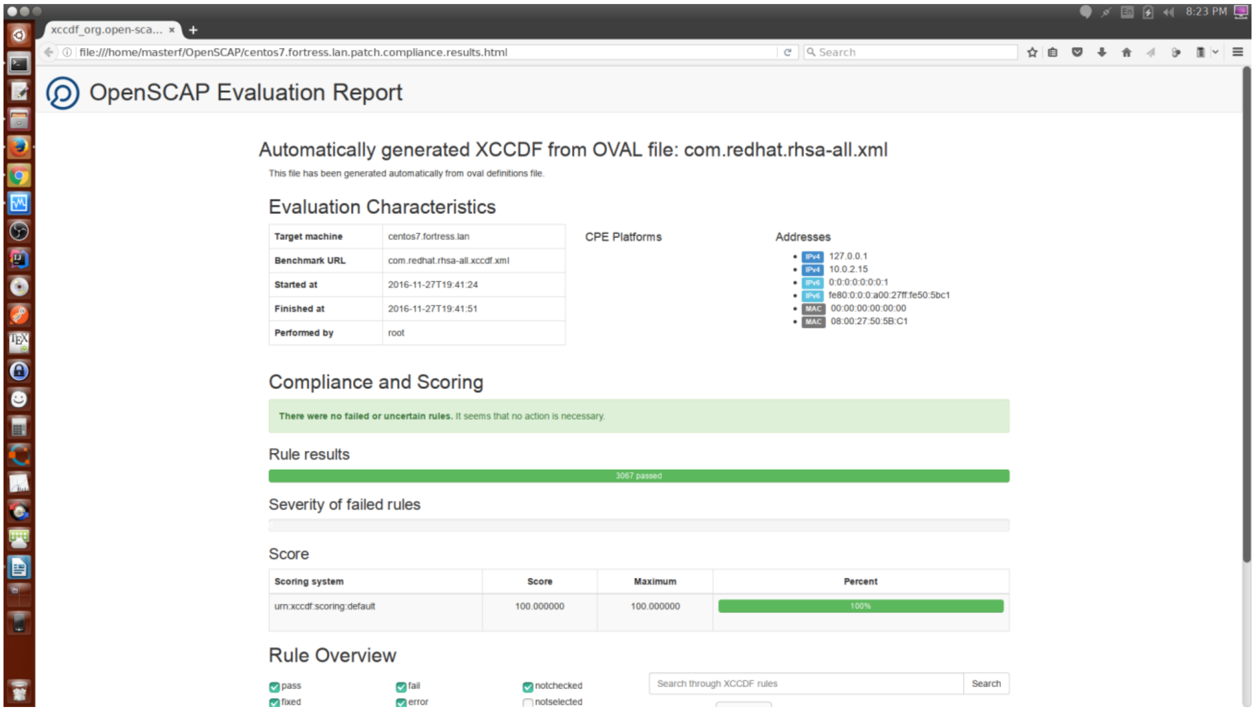
Complete.

Use SCP to get the reports off the server to your workstation for analysis, i.e.:

```
$ mkdir ~/OpenSCAP_Resutls
$ cd ~/OpenSCAP_Results/
$ scp user_name@172.20.0.105:/var/tmp/* .
```

That last command has a period on the end for the destination being the local directory.

Now, review the above results in a web browser.



file:///home/masterf/OpenSCAP/centos7.fortress.lan.patch.compliance.results.html

OpenSCAP Evaluation Report

Automatically generated XCCDF from OVAL file: com.redhat.rhsa-all.xml

This file has been generated automatically from oval definitions file.

Evaluation Characteristics

Target machine	centos7.fortress.lan
Benchmark URL	com.redhat.rhsa-all.xccdf.xml
Started at	2016-11-27T19:41:24
Finished at	2016-11-27T19:41:51
Performed by	root

CPE Platforms

Addresses

- IPv4 127.0.0.1
- IPv4 10.0.2.15
- IPv6 0:0:0:0:0:0:0:1
- IPv6 fe80:0:0:0:a00:27ff:fe50:5bc1
- MAC 00:00:00:00:00:00
- MAC 08:00:27:50:5B:C1

Compliance and Scoring

There were no failed or uncertain rules. It seems that no action is necessary.

Rule results

3067 passed

Severity of failed rules

Score

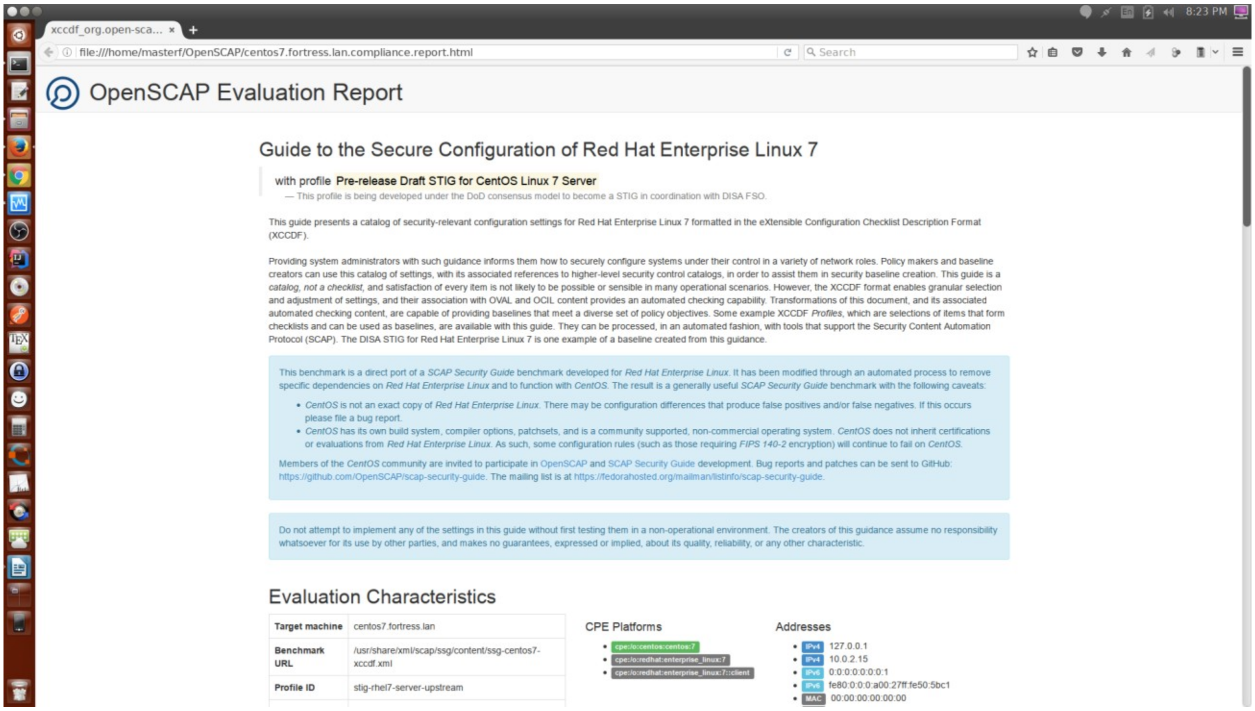
Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	100.000000	100.000000	100%

Rule Overview

☑ pass ☑ fail ☑ notchecked
☑ fixed ☑ error □ notselected

Search through XCCDF rules Search

This is just the patch report. All good here, Sir!



file:///home/masterf/OpenSCAP/centos7.fortress.lan.compliance.report.html

OpenSCAP Evaluation Report

Guide to the Secure Configuration of Red Hat Enterprise Linux 7

with profile Pre-release Draft STIG for CentOS Linux 7 Server

— This profile is being developed under the DoD consensus model to become a STIG in coordination with DISA FSO.

This guide presents a catalog of security-relevant configuration settings for Red Hat Enterprise Linux 7 formatted in the eXtensible Configuration Checklist Description Format (XCCDF).

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 for Red Hat Enterprise Linux 7 is one example of a baseline created from this guidance.

This benchmark is a direct port of a *SCAP Security Guide* benchmark developed for *Red Hat Enterprise Linux*. It has been modified through an automated process to remove specific dependencies on *Red Hat Enterprise Linux* and to function with *CentOS*. The result is a generally useful *SCAP Security Guide* benchmark with the following caveats:

- *CentOS* is not an exact copy of *Red Hat Enterprise Linux*. There may be configuration differences that produce false positives and/or false negatives. If this occurs please file a bug report.
- *CentOS* has its own build system, compiler options, patchsets, and is a community supported, non-commercial operating system. *CentOS* does not inherit certifications or evaluations from *Red Hat Enterprise Linux*. As such, some configuration rules (such as those requiring *FIPS 140-2* encryption) will continue to fail on *CentOS*.

Members of the *CentOS* community are invited to participate in OpenSCAP and SCAP Security Guide development. Bug reports and patches can be sent to GitHub: https://github.com/OpenSCAP/scap-security-guide. The mailing list is at https://fedorahosted.org/mailman/listinfo/scap-security-guide.

Do not attempt to implement any of the settings in this guide without first testing them in a non-operational environment. The creators of this guidance assume no responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic.

Evaluation Characteristics

Target machine	centos7.fortress.lan
Benchmark URL	/usr/share/xml/scap/ssg/content/ssg-centos7-xccdf.xml
Profile ID	stig-rhel7-server-upstream

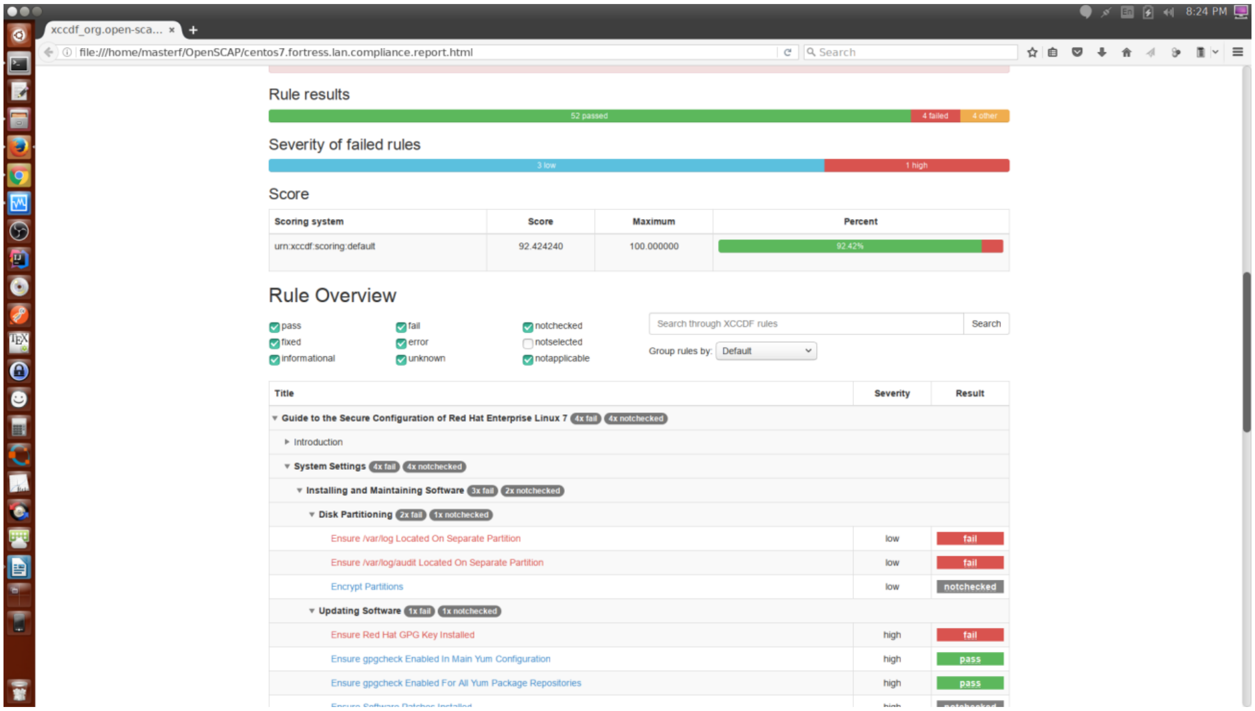
CPE Platforms

- cpe:/o:centos:centos:7
- cpe:/o:redhat:enterprise_linux:7
- cpe:/o:redhat:enterprise_linux:7::client

Addresses

- IPv4 127.0.0.1
- IPv4 10.0.2.15
- IPv6 0:0:0:0:0:0:0:1
- IPv6 fe80:0:0:0:a00:27ff:fe50:5bc1
- MAC 00:00:00:00:00:00

Now the real report, for the STIG findings.


xccdf_org.open-sca... ×
file:///home/masterf/OpenSCAP/centos7.fortress.lan.compliance.report.html
Search
8:24 PM

Rule results

52 passed
4 failed
4 other

Severity of failed rules

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	92.424240	100.000000	92.42%

Rule Overview

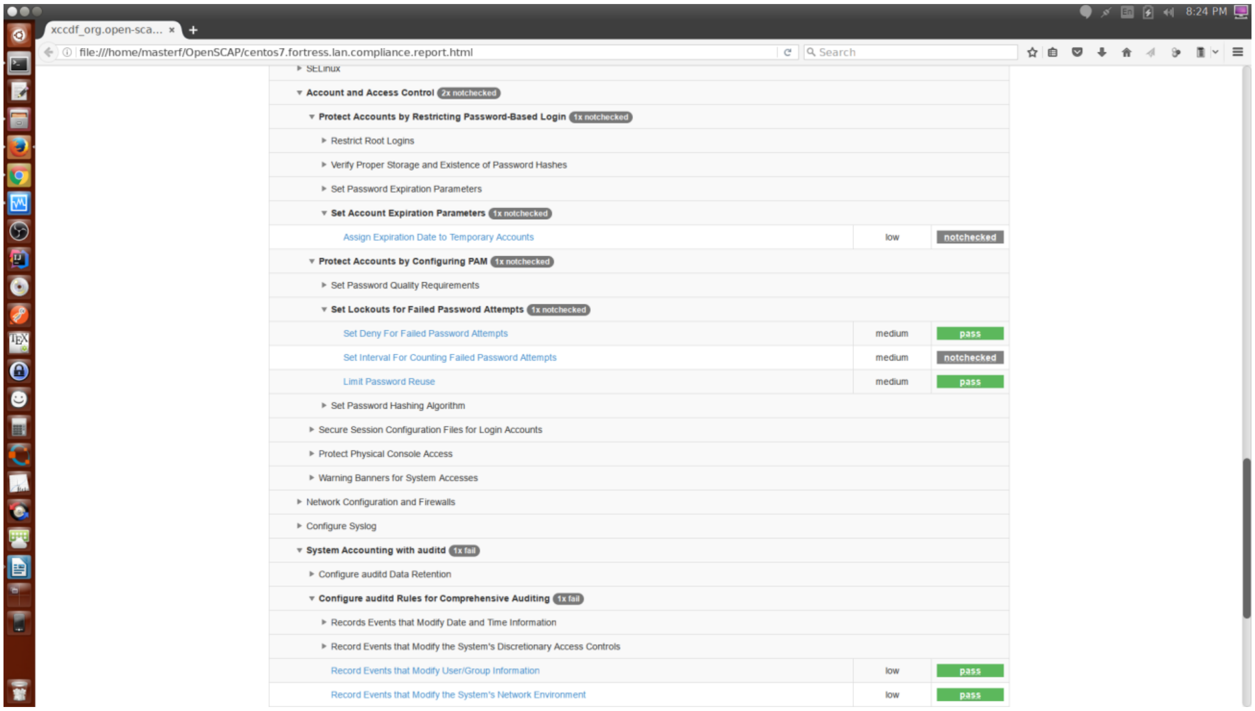
☑ pass ☑ fail ☑ notchecked
☑ fixed ☑ error □ notselected
☑ informational ☑ unknown ☑ notapplicable

Search through XCCDF rules
Search

Group rules by: Default

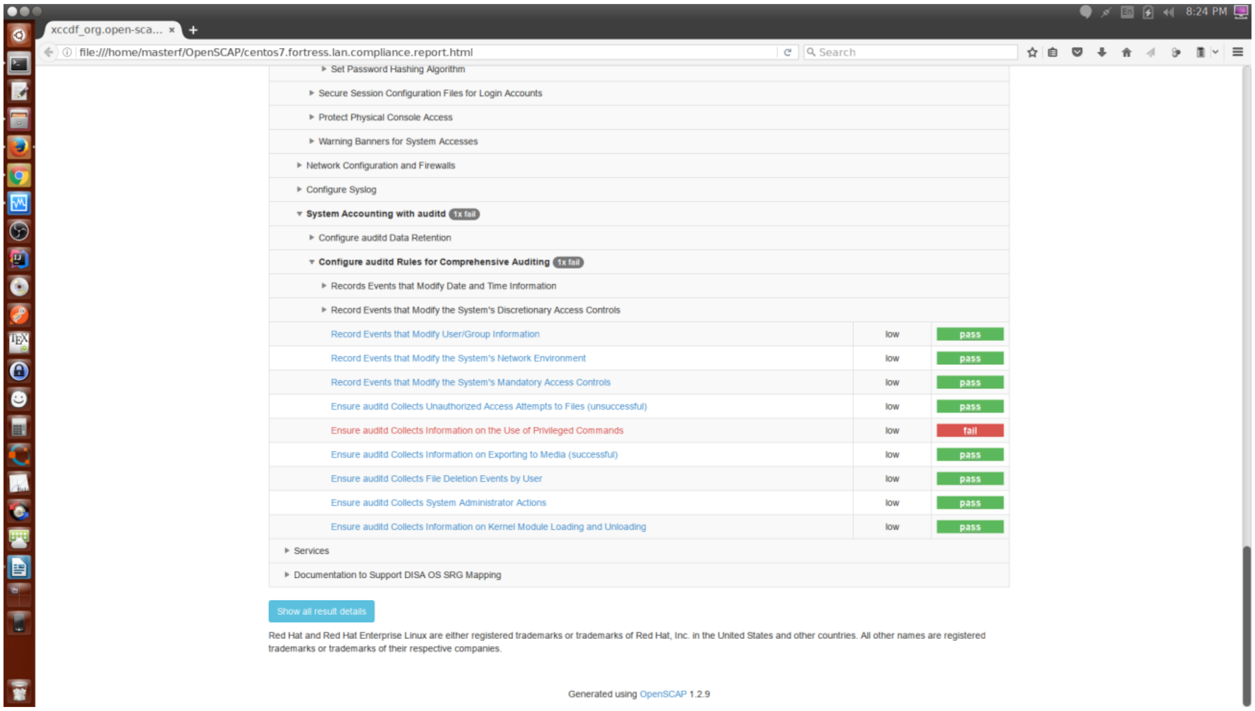
Title	Severity	Result
▾ **Guide to the Secure Configuration of Red Hat Enterprise Linux 7** 4x fail 4x notchecked		
▸ Introduction		
▾ **System Settings** 4x fail 4x notchecked		
▾ **Installing and Maintaining Software** 3x fail 2x notchecked		
▾ **Disk Partitioning** 2x fail 1x notchecked		
Ensure /var/log Located On Separate Partition	low	fail
Ensure /var/log/audit Located On Separate Partition	low	fail
Encrypt Partitions	low	notchecked
▾ **Updating Software** 1x fail 1x notchecked		
Ensure Red Hat GPG Key Installed	high	fail
Ensure gpgcheck Enabled In Main Yum Configuration	high	pass
Ensure gpgcheck Enabled For All Yum Package Repositories	high	pass
Ensure Software Patches Installed	high	notchecked

Uh Oh! We have some findings.


xccdf_org.open-sca... ×
file:///home/masterf/OpenSCAP/centos7.fortress.lan.compliance.report.html
Search
8:24 PM

▸ SELinux		
▾ **Account and Access Control** 2x notchecked		
▾ **Protect Accounts by Restricting Password-Based Login** 1x notchecked		
▸ Restrict Root Logins		
▸ Verify Proper Storage and Existence of Password Hashes		
▸ Set Password Expiration Parameters		
▾ **Set Account Expiration Parameters** 1x notchecked		
Assign Expiration Date to Temporary Accounts	low	notchecked
▾ **Protect Accounts by Configuring PAM** 1x notchecked		
▸ Set Password Quality Requirements		
▾ **Set Lockouts for Failed Password Attempts** 1x notchecked		
Set Deny For Failed Password Attempts	medium	pass
Set Interval For Counting Failed Password Attempts	medium	notchecked
Limit Password Reuse	medium	pass
▸ Set Password Hashing Algorithm		
▸ Secure Session Configuration Files for Login Accounts		
▸ Protect Physical Console Access		
▸ Warning Banners for System Accesses		
▸ Network Configuration and Firewalls		
▸ Configure Syslog		
▾ **System Accounting with auditd** 1x fail		
▸ Configure auditd Data Retention		
▾ **Configure auditd Rules for Comprehensive Auditing** 1x fail		
▸ Records Events that Modify Date and Time Information		
▸ Record Events that Modify the System's Discretionary Access Controls		
Record Events that Modify User/Group Information	low	pass
Record Events that Modify the System's Network Environment	low	pass

Some passes.


8:24 PM
xccdf_org.open-sca...
file:///home/masterf/OpenSCAP/centos7.fortress.lan.compliance.report.html
Search

- Set Password Hashing Algorithm
- Secure Session Configuration Files for Login Accounts
- Protect Physical Console Access
- Warning Banners for System Accesses
- Network Configuration and Firewalls
- Configure Syslog
- **System Accounting with auditd** 1x fail
  - Configure auditd Data Retention
  - **Configure auditd Rules for Comprehensive Auditing** 1x fail
    - Records Events that Modify Date and Time Information
    - Record Events that Modify the System's Discretionary Access Controls

Record Events that Modify User/Group Information	low	pass
Record Events that Modify the System's Network Environment	low	pass
Record Events that Modify the System's Mandatory Access Controls	low	pass
Ensure auditd Collects Unauthorized Access Attempts to Files (unsuccessful)	low	pass
Ensure auditd Collects Information on the Use of Privileged Commands	low	fail
Ensure auditd Collects Information on Exporting to Media (successful)	low	pass
Ensure auditd Collects File Deletion Events by User	low	pass
Ensure auditd Collects System Administrator Actions	low	pass
Ensure auditd Collects Information on Kernel Module Loading and Unloading	low	pass

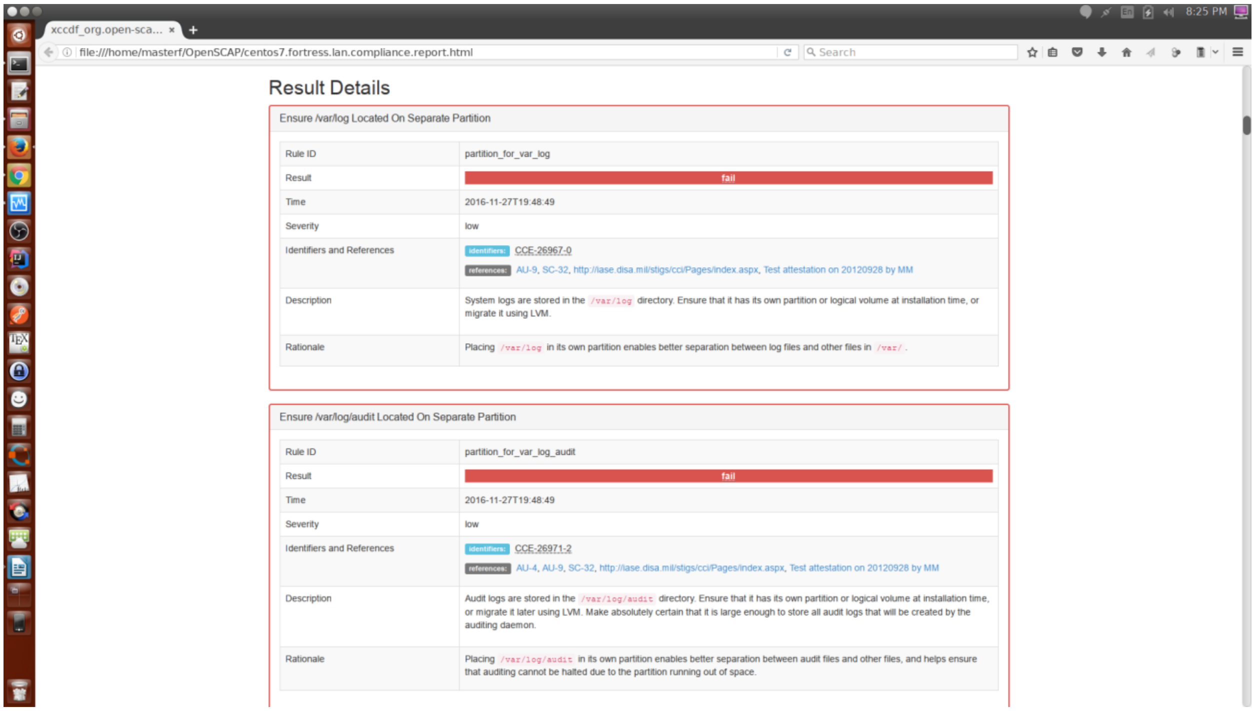
- Services
- Documentation to Support DISA OS SRG Mapping

Show all result details

Red Hat and Red Hat Enterprise Linux are either registered trademarks or trademarks of Red Hat, Inc. in the United States and other countries. All other names are registered trademarks or trademarks of their respective companies.

Generated using OpenSCAP 1.2.9

Some failures.


8:25 PM
xccdf_org.open-sca...
file:///home/masterf/OpenSCAP/centos7.fortress.lan.compliance.report.html
Search

Result Details

Ensure /var/log Located On Separate Partition

Rule ID	partition_for_var_log
Result	fail
Time	2016-11-27T19:48:49
Severity	low
Identifiers and References	identifiers: CCE-26967-0 references: AU-9, SC-32, http://iase.disa.mil/stigs/cci/Pages/index.aspx, Test attestation on 20120928 by MM
Description	System logs are stored in the `/var/log` directory. Ensure that it has its own partition or logical volume at installation time, or migrate it using LVM.
Rationale	Placing `/var/log` in its own partition enables better separation between log files and other files in `/var/` .

Ensure /var/log/audit Located On Separate Partition

Rule ID	partition_for_var_log_audit
Result	fail
Time	2016-11-27T19:48:49
Severity	low
Identifiers and References	identifiers: CCE-26971-2 references: AU-4, AU-9, SC-32, http://iase.disa.mil/stigs/cci/Pages/index.aspx, Test attestation on 20120928 by MM
Description	Audit logs are stored in the `/var/log/audit` directory. Ensure that it has its own partition or logical volume at installation time, or migrate it later using LVM. Make absolutely certain that it is large enough to store all audit logs that will be created by the auditing daemon.
Rationale	Placing `/var/log/audit` in its own partition enables better separation between audit files and other files, and helps ensure that auditing cannot be halted due to the partition running out of space.

And digging into the detailed results.

Conclusion

By following this guide, you now have a “mostly” locked down system. You will have a few stragglers you must address. If you look above for my findings, you will see I don’t have the disk partitioning correct. So this image is a no-go from the start. The only way to get this right is to go back and repartition this system with a clean install (it could be done manually, but it would take many hours to get it re-allocated). Follow the recommendations and test your application(s) frequently to make sure they still work. I have not broken a system yet with this method. It will happen, I know it; but I keep testing everything in case I have to back out of my changes.

Appendix

Command sequence:

```
yum install -y openscap openscap-utils scap-security-guide

## Verify Patch Compliance:
mkdir /root/Compliance
chmod 0700 /root/Compliance
cd /root/Compliance
wget http://www.redhat.com/security/data/oval/com.redhat.rhsa-all.xml
wget http://www.redhat.com/security/data/metrics/com.redhat.rhsa-all.xccdf.xml

oscap xccdf eval --results /var/tmp/$(hostname).patch.comp.results.xml \
  --report /var/tmp/$(hostname).patch.compliance.results.html \
  com.redhat.rhsa-all.xccdf.xml



#TEST#  Lock down the OS:
oscap xccdf eval --profile stig-rhel7-server-upstream --remediate \
  --results /var/tmp/$(hostname).SSG.lockdown.xml \
  --cpe /usr/share/xml/scap/ssg/content/ssg-rhel7-cpe-dictionary.xml \
  /usr/share/xml/scap/ssg/content/ssg-centos7-xccdf.xml


## verify systems compliance level:
oscap xccdf eval --profile stig-rhel7-server-upstream \
  --results /var/tmp/$(hostname).compliance.results.xml \
  --report /var/tmp/$(hostname).compliance.report.html \
  --cpe /usr/share/xml/scap/ssg/content/ssg-rhel7-cpe-dictionary.xml \
  /usr/share/xml/scap/ssg/content/ssg-centos7-xccdf.xml
```