Server

Security

Automation with

Ansible

Chemnitzer Linux-Tage
13th and 14th March 2021

2021.03.14 18:00 V3

Dr. Benjamin Aleritsch

Dr. Benjamin Aleritsch

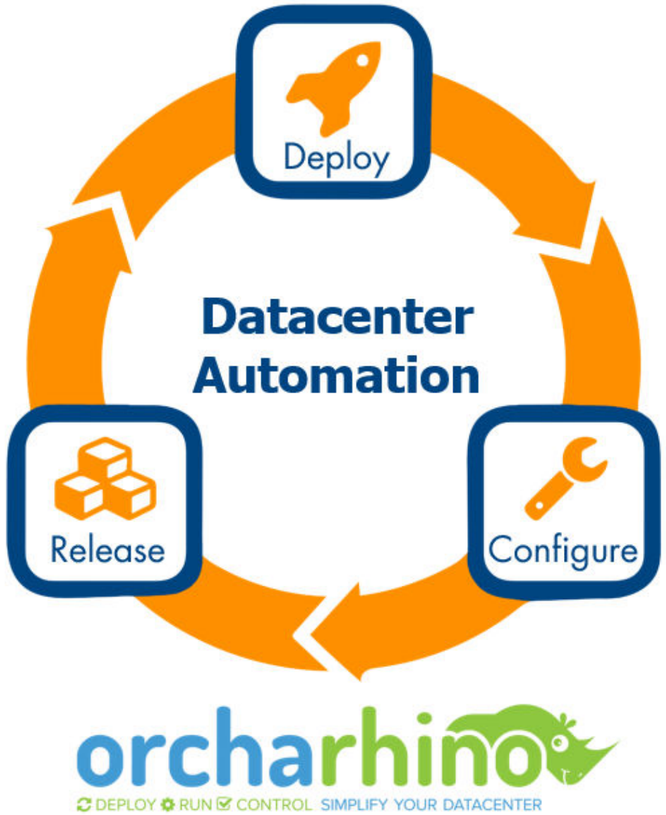
IT Consultant

kubernetes

RED HAT OPENSHIFT

APACHE kafka

Red Hat



ANSIBLE

SUSE CaaS Platform

puppet

RANCHER

orcharhino

DEPLOY RUN CONTROL SIMPLIFY YOUR DATACENTER

Prometheus

docker

SALTSTACK

Grafana

Server Security Automation with Ansible

- Ansible
- Security: SCAP
  - OpenSCAP
  - OpenSCAP Demo
- Ansible: OSPP Code Audit
- Security: STIG
- Ansible: STIG Code Audit
  - STIG Demo
  - DISA STIG Code Audit
  - DISA STIG Demo
- Bonus

Ansible

“is a category of fictional devices or technology capable of near-instantaneous or faster-than-light communication. It can send and receive messages to and from a corresponding device over any distance or obstacle whatsoever with no delay, even between star systems”

https://en.wikipedia.org/wiki/Ansible

Ansible

“is a category of fictional devices or technology capable of near-instantaneous or faster-than-light communication. It can send and receive messages to and from a corresponding device over any distance or obstacle whatsoever with no delay, even between star systems”

https://en.wikipedia.org/wiki/Ansible

- SSH Connect

Ansible

“is a category of fictional devices or technology capable of near-instantaneous or faster-than-light communication. It can send and receive messages to and from a corresponding device over any distance or obstacle whatsoever with no delay, even between star systems”

https://en.wikipedia.org/wiki/Ansible

- SSH Connect

Ansible

“is a category of fictional devices or technology capable of near-instantaneous or faster-than-light communication. It can send and receive messages to and from a corresponding device over any distance or obstacle whatsoever with no delay, even between star systems”

https://en.wikipedia.org/wiki/Ansible

- SSH Connect

Ansible

“is a category of fictional devices or technology capable of near-instantaneous or faster-than-light communication. It can send and receive messages to and from a corresponding device over any distance or obstacle whatsoever with no delay, even between star systems”

https://en.wikipedia.org/wiki/Ansible

- SSH Connect

- YAML (& INI) Parser

Ansible

"is a category of fictional devices or technology capable of near-instantaneous or faster-than-light communication. It can send and receive messages to and from a corresponding device over any distance or obstacle whatsoever with no delay, even between star systems"

https://en.wikipedia.org/wiki/Ansible

- SSH Connect
- YAML (& INI) Parser
- Inventory: Servergroups

Ansible

“is a category of fictional devices or technology capable of near-instantaneous or faster-than-light communication. It can send and receive messages to and from a corresponding device over any distance or obstacle whatsoever with no delay, even between star systems”

https://en.wikipedia.org/wiki/Ansible

- SSH Connect
- YAML (& INI) Parser
- Inventory: Servergroups

```
---
all:
  vars:
    ansible_user: ben
    ansible_ssh_pass: 0815
    ansible_become_pass: 0815

first_hostgroup:
  hosts:
    192.168.178.50:
      ansible_host: hostname0815-1
    192.168.178.51:
      ansible_host: hostname0815-2

second_hostgroup:
  hosts:
    192.168.178.60:
      ansible_host: hostname0816-1
    192.168.178.61:
      ansible_host: hostname0816-2
    192.168.178.62:
      ansible_host: hostname0816-3
...
```

Ansible

"is a category of fictional devices or technology capable of near-instantaneous or faster-than-light communication. It can send and receive messages to and from a corresponding device over any distance or obstacle whatsoever with no delay, even between star systems"

https://en.wikipedia.org/wiki/Ansible

- SSH Connect
- YAML (& INI) Parser
- Inventory: Servergroups
- Written in Python

Ansible

“is a category of fictional devices or technology capable of near-instantaneous or faster-than-light communication. It can send and receive messages to and from a corresponding device over any distance or obstacle whatsoever with no delay, even between star systems”

https://en.wikipedia.org/wiki/Ansible

- SSH Connect
- YAML (& INI) Parser
- Inventory: Servergroups
- Written in Python
- "Clientless"

Ansible

> “is a category of fictional devices or technology capable of near-instantaneous or faster-than-light communication. It can send and receive messages to and from a corresponding device over any distance or obstacle whatsoever with no delay, even between star systems”
>
> https://en.wikipedia.org/wiki/Ansible

- SSH Connect
- YAML (& INI) Parser
- Inventory: Servergroups
- Written in Python
- "Clientless"
- Playbook: Tasks

Ansible

“is a category of fictional devices or technology capable of near-instantaneous or faster-than-light communication. It can send and receive messages to and from a corresponding device over any distance or obstacle whatsoever with no delay, even between star systems”

https://en.wikipedia.org/wiki/Ansible

- SSH Connect
- YAML (& INI) Parser
- Inventory: Servergroups
- Written in Python
- "Clientless"
- Playbook: Tasks

```
---
- hosts: localhost
  tasks:
    - debug:
        msg: "Hello World!"
...
```

Ansible

> “is a category of fictional devices or technology capable of near-instantaneous or faster-than-light communication. It can send and receive messages to and from a corresponding device over any distance or obstacle whatsoever with no delay, even between star systems”
>
> https://en.wikipedia.org/wiki/Ansible

- SSH Connect
- YAML (& INI) Parser
- Inventory: Servergroups
- Written in Python
- "Clientless"
- Playbook: Tasks
- Tasks from Modules

Ansible

“is a category of fictional devices or technology capable of near-instantaneous or faster-than-light communication. It can send and receive messages to and from a corresponding device over any distance or obstacle whatsoever with no delay, even between star systems”

https://en.wikipedia.org/wiki/Ansible

- SSH Connect
- YAML (& INI) Parser
- Inventory: Servergroups
- Written in Python
- "Clientless"
- Playbook: Tasks
- Tasks from Modules

Examples

```yaml
- name: install the latest version of Apache
  yum:
    name: httpd
    state: latest

- name: ensure a list of packages installed
  yum:
    name: "{{ packages }}"
  vars:
    packages:
    - httpd
    - httpd-tools

- name: Download the nginx package but do not install it
  yum:
    name:
      - nginx
    state: latest
    download_only: true
```

Ansible

“is a category of fictional devices or technology capable of near-instantaneous or faster-than-light communication. It can send and receive messages to and from a corresponding device over any distance or obstacle whatsoever with no delay, even between star systems”

https://en.wikipedia.org/wiki/Ansible

- SSH Connect
- YAML (& INI) Parser
- Inventory: Servergroups
- Written in Python
- "Clientless"
- Playbook: Tasks
- Tasks from Modules

Examples

```
- name: install the latest version of Apache
  yum:
    name: httpd
    state: latest

- name: ensure a list of packages installed
  yum:
    name: "{{ packages }}"
  vars:
    packages:
    - httpd
    - httpd-tools

- name: Download the nginx package but do not install it
  yum:
    name:
      - nginx
    state: latest
    download_only: true
```

Ansible

“is a category of fictional devices or technology capable of near-instantaneous or faster-than-light communication. It can send and receive messages to and from a corresponding device over any distance or obstacle whatsoever with no delay, even between star systems”

https://en.wikipedia.org/wiki/Ansible

- SSH Connect
- YAML (& INI) Parser
- Inventory: Servergroups
- Written in Python
- "Clientless"
- Playbook: Tasks
- Tasks from Modules

Examples

```
- name: install the latest version of Apache
  yum:
    name: httpd
    state: latest

- name: ensure a list of packages installed
  yum:
    name: "{{ packages }}"
  vars:
    packages:
    - httpd
    - httpd-tools

- name: Download the nginx package but do not install it
  yum:
    name:
      - nginx
    state: latest
    download_only: true
```

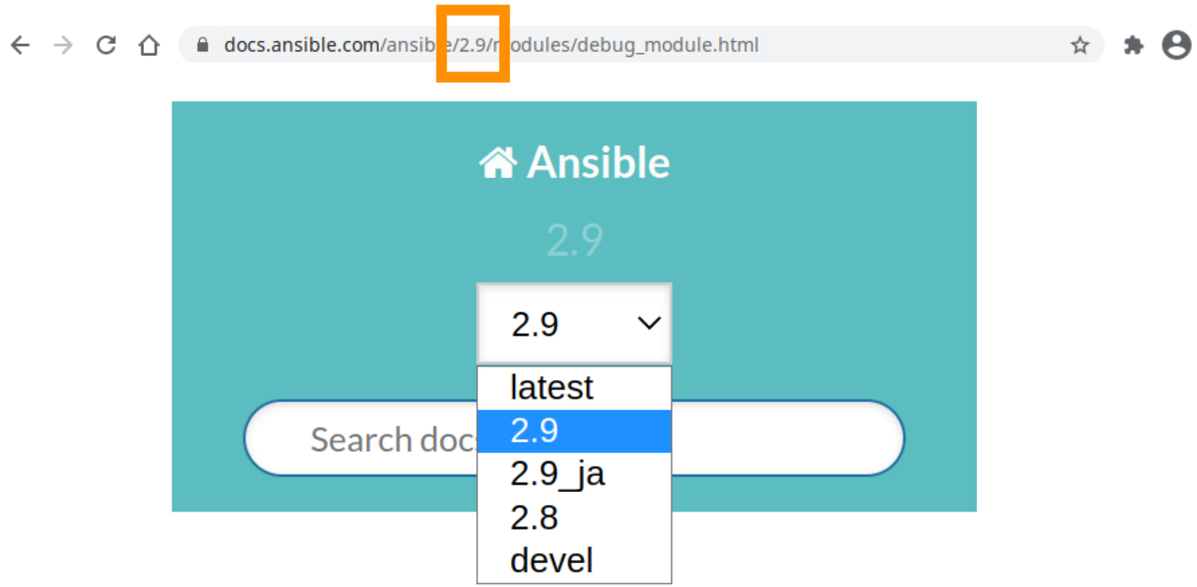
https://docs.ansible.com/ansible/latest/collections/ansible/builtin/yum_module.html

Ansible

"is a category of fictional devices or technology capable of near-instantaneous or faster-than-light communication. It can send and receive messages to and from a corresponding device over any distance or obstacle whatsoever with no delay, even between star systems"

https://en.wikipedia.org/wiki/Ansible

- SSH Connect
- YAML (& INI) Parser
- Inventory: Servergroups
- Written in Python
- "Clientless"
- Playbook: Tasks
- Tasks from Modules
- Beware Version: 2.9 vs. 2.10 vs. 3.0



Ansible

> “is a category of fictional devices or technology capable of near-instantaneous or faster-than-light communication. It can send and receive messages to and from a corresponding device over any distance or obstacle whatsoever with no delay, even between star systems”
>
> https://en.wikipedia.org/wiki/Ansible

- SSH Connect
- YAML (& INI) Parser
- Inventory: Servergroups
- Written in Python
- "Clientless"
- Playbook: Tasks
- Tasks from Modules
- Beware Version: 2.9 vs. 2.10 vs. 3.0
- Group Tasks in Roles & Blocks

Security: SCAP

Security Content Automation Protocol

SCAP v1.3 Components (February 2018)

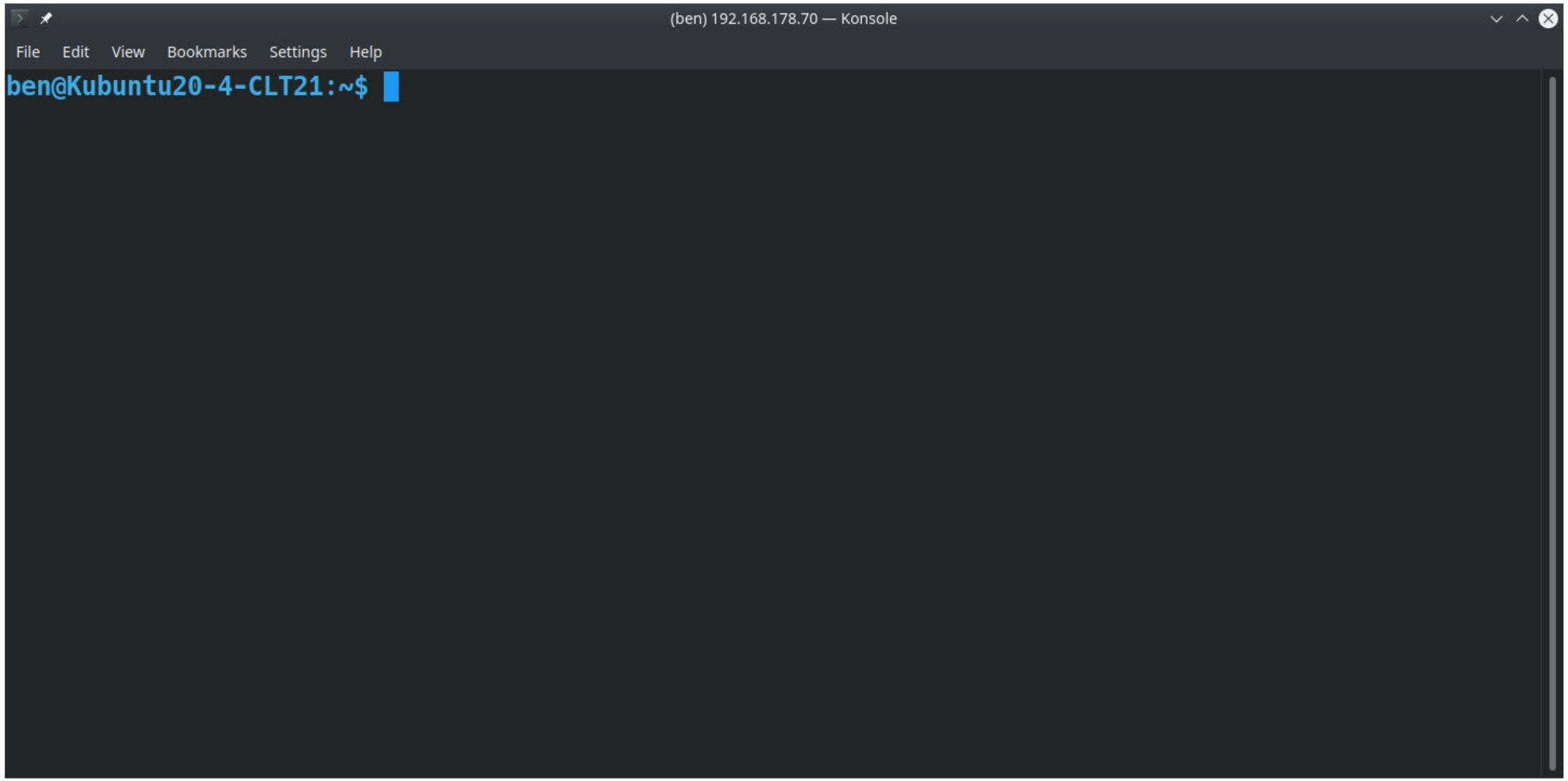
- Common Vulnerabilities and Exposures	CVE
- Common Configuration Enumeration	CCE
- Common Platform Enumeration	CPE
- Common Vulnerability Scoring System	CVSS
- Extensible Configuration Checklist Description Form	XCCDF
- Open Vulnerability and Assessment Language	OVAL
- Open Checklist Interactive Language	OCIL
- Asset Identification	AID
- Asset Reporting Format	ARF
- Common Configuration Scoring System	CCSS
- Trust Model for Security Automation Data	TMSAD
- Software Identification tags	SWID

Security: OpenSCAP

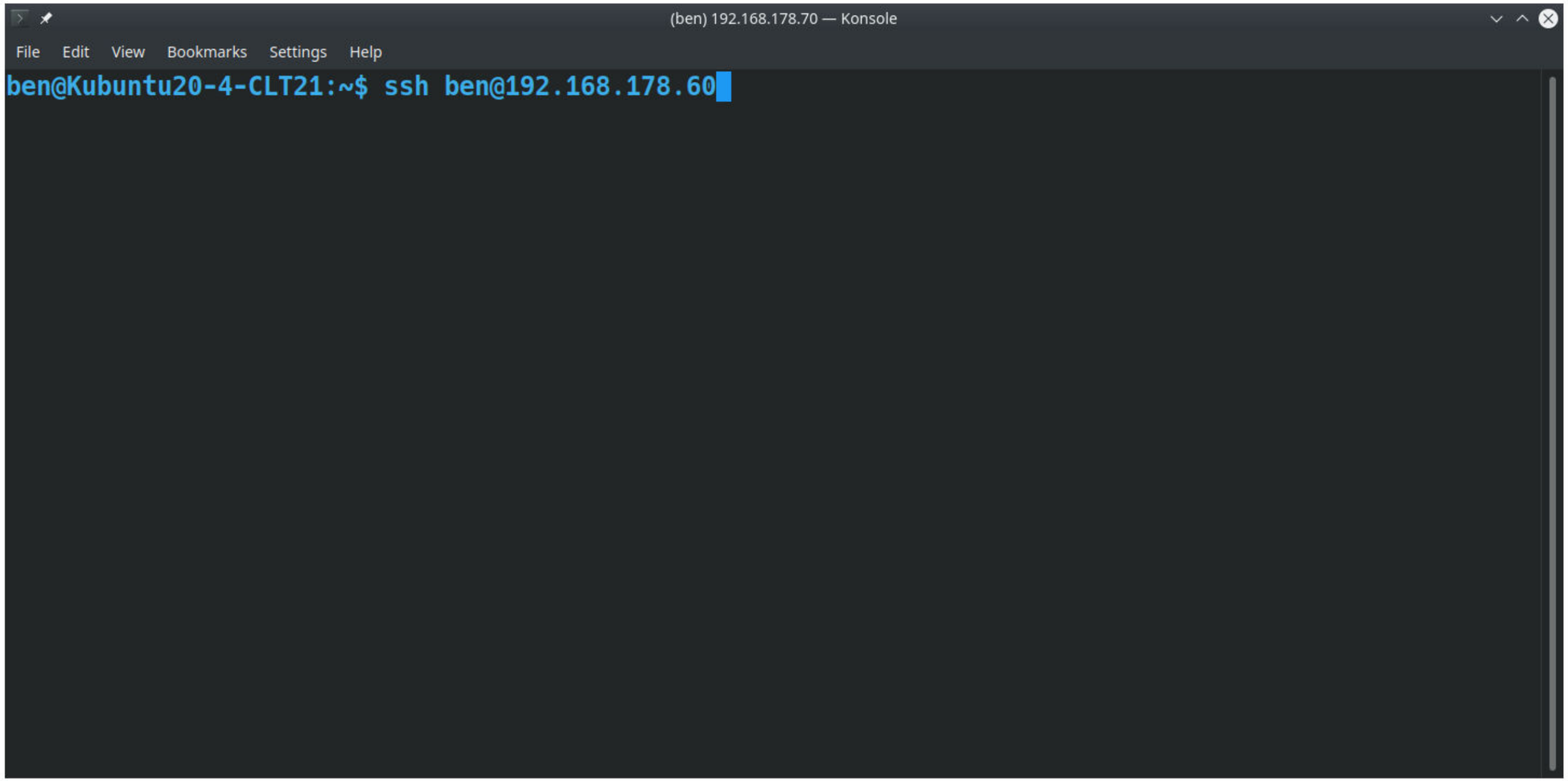
OpenSCAP Base:	oscap Command Line Interface
OpenSCAP Daemon:	Continuous SCAP Compliance Evaluation
SCAP Workbench:	Custom Security Profile / Scan Systems remotely
SCAPTimony:	Organize SCAP Scan Result Storage
Anaconda:	Compliant System Image Creation

Security: OpenSCAP Demo

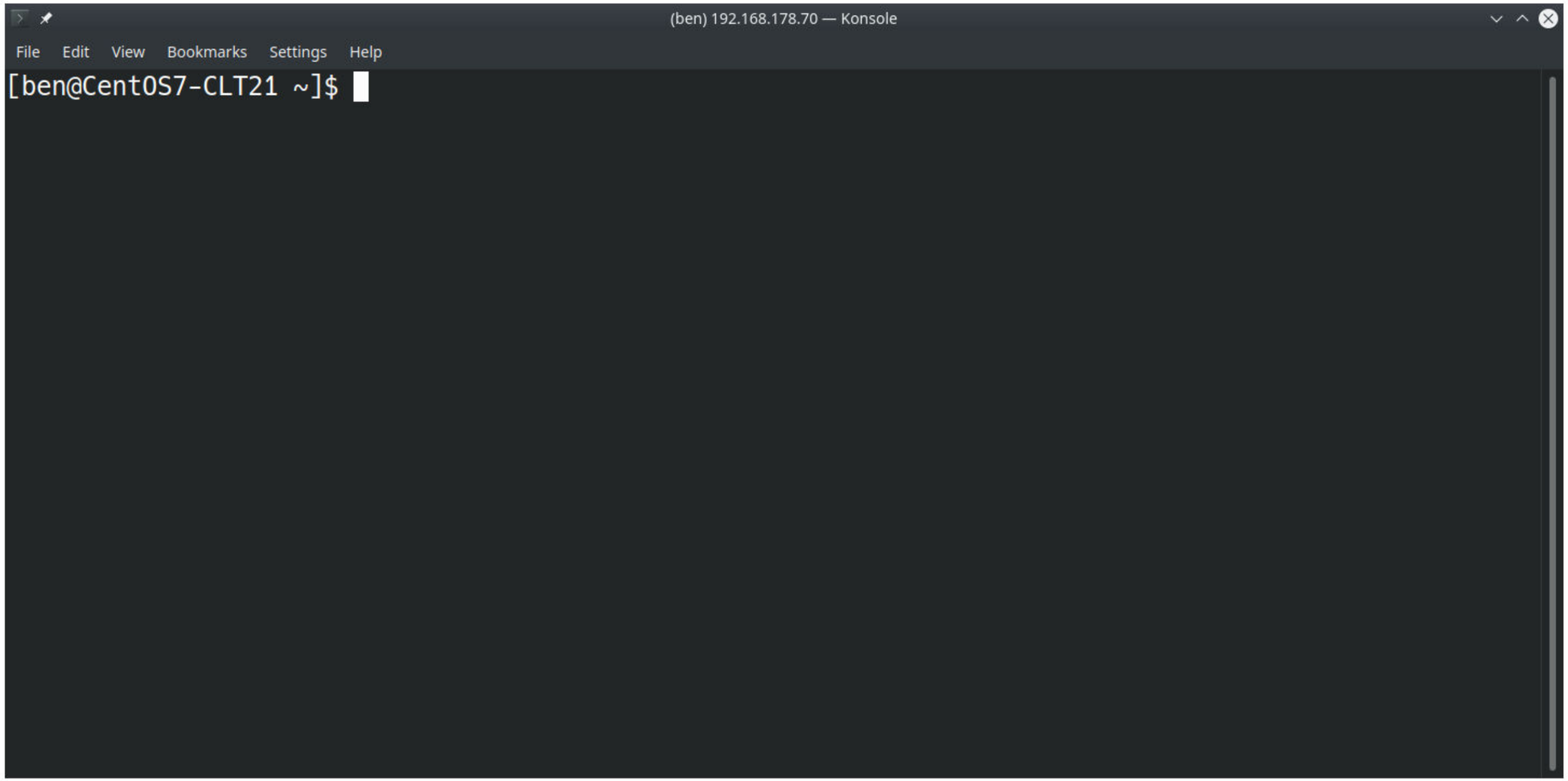
Security: OpenSCAP Demo



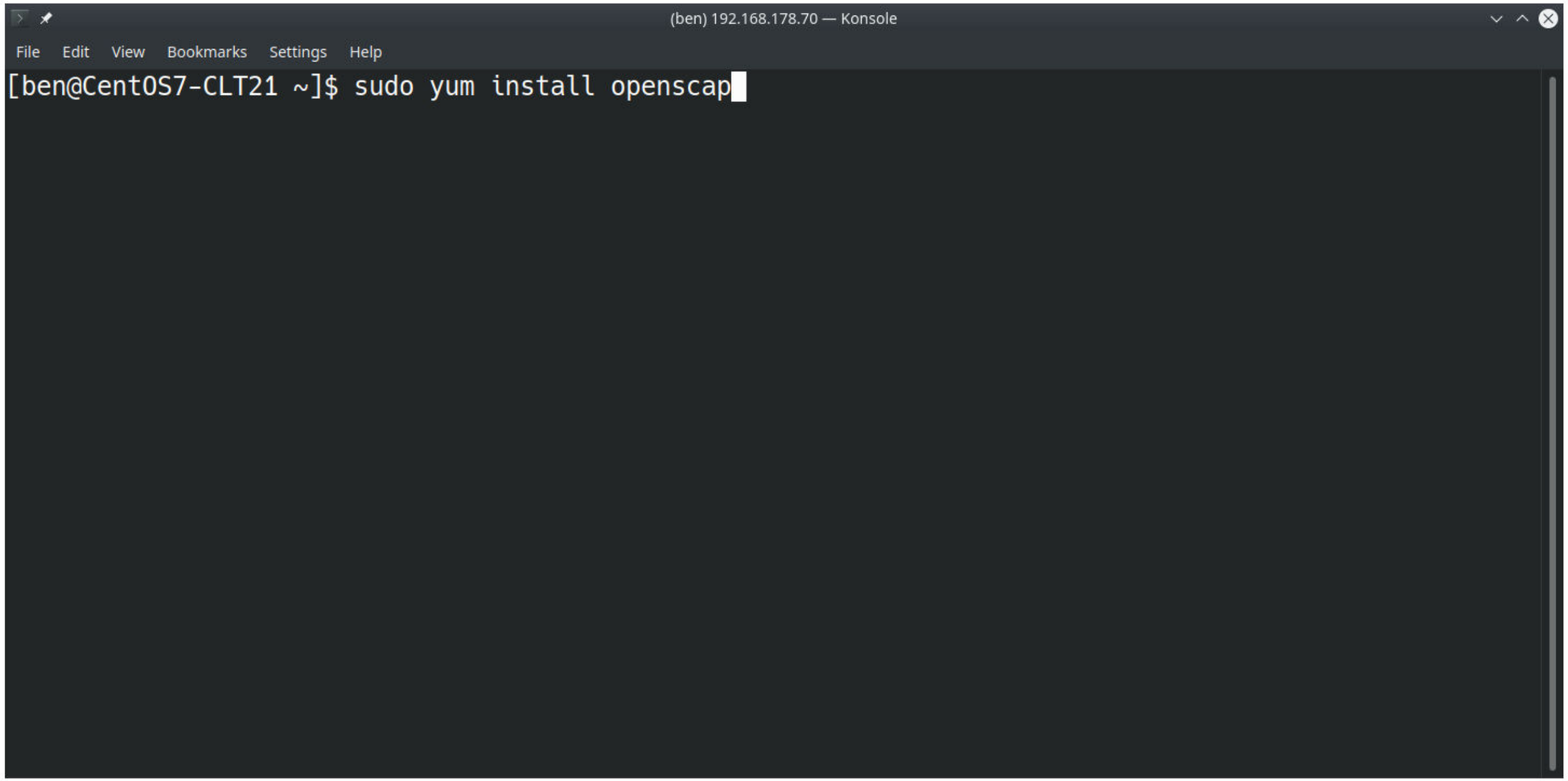
Security: OpenSCAP Demo



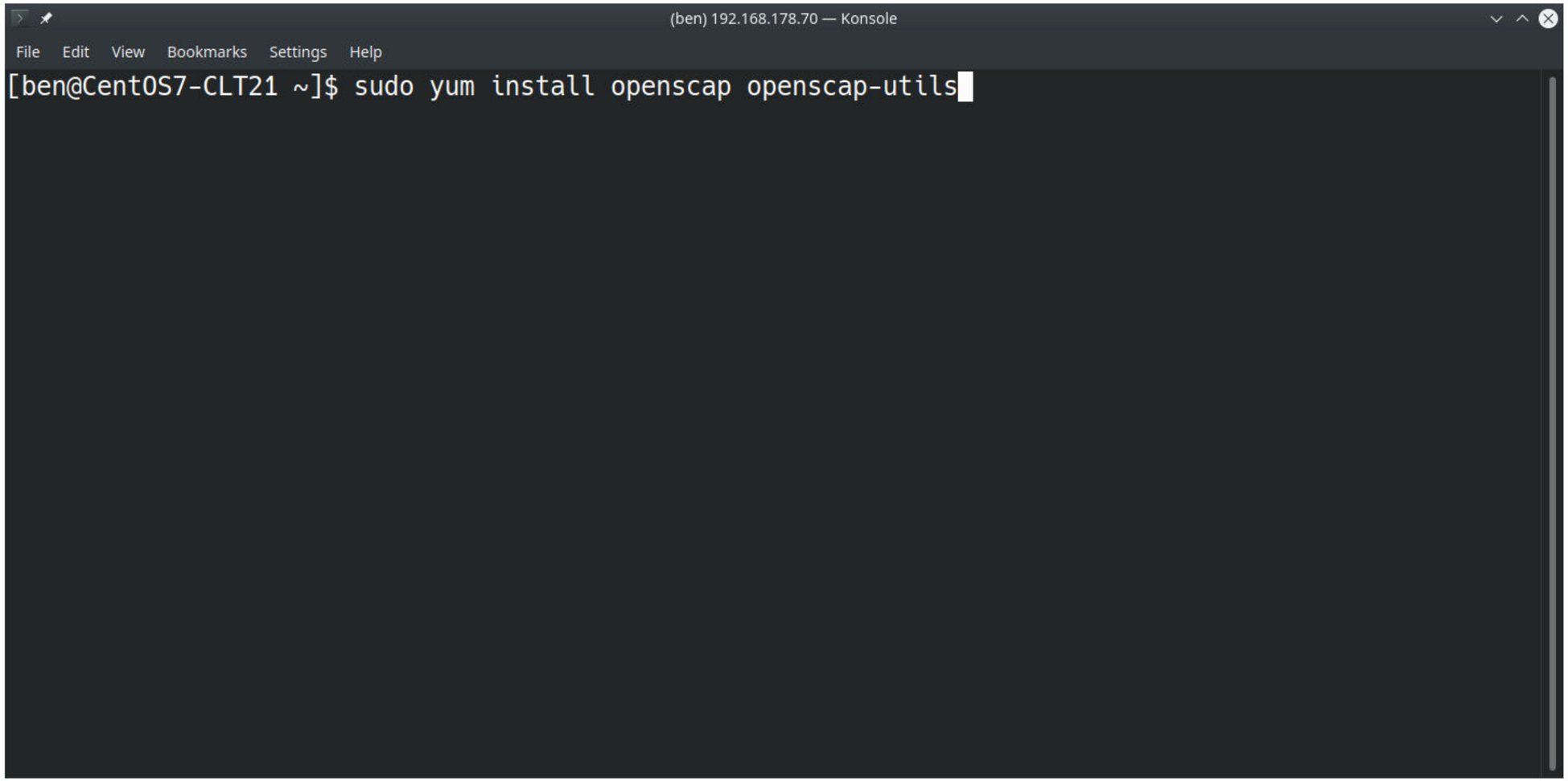
Security: OpenSCAP Demo



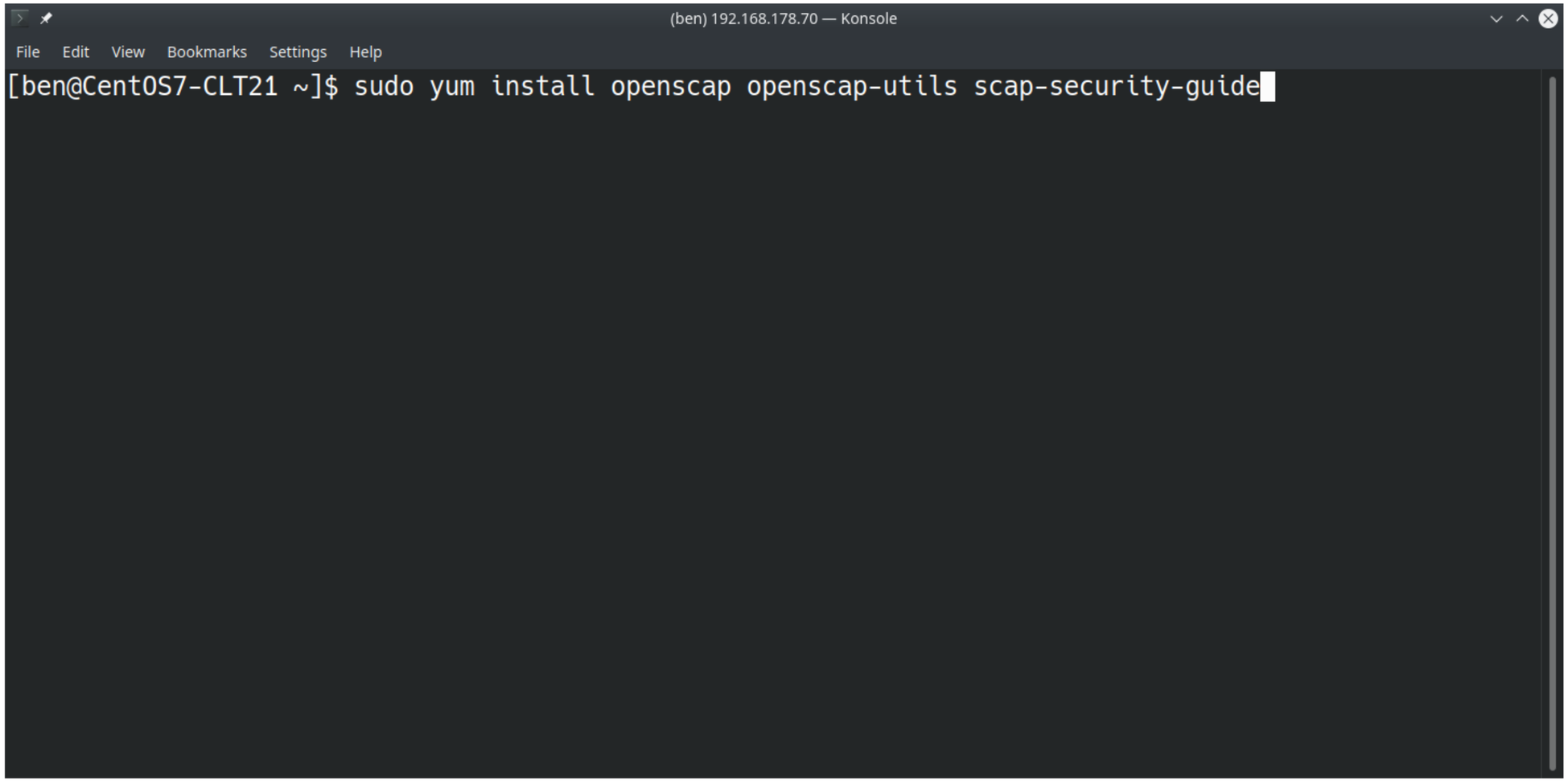
Security: OpenSCAP Demo



Security: OpenSCAP Demo



Security: OpenSCAP Demo



Security: OpenSCAP Demo

(ben) 192.168.178.70 — Konsole

File Edit View Bookmarks Settings Help

```
[ben@CentOS7-CLT21 ~]$ sudo yum install openscap openscap-utils scap-security-guide git nano epel-rel
ease -y
```

Security: OpenSCAP Demo

(ben) 192.168.178.70 — Konsole

File Edit View Bookmarks Settings Help

```
  perl-Error.noarch 1:0.17020-2.el7                perl-Exporter.noarch 0:5.68-3.el7
  perl-File-Path.noarch 0:2.09-2.el7               perl-File-Temp.noarch 0:0.23.01-3.el7
  perl-Filter.x86_64 0:1.49-3.el7                  perl-Getopt-Long.noarch 0:2.40-3.el7
  perl-Git.noarch 0:1.8.3.1-23.el7_8               perl-HTTP-Tiny.noarch 0:0.033-3.el7
  perl-PathTools.x86_64 0:3.40-5.el7               perl-Pod-Escapes.noarch 1:1.04-299.el7_9
  perl-Pod-Perldoc.noarch 0:3.20-4.el7             perl-Pod-Simple.noarch 1:3.28-4.el7
  perl-Pod-Usage.noarch 0:1.63-3.el7               perl-Scalar-List-Utils.x86_64 0:1.27-248.el7
  perl-Socket.x86_64 0:2.010-5.el7                 perl-Storable.x86_64 0:2.45-3.el7
  perl-TermReadKey.x86_64 0:2.30-20.el7            perl-Text-ParseWords.noarch 0:3.29-4.el7
  perl-Thread-Queue.noarch 0:3.02-2.el7            perl-Time-HiRes.x86_64 4:1.9725-3.el7
  perl-Time-Local.noarch 0:1.2300-2.el7            perl-constant.noarch 0:1.27-2.el7
  perl-libs.x86_64 4:5.16.3-299.el7_9              perl-macros.x86_64 4:5.16.3-299.el7_9
  perl-parent.noarch 1:0.225-244.el7               perl-podlators.noarch 0:2.5.1-3.el7
  perl-srpm-macros.noarch 0:1-8.el7                perl-threads.x86_64 0:1.87-4.el7
  perl-threads-shared.x86_64 0:1.43-6.el7          python-srpm-macros.noarch 0:3-34.el7
  redhat-rpm-config.noarch 0:9.1.0-88.el7.centos   rpm-build.x86_64 0:4.11.3-45.el7
  rpmdevtools.noarch 0:8.3-8.el7_9                 rsync.x86_64 0:3.1.2-10.el7
  unzip.x86_64 0:6.0-21.el7                        xml-common.noarch 0:0.6.3-39.el7
  zip.x86_64 0:3.0-11.el7

Complete!
[ben@CentOS7-CLT21 ~]$ sudo yum install ansible -y
```

Security: OpenSCAP Demo

(ben) 192.168.178.70 — Konsole

File Edit View Bookmarks Settings Help

```
  Verifying  : ansible-2.9.17-1.el7.noarch                                  21/22
  Verifying  : python2-cryptography-1.7.2-2.el7.x86_64                      22/22

Installed:
  ansible.noarch 0:2.9.17-1.el7

Dependency Installed:
  PyYAML.x86_64 0:3.10-11.el7                       libyaml.x86_64 0:0.1.4-11.el7_0
  python-babel.noarch 0:0.9.6-8.el7                 python-backports.x86_64 0:1.0-8.el7
  python-backports-ssl_match_hostname.noarch 0:3.5.0.1-1.el7  python-cffi.x86_64 0:1.6.0-5.el7
  python-enum34.noarch 0:1.0.4-1.el7                python-idna.noarch 0:2.4-1.el7
  python-ipaddress.noarch 0:1.0.16-2.el7            python-jinja2.noarch 0:2.7.2-4.el7
  python-markupsafe.x86_64 0:0.11-10.el7            python-paramiko.noarch 0:2.1.1-9.el7
  python-ply.noarch 0:3.4-11.el7                    python-pycparser.noarch 0:2.14-1.el7
  python-setuptools.noarch 0:0.9.8-7.el7            python-six.noarch 0:1.9.0-2.el7
  python2-cryptography.x86_64 0:1.7.2-2.el7         python2-httplib2.noarch 0:0.18.1-3.el7
  python2-jmespath.noarch 0:0.9.4-2.el7             python2-pyasn1.noarch 0:0.1.9-7.el7
  sshpass.x86_64 0:1.06-2.el7

Complete!
[ben@CentOS7-CLT21 ~]$ cd /usr/share/xml/scap/ssg/content
```

Security: OpenSCAP Demo

(ben) 192.168.178.70 — Konsole

File Edit View Bookmarks Settings Help

```
  python-ply.noarch 0:3.4-11.el7                    python-pycparser.noarch 0:2.14-1.el7
  python-setuptools.noarch 0:0.9.8-7.el7            python-six.noarch 0:1.9.0-2.el7
  python2-cryptography.x86_64 0:1.7.2-2.el7         python2-httplib2.noarch 0:0.18.1-3.el7
  python2-jmespath.noarch 0:0.9.4-2.el7             python2-pyasn1.noarch 0:0.1.9-7.el7
  sshpass.x86_64 0:1.06-2.el7

Complete!
[ben@CentOS7-CLT21 ~]$ cd /usr/share/xml/scap/ssg/content
[ben@CentOS7-CLT21 content]$ ls
ssg-firefox-cpe-dictionary.xml  ssg-jre-oval.xml              ssg-rhel7-ds.xml
ssg-firefox-cpe-oval.xml        ssg-jre-xccdf.xml             ssg-rhel7-ocil.xml
ssg-firefox-ds-1.2.xml          ssg-rhel6-cpe-dictionary.xml  ssg-rhel7-oval.xml
ssg-firefox-ds.xml              ssg-rhel6-cpe-oval.xml        ssg-rhel7-xccdf.xml
ssg-firefox-ocil.xml            ssg-rhel6-ds-1.2.xml          ssg-rhel8-cpe-dictionary.xml
ssg-firefox-oval.xml            ssg-rhel6-ds.xml              ssg-rhel8-cpe-oval.xml
ssg-firefox-xccdf.xml           ssg-rhel6-ocil.xml            ssg-rhel8-ds-1.2.xml
ssg-jre-cpe-dictionary.xml      ssg-rhel6-oval.xml            ssg-rhel8-ds.xml
ssg-jre-cpe-oval.xml            ssg-rhel6-xccdf.xml           ssg-rhel8-ocil.xml
ssg-jre-ds-1.2.xml              ssg-rhel7-cpe-dictionary.xml  ssg-rhel8-oval.xml
ssg-jre-ds.xml                  ssg-rhel7-cpe-oval.xml        ssg-rhel8-xccdf.xml
ssg-jre-ocil.xml                ssg-rhel7-ds-1.2.xml
[ben@CentOS7-CLT21 content]$
```

Security: OpenSCAP Demo

(ben) 192.168.178.70 — Konsole

File Edit View Bookmarks Settings Help

```
  python-ply.noarch 0:3.4-11.el7                    python-pycparser.noarch 0:2.14-1.el7
  python-setuptools.noarch 0:0.9.8-7.el7            python-six.noarch 0:1.9.0-2.el7
  python2-cryptography.x86_64 0:1.7.2-2.el7         python2-httplib2.noarch 0:0.18.1-3.el7
  python2-jmespath.noarch 0:0.9.4-2.el7             python2-pyasn1.noarch 0:0.1.9-7.el7
  sshpass.x86_64 0:1.06-2.el7

Complete!
[ben@CentOS7-CLT21 ~]$ cd /usr/share/xml/scap/ssg/content
[ben@CentOS7-CLT21 content]$ ls
ssg-firefox-cpe-dictionary.xml  ssg-jre-oval.xml              ssg-rhel7-ds.xml
ssg-firefox-cpe-oval.xml        ssg-jre-xccdf.xml             ssg-rhel7-ocil.xml
ssg-firefox-ds-1.2.xml          ssg-rhel6-cpe-dictionary.xml  ssg-rhel7-oval.xml
ssg-firefox-ds.xml              ssg-rhel6-cpe-oval.xml        ssg-rhel7-xccdf.xml
ssg-firefox-ocil.xml            ssg-rhel6-ds-1.2.xml          ssg-rhel8-cpe-dictionary.xml
ssg-firefox-oval.xml            ssg-rhel6-ds.xml              ssg-rhel8-cpe-oval.xml
ssg-firefox-xccdf.xml           ssg-rhel6-ocil.xml            ssg-rhel8-ds-1.2.xml
ssg-jre-cpe-dictionary.xml      ssg-rhel6-oval.xml            ssg-rhel8-ds.xml
ssg-jre-cpe-oval.xml            ssg-rhel6-xccdf.xml           ssg-rhel8-ocil.xml
ssg-jre-ds-1.2.xml              ssg-rhel7-cpe-dictionary.xml  ssg-rhel8-oval.xml
ssg-jre-ds.xml                  ssg-rhel7-cpe-oval.xml        ssg-rhel8-xccdf.xml
ssg-jre-ocil.xml                ssg-rhel7-ds-1.2.xml
[ben@CentOS7-CLT21 content]$ oscap info ssg-rhel7-ds.xml
```

Security: OpenSCAP Demo

(ben) 192.168.178.70 — Konsole

File Edit View Bookmarks Settings Help

```
Imported: 2020-12-15T17:39:29

Stream: scap_org.open-scap_datastream_from_xccdf_ssg-rhel7-xccdf-1.2.xml
Generated: (null)
Version: 1.3
Checklists:
        Ref-Id: scap_org.open-scap_cref_ssg-rhel7-xccdf-1.2.xml
WARNING: Datastream component 'scap_org.open-scap_cref_security-data-oval-com.redhat.rhsa-RHEL7.xml'
points out to the remote 'https://www.redhat.com/security/data/oval/com.redhat.rhsa-RHEL7.xml'. Use '
--fetch-remote-resources' option to download it.
WARNING: Skipping 'https://www.redhat.com/security/data/oval/com.redhat.rhsa-RHEL7.xml' file which is
 referenced from datastream
                Status: draft
                Generated: 2020-12-15
                Resolved: true
                Profiles:
                        Title: NIST National Checklist Program Security Guide
                                Id: xccdf_org.ssgproject.content_profile_ncp
                        Title: DRAFT - ANSSI DAT-NT28 (high)
                                Id: xccdf_org.ssgproject.content_profile_anssi_nt28_high
                        Title: OSPP - Protection Profile for General Purpose Operating Systems v4.2.1
                                Id: xccdf_org.ssgproject.content_profile_ospp
```

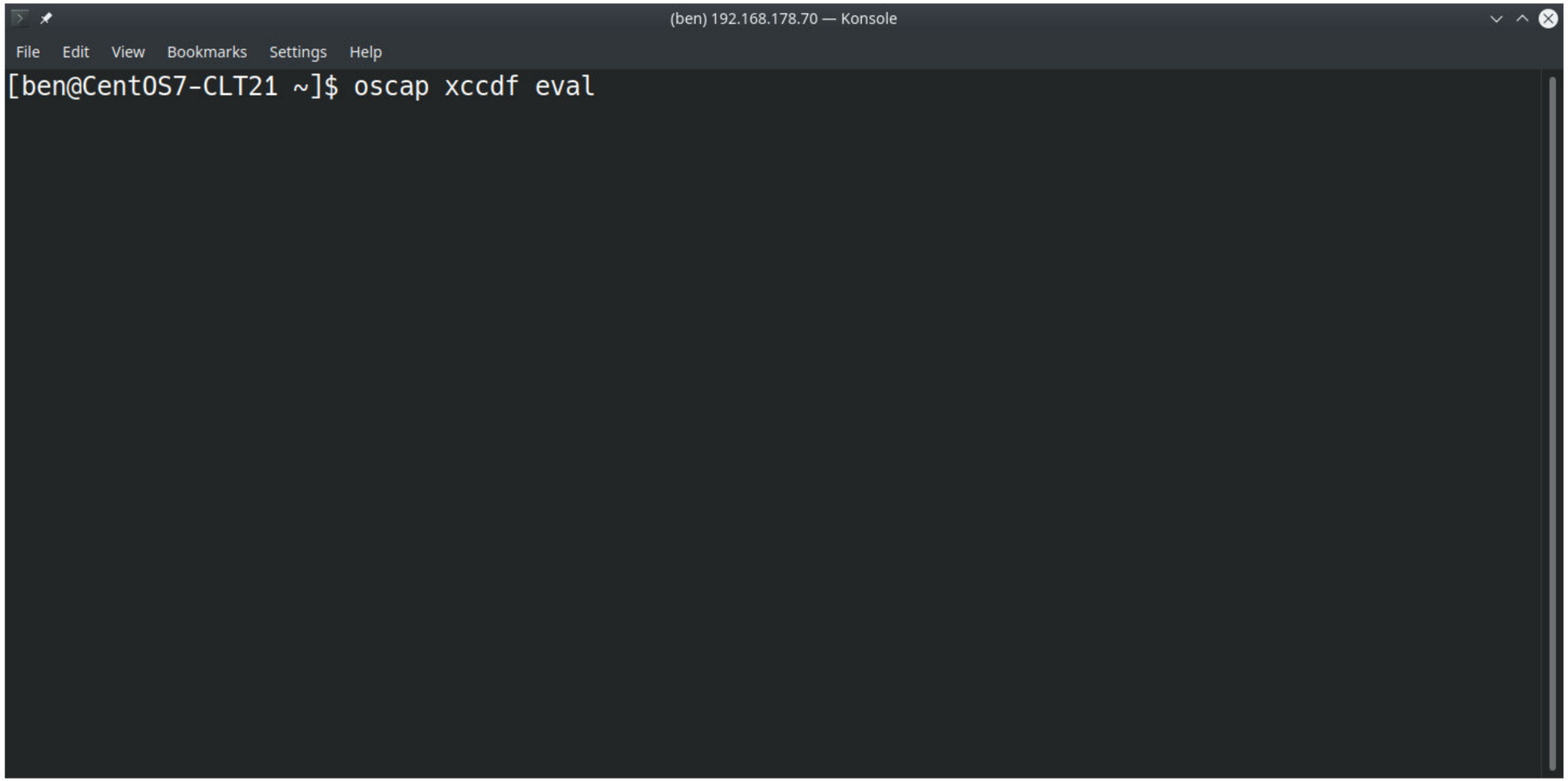
Security: OpenSCAP Demo

(ben) 192.168.178.70 — Konsole

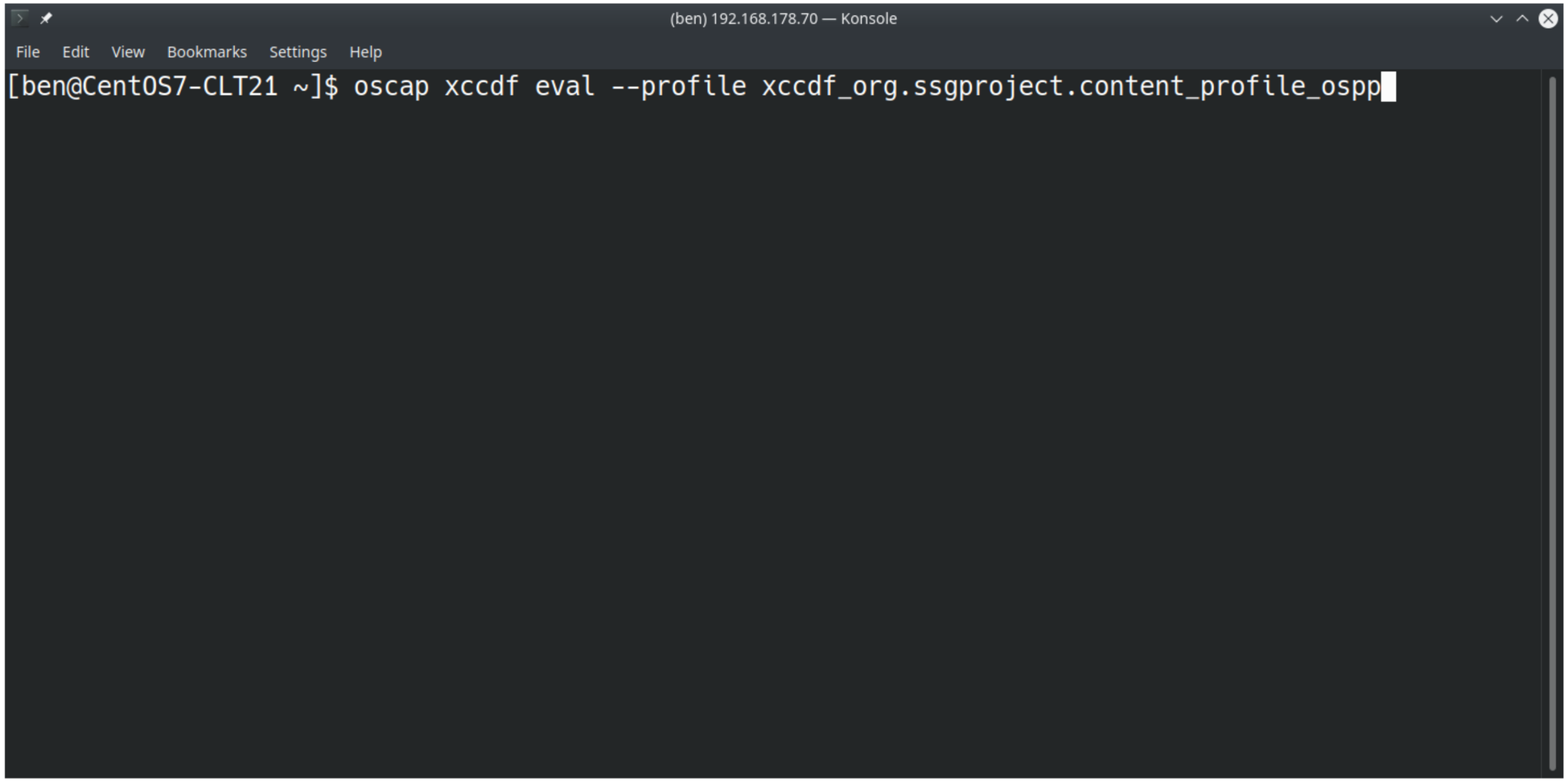
File Edit View Bookmarks Settings Help

```
Imported: 2020-12-15T17:39:29

Stream: scap_org.open-scap_datastream_from_xccdf_ssg-rhel7-xccdf-1.2.xml
Generated: (null)
Version: 1.3
Checklists:
        Ref-Id: scap_org.open-scap_cref_ssg-rhel7-xccdf-1.2.xml
WARNING: Datastream component 'scap_org.open-scap_cref_security-data-oval-com.redhat.rhsa-RHEL7.xml'
points out to the remote 'https://www.redhat.com/security/data/oval/com.redhat.rhsa-RHEL7.xml'. Use '
--fetch-remote-resources' option to download it.
WARNING: Skipping 'https://www.redhat.com/security/data/oval/com.redhat.rhsa-RHEL7.xml' file which is
 referenced from datastream
                Status: draft
                Generated: 2020-12-15
                Resolved: true
                Profiles:
                        Title: NIST National Checklist Program Security Guide
                                Id: xccdf_org.ssgproject.content_profile_ncp
                        Title: DRAFT - ANSSI DAT-NT28 (high)
                                Id: xccdf_org.ssgproject.content_profile_anssi_nt28_high
                        Title: OSPP - Protection Profile for General Purpose Operating Systems v4.2.1
                                Id: xccdf_org.ssgproject.content_profile_ospp
```

Security: OpenSCAP Demo



Security: OpenSCAP Demo



Security: OpenSCAP Demo

(ben) 192.168.178.70 — Konsole

File Edit View Bookmarks Settings Help

```
[ben@CentOS7-CLT21 ~]$ oscap xccdf eval --profile xccdf_org.ssgproject.content_profile_ospp --results
-arf arf.xml
```

Security: OpenSCAP Demo

(ben) 192.168.178.70 — Konsole

File Edit View Bookmarks Settings Help

```
[ben@CentOS7-CLT21 ~]$ oscap xccdf eval --profile xccdf_org.ssgproject.content_profile_ospp --results
-arf arf.xml --report report.html
```

Security: OpenSCAP Demo

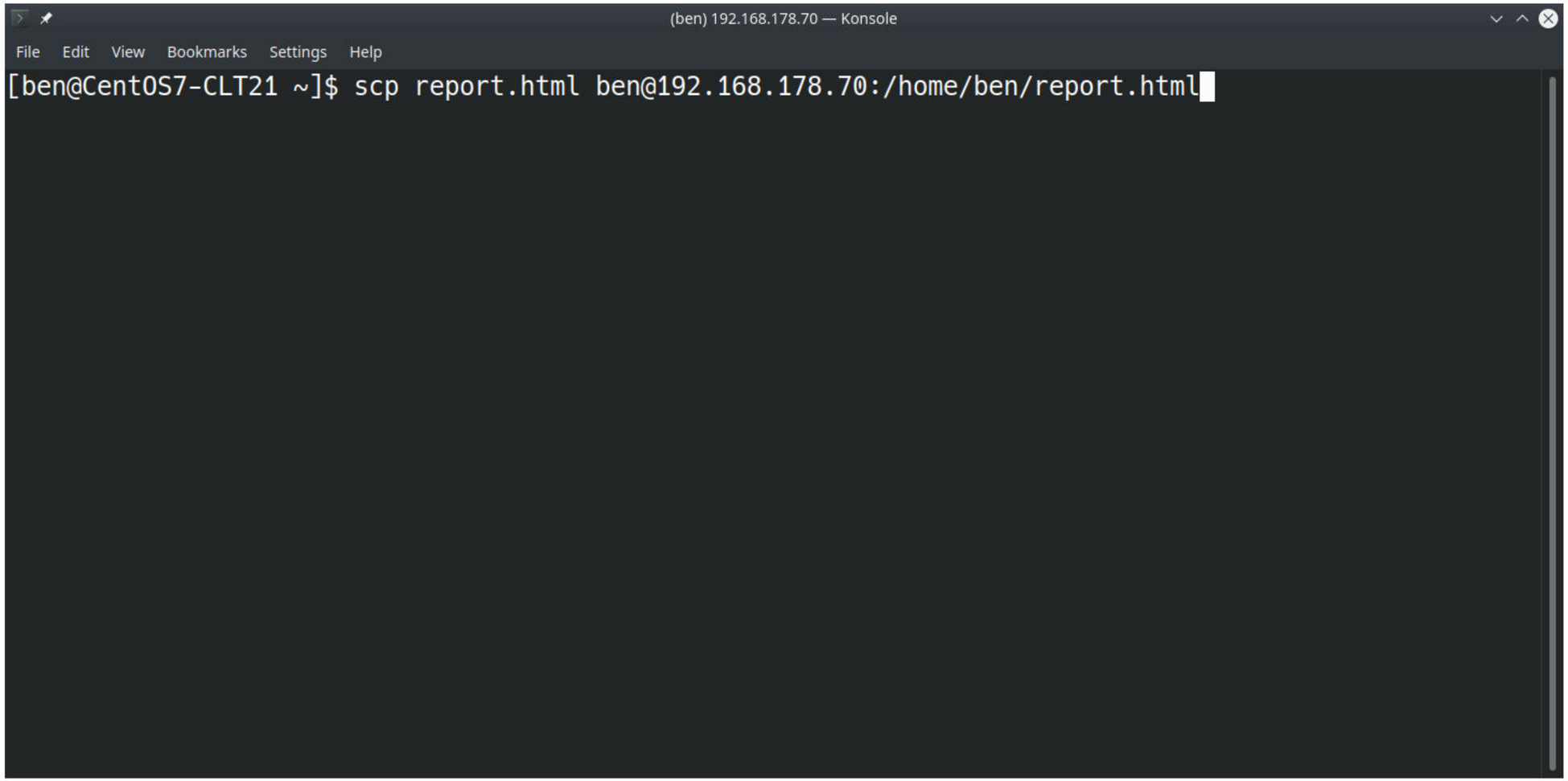
Security: OpenSCAP Demo

(ben) 192.168.178.70 — Konsole

File Edit View Bookmarks Settings Help

```
Title   Use Only FIPS 140-2 Validated Ciphers
Rule    xccdf_org.ssgproject.content_rule_sshd_use_approved_ciphers
Ident   CCE-27295-5
Result  notapplicable

Title   Disable Host-Based Authentication
Rule    xccdf_org.ssgproject.content_rule_disable_host_auth
Ident   CCE-27413-4
Result  notapplicable

Title   Disable GSSAPI Authentication
Rule    xccdf_org.ssgproject.content_rule_sshd_disable_gssapi_auth
Ident   CCE-80220-7
Result  notapplicable

Title   Disable SSH Root Login
Rule    xccdf_org.ssgproject.content_rule_sshd_disable_root_login
Ident   CCE-27445-6
Result  notapplicable
```

Security: OpenSCAP Demo



Security: OpenSCAP Demo

(ben) 192.168.178.70 — Konsole

File Edit View Bookmarks Settings Help

```
[ben@CentOS7-CLT21 ~]$ cd /usr/share/scap-security-guide/ansible/
```

(ben) 192.168.178.70 | ~ : bash

Security: OpenSCAP Demo

(ben) 192.168.178.70 — Konsole

File Edit View Bookmarks Settings Help

```
[ben@CentOS7-CLT21 ansible]$ ls
firefox-playbook-stig.yml                       rhel7-playbook-cis.yml
jre-playbook-stig.yml                           rhel7-playbook-cjis.yml
rhel6-playbook-C2S.yml                          rhel7-playbook-cui.yml
rhel6-playbook-CS2.yml                          rhel7-playbook-e8.yml
rhel6-playbook-CSCF-RHEL6-MLS.yml               rhel7-playbook-hipaa.yml
rhel6-playbook-desktop.yml                      rhel7-playbook-ncp.yml
rhel6-playbook-fisma-medium-rhel6-server.yml    rhel7-playbook-ospp.yml
rhel6-playbook-ftp-server.yml                   rhel7-playbook-pci-dss.yml
rhel6-playbook-nist-CL-IL-AL.yml                rhel7-playbook-rhelh-stig.yml
rhel6-playbook-pci-dss.yml                      rhel7-playbook-rhelh-vpp.yml
rhel6-playbook-rht-ccp.yml                      rhel7-playbook-rht-ccp.yml
rhel6-playbook-server.yml                       rhel7-playbook-standard.yml
rhel6-playbook-standard.yml                     rhel7-playbook-stig.yml
rhel6-playbook-stig.yml                         rhel8-playbook-cis.yml
rhel6-playbook-usgcb-rhel6-server.yml           rhel8-playbook-cui.yml
rhel7-playbook-anssi_nt28_enhanced.yml          rhel8-playbook-e8.yml
rhel7-playbook-anssi_nt28_high.yml              rhel8-playbook-hipaa.yml
rhel7-playbook-anssi_nt28_intermediary.yml      rhel8-playbook-ospp.yml
rhel7-playbook-anssi_nt28_minimal.yml           rhel8-playbook-pci-dss.yml
rhel7-playbook-C2S.yml                          rhel8-playbook-stig.yml
[ben@CentOS7-CLT21 ansible]$
```

Security: OpenSCAP Demo

(ben) 192.168.178.70 — Konsole

File Edit View Bookmarks Settings Help

```
[ben@CentOS7-CLT21 ansible]$ ls
firefox-playbook-stig.yml                       rhel7-playbook-cis.yml
jre-playbook-stig.yml                           rhel7-playbook-cjis.yml
rhel6-playbook-C2S.yml                          rhel7-playbook-cui.yml
rhel6-playbook-CS2.yml                          rhel7-playbook-e8.yml
rhel6-playbook-CSCF-RHEL6-MLS.yml               rhel7-playbook-hipaa.yml
rhel6-playbook-desktop.yml                      rhel7-playbook-ncp.yml
rhel6-playbook-fisma-medium-rhel6-server.yml    rhel7-playbook-ospp.yml
rhel6-playbook-ftp-server.yml                   rhel7-playbook-pci-dss.yml
rhel6-playbook-nist-CL-IL-AL.yml                rhel7-playbook-rhelh-stig.yml
rhel6-playbook-pci-dss.yml                      rhel7-playbook-rhelh-vpp.yml
rhel6-playbook-rht-ccp.yml                      rhel7-playbook-rht-ccp.yml
rhel6-playbook-server.yml                       rhel7-playbook-standard.yml
rhel6-playbook-standard.yml                     rhel7-playbook-stig.yml
rhel6-playbook-stig.yml                         rhel8-playbook-cis.yml
rhel6-playbook-usgcb-rhel6-server.yml           rhel8-playbook-cui.yml
rhel7-playbook-anssi_nt28_enhanced.yml          rhel8-playbook-e8.yml
rhel7-playbook-anssi_nt28_high.yml              rhel8-playbook-hipaa.yml
rhel7-playbook-anssi_nt28_intermediary.yml      rhel8-playbook-ospp.yml
rhel7-playbook-anssi_nt28_minimal.yml           rhel8-playbook-pci-dss.yml
rhel7-playbook-C2S.yml                          rhel8-playbook-stig.yml
[ben@CentOS7-CLT21 ansible]$ scp rhel7-playbook-ospp.yml ben@192.168.178.70:/home/ben/ospp.yml
```

Security: OpenSCAP Demo

(ben) 192.168.178.70 — Konsole

File Edit View Bookmarks Settings Help

```
firefox-playbook-stig.yml                       rhel7-playbook-cis.yml
jre-playbook-stig.yml                           rhel7-playbook-cjis.yml
rhel6-playbook-C2S.yml                          rhel7-playbook-cui.yml
rhel6-playbook-CS2.yml                          rhel7-playbook-e8.yml
rhel6-playbook-CSCF-RHEL6-MLS.yml               rhel7-playbook-hipaa.yml
rhel6-playbook-desktop.yml                      rhel7-playbook-ncp.yml
rhel6-playbook-fisma-medium-rhel6-server.yml    rhel7-playbook-ospp.yml
rhel6-playbook-ftp-server.yml                   rhel7-playbook-pci-dss.yml
rhel6-playbook-nist-CL-IL-AL.yml                rhel7-playbook-rhelh-stig.yml
rhel6-playbook-pci-dss.yml                      rhel7-playbook-rhelh-vpp.yml
rhel6-playbook-rht-ccp.yml                      rhel7-playbook-rht-ccp.yml
rhel6-playbook-server.yml                       rhel7-playbook-standard.yml
rhel6-playbook-standard.yml                     rhel7-playbook-stig.yml
rhel6-playbook-stig.yml                         rhel8-playbook-cis.yml
rhel6-playbook-usgcb-rhel6-server.yml           rhel8-playbook-cui.yml
rhel7-playbook-anssi_nt28_enhanced.yml          rhel8-playbook-e8.yml
rhel7-playbook-anssi_nt28_high.yml              rhel8-playbook-hipaa.yml
rhel7-playbook-anssi_nt28_intermediary.yml      rhel8-playbook-ospp.yml
rhel7-playbook-anssi_nt28_minimal.yml           rhel8-playbook-pci-dss.yml
rhel7-playbook-C2S.yml                          rhel8-playbook-stig.yml
[ben@CentOS7-CLT21 ansible]$ scp rhel7-playbook-ospp.yml ben@192.168.178.70:/home/ben/ospp.yml
[ben@CentOS7-CLT21 ansible]$ scp rhel7-playbook-stig.yml ben@192.168.178.70:/home/ben/stig.yml
```

Ansible: OSPP Code Audit

ospp.yml * — Kate

File Edit View Projects Bookmarks Sessions Tools Settings Help

Documents Projects Filesystem Browser

ospp.yml

```
5051     - name: Disable SSH Root Login
5052       block:
5053
5054         - name: Deduplicate values from /etc/ssh/sshd_config
5055           lineinfile:
5056             path: /etc/ssh/sshd_config
5057             create: false
5058             regexp: (?i)^\s*PermitRootLogin\s+
5059             state: absent
5060
5061         - name: Insert correct line to /etc/ssh/sshd_config
5062           lineinfile:
5063             path: /etc/ssh/sshd_config
5064             create: true
5065             line: PermitRootLogin no
5066             state: present
5067             insertbefore: ^[#\s]*Match
5068             validate: /usr/sbin/sshd -t -f %s
5069       when: ansible_virtualization_type not in ["docker", "lxc", "openvz"]
5070       tags:
5071         - CCE-27445-6
5072         - CJIS-5.5.6
5073         - DISA-STIG-RHEL-07-040370
5074         - NIST-800-171-3.1.1
5075         - NIST-800-171-3.1.5
5076         - NIST-800-53-
5077         - NIST-800-53-AC-17(a)
5078         - NIST-800-53-AC-6(2)
5079         - NIST-800-53-CM-6(a)
5080         - NIST-800-53-CM-7(a)
5081         - NIST-800-53-CM-7(b)
5082         - NIST-800-53-IA-2
5083         - NIST-800-53-IA-2(5)
```

Line 5.051, Column 35 INSERT en_US Soft Tabs: 4 UTF-8 YAML

Search and Replace Current Project Terminal

Ansible: OSPP Code Audit

ospp.yml * — Kate

File Edit View Projects Bookmarks Sessions Tools Settings Help

Documents Projects Filesystem Browser

ospp.yml

```
5051     - name: Disable SSH Root Login
5052       block:
5053
5054         - name: Deduplicate values from /etc/ssh/sshd_config
5055           lineinfile:
5056             path: /etc/ssh/sshd_config
5057             create: false
5058             regexp: (?i)^\s*PermitRootLogin\s+
5059             state: absent
5060
5061         - name: Insert correct line to /etc/ssh/sshd_config
5062           lineinfile:
5063             path: /etc/ssh/sshd_config
5064             create: true
5065             line: PermitRootLogin no
5066             state: present
5067             insertbefore: ^[#\s]*Match
5068             validate: /usr/sbin/sshd -t -f %s
5069       when: ansible_virtualization_type not in ["docker", "lxc", "openvz"]
5070       tags:
5071         - CCE-27445-6
5072         - CJIS-5.5.6
5073         - DISA-STIG-RHEL-07-040370
5074         - NIST-800-171-3.1.1
5075         - NIST-800-171-3.1.5
5076         - NIST-800-53-
5077         - NIST-800-53-AC-17(a)
5078         - NIST-800-53-AC-6(2)
5079         - NIST-800-53-CM-6(a)
5080         - NIST-800-53-CM-7(a)
5081         - NIST-800-53-CM-7(b)
5082         - NIST-800-53-IA-2
5083         - NIST-800-53-IA-2(5)
```

Line 5.051, Column 35 INSERT en_US Soft Tabs: 4 UTF-8 YAML

Search and Replace Current Project Terminal

Ansible: OSPP Code Audit

ospp.yml * — Kate

File Edit View Projects Bookmarks Sessions Tools Settings Help

Documents Projects Filesystem Browser

ospp.yml

```
5051    - name: Disable SSH Root Login
5052      block:
5053
5054        - name: Deduplicate values from /etc/ssh/sshd_config
5055          lineinfile:
5056            path: /etc/ssh/sshd_config
5057            create: false
5058            regexp: (?i)^\s*PermitRootLogin\s+
5059            state: absent
5060
5061        - name: Insert correct line to /etc/ssh/sshd_config
5062          lineinfile:
5063            path: /etc/ssh/sshd_config
5064            create: true
5065            line: PermitRootLogin no
5066            state: present
5067            insertbefore: ^[#\s]*Match
5068            validate: /usr/sbin/sshd -t -f %s
5069      when: ansible_virtualization_type not in ["docker", "lxc", "openvz"]
5070      tags:
5071        - CCE-27445-6
5072        - CJIS-5.5.6
5073        - DISA-STIG-RHEL-07-040370
5074        - NIST-800-171-3.1.1
5075        - NIST-800-171-3.1.5
5076        - NIST-800-53-
5077        - NIST-800-53-AC-17(a)
5078        - NIST-800-53-AC-6(2)
5079        - NIST-800-53-CM-6(a)
5080        - NIST-800-53-CM-7(a)
5081        - NIST-800-53-CM-7(b)
5082        - NIST-800-53-IA-2
5083        - NIST-800-53-IA-2(5)
```

Line 5.051, Column 35 INSERT en_US Soft Tabs: 4 UTF-8 YAML

Search and Replace Current Project Terminal

Ansible: OSPP Code Audit

ospp.yml * — Kate

File Edit View Projects Bookmarks Sessions Tools Settings Help

Documents Projects Filesystem Browser

ospp.yml

```
5051     - name: Disable SSH Root Login
5052       block:
5053
5054         - name: Deduplicate values from /etc/ssh/sshd_config
5055           lineinfile:
5056             path: /etc/ssh/sshd_config
5057             create: false
5058             regexp: (?i)^\s*PermitRootLogin\s+
5059             state: absent
5060
5061         - name: Insert correct line to /etc/ssh/sshd_config
5062           lineinfile:
5063             path: /etc/ssh/sshd_config
5064             create: true
5065             line: PermitRootLogin no
5066             state: present
5067             insertbefore: ^[#\s]*Match
5068             validate: /usr/sbin/sshd -t -f %s
5069       when: ansible_virtualization_type not in ["docker", "lxc", "openvz"]
5070       tags:
5071         - CCE-27445-6
5072         - CJIS-5.5.6
5073         - DISA-STIG-RHEL-07-040370
5074         - NIST-800-171-3.1.1
5075         - NIST-800-171-3.1.5
5076         - NIST-800-53-
5077         - NIST-800-53-AC-17(a)
5078         - NIST-800-53-AC-6(2)
5079         - NIST-800-53-CM-6(a)
5080         - NIST-800-53-CM-7(a)
5081         - NIST-800-53-CM-7(b)
5082         - NIST-800-53-IA-2
5083         - NIST-800-53-IA-2(5)
```

Line 5.051, Column 35 INSERT en_US Soft Tabs: 4 UTF-8 YAML

Search and Replace Current Project Terminal

Ansible: OSPP Code Audit

ospp.yml * — Kate

File Edit View Projects Bookmarks Sessions Tools Settings Help

Documents Projects Filesystem Browser

ospp.yml

```
4901    - name: Set SSH Idle Timeout Interval
4902      block:
4903
4904        - name: Deduplicate values from /etc/ssh/sshd_config
4905          lineinfile:
4906            path: /etc/ssh/sshd_config
4907            create: false
4908            regexp: (?i)^\s*ClientAliveInterval\s+
4909            state: absent
4910
4911        - name: Insert correct line to /etc/ssh/sshd_config
4912          lineinfile:
4913            path: /etc/ssh/sshd_config
4914            create: true
4915            line: ClientAliveInterval {{ sshd_idle_timeout_value }}
4916            state: present
4917            insertbefore: ^[#\s]*Match
4918            validate: /usr/sbin/sshd -t -f %s
4919      when: ansible_virtualization_type not in ["docker", "lxc", "openvz"]
4920      tags:
4921        - CCE-27433-2
4922        - CJIS-5.5.6
4923        - DISA-STIG-RHEL-07-040320
4924        - NIST-800-171-3.1.11
4925        - NIST-800-53-AC-12
4926        - NIST-800-53-AC-17(a)
4927        - NIST-800-53-AC-17(a)
4928        - NIST-800-53-AC-2(5)
4929        - NIST-800-53-CM-6(a)
4930        - NIST-800-53-CM-6(a)
4931        - NIST-800-53-SC-10
4932        - PCI-DSS-Req-8.1.8
4933        - low_complexity
```

Line 5.051, Column 35 INSERT en_US Soft Tabs: 4 UTF-8 YAML

Search and Replace Current Project Terminal

Ansible: OSPP Code Audit

ospp.yml * — Kate

File Edit View Projects Bookmarks Sessions Tools Settings Help

Documents Projects Filesystem Browser

ospp.yml

```
4901     - name: Set SSH Idle Timeout Interval
4902       block:
4903
4904         - name: Deduplicate values from /etc/ssh/sshd_config
4905           lineinfile:
4906             path: /etc/ssh/sshd_config
4907             create: false
4908             regexp: (?i)^\s*ClientAliveInterval\s+
4909             state: absent
4910
4911         - name: Insert correct line to /etc/ssh/sshd_config
4912           lineinfile:
4913             path: /etc/ssh/sshd_config
4914             create: true
4915             line: ClientAliveInterval {{ sshd_idle_timeout_value }}
4916             state: present
4917             insertbefore: ^[#\s]*Match
4918             validate: /usr/sbin/sshd -t -f %s
4919       when: ansible_virtualization_type not in ["docker", "lxc", "openvz"]
4920       tags:
4921         - CCE-27433-2
4922         - CJIS-5.5.6
4923         - DISA-STIG-RHEL-07-040320
4924         - NIST-800-171-3.1.11
4925         - NIST-800-53-AC-12
4926         - NIST-800-53-AC-17(a)
4927         - NIST-800-53-AC-17(a)
4928         - NIST-800-53-AC-2(5)
4929         - NIST-800-53-CM-6(a)
4930         - NIST-800-53-CM-6(a)
4931         - NIST-800-53-SC-10
4932         - PCI-DSS-Req-8.1.8
4933         - low_complexity
```

Line 5.051, Column 35 INSERT en_US Soft Tabs: 4 UTF-8 YAML

Search and Replace Current Project Terminal

Ansible: OSPP Code Audit

ospp.yml * — Kate

File Edit View Projects Bookmarks Sessions Tools Settings Help

Documents Projects Filesystem Browser

ospp.yml

```
4901    - name: Set SSH Idle Timeout Interval
4902      block:
4903
4904        - name: Deduplicate values from /etc/ssh/sshd_config
4905          lineinfile:
4906            path: /etc/ssh/sshd_config
4907            create: false
4908            regexp: (?i)^\s*ClientAliveInterval\s+
4909            state: absent
4910
4911        - name: Insert correct line to /etc/ssh/sshd_config
4912          lineinfile:
4913            path: /etc/ssh/sshd_config
4914            create: true
4915            line: ClientAliveInterval {{ sshd_idle_timeout_value }}
4916            state: present
4917            insertbefore: ^[#\s]*Match
4918            validate: /usr/sbin/sshd -t -f %s
4919      when: ansible_virtualization_type not in ["docker", "lxc", "openvz"]
4920      tags:
4921        - CCE-27433-2
4922        - CJIS-5.5.6
4923        - DISA-STIG-RHEL-07-040320
4924        - NIST-800-171-3.1.11
4925        - NIST-800-53-AC-12
4926        - NIST-800-53-AC-17(a)
4927        - NIST-800-53-AC-17(a)
4928        - NIST-800-53-AC-2(5)
4929        - NIST-800-53-CM-6(a)
4930        - NIST-800-53-CM-6(a)
4931        - NIST-800-53-SC-10
4932        - PCI-DSS-Req-8.1.8
4933        - low_complexity
```

Line 5.051, Column 35 INSERT en_US Soft Tabs: 4 UTF-8 YAML

Search and Replace Current Project Terminal

Ansible: OSPP Code Audit

ospp.yml * — Kate

File Edit View Projects Bookmarks Sessions Tools Settings Help

Documents Projects Filesystem Browser

ospp.yml

```
4901     - name: Set SSH Idle Timeout Interval
4902       block:
4903
4904         - name: Deduplicate values from /etc/ssh/sshd_config
4905           lineinfile:
4906             path: /etc/ssh/sshd_config
4907             create: false
4908             regexp: (?i)^\s*ClientAliveInterval\s+
4909             state: absent
4910
4911         - name: Insert correct line to /etc/ssh/sshd_config
4912           lineinfile:
4913             path: /etc/ssh/sshd_config
4914             create: true
4915             line: ClientAliveInterval {{ sshd_idle_timeout_value }}
4916             state: present
4917             insertbefore: ^[#\s]*Match
4918             validate: /usr/sbin/sshd -t -f %s
4919       when: ansible_virtualization_type not in ["docker", "lxc", "openvz"]
4920       tags:
4921         - CCE-27433-2
4922         - CJIS-5.5.6
4923         - DISA-STIG-RHEL-07-040320
4924         - NIST-800-171-3.1.11
4925         - NIST-800-53-AC-12
4926         - NIST-800-53-AC-17(a)
4927         - NIST-800-53-AC-17(a)
4928         - NIST-800-53-AC-2(5)
4929         - NIST-800-53-CM-6(a)
4930         - NIST-800-53-CM-6(a)
4931         - NIST-800-53-SC-10
4932         - PCI-DSS-Req-8.1.8
4933         - low_complexity
```

Line 5.051, Column 35 INSERT en_US Soft Tabs: 4 UTF-8 YAML

Search and Replace Current Project Terminal

Ansible: OSPP Code Audit

ospp.yml * — Kate

File Edit View Projects Bookmarks Sessions Tools Settings Help

Documents Projects Filesystem Browser

ospp.yml

```
2436     - name: Enable service firewalld
2437       block:
2438
2439         - name: Gather the package facts
2440           package_facts:
2441             manager: auto
2442
2443         - name: Enable service firewalld
2444           service:
2445             name: firewalld
2446             enabled: 'yes'
2447             state: started
2448           when:
2449             - '"firewalld" in ansible_facts.packages'
2450       when: ansible_virtualization_type not in ["docker", "lxc", "openvz"]
2451       tags:
2452         - CCE-80998-8
2453         - DISA-STIG-RHEL-07-040520
2454         - NIST-800-171-3.1.3
2455         - NIST-800-171-3.4.7
2456         - NIST-800-53-AC-4
2457         - NIST-800-53-CA-3(5)
2458         - NIST-800-53-CM-6(a)
2459         - NIST-800-53-CM-7(b)
2460         - NIST-800-53-SC-7(21)
2461         - enable_strategy
2462         - low_complexity
2463         - low_disruption
2464         - medium_severity
2465         - no_reboot_needed
2466         - service_firewalld_enabled
2467
2468     - name: Ensure sysctl net.ipv6.conf.default.accept_source_route is set
```

Line 4.974, Column 25 INSERT en_US Soft Tabs: 4 UTF-8 YAML

Search and Replace Current Project Terminal

Ansible: OSPP Code Audit

ospp.yml * — Kate

File Edit View Projects Bookmarks Sessions Tools Settings Help

Documents Projects Filesystem Browser

ospp.yml

```
2436     - name: Enable service firewalld
2437       block:
2438
2439         - name: Gather the package facts
2440           package_facts:
2441             manager: auto
2442
2443         - name: Enable service firewalld
2444           service:
2445             name: firewalld
2446             enabled: 'yes'
2447             state: started
2448           when:
2449             - '"firewalld" in ansible_facts.packages'
2450       when: ansible_virtualization_type not in ["docker", "lxc", "openvz"]
2451       tags:
2452         - CCE-80998-8
2453         - DISA-STIG-RHEL-07-040520
2454         - NIST-800-171-3.1.3
2455         - NIST-800-171-3.4.7
2456         - NIST-800-53-AC-4
2457         - NIST-800-53-CA-3(5)
2458         - NIST-800-53-CM-6(a)
2459         - NIST-800-53-CM-7(b)
2460         - NIST-800-53-SC-7(21)
2461         - enable_strategy
2462         - low_complexity
2463         - low_disruption
2464         - medium_severity
2465         - no_reboot_needed
2466         - service_firewalld_enabled
2467
2468     - name: Ensure sysctl net.ipv6.conf.default.accept_source_route is set
```

Line 4.974, Column 25 INSERT en_US Soft Tabs: 4 UTF-8 YAML

Search and Replace Current Project Terminal

Ansible: OSPP Code Audit

ospp.yml * — Kate

File Edit View Projects Bookmarks Sessions Tools Settings Help

Documents Projects Filesystem Browser

ospp.yml

```
2436    - name: Enable service firewalld
2437      block:
2438
2439        - name: Gather the package facts
2440          package_facts:
2441            manager: auto
2442
2443        - name: Enable service firewalld
2444          service:
2445            name: firewalld
2446            enabled: 'yes'
2447            state: started
2448          when:
2449            - '"firewalld" in ansible_facts.packages'
2450      when: ansible_virtualization_type not in ["docker", "lxc", "openvz"]
2451      tags:
2452        - CCE-80998-8
2453        - DISA-STIG-RHEL-07-040520
2454        - NIST-800-171-3.1.3
2455        - NIST-800-171-3.4.7
2456        - NIST-800-53-AC-4
2457        - NIST-800-53-CA-3(5)
2458        - NIST-800-53-CM-6(a)
2459        - NIST-800-53-CM-7(b)
2460        - NIST-800-53-SC-7(21)
2461        - enable_strategy
2462        - low_complexity
2463        - low_disruption
2464        - medium_severity
2465        - no_reboot_needed
2466        - service_firewalld_enabled
2467
2468    - name: Ensure sysctl net.ipv6.conf.default.accept_source_route is set
```

Line 4.974, Column 25 INSERT en_US Soft Tabs: 4 UTF-8 YAML

Search and Replace Current Project Terminal

Security: STIG

Security Technical Implementation Guide

- cybersecurity requirements of a specific product

- enhance security for software, hardware, physical and logical architectures

- reduce vulnerabilities

- desktop computer or an enterprise server

- might cover network design, router configurations, databases, firewalls etc.

Ansible: STIG Code Audit

stig.yml — Kate

File Edit View Projects Bookmarks Sessions Tools Settings Help

Documents Projects Filesystem Browser

stig.yml

```
197
198   - name: Set Password Maximum Age
199     lineinfile:
200       create: true
201       dest: /etc/login.defs
202       regexp: ^#?PASS_MAX_DAYS
203       line: PASS_MAX_DAYS {{ var_accounts_maximum_age_login_defs }}
204     when: '"shadow-utils" in ansible_facts.packages'
205     tags:
206       - CCE-27051-2
207       - CJIS-5.6.2.1
208       - DISA-STIG-RHEL-07-010250
209       - NIST-800-171-3.5.6
210       - NIST-800-53-CM-6(a)
211       - NIST-800-53-IA-5(1)(d)
212       - NIST-800-53-IA-5(f)
213       - PCI-DSS-Req-8.2.4
214       - accounts_maximum_age_login_defs
215       - low_complexity
216       - low_disruption
217       - medium_severity
218       - no_reboot_needed
219       - restrict_strategy
220
221   - name: Prevent Log In to Accounts With Empty Password - system-auth
222     replace:
223       dest: /etc/pam.d/system-auth
224       follow: true
225       regexp: nullok
226     tags:
227       - CCE-27286-4
228       - CJIS-5.5.2
229       - DISA-STIG-RHEL-07-010290
```

Line 33, Column 1 INSERT en_US Soft Tabs: 4 UTF-8 YAML

Search and Replace Current Project Terminal

Ansible: STIG Code Audit

stig.yml — Kate

File Edit View Projects Bookmarks Sessions Tools Settings Help

Documents Projects Filesystem Browser

stig.yml

```
197
198   - name: Set Password Maximum Age
199     lineinfile:
200       create: true
201       dest: /etc/login.defs
202       regexp: ^#?PASS_MAX_DAYS
203       line: PASS_MAX_DAYS {{ var_accounts_maximum_age_login_defs }}
204     when: '"shadow-utils" in ansible_facts.packages'
205     tags:
206       - CCE-27051-2
207       - CJIS-5.6.2.1
208       - DISA-STIG-RHEL-07-010250
209       - NIST-800-171-3.5.6
210       - NIST-800-53-CM-6(a)
211       - NIST-800-53-IA-5(1)(d)
212       - NIST-800-53-IA-5(f)
213       - PCI-DSS-Req-8.2.4
214       - accounts_maximum_age_login_defs
215       - low_complexity
216       - low_disruption
217       - medium_severity
218       - no_reboot_needed
219       - restrict_strategy
220
221   - name: Prevent Log In to Accounts With Empty Password - system-auth
222     replace:
223       dest: /etc/pam.d/system-auth
224       follow: true
225       regexp: nullok
226     tags:
227       - CCE-27286-4
228       - CJIS-5.5.2
229       - DISA-STIG-RHEL-07-010290
```

Line 33, Column 1 INSERT en_US Soft Tabs: 4 UTF-8 YAML

Search and Replace Current Project Terminal

Ansible: STIG Code Audit

stig.yml — Kate

File Edit View Projects Bookmarks Sessions Tools Settings Help

stig.yml

```
197
198   - name: Set Password Maximum Age
199     lineinfile:
200       create: true
201       dest: /etc/login.defs
202       regexp: ^#?PASS_MAX_DAYS
203       line: PASS_MAX_DAYS {{ var_accounts_maximum_age_login_defs }}
204       when: "ansible_facts['os_family'] in ['RedHat', 'Suse']"
205     tags:
206       - CCE-27051-2
207       - CJIS-5.6.2.1
208       - DISA-STIG-RHEL-07-010250
209       - NIST-800-171-3.5.6
210       - NIST-800-53-CM-6(a)
211       - NIST-800-53-IA-5(1)(d)
212       - NIST-800-53-IA-5(f)
213       - PCI-DSS-Req-8.2.4
214       - accounts_maximum_age_login_defs
215       - low_complexity
216       - low_disruption
217       - medium_severity
218       - no_reboot_needed
219       - restrict_strategy
220
221   - name: Prevent Log In to Accounts With Empty Password - system-auth
222     replace:
223       dest: /etc/pam.d/system-auth
224       follow: true
225       regexp: nullok
226     tags:
227       - CCE-27286-4
228       - CJIS-5.5.2
229       - DISA-STIG-RHEL-07-010290
```

Documents Projects Filesystem Browser

Line 33, Column 1 INSERT en_US Soft Tabs: 4 UTF-8 YAML

Search and Replace Current Project Terminal

Ansible: STIG Code Audit

stig.yml — Kate

File Edit View Projects Bookmarks Sessions Tools Settings Help

Documents Projects Filesystem Browser

stig.yml

```
794
795   - name: Set Password Hashing Algorithm in /etc/login.defs
796     lineinfile:
797       dest: /etc/login.defs
798       regexp: ^#?ENCRYPT_METHOD
799       line: ENCRYPT_METHOD SHA512
800       state: present
801       create: true
802     when: '"shadow-utils" in ansible_facts.packages'
803     tags:
804       - CCE-82050-6
805       - CJIS-5.6.2.2
806       - DISA-STIG-RHEL-07-010210
807       - NIST-800-171-3.13.11
808       - NIST-800-53-CM-6(a)
809       - NIST-800-53-IA-5(1)(c)
810       - NIST-800-53-IA-5(c)
811       - PCI-DSS-Req-8.2.1
812       - low_complexity
813       - low_disruption
814       - medium_severity
815       - no_reboot_needed
816       - restrict_strategy
817       - set_password_hashing_algorithm_logindefs
818
819   - package_facts:
820       manager: auto
821     name: Gather the package facts
822     tags:
823       - CCE-82038-1
824       - CJIS-5.6.2.2
825       - DISA-STIG-RHEL-07-010220
826       - NIST-800-171-3.13.11
```

Line 828, Column 23 INSERT en_US Soft Tabs: 4 UTF-8 YAML

Search and Replace Current Project Terminal

Ansible: STIG Code Audit

stig.yml — Kate

File Edit View Projects Bookmarks Sessions Tools Settings Help

Documents Projects Filesystem Browser

stig.yml

```
794
795   - name: Set Password Hashing Algorithm in /etc/login.defs
796     lineinfile:
797       dest: /etc/login.defs
798       regexp: ^#?ENCRYPT_METHOD
799       line: ENCRYPT_METHOD SHA512
800       state: present
801       create: true
802     when: '"shadow-utils" in ansible_facts.packages'
803     tags:
804       - CCE-82050-6
805       - CJIS-5.6.2.2
806       - DISA-STIG-RHEL-07-010210
807       - NIST-800-171-3.13.11
808       - NIST-800-53-CM-6(a)
809       - NIST-800-53-IA-5(1)(c)
810       - NIST-800-53-IA-5(c)
811       - PCI-DSS-Req-8.2.1
812       - low_complexity
813       - low_disruption
814       - medium_severity
815       - no_reboot_needed
816       - restrict_strategy
817       - set_password_hashing_algorithm_logindefs
818
819   - package_facts:
820       manager: auto
821     name: Gather the package facts
822     tags:
823       - CCE-82038-1
824       - CJIS-5.6.2.2
825       - DISA-STIG-RHEL-07-010220
826       - NIST-800-171-3.13.11
```

Line 828, Column 23 INSERT en_US Soft Tabs: 4 UTF-8 YAML

Search and Replace Current Project Terminal

Ansible: STIG Code Audit

stig.yml — Kate

File Edit View Projects Bookmarks Sessions Tools Settings Help

stig.yml

Documents Projects Filesystem Browser

```
794
795   - name: Set Password Hashing Algorithm in /etc/login.defs
796     lineinfile:
797       dest: /etc/login.defs
798       regexp: ^#?ENCRYPT_METHOD
799       line: ENCRYPT_METHOD SHA512
800       state: present
801       create: true
802     when: '"shadow-utils" in ansible_facts.packages'
803     tags:
804       - CCE-82050-6
805       - CJIS-5.6.2.2
806       - DISA-STIG-RHEL-07-010210
807       - NIST-800-171-3.13.11
808       - NIST-800-53-CM-6(a)
809       - NIST-800-53-IA-5(1)(c)
810       - NIST-800-53-IA-5(c)
811       - PCI-DSS-Req-8.2.1
812       - low_complexity
813       - low_disruption
814       - medium_severity
815       - no_reboot_needed
816       - restrict_strategy
817       - set_password_hashing_algorithm_logindefs
818
819   - package_facts:
820       manager: auto
821     name: Gather the package facts
822     tags:
823       - CCE-82038-1
824       - CJIS-5.6.2.2
825       - DISA-STIG-RHEL-07-010220
826       - NIST-800-171-3.13.11
```

Line 828, Column 23 INSERT en_US Soft Tabs: 4 UTF-8 YAML

Search and Replace Current Project Terminal

Ansible: STIG Code Audit

stig.yml — Kate

File Edit View Projects Bookmarks Sessions Tools Settings Help

Documents Projects Filesystem Browser

stig.yml

```
14939
14940     - name: Ensure openssh-server is installed
14941       package:
14942         name: openssh-server
14943         state: present
14944       when: ansible_virtualization_type not in ["docker", "lxc", "openvz"]
14945       tags:
14946         - CCE-80215-7
14947         - DISA-STIG-RHEL-07-040300
14948         - NIST-800-53-CM-6(a)
14949         - enable_strategy
14950         - low_complexity
14951         - low_disruption
14952         - medium_severity
14953         - no_reboot_needed
14954         - package_openssh-server_installed
14955
14956     - name: Enable service sshd
14957       block:
14958
14959         - name: Gather the package facts
14960           package_facts:
14961             manager: auto
14962
14963         - name: Enable service sshd
14964           service:
14965             name: sshd
14966             enabled: 'yes'
14967             state: started
14968           when:
14969             - '"openssh-server" in ansible_facts.packages'
14970       when: ansible_virtualization_type not in ["docker", "lxc", "openvz"]
14971       tags:
```

Line 14.938, Column 27 INSERT en_US Soft Tabs: 4 UTF-8 YAML

Search and Replace Current Project Terminal

Ansible: STIG Code Audit

stig.yml — Kate

File Edit View Projects Bookmarks Sessions Tools Settings Help

Documents Projects Filesystem Browser

stig.yml

```
14939
14940     - name: Ensure openssh-server is installed
14941       package:
14942         name: openssh-server
14943         state: present
14944       when: ansible_virtualization_type not in ["docker", "lxc", "openvz"]
14945       tags:
14946         - CCE-80215-7
14947         - DISA-STIG-RHEL-07-040300
14948         - NIST-800-53-CM-6(a)
14949         - enable_strategy
14950         - low_complexity
14951         - low_disruption
14952         - medium_severity
14953         - no_reboot_needed
14954         - package_openssh-server_installed
14955
14956     - name: Enable service sshd
14957       block:
14958
14959         - name: Gather the package facts
14960           package_facts:
14961             manager: auto
14962
14963         - name: Enable service sshd
14964           service:
14965             name: sshd
14966             enabled: 'yes'
14967             state: started
14968           when:
14969             - '"openssh-server" in ansible_facts.packages'
14970       when: ansible_virtualization_type not in ["docker", "lxc", "openvz"]
14971       tags:
```

Line 14.938, Column 27 INSERT en_US Soft Tabs: 4 UTF-8 YAML

Search and Replace Current Project Terminal

Ansible: STIG Code Audit

stig.yml — Kate

File Edit View Projects Bookmarks Sessions Tools Settings Help

Documents Projects Filesystem Browser

stig.yml

```
14939
14940     - name: Ensure openssh-server is installed
14941       package:
14942         name: openssh-server
14943         state: present
14944       when: ansible_virtualization_type not in ["docker", "lxc", "openvz"]
14945       tags:
14946         - CCE-80215-7
14947         - DISA-STIG-RHEL-07-040300
14948         - NIST-800-53-CM-6(a)
14949         - enable_strategy
14950         - low_complexity
14951         - low_disruption
14952         - medium_severity
14953         - no_reboot_needed
14954         - package_openssh-server_installed
14955
14956     - name: Enable service sshd
14957       block:
14958
14959         - name: Gather the package facts
14960           package_facts:
14961             manager: auto
14962
14963         - name: Enable service sshd
14964           service:
14965             name: sshd
14966             enabled: 'yes'
14967             state: started
14968           when:
14969             - '"openssh-server" in ansible_facts.packages'
14970       when: ansible_virtualization_type not in ["docker", "lxc", "openvz"]
14971       tags:
```

Line 14.938, Column 27 INSERT en_US Soft Tabs: 4 UTF-8 YAML

Search and Replace Current Project Terminal

Ansible: STIG Demo

(ben) 192.168.178.70 — Konsole

File Edit View Bookmarks Settings Help

```
[ben@CentOS7-CLT21 ansible]$ ls
firefox-playbook-stig.yml                       rhel7-playbook-cis.yml
jre-playbook-stig.yml                           rhel7-playbook-cjis.yml
rhel6-playbook-C2S.yml                          rhel7-playbook-cui.yml
rhel6-playbook-CS2.yml                          rhel7-playbook-e8.yml
rhel6-playbook-CSCF-RHEL6-MLS.yml               rhel7-playbook-hipaa.yml
rhel6-playbook-desktop.yml                      rhel7-playbook-ncp.yml
rhel6-playbook-fisma-medium-rhel6-server.yml    rhel7-playbook-ospp.yml
rhel6-playbook-ftp-server.yml                   rhel7-playbook-pci-dss.yml
rhel6-playbook-nist-CL-IL-AL.yml                rhel7-playbook-rhelh-stig.yml
rhel6-playbook-pci-dss.yml                      rhel7-playbook-rhelh-vpp.yml
rhel6-playbook-rht-ccp.yml                      rhel7-playbook-rht-ccp.yml
rhel6-playbook-server.yml                       rhel7-playbook-standard.yml
rhel6-playbook-standard.yml                     rhel7-playbook-stig.yml
rhel6-playbook-stig.yml                         rhel8-playbook-cis.yml
rhel6-playbook-usgcb-rhel6-server.yml           rhel8-playbook-cui.yml
rhel7-playbook-anssi_nt28_enhanced.yml          rhel8-playbook-e8.yml
rhel7-playbook-anssi_nt28_high.yml              rhel8-playbook-hipaa.yml
rhel7-playbook-anssi_nt28_intermediary.yml      rhel8-playbook-ospp.yml
rhel7-playbook-anssi_nt28_minimal.yml           rhel8-playbook-pci-dss.yml
rhel7-playbook-C2S.yml                          rhel8-playbook-stig.yml
[ben@CentOS7-CLT21 ansible]$
```

Ansible: STIG Demo

(ben) 192.168.178.70 — Konsole

File Edit View Bookmarks Settings Help

```
[ben@CentOS7-CLT21 ansible]$ sudo ansible-playbook -i "localhost," -c local rhel7-playbook-stig.yml
```

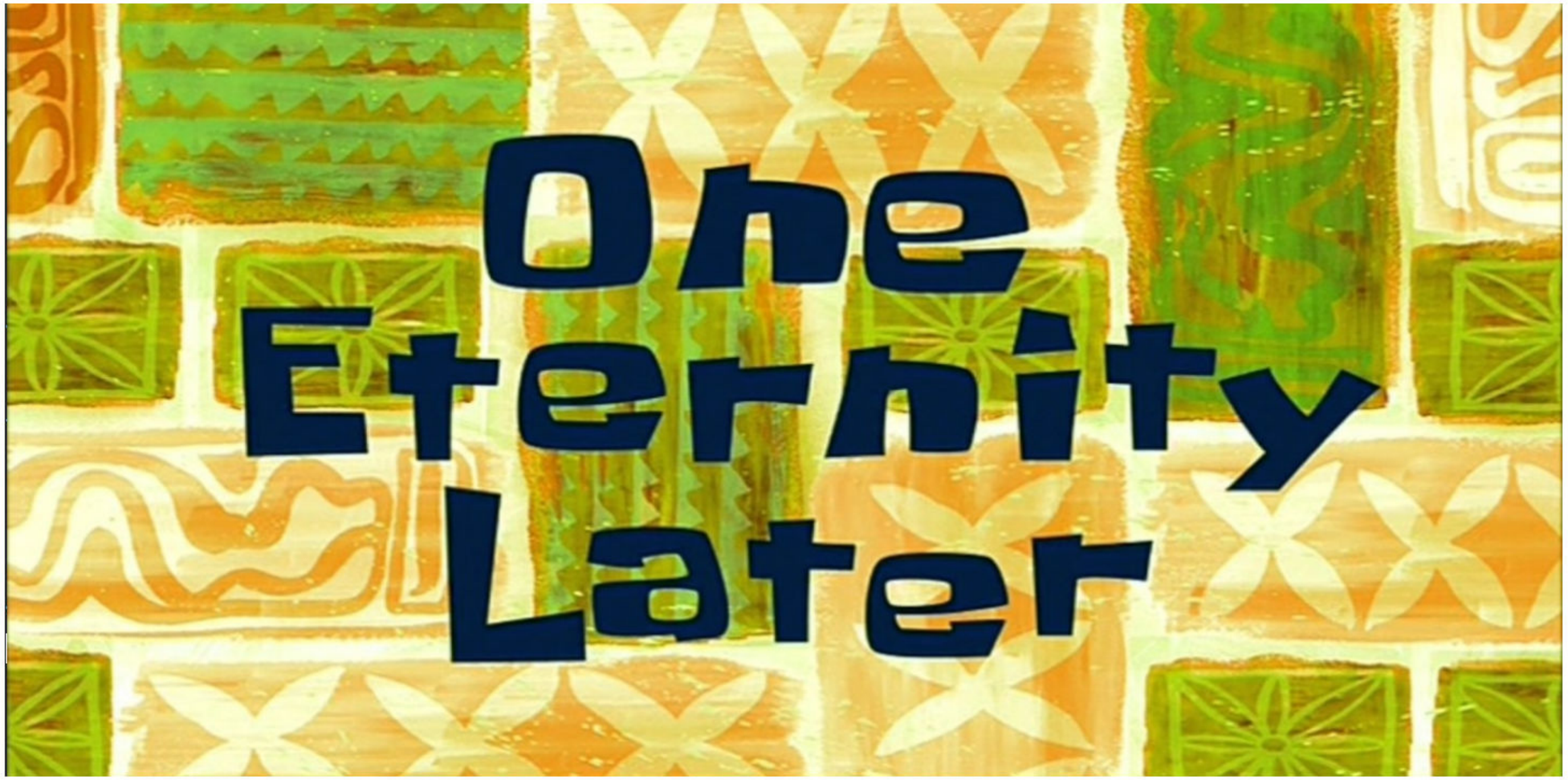
Ansible: STIG Demo

(ben) 192.168.178.70 — Konsole

File Edit View Bookmarks Settings Help

```
[ben@CentOS7-CLT21 ansible]$ sudo ansible-playbook -i "localhost," -c local rhel7-playbook-stig.yml
[sudo] password for ben:
[WARNING]: While constructing a mapping from /usr/share/scap-security-guide/ansible/rhel7-playbook-
stig.yml, line 48, column 7, found a duplicate dict key (login_banner_text). Using last defined
value only.

PLAY [all] *********************************************************************************

TASK [Gathering Facts] *********************************************************************
ok: [localhost]

TASK [Verify Ansible meets SCAP-Security-Guide version requirements.] **********************
ok: [localhost] => {
    "changed": false,
    "msg": "All assertions passed"
}

TASK [Gather the package facts] ************************************************************
```

Ansible: STIG Demo



Ansible: STIG Demo

(ben) 192.168.178.70 — Konsole

File Edit View Bookmarks Settings Help

```
changed: [localhost]

TASK [Insert correct line to /etc/ssh/sshd_config] *****************************************************
changed: [localhost]

TASK [Deduplicate values from /etc/ssh/sshd_config] ****************************************************
ok: [localhost]

TASK [Insert correct line to /etc/ssh/sshd_config] *****************************************************
changed: [localhost]

TASK [Deduplicate values from /etc/ssh/sshd_config] ****************************************************
ok: [localhost]

TASK [Insert correct line to /etc/ssh/sshd_config] *****************************************************
changed: [localhost]

PLAY RECAP *********************************************************************************************
localhost                  : ok=564  changed=272  unreachable=0    failed=0    skipped=137  rescued=0
    ignored=0

[ben@CentOS7-CLT21 ansible]$
```

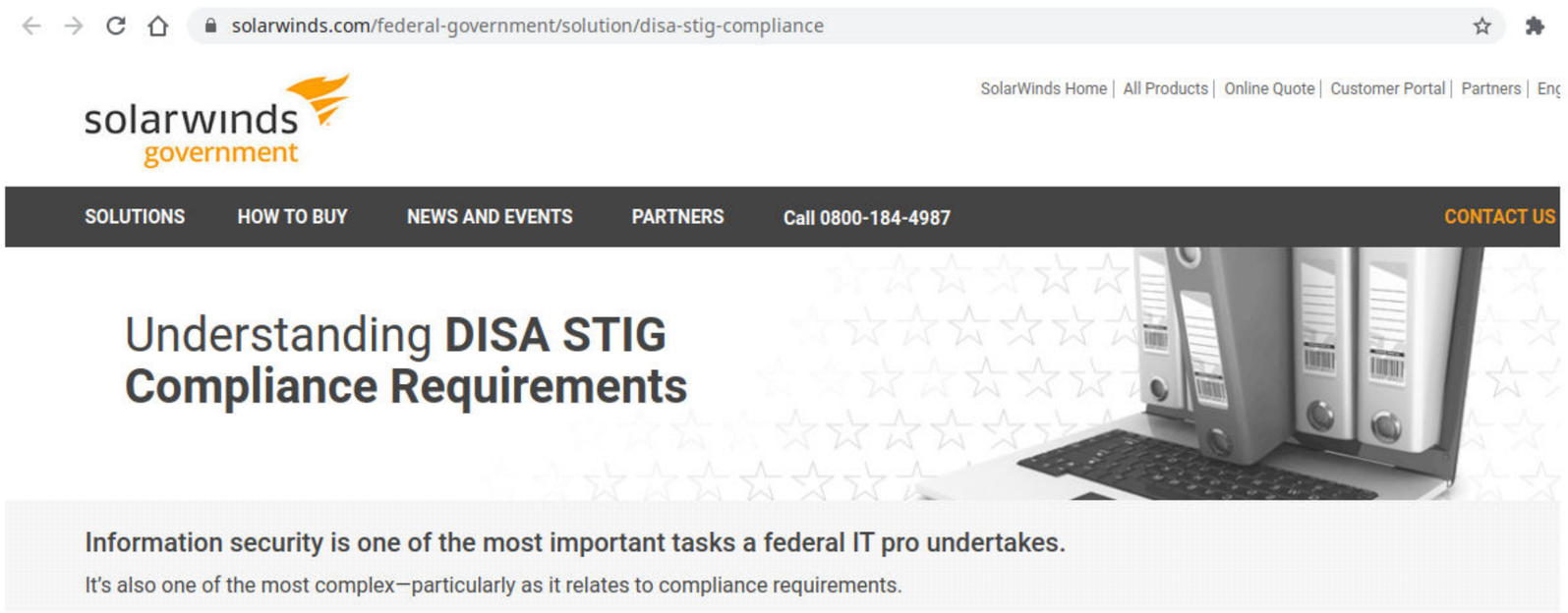
Ansible: STIG Demo

(ben) 192.168.178.70 — Konsole

File Edit View Bookmarks Settings Help

```
changed: [localhost]

TASK [Insert correct line to /etc/ssh/sshd_config] *****************************************************
changed: [localhost]

TASK [Deduplicate values from /etc/ssh/sshd_config] ****************************************************
ok: [localhost]

TASK [Insert correct line to /etc/ssh/sshd_config] *****************************************************
changed: [localhost]

TASK [Deduplicate values from /etc/ssh/sshd_config] ****************************************************
ok: [localhost]

TASK [Insert correct line to /etc/ssh/sshd_config] *****************************************************
changed: [localhost]

PLAY RECAP *********************************************************************************************
localhost                  : ok=564  changed=272  unreachable=0    failed=0    skipped=137  rescued=0
    ignored=0

[ben@CentOS7-CLT21 ansible]$
```

Ansible: DISA STIG Code Audit



Ansible: DISA STIG Code Audit

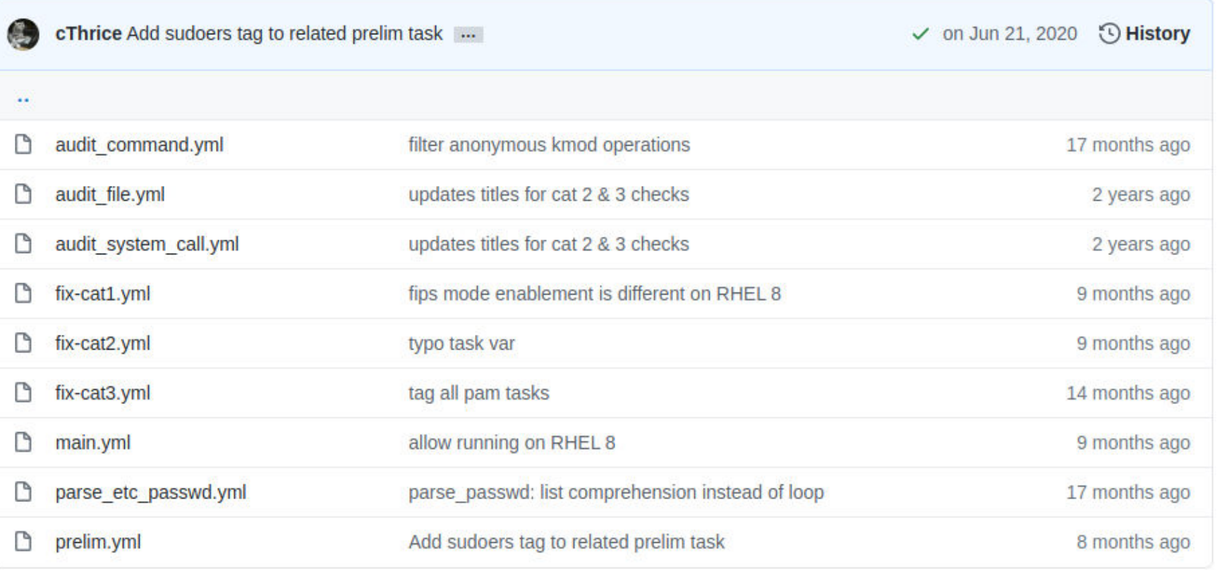
jamescassell Merge pull request #324 from cThrice/patch-1 ···	b859ecc on Jun 21, 2020	**488** commits
defaults	rhel8: hardcode hash for default password	9 months ago
doc	Documentation generation notes	11 months ago
filter_plugins	grub2_hash support for older (<1.7) passlib versions (#59)	3 years ago
handlers	Update to fix handler output in playbook	12 months ago
meta	null value in YAML causing issues for Ansible Galaxy import	3 years ago
molecule	update registry loc in Dockerfile as well	2 years ago
tasks	Add sudoers tag to related prelim task	8 months ago
templates	generate /etc/default/grub if not present	3 years ago
test_plugins	add compatability jinja tests	16 months ago
tests	Fix testing (#187)	2 years ago
vars	add option to unconditionally configure dconf rules	17 months ago
.gitignore	Docker updates (#181)	2 years ago
.travis.yml	Merge in documentation generation stuff (#201)	2 years ago
.yamllint	Fix testing (#187)	2 years ago
LICENSE	add license file	3 years ago
README.md	V2R7	10 months ago
local.yml	fix local.yml for ansible-2.4	2 years ago
rh-creds.env.sample	Docker updates (#181)	2 years ago
travis.env.sample	Docker updates (#181)	2 years ago

Ansible: DISA STIG Code Audit

jamescassell Merge pull request #324 from cThrice/patch-1 ··· ✕ b859ecc on Jun 21, 2020 **488** commits

defaults	rhel8: hardcode hash for default password	9 months ago
doc	Documentation generation notes	11 months ago
filter_plugins	grub2_hash support for older (<1.7) passlib versions (#59)	3 years ago
handlers	Update to fix handler output in playbook	12 months ago
meta	null value in YAML causing issues for Ansible Galaxy import	3 years ago
molecule	update registry loc in Dockerfile as well	2 years ago
tasks	Add sudoers tag to related prelim task	8 months ago
templates	generate /etc/default/grub if not present	3 years ago
test_plugins	add compatability jinja tests	16 months ago
tests	Fix testing (#187)	2 years ago
vars	add option to unconditionally configure dconf rules	17 months ago
.gitignore	Docker updates (#181)	2 years ago
.travis.yml	Merge in documentation generation stuff (#201)	2 years ago
.yamllint	Fix testing (#187)	2 years ago
LICENSE	add license file	3 years ago
README.md	V2R7	10 months ago
local.yml	fix local.yml for ansible-2.4	2 years ago
rh-creds.env.sample	Docker updates (#181)	2 years ago
travis.env.sample	Docker updates (#181)	2 years ago

Ansible: DISA STIG Code Audit



cThrice Add sudoers tag to related prelim task ... on Jun 21, 2020 **History**

..

audit_command.yml	filter anonymous kmod operations	17 months ago
audit_file.yml	updates titles for cat 2 & 3 checks	2 years ago
audit_system_call.yml	updates titles for cat 2 & 3 checks	2 years ago
fix-cat1.yml	fips mode enablement is different on RHEL 8	9 months ago
fix-cat2.yml	typo task var	9 months ago
fix-cat3.yml	tag all pam tasks	14 months ago
main.yml	allow running on RHEL 8	9 months ago
parse_etc_passwd.yml	parse_passwd: list comprehension instead of loop	17 months ago
prelim.yml	Add sudoers tag to related prelim task	8 months ago

Ansible: DISA STIG Code Audit

cThrice Add sudoers tag to related prelim task ... ✓ on Jun 21, 2020 **History**

..

audit_command.yml	filter anonymous kmod operations	17 months ago
audit_file.yml	updates titles for cat 2 & 3 checks	2 years ago
audit_system_call.yml	updates titles for cat 2 & 3 checks	2 years ago
fix-cat1.yml	fips mode enablement is different on RHEL 8	9 months ago
fix-cat2.yml	typo task var	9 months ago
fix-cat3.yml	tag all pam tasks	14 months ago
main.yml	allow running on RHEL 8	9 months ago
parse_etc_passwd.yml	parse_passwd: list comprehension instead of loop	17 months ago
prelim.yml	Add sudoers tag to related prelim task	8 months ago