Foundations of Information Assurance

Lab Assignment 6 Report

Team 20

Sonam Ghatode

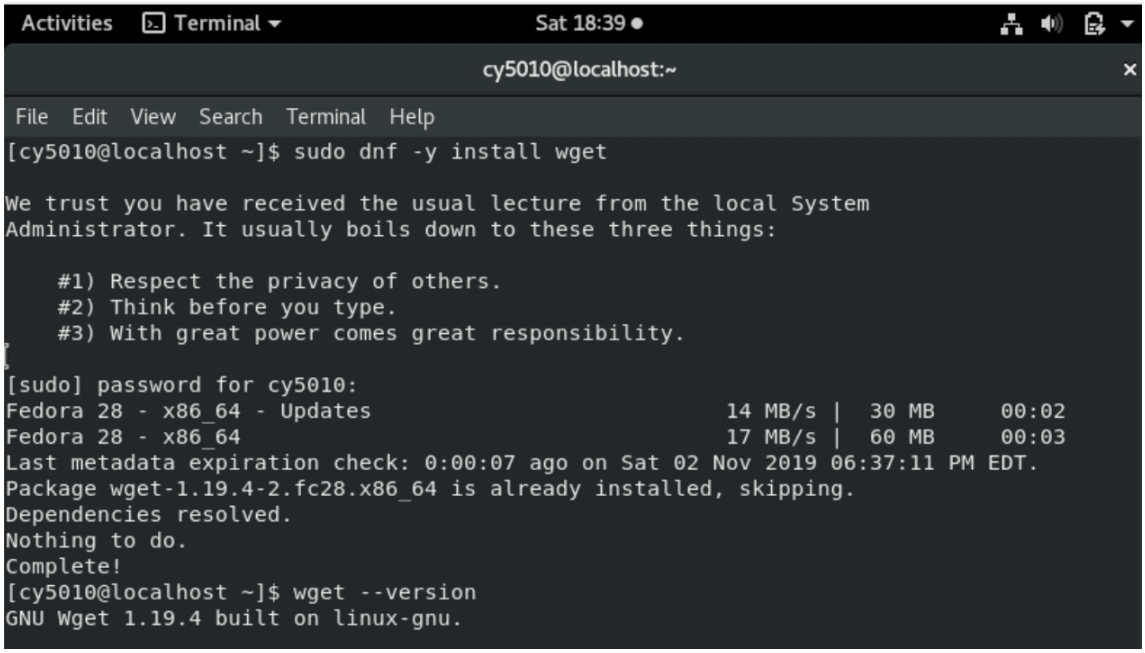
Vishal Maurya

11.02.2019
CY5010

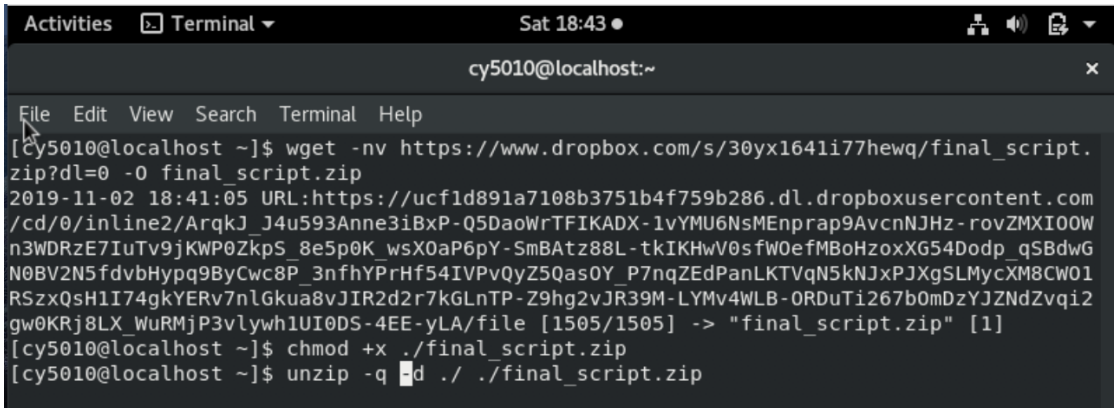
Index

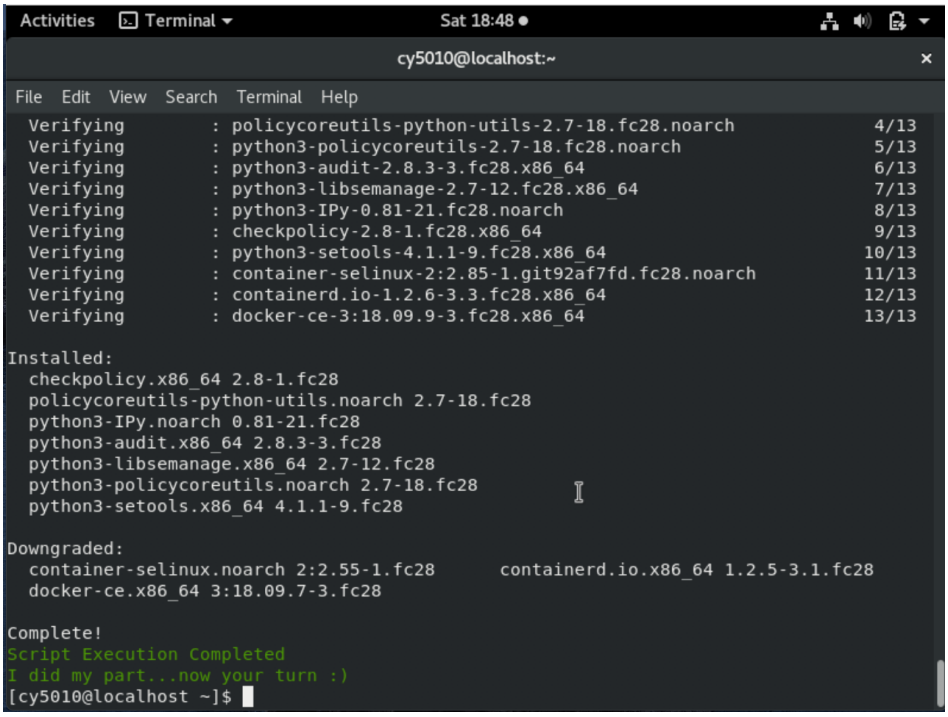
Setup :

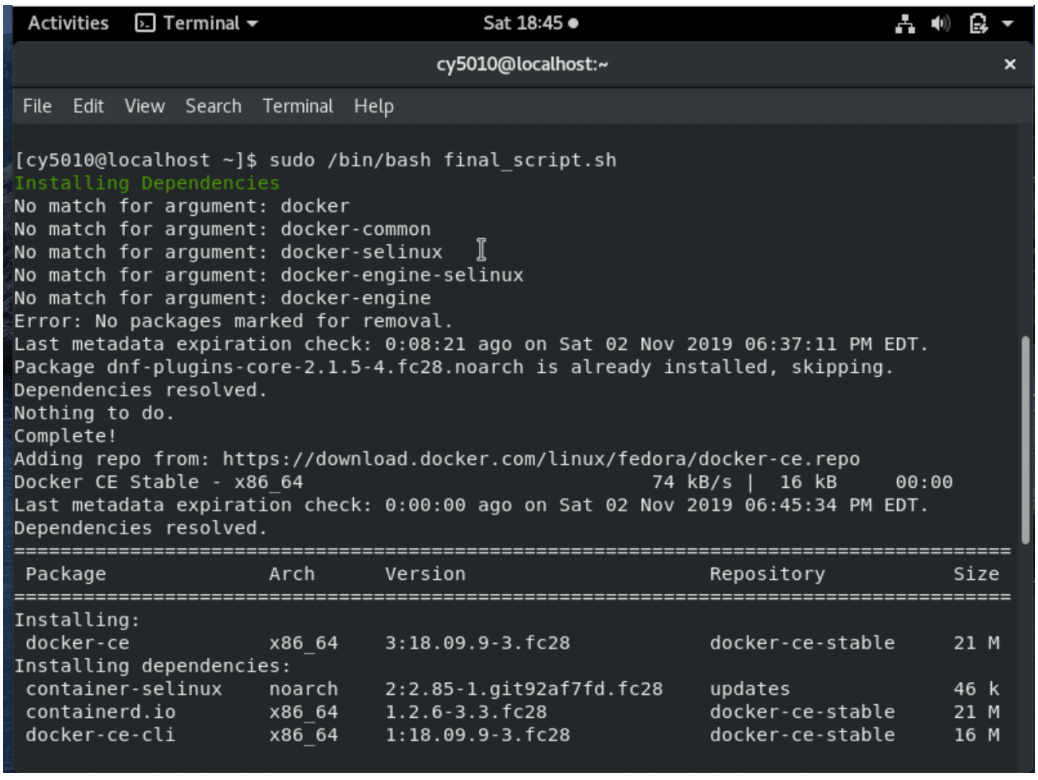
After downloading the Fedora VM and getting it running. We started with the Lab setup by first installing wget and running the script to install OpenSCAP,



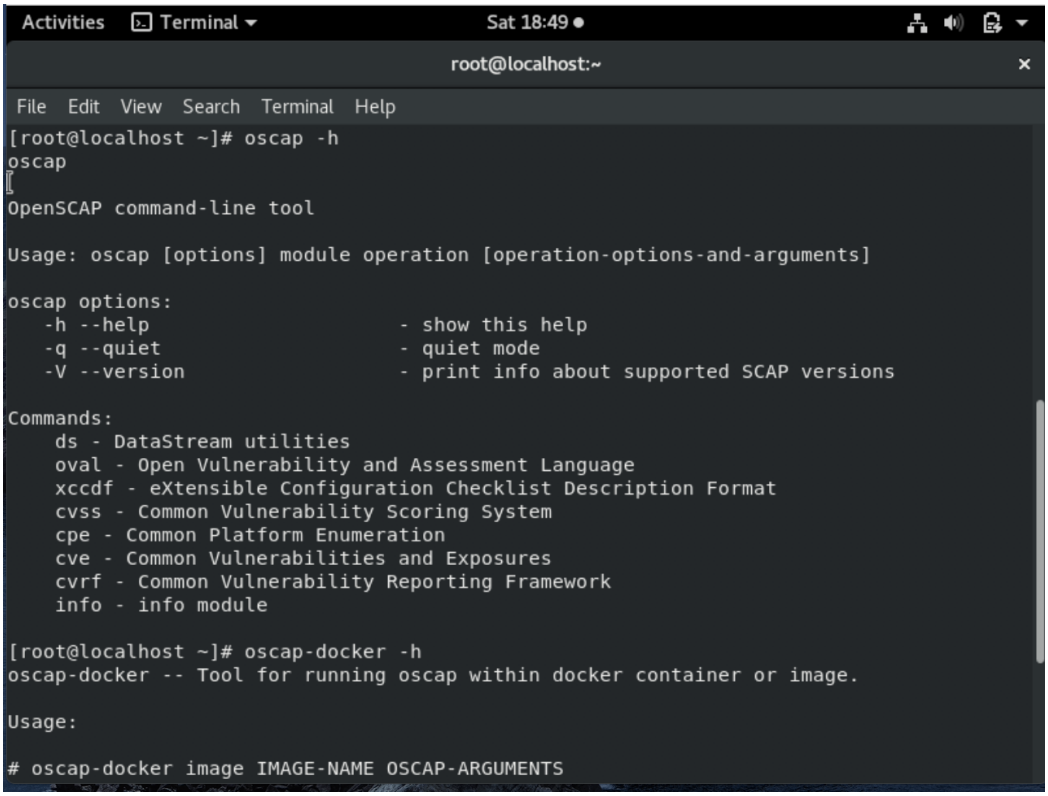
OSCAP-Docker and SCAP-Security-Guide.




Activities
Terminal
Sat 18:48
cy5010@localhost:~
File Edit View Search Terminal Help
Verifying : policycoreutils-python-utils-2.7-18.fc28.noarch 4/13
Verifying : python3-policycoreutils-2.7-18.fc28.noarch 5/13
Verifying : python3-audit-2.8.3-3.fc28.x86_64 6/13
Verifying : python3-libsemanage-2.7-12.fc28.x86_64 7/13
Verifying : python3-IPy-0.81-21.fc28.noarch 8/13
Verifying : checkpolicy-2.8-1.fc28.x86_64 9/13
Verifying : python3-setools-4.1.1-9.fc28.x86_64 10/13
Verifying : container-selinux-2:2.85-1.git92af7fd.fc28.noarch 11/13
Verifying : containerd.io-1.2.6-3.3.fc28.x86_64 12/13
Verifying : docker-ce-3:18.09.9-3.fc28.x86_64 13/13
Installed:
checkpolicy.x86_64 2.8-1.fc28
policycoreutils-python-utils.noarch 2.7-18.fc28
python3-IPy.noarch 0.81-21.fc28
python3-audit.x86_64 2.8.3-3.fc28
python3-libsemanage.x86_64 2.7-12.fc28
python3-policycoreutils.noarch 2.7-18.fc28
python3-setools.x86_64 4.1.1-9.fc28
Downgraded:
container-selinux.noarch 2:2.55-1.fc28
containerd.io.x86_64 1.2.5-3.1.fc28
docker-ce.x86_64 3:18.09.7-3.fc28
Complete!
Script Execution Completed
I did my part...now your turn :)
[cy5010@localhost ~]$


Activities
Terminal
Sat 18:45
cy5010@localhost:~
File Edit View Search Terminal Help
[cy5010@localhost ~]$ sudo /bin/bash final_script.sh
Installing Dependencies
No match for argument: docker
No match for argument: docker-common
No match for argument: docker-selinux
No match for argument: docker-engine-selinux
No match for argument: docker-engine
Error: No packages marked for removal.
Last metadata expiration check: 0:08:21 ago on Sat 02 Nov 2019 06:37:11 PM EDT.
Package dnf-plugins-core-2.1.5-4.fc28.noarch is already installed, skipping.
Dependencies resolved.
Nothing to do.
Complete!
Adding repo from: https://download.docker.com/linux/fedora/docker-ce.repo
Docker CE Stable - x86_64 74 kB/s | 16 kB 00:00
Last metadata expiration check: 0:00:00 ago on Sat 02 Nov 2019 06:45:34 PM EDT.
Dependencies resolved.
Package Arch Version Repository Size
Installing:
docker-ce x86_64 3:18.09.9-3.fc28 docker-ce-stable 21 M
Installing dependencies:
container-selinux noarch 2:2.85-1.git92af7fd.fc28 updates 46 k
containerd.io x86_64 1.2.6-3.3.fc28 docker-ce-stable 21 M
docker-ce-cli x86_64 1:18.09.9-3.fc28 docker-ce-stable 16 M

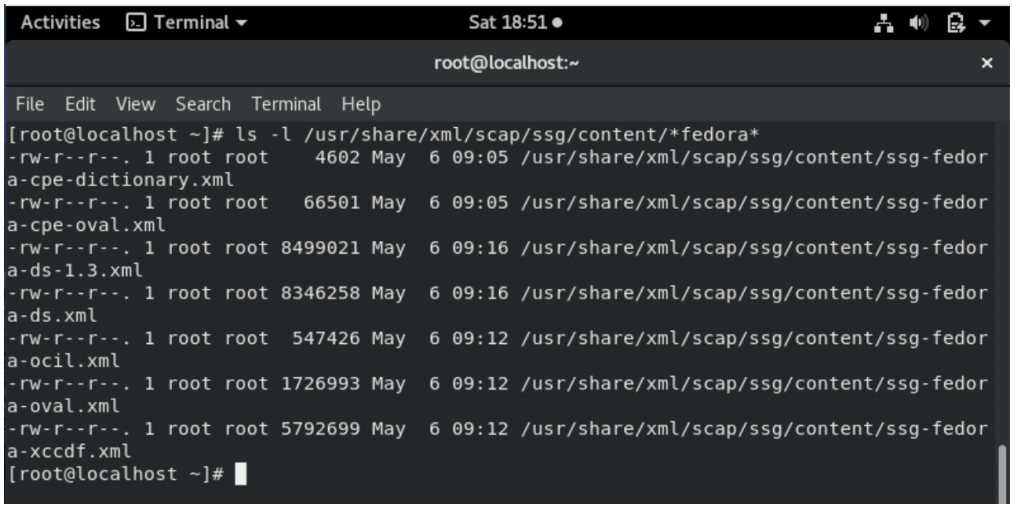
Now we checked if the command line tools are installed properly.

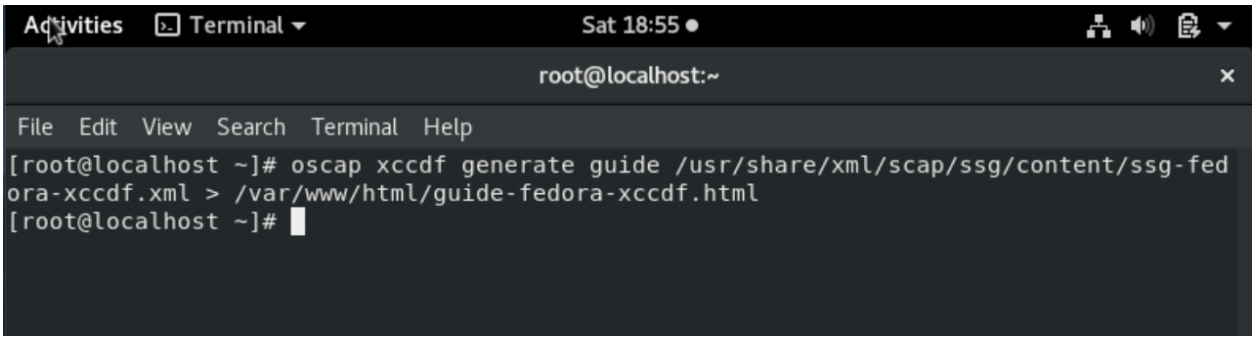


It showed that the command line tools are ready to use.

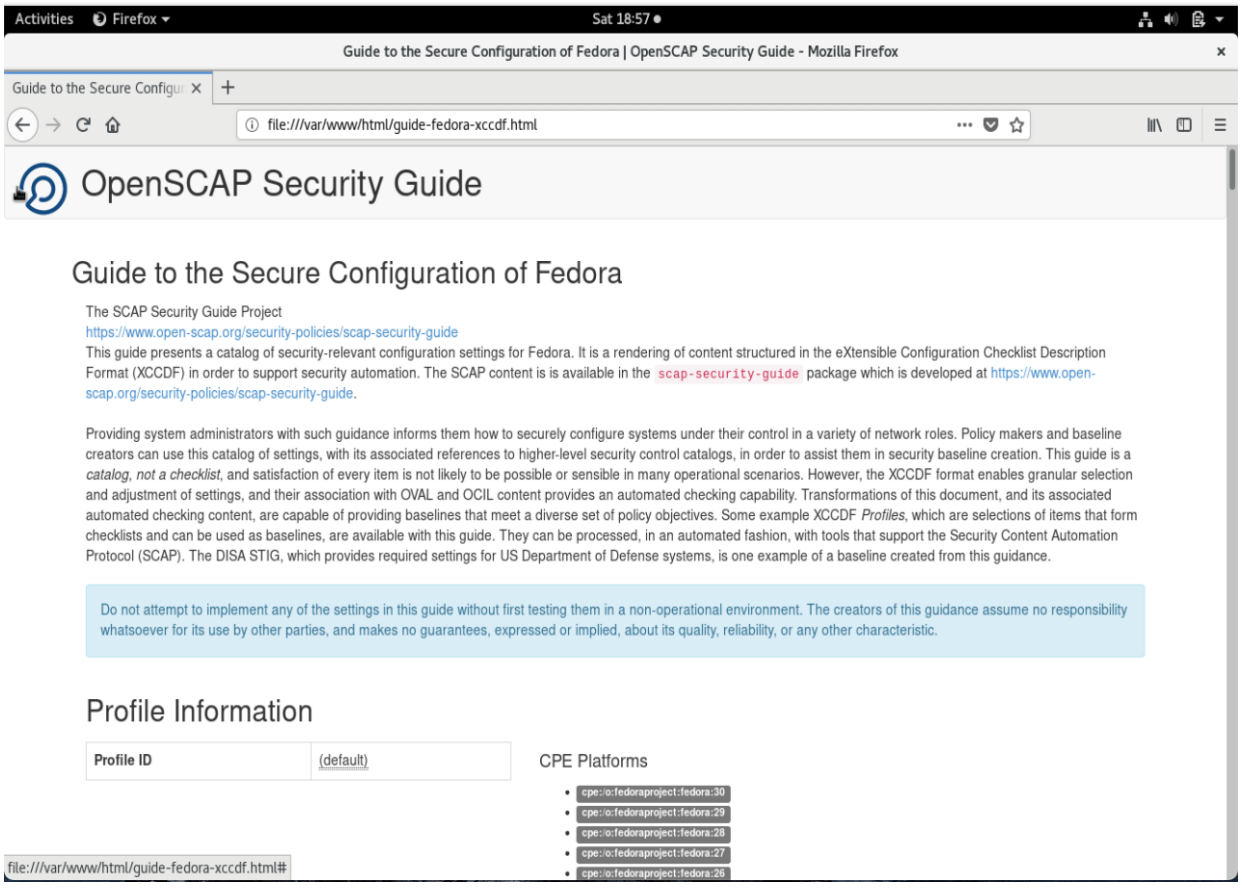
PART 1: EXPLORING SCAP PROFILES :

We looked at the profiles available in the SCAP Security Guide (SSG) for fedora :





We created a guide explaining the checks :
And navigated to the html page using the browser inside the VM :



We will be explaining the following checks that are mentioned in the checklist from the security guide we created :

1. Restrict at and cron to Authorized Users if Necessary :

at : is a service in linux systems used to run a specific command or task at a given time (only once).

cron : is a service in linux used to run a specific command or task in regular intervals.

- Considering the function of these services, it is a favourite attack vector used by attackers through a service which is already running with access to these services.
- Hence we should implement an access control on these services by implementing allow/deny rules for these rules by implementing .allow rules and removing .deny rules.
- By doing this we will allow only those users who are listed in .allow files. This can be done by creating the following files and listing the users in them :
  -> /etc/at.allow
  -> /etc/cron.allow
  and remove the following files :
  -> /etc/at.deny
  -> /etc/cron.deny

2. Network Time Protocol :

NTP is a service used to enable time synchronization.

Why was this service needed ?

- When deploying huge network of systems, wherein each system communicates with many other systems or services running on these systems, the communication of packets in between them requires time synchronization so that the TCP communications can be synchronized with valid SYN and ACK numbers.

How does NTP help in security ?

- Depending on which daemon you use in your network implementation, you get added layer of security.
- If you use ***chronyd***, which is more suitable for frequently suspended or otherwise intermittently disconnected and reconnected to a network, you get faster connection and synchronization as compares to ntpd.
- If you use ***ntpd***, which is more suited for systems which are permanently on and continuously in use, it helps performing

authentication of packets with the Autokey protocol.

3. Use Appropriate Modules to Improve httpd's Security :

- Being one of the most popular web server, for static hosting or reverse proxying dynamic pages to other deamons. It is important to ensure we secure the web server from attacks like XSS, SQL injection etc.
- This can be easily done by using ***mod_security*** httpd module, which readily provides the protection from attacks mentioned above, we just need to include these rules in out vhost config or httpd.conf file to be applied across all vhost we use.
- Another method to ensure security at the web server level is using mod_ssl to deploy SSL certificates and listening on https, which provides Authenticity.

4. Configure Operating System to Protect Web Server :

- *Restrict Web Server Information Leakage :*
  - Some important directives in apache/httpd like ServerTokens and ServerSignature should be used, as they determine the level of granularity to disclose information about the web server.
- *Use Denial-of-Service Protection Modules* :
  - Httpd provides a concept called as *rate limiting*, which is a basic feature provided in almost all modern web-app servers like nginx, tomcat, and passenger. Rate limiting allows us to ensure that the rate of a certain attribute on the web request or response is in limit and not alarming to result in a Denial of service attack. One such rate limiting feature in httpd is :

    - mod_qos : it controls the maximum number of concurrent requests to a location/resource (URL) or virtual host.

    Other modules which help with rate limiting in apache are : mod_cband mod_bwshare mod_limitipconn mod_evasive.

    Hence, we should enable these modules to avoid DoS attacks on web server.
- *Configure HTTPD-Served Web Content Securely* :
  - One powerful functionality provided by Linux Operating system is chroot, which is sort of a jail and limits the access to filesystem to that process. Hence when a process is attacked successfully only a part of the file system is hampered. We can chroot httpd

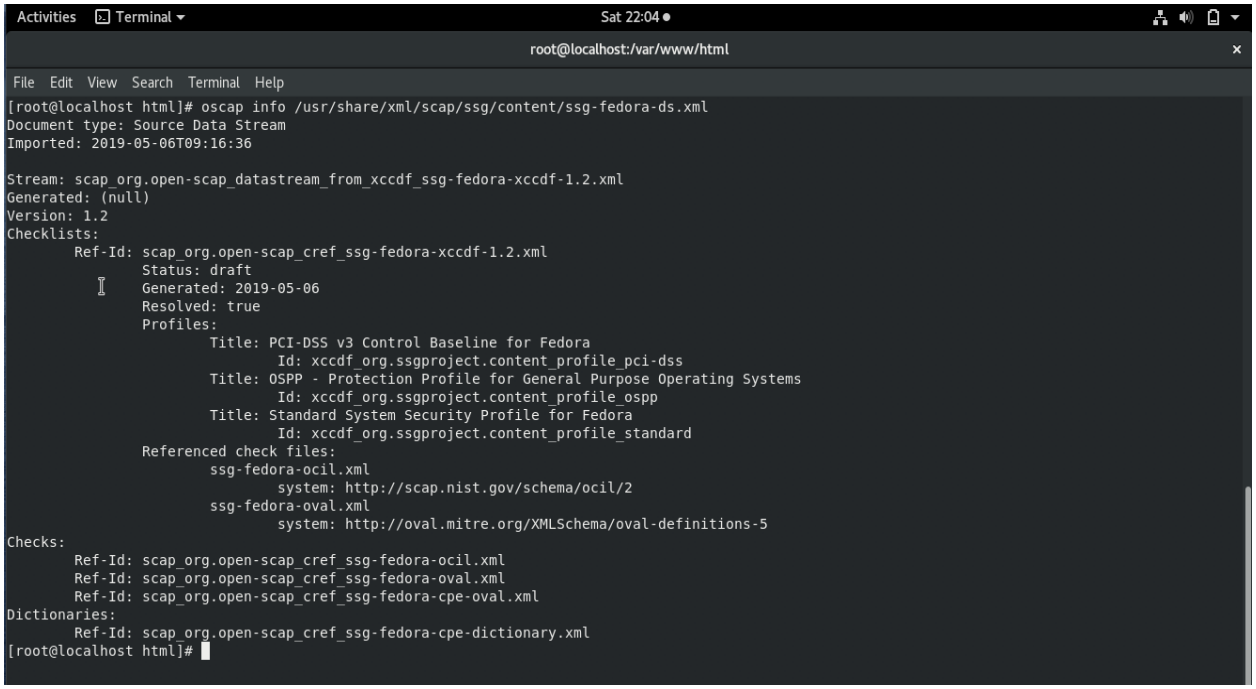
service by using *ChrootDir /chroot/apache* in httpd.conf.

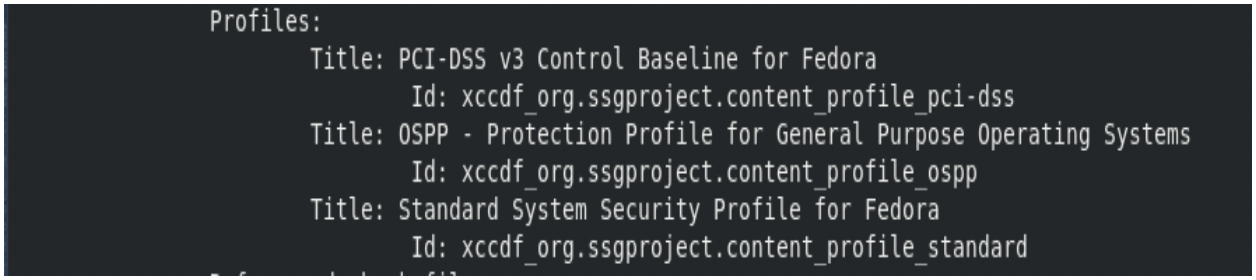
- Directory Tags :

  Httpd provides the functionality to separate each web server serving pages based on directory tag matching/evaluation. Hence providing a layer of security by restricting actions within a directory.

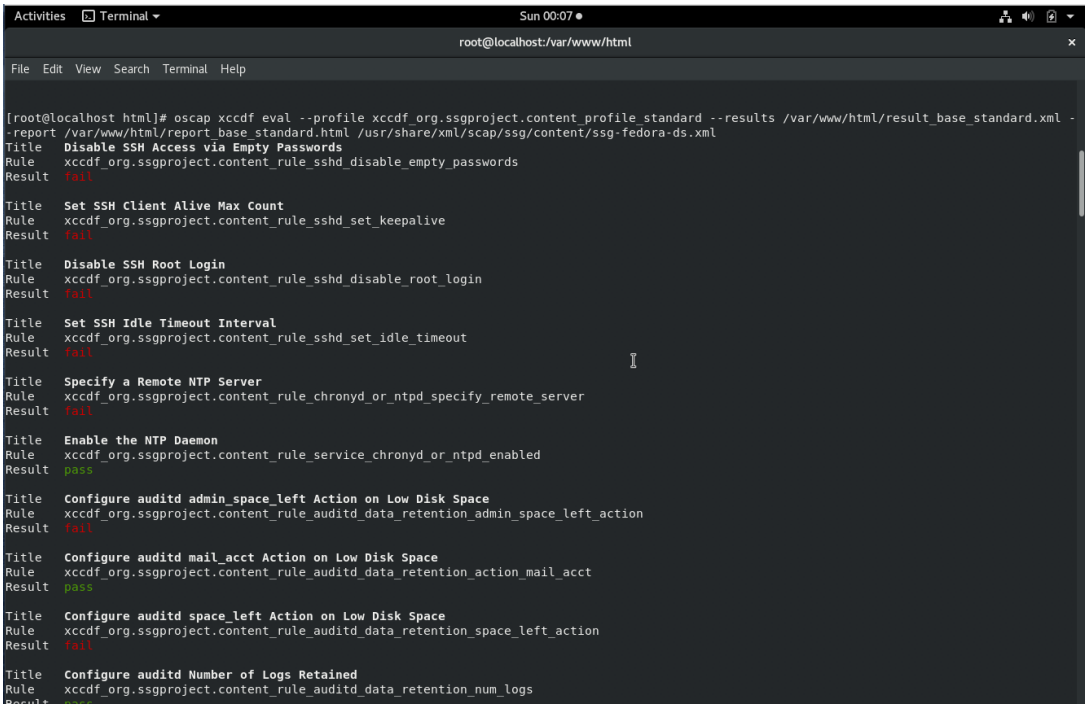
PART 2: SCANNING AND REMEDIATING FEDORA BASE SYSTEM:

Profiles listed in fedora-ds.xml file :

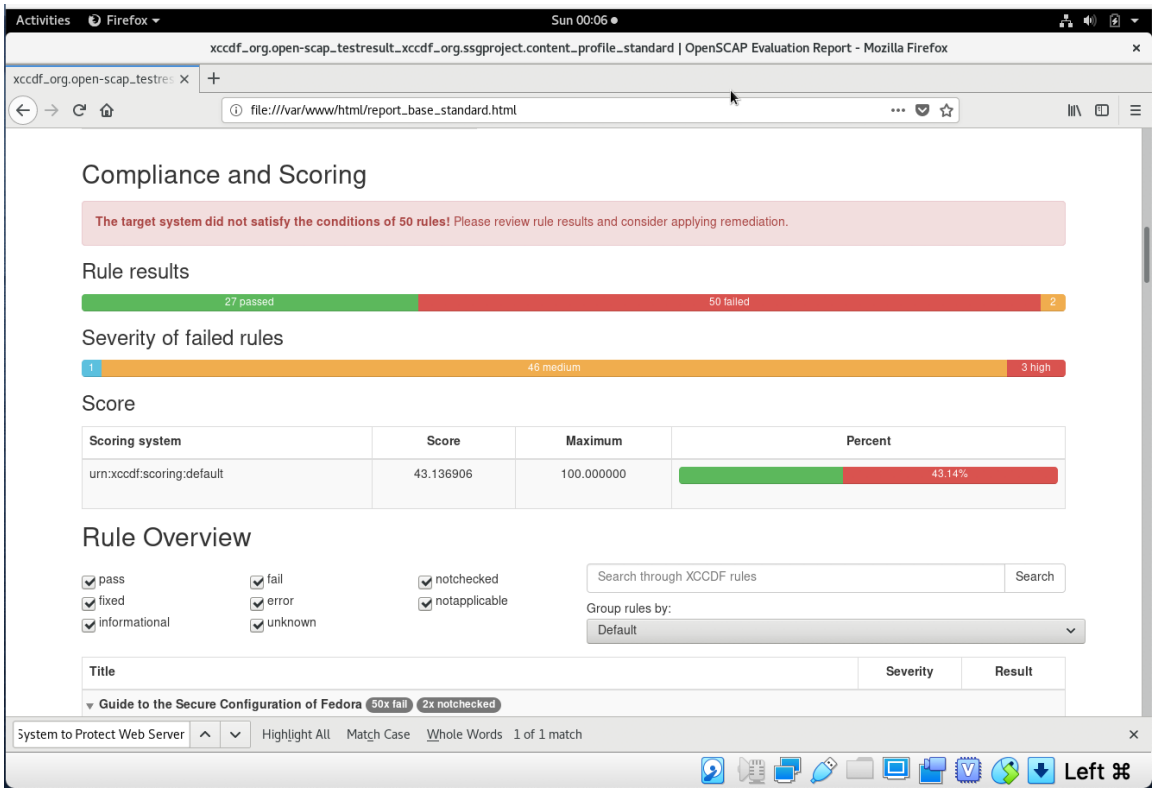


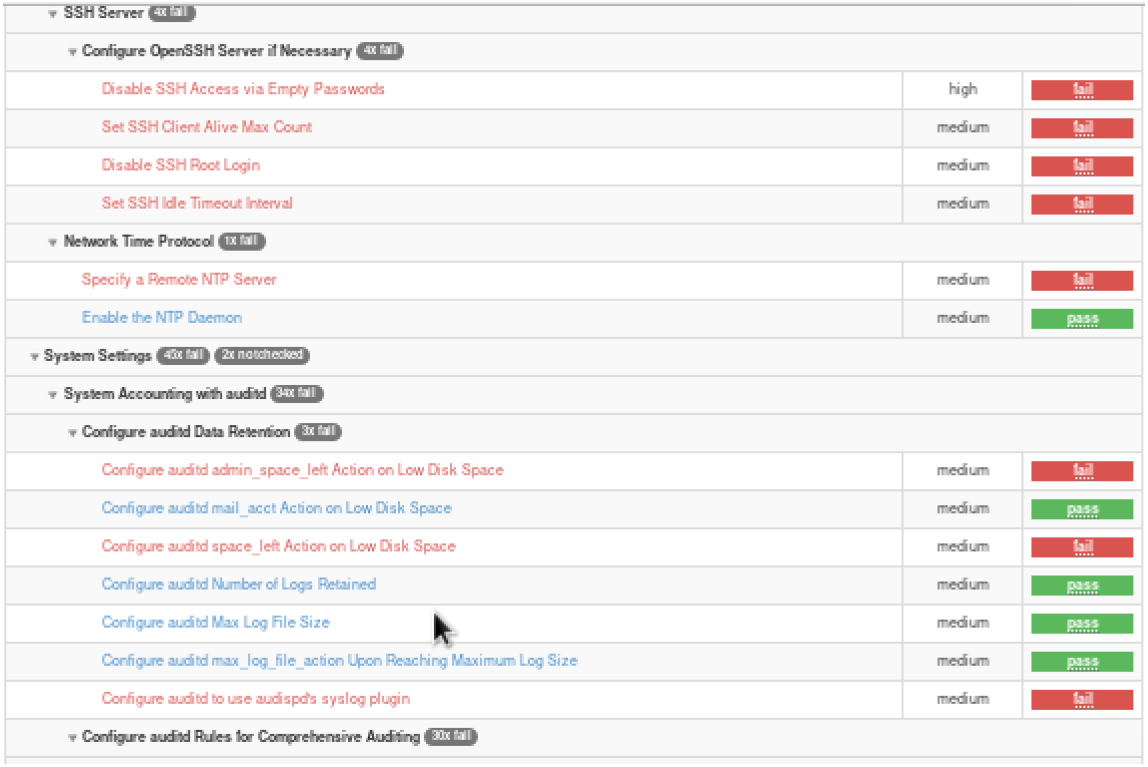


Now we will scan for our base VM and look at the compliant and non-complaint configurations :

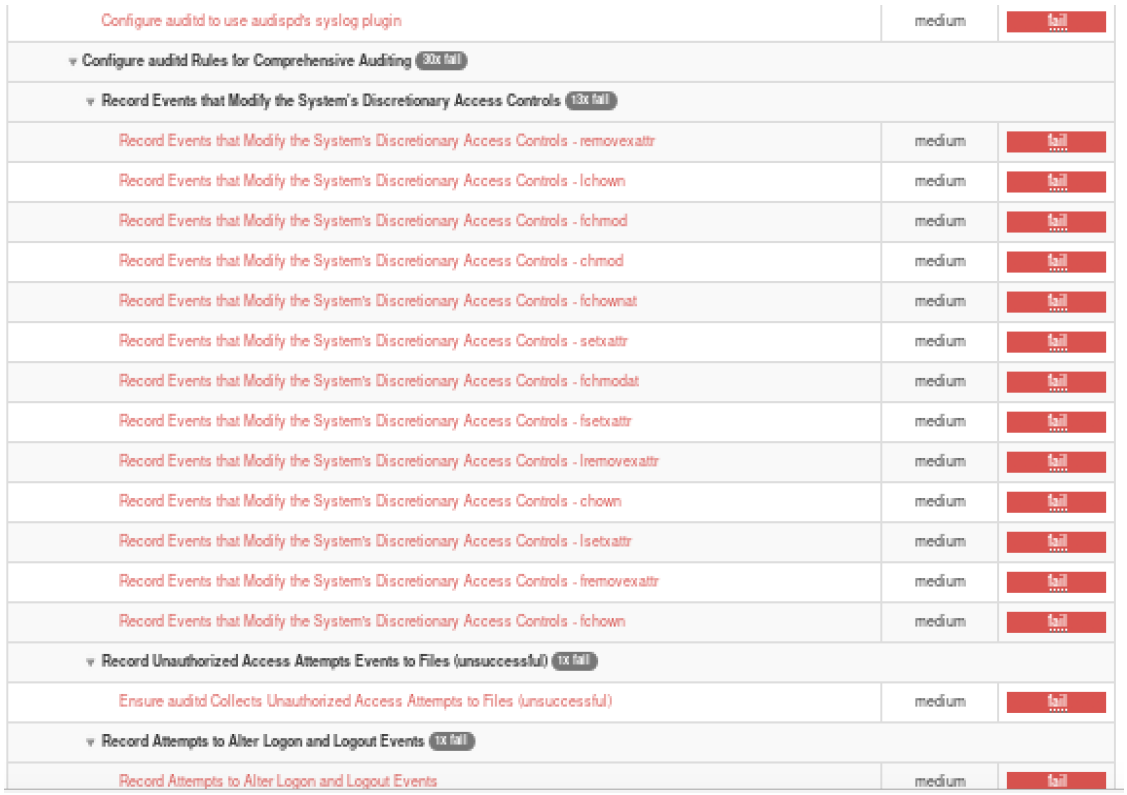


After the evaluation we saw the report which showed :





▾ SSH Server (4x fail)		
▾ Configure OpenSSH Server if Necessary (4x fail)		
Disable SSH Access via Empty Passwords	high	fail
Set SSH Client Alive Max Count	medium	fail
Disable SSH Root Login	medium	fail
Set SSH Idle Timeout Interval	medium	fail
▾ Network Time Protocol (1x fail)		
Specify a Remote NTP Server	medium	fail
Enable the NTP Daemon	medium	pass
▾ System Settings (40x fail) (2x notchecked)		
▾ System Accounting with auditd (34x fail)		
▾ Configure auditd Data Retention (3x fail)		
Configure auditd admin_space_left Action on Low Disk Space	medium	fail
Configure auditd mail_acct Action on Low Disk Space	medium	pass
Configure auditd space_left Action on Low Disk Space	medium	fail
Configure auditd Number of Logs Retained	medium	pass
Configure auditd Max Log File Size	medium	pass
Configure auditd max_log_file_action Upon Reaching Maximum Log Size	medium	pass
Configure auditd to use audispd's syslog plugin	medium	fail
▾ Configure auditd Rules for Comprehensive Auditing (30x fail)		



Configure auditd to use audispd's syslog plugin	medium	fail
▾ Configure auditd Rules for Comprehensive Auditing (30x fail)		
▾ Record Events that Modify the System's Discretionary Access Controls (13x fail)		
Record Events that Modify the System's Discretionary Access Controls - removexattr	medium	fail
Record Events that Modify the System's Discretionary Access Controls - lchown	medium	fail
Record Events that Modify the System's Discretionary Access Controls - fchmod	medium	fail
Record Events that Modify the System's Discretionary Access Controls - chmod	medium	fail
Record Events that Modify the System's Discretionary Access Controls - fchownat	medium	fail
Record Events that Modify the System's Discretionary Access Controls - setxattr	medium	fail
Record Events that Modify the System's Discretionary Access Controls - fchmodat	medium	fail
Record Events that Modify the System's Discretionary Access Controls - fsetxattr	medium	fail
Record Events that Modify the System's Discretionary Access Controls - lremovexattr	medium	fail
Record Events that Modify the System's Discretionary Access Controls - chown	medium	fail
Record Events that Modify the System's Discretionary Access Controls - lsetxattr	medium	fail
Record Events that Modify the System's Discretionary Access Controls - fremovexattr	medium	fail
Record Events that Modify the System's Discretionary Access Controls - fchown	medium	fail
▾ Record Unauthorized Access Attempts Events to Files (unsuccessful) (1x fail)		
Ensure auditd Collects Unauthorized Access Attempts to Files (unsuccessful)	medium	fail
▾ Record Attempts to Alter Logon and Logout Events (1x fail)		
Record Attempts to Alter Logon and Logout Events	medium	fail

▾ Record Attempts to Alter Logon and Logout Events (1x fail)		
Record Attempts to Alter Logon and Logout Events	medium	fail
▾ Record Information on the Use of Privileged Commands (1x fail)		
Ensure auditd Collects Information on the Use of Privileged Commands	medium	fail
▾ Records Events that Modify Date and Time Information (6x fail)		
Record Attempts to Alter Time Through stime	medium	fail
Record Attempts to Alter the localtime File	medium	fail
Record attempts to alter time through adjtimex	medium	fail
Record Attempts to Alter Time Through clock_settime	medium	fail
Record attempts to alter time through settimeofday	medium	fail
▾ Record File Deletion Events by User (1x fail)		
Ensure auditd Collects File Deletion Events by User	medium	fail
▾ Record Information on Kernel Modules Loading and Unloading (1x fail)		
Ensure auditd Collects Information on Kernel Module Loading and Unloading	medium	fail
Record Events that Modify the System's Network Environment	medium	fail
Record Attempts to Alter Process and Session Initiation Information	medium	fail
Record Events that Modify User/Group Information	medium	fail
Record Events that Modify the System's Mandatory Access Controls	medium	fail
System Audit Logs Must Be Owned By Root	medium	pass

System Audit Logs Must Be Owned By Root	medium	pass
Ensure auditd Collects System Administrator Actions	medium	fail
Ensure auditd Collects Information on Exporting to Media (successful)	medium	fail
Make the auditd Configuration Immutable	medium	fail
Enable auditd Service	high	pass
Enable Auditing for Processes Which Start Prior to the Audit Daemon	medium	fail
▾ Account and Access Control (6x fail)		
▸ Secure Session Configuration Files for Login Accounts		
▾ Protect Accounts by Restricting Password-Based Login (5x fail)		
▸ Set Account Expiration Parameters		
▾ Verify Proper Storage and Existence of Password Hashes (1x fail)		
Prevent Login to Accounts With Empty Password	high	fail
All GIDs referenced in /etc/passwd must be defined in /etc/group	low	pass
Verify All Account Password Hashes are Shadowed	medium	pass
Verify No netrc Files Exist	medium	pass
▾ Restrict Root Logins (1x fail)		
Direct root Logins Not Allowed	medium	fail
Restrict Virtual Console Root Logins	medium	pass
Verify Only Root Has UID 0	high	pass
Restrict Serial Port Root Logins	medium	pass

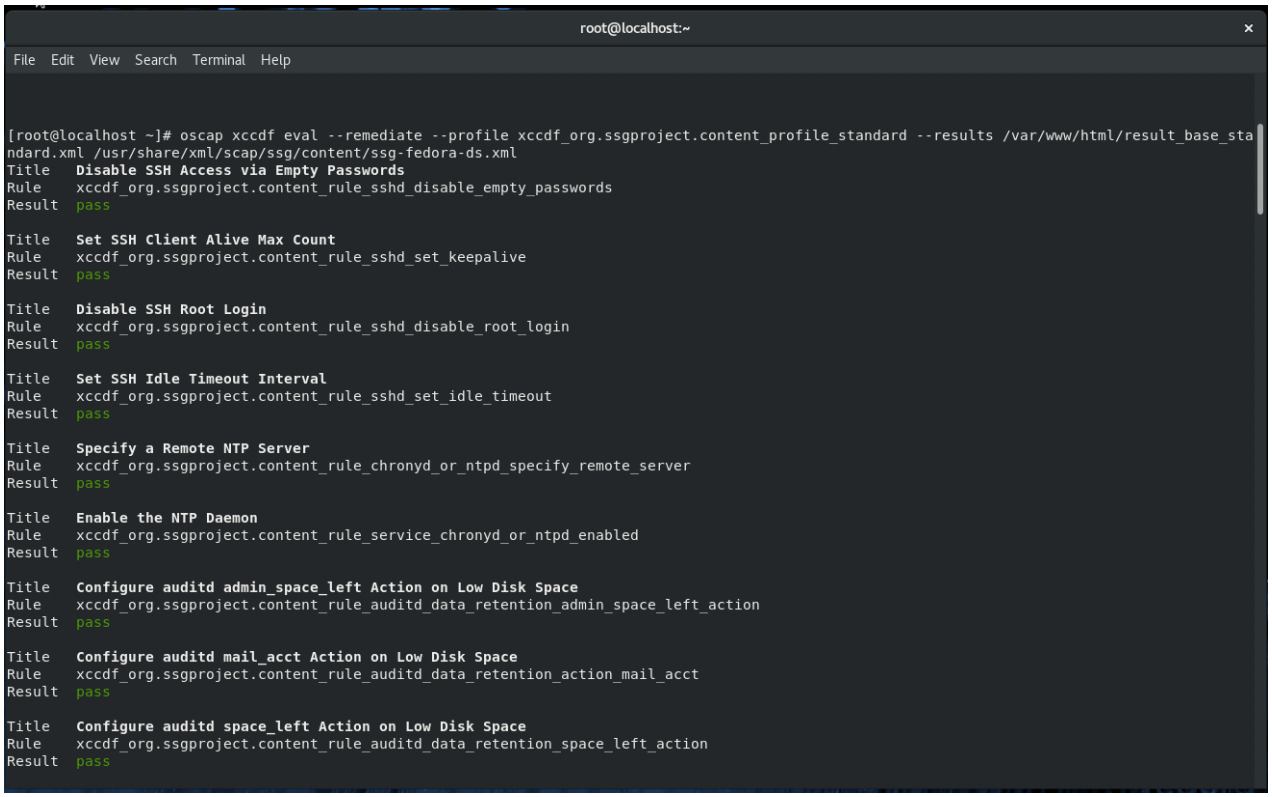
Direct root Logins Not Allowed	medium	fail
Restrict Virtual Console Root Logins	medium	pass
Verify Only Root Has UID 0	high	pass
Restrict Serial Port Root Logins	medium	pass
Set Password Expiration Parameters 3x fail		
Set Password Warning Age	medium	pass
Set Password Minimum Length in login.defs	medium	fail
Set Password Maximum Age	medium	fail
Set Password Minimum Age	medium	fail
Protect Accounts by Configuring PAM 1x fail		
Ensure PAM Displays Last Logon/Access Notification	low	fail
Installing and Maintaining Software 3x fail 1x notchecked		
System and Software Integrity 3x fail 1x notchecked		
System Cryptographic Policies 1x fail 1x notchecked		
Configure OpenSSL library to use System Crypto Policy	medium	fail
Configure Libreswan to use System Crypto Policy	medium	pass
Configure SSH to use System Crypto Policy	medium	pass
Configure Kerberos to use System Crypto Policy	medium	pass
Configure System Cryptography Policy	high	pass
Configure BIND to use System Crypto Policy	medium	notchecked

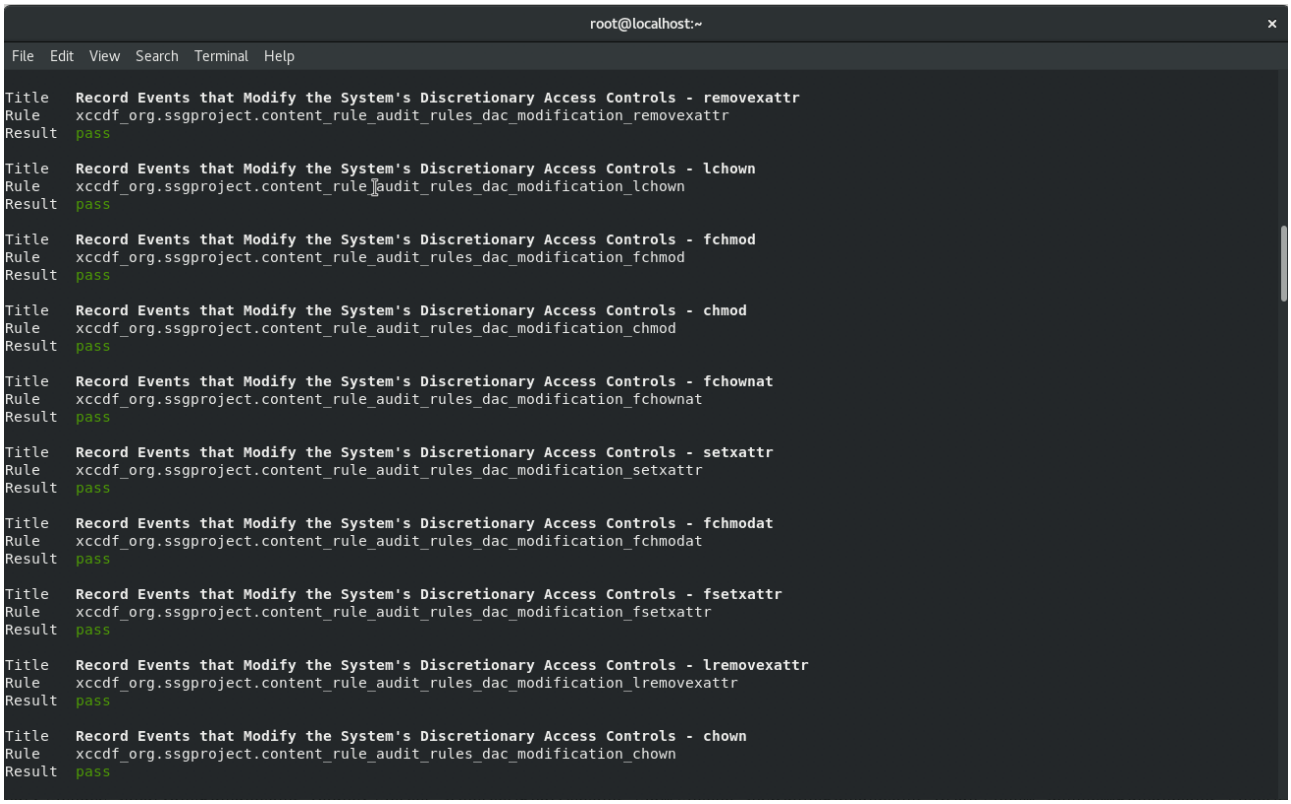
Configure BIND to use System Crypto Policy	medium	notchecked
Software Integrity Checking 2x fail		
Verify Integrity with AIDE 1x fail		
Build and Test AIDE Database	medium	fail
Verify Integrity with RPM 1x fail		
Verify and Correct File Permissions with RPM	high	fail
Verify File Hashes with RPM	high	pass
Disable Prelinking	medium	pass
Updating Software		
File Permissions and Masks 1x fail 1x notchecked		
Restrict Dynamic Mounting and Unmounting of Filesystems 1x notchecked		
Disable Kernel Support for USB via Bootloader Configuration	unknown	notchecked
Verify Permissions on Important Files and Directories 1x fail		
Verify File Permissions Within Some Important Directories 1x fail		
Verify that System Executables Have Root Ownership	medium	fail
Verify that Shared Library Files Have Restrictive Permissions	medium	pass
Verify that System Executables Have Restrictive Permissions	medium	pass
Verify that Shared Library Files Have Root Ownership	medium	pass
Network Configuration and Firewalls 1x fail		
firewalld 1x fail		

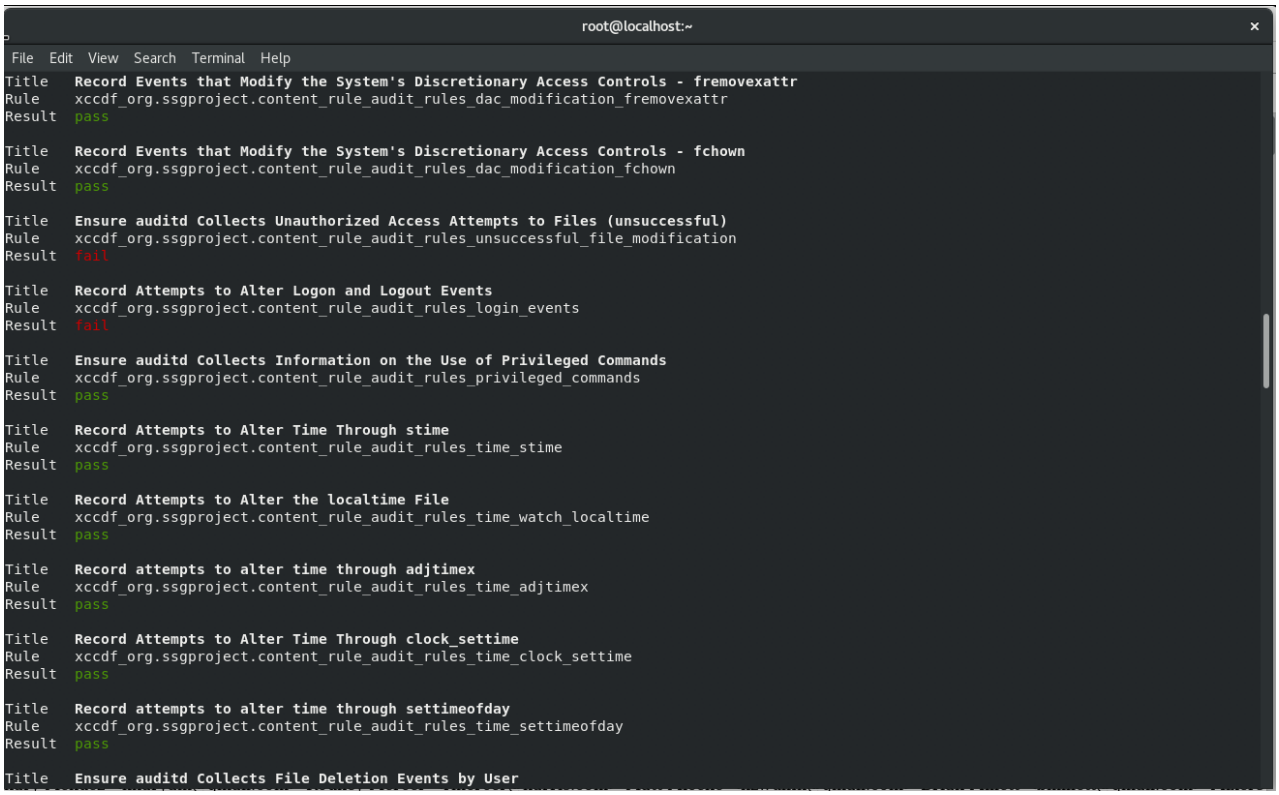
▸ Updating Software		
▾ File Permissions and Masks tx fail tx notchecked		
▾ Restrict Dynamic Mounting and Unmounting of Filesystems tx notchecked		
Disable Kernel Support for USB via Bootloader Configuration	unknown	notchecked
▾ Verify Permissions on Important Files and Directories tx fail		
▾ Verify File Permissions Within Some Important Directories tx fail		
Verify that System Executables Have Root Ownership	medium	fail
Verify that Shared Library Files Have Restrictive Permissions	medium	pass
Verify that System Executables Have Restrictive Permissions	medium	pass
Verify that Shared Library Files Have Root Ownership	medium	pass
▾ Network Configuration and Firewalls tx fail		
▾ firewalld tx fail		
▸ Inspect and Activate Default firewalld Rules		
▾ Strengthen the Default Ruleset tx fail		
Set Default firewalld Zone for Incoming Packets	medium	fail

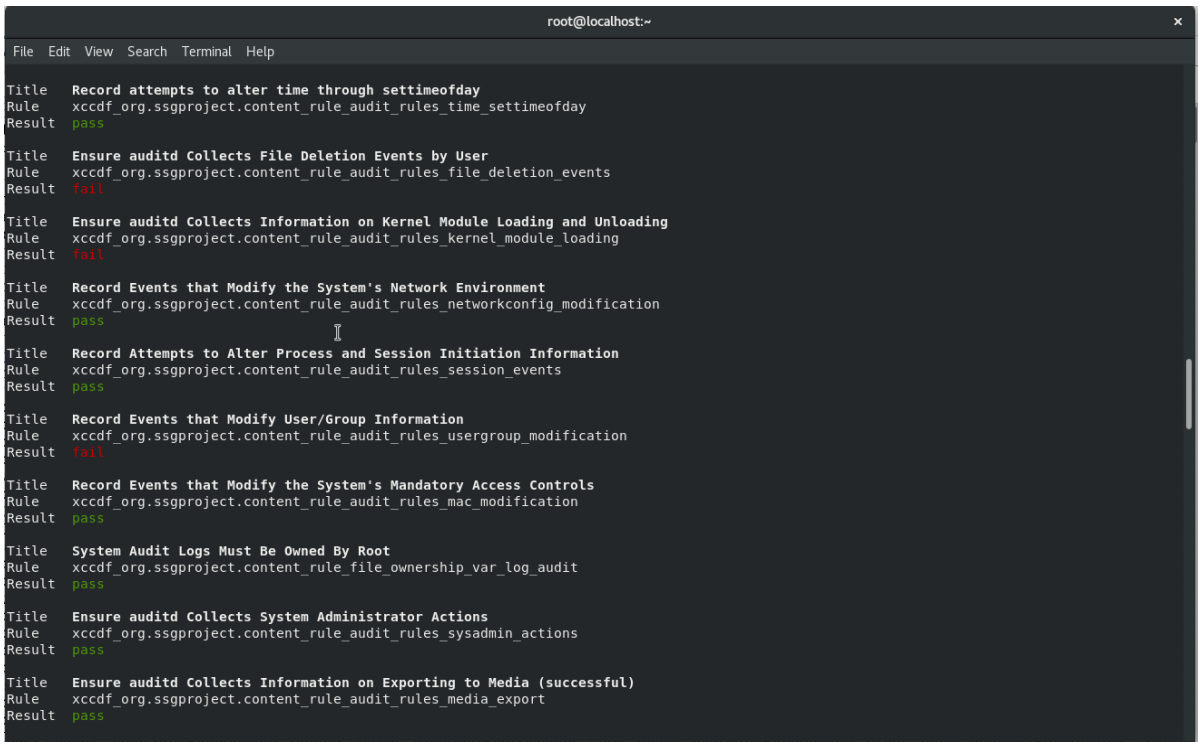
Now we will try the remediation feature provided by open scap, here is the output for various profiles of remediation:

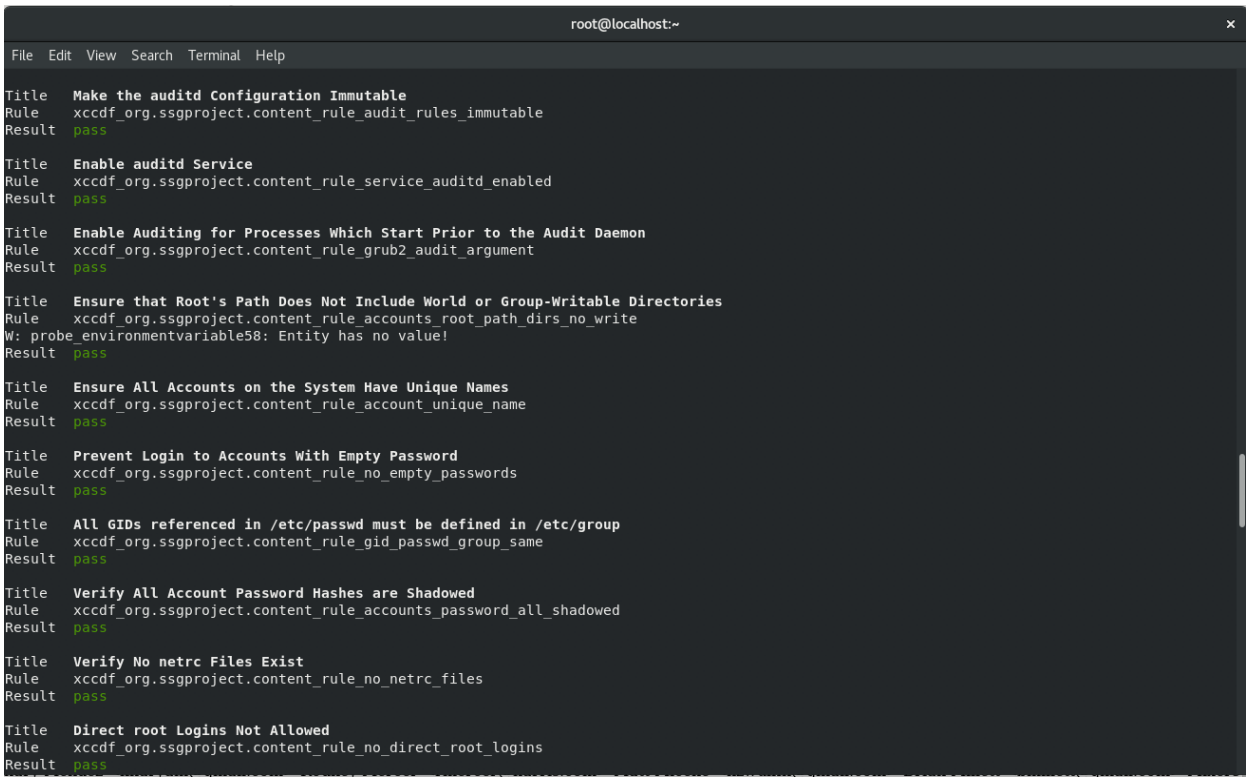
STANDARD :

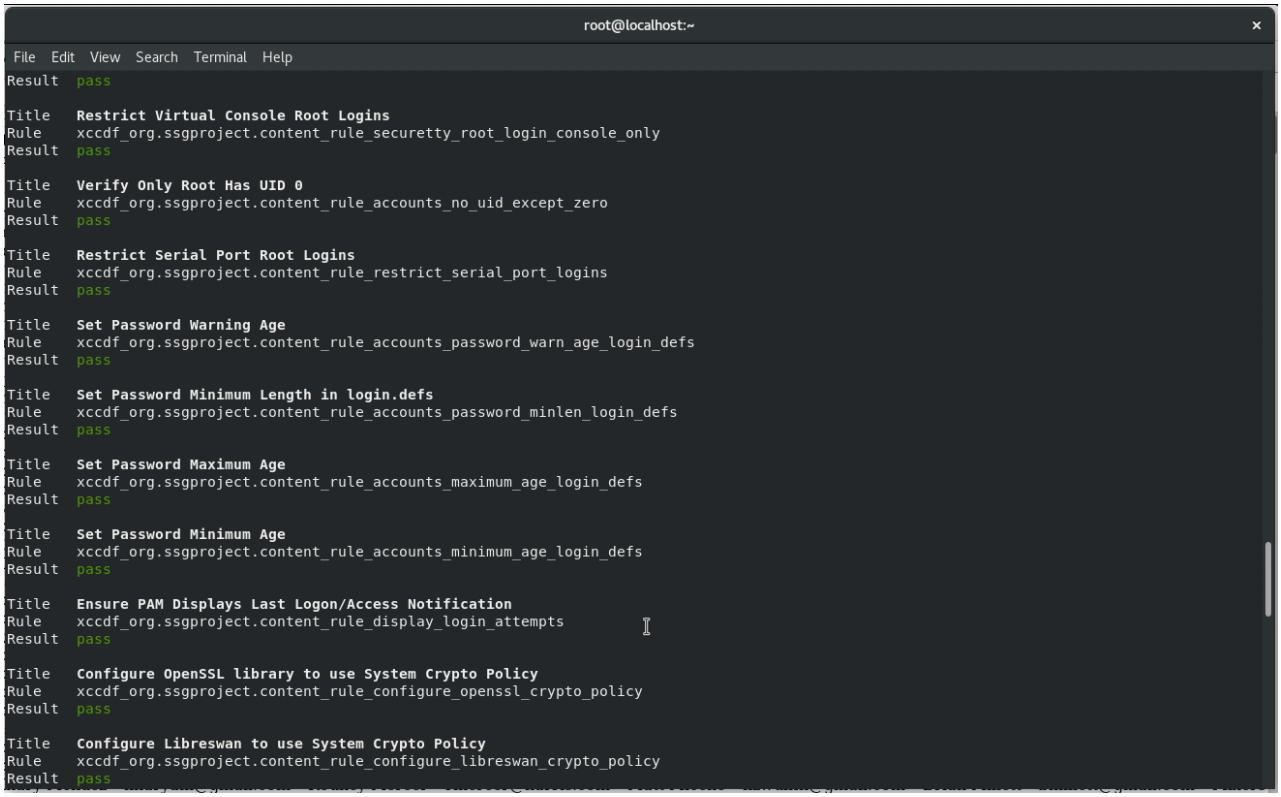


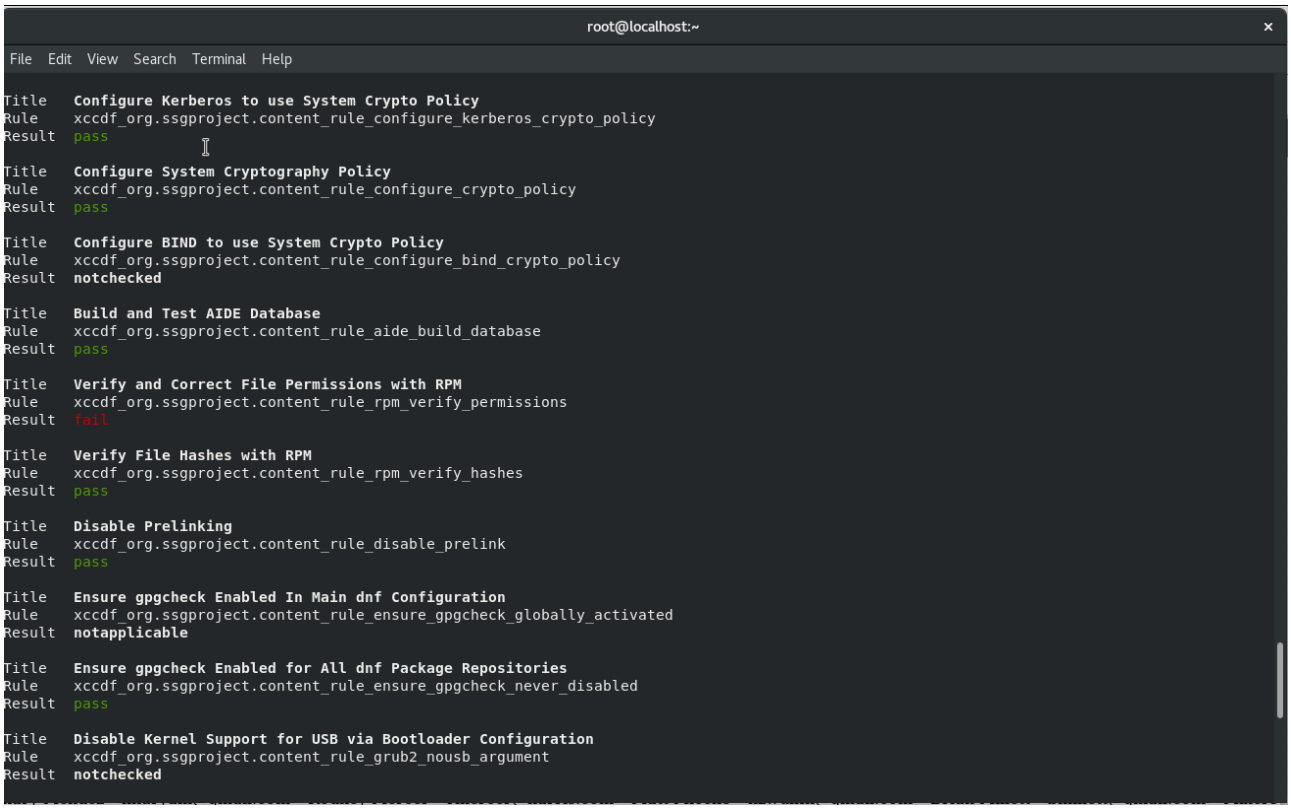

root@localhost:~
File Edit View Search Terminal Help
Title Record Events that Modify the System's Discretionary Access Controls - removexattr
Rule xccdf_org.ssgproject.content_rule_audit_rules_dac_modification_removexattr
Result pass
Title Record Events that Modify the System's Discretionary Access Controls - lchown
Rule xccdf_org.ssgproject.content_rule_audit_rules_dac_modification_lchown
Result pass
Title Record Events that Modify the System's Discretionary Access Controls - fchmod
Rule xccdf_org.ssgproject.content_rule_audit_rules_dac_modification_fchmod
Result pass
Title Record Events that Modify the System's Discretionary Access Controls - chmod
Rule xccdf_org.ssgproject.content_rule_audit_rules_dac_modification_chmod
Result pass
Title Record Events that Modify the System's Discretionary Access Controls - fchownat
Rule xccdf_org.ssgproject.content_rule_audit_rules_dac_modification_fchownat
Result pass
Title Record Events that Modify the System's Discretionary Access Controls - setxattr
Rule xccdf_org.ssgproject.content_rule_audit_rules_dac_modification_setxattr
Result pass
Title Record Events that Modify the System's Discretionary Access Controls - fchmodat
Rule xccdf_org.ssgproject.content_rule_audit_rules_dac_modification_fchmodat
Result pass
Title Record Events that Modify the System's Discretionary Access Controls - fsetxattr
Rule xccdf_org.ssgproject.content_rule_audit_rules_dac_modification_fsetxattr
Result pass
Title Record Events that Modify the System's Discretionary Access Controls - lremovexattr
Rule xccdf_org.ssgproject.content_rule_audit_rules_dac_modification_lremovexattr
Result pass
Title Record Events that Modify the System's Discretionary Access Controls - chown
Rule xccdf_org.ssgproject.content_rule_audit_rules_dac_modification_chown
Result pass

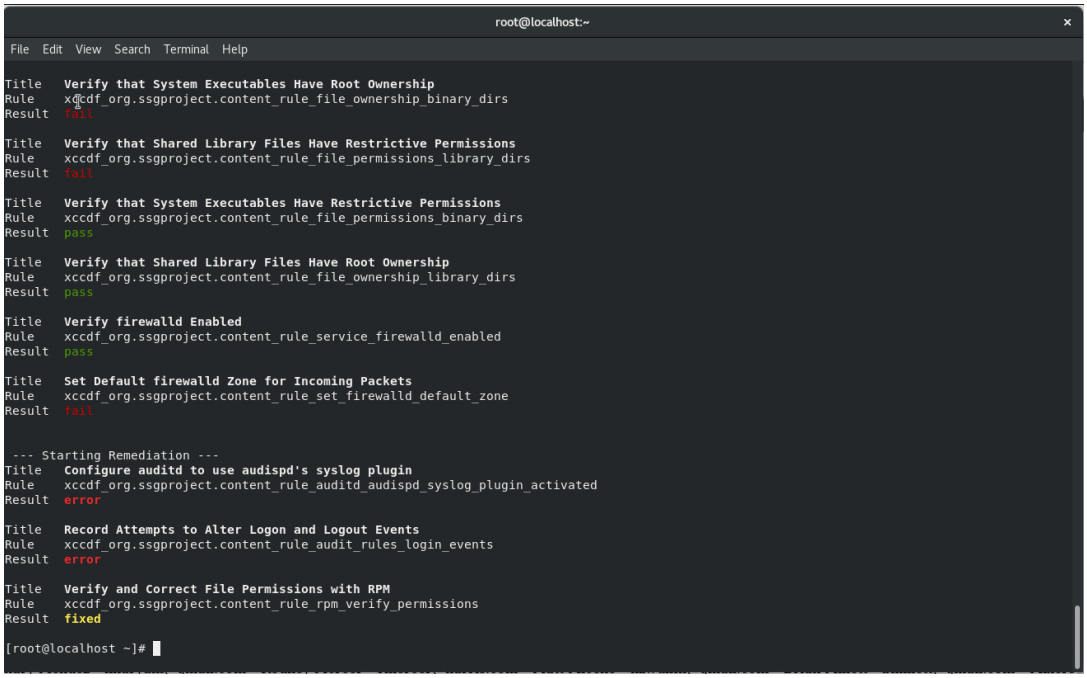

root@localhost:~
File Edit View Search Terminal Help
Title Record Events that Modify the System's Discretionary Access Controls - fremovexattr
Rule xccdf_org.ssgproject.content_rule_audit_rules_dac_modification_fremovexattr
Result pass
Title Record Events that Modify the System's Discretionary Access Controls - fchown
Rule xccdf_org.ssgproject.content_rule_audit_rules_dac_modification_fchown
Result pass
Title Ensure auditd Collects Unauthorized Access Attempts to Files (unsuccessful)
Rule xccdf_org.ssgproject.content_rule_audit_rules_unsuccessful_file_modification
Result fail
Title Record Attempts to Alter Logon and Logout Events
Rule xccdf_org.ssgproject.content_rule_audit_rules_login_events
Result fail
Title Ensure auditd Collects Information on the Use of Privileged Commands
Rule xccdf_org.ssgproject.content_rule_audit_rules_privileged_commands
Result pass
Title Record Attempts to Alter Time Through stime
Rule xccdf_org.ssgproject.content_rule_audit_rules_time_stime
Result pass
Title Record Attempts to Alter the localtime File
Rule xccdf_org.ssgproject.content_rule_audit_rules_time_watch_localtime
Result pass
Title Record attempts to alter time through adjtimex
Rule xccdf_org.ssgproject.content_rule_audit_rules_time_adjtimex
Result pass
Title Record Attempts to Alter Time Through clock_settime
Rule xccdf_org.ssgproject.content_rule_audit_rules_time_clock_settime
Result pass
Title Record attempts to alter time through settimeofday
Rule xccdf_org.ssgproject.content_rule_audit_rules_time_settimeofday
Result pass
Title Ensure auditd Collects File Deletion Events by User


root@localhost:~
File Edit View Search Terminal Help
Title Record attempts to alter time through settimeofday
Rule xccdf_org.ssgproject.content_rule_audit_rules_time_settimeofday
Result pass
Title Ensure auditd Collects File Deletion Events by User
Rule xccdf_org.ssgproject.content_rule_audit_rules_file_deletion_events
Result fail
Title Ensure auditd Collects Information on Kernel Module Loading and Unloading
Rule xccdf_org.ssgproject.content_rule_audit_rules_kernel_module_loading
Result fail
Title Record Events that Modify the System's Network Environment
Rule xccdf_org.ssgproject.content_rule_audit_rules_networkconfig_modification
Result pass
Title Record Attempts to Alter Process and Session Initiation Information
Rule xccdf_org.ssgproject.content_rule_audit_rules_session_events
Result pass
Title Record Events that Modify User/Group Information
Rule xccdf_org.ssgproject.content_rule_audit_rules_usergroup_modification
Result fail
Title Record Events that Modify the System's Mandatory Access Controls
Rule xccdf_org.ssgproject.content_rule_audit_rules_mac_modification
Result pass
Title System Audit Logs Must Be Owned By Root
Rule xccdf_org.ssgproject.content_rule_file_ownership_var_log_audit
Result pass
Title Ensure auditd Collects System Administrator Actions
Rule xccdf_org.ssgproject.content_rule_audit_rules_sysadmin_actions
Result pass
Title Ensure auditd Collects Information on Exporting to Media (successful)
Rule xccdf_org.ssgproject.content_rule_audit_rules_media_export
Result pass

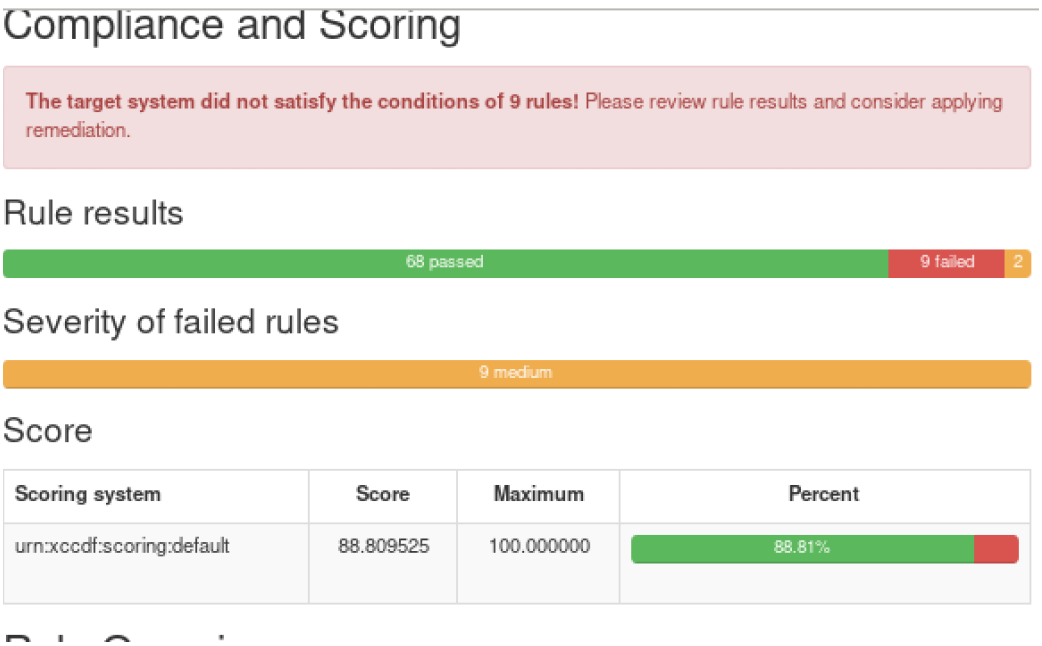

root@localhost:~
File Edit View Search Terminal Help
Title Make the auditd Configuration Immutable
Rule xccdf_org.ssgproject.content_rule_audit_rules_immutable
Result pass
Title Enable auditd Service
Rule xccdf_org.ssgproject.content_rule_service_auditd_enabled
Result pass
Title Enable Auditing for Processes Which Start Prior to the Audit Daemon
Rule xccdf_org.ssgproject.content_rule_grub2_audit_argument
Result pass
Title Ensure that Root's Path Does Not Include World or Group-Writable Directories
Rule xccdf_org.ssgproject.content_rule_accounts_root_path_dirs_no_write
W: probe_environmentvariable58: Entity has no value!
Result pass
Title Ensure All Accounts on the System Have Unique Names
Rule xccdf_org.ssgproject.content_rule_account_unique_name
Result pass
Title Prevent Login to Accounts With Empty Password
Rule xccdf_org.ssgproject.content_rule_no_empty_passwords
Result pass
Title All GIDs referenced in /etc/passwd must be defined in /etc/group
Rule xccdf_org.ssgproject.content_rule_gid_passwd_group_same
Result pass
Title Verify All Account Password Hashes are Shadowed
Rule xccdf_org.ssgproject.content_rule_accounts_password_all_shadowed
Result pass
Title Verify No netrc Files Exist
Rule xccdf_org.ssgproject.content_rule_no_netrc_files
Result pass
Title Direct root Logins Not Allowed
Rule xccdf_org.ssgproject.content_rule_no_direct_root_logins
Result pass

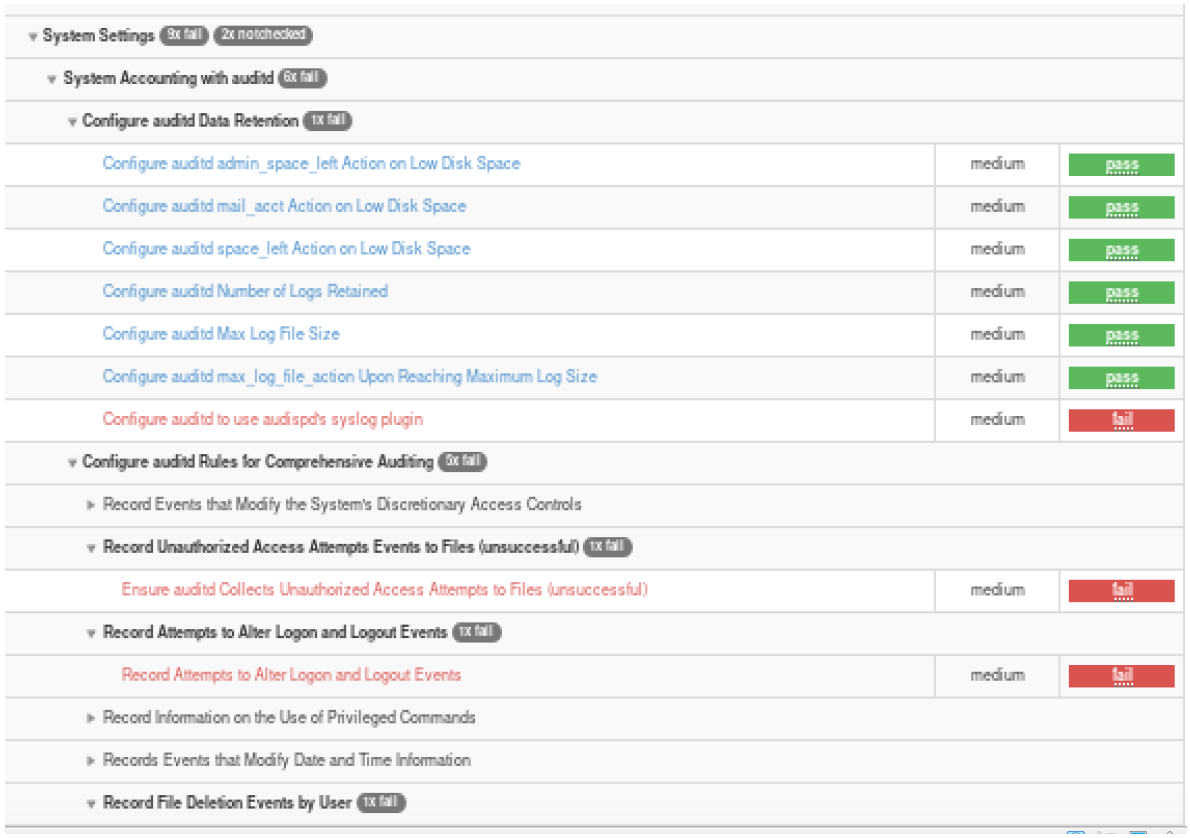

root@localhost:~
File Edit View Search Terminal Help
Result pass
Title Restrict Virtual Console Root Logins
Rule xccdf_org.ssgproject.content_rule_securetty_root_login_console_only
Result pass
Title Verify Only Root Has UID 0
Rule xccdf_org.ssgproject.content_rule_accounts_no_uid_except_zero
Result pass
Title Restrict Serial Port Root Logins
Rule xccdf_org.ssgproject.content_rule_restrict_serial_port_logins
Result pass
Title Set Password Warning Age
Rule xccdf_org.ssgproject.content_rule_accounts_password_warn_age_login_defs
Result pass
Title Set Password Minimum Length in login.defs
Rule xccdf_org.ssgproject.content_rule_accounts_password_minlen_login_defs
Result pass
Title Set Password Maximum Age
Rule xccdf_org.ssgproject.content_rule_accounts_maximum_age_login_defs
Result pass
Title Set Password Minimum Age
Rule xccdf_org.ssgproject.content_rule_accounts_minimum_age_login_defs
Result pass
Title Ensure PAM Displays Last Logon/Access Notification
Rule xccdf_org.ssgproject.content_rule_display_login_attempts
Result pass
Title Configure OpenSSL library to use System Crypto Policy
Rule xccdf_org.ssgproject.content_rule_configure_openssl_crypto_policy
Result pass
Title Configure Libreswan to use System Crypto Policy
Rule xccdf_org.ssgproject.content_rule_configure_libreswan_crypto_policy
Result pass


root@localhost:~
File Edit View Search Terminal Help
Title Configure Kerberos to use System Crypto Policy
Rule xccdf_org.ssgproject.content_rule_configure_kerberos_crypto_policy
Result pass
Title Configure System Cryptography Policy
Rule xccdf_org.ssgproject.content_rule_configure_crypto_policy
Result pass
Title Configure BIND to use System Crypto Policy
Rule xccdf_org.ssgproject.content_rule_configure_bind_crypto_policy
Result notchecked
Title Build and Test AIDE Database
Rule xccdf_org.ssgproject.content_rule_aide_build_database
Result pass
Title Verify and Correct File Permissions with RPM
Rule xccdf_org.ssgproject.content_rule_rpm_verify_permissions
Result fail
Title Verify File Hashes with RPM
Rule xccdf_org.ssgproject.content_rule_rpm_verify_hashes
Result pass
Title Disable Prelinking
Rule xccdf_org.ssgproject.content_rule_disable_prelink
Result pass
Title Ensure gpgcheck Enabled In Main dnf Configuration
Rule xccdf_org.ssgproject.content_rule_ensure_gpgcheck_globally_activated
Result notapplicable
Title Ensure gpgcheck Enabled for All dnf Package Repositories
Rule xccdf_org.ssgproject.content_rule_ensure_gpgcheck_never_disabled
Result pass
Title Disable Kernel Support for USB via Bootloader Configuration
Rule xccdf_org.ssgproject.content_rule_grub2_nousb_argument
Result notchecked



We ran the test again and checked the report for updated Test results :



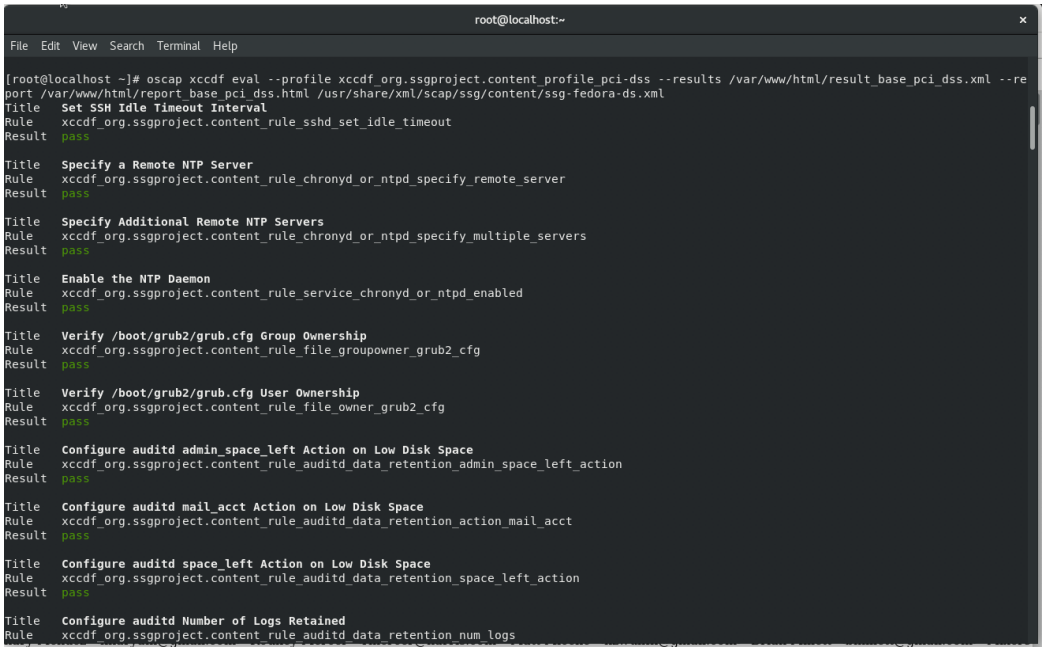


▼ System Settings 9x fail 2x notchecked		
▼ System Accounting with auditd 6x fail		
▼ Configure auditd Data Retention 1x fail		
Configure auditd admin_space_left Action on Low Disk Space	medium	pass
Configure auditd mail_acct Action on Low Disk Space	medium	pass
Configure auditd space_left Action on Low Disk Space	medium	pass
Configure auditd Number of Logs Retained	medium	pass
Configure auditd Max Log File Size	medium	pass
Configure auditd max_log_file_action Upon Reaching Maximum Log Size	medium	pass
Configure auditd to use audispd's syslog plugin	medium	fail
▼ Configure auditd Rules for Comprehensive Auditing 5x fail		
▶ Record Events that Modify the System's Discretionary Access Controls		
▼ Record Unauthorized Access Attempts Events to Files (unsuccessful) 1x fail		
Ensure auditd Collects Unauthorized Access Attempts to Files (unsuccessful)	medium	fail
▼ Record Attempts to Alter Logon and Logout Events 1x fail		
Record Attempts to Alter Logon and Logout Events	medium	fail
▶ Record Information on the Use of Privileged Commands		
▶ Records Events that Modify Date and Time Information		
▼ Record File Deletion Events by User 1x fail		
Ensure auditd Collects File Deletion Events by User	medium	fail
▼ Record Information on Kernel Modules Loading and Unloading 1x fail		
Ensure auditd Collects Information on Kernel Module Loading and Unloading	medium	fail
Record Events that Modify the System's Network Environment	medium	pass
Record Attempts to Alter Process and Session Initiation Information	medium	pass
Record Events that Modify User/Group Information	medium	fail
Record Events that Modify the System's Mandatory Access Controls	medium	pass
System Audit Logs Must Be Owned By Root	medium	pass
Ensure auditd Collects System Administrator Actions	medium	pass
Ensure auditd Collects Information on Exporting to Media (successful)	medium	pass
Make the auditd Configuration Immutable	medium	pass
Enable auditd Service	high	pass
Enable Auditing for Processes Which Start Prior to the Audit Daemon	medium	pass
▶ Account and Access Control		
▼ Installing and Maintaining Software 1x notchecked		
▼ System and Software Integrity 1x notchecked		
▼ System Cryptographic Policies 1x notchecked		
Configure OpenSSL library to use System Crypto Policy	medium	pass
Configure Libreswan to use System Crypto Policy	medium	pass

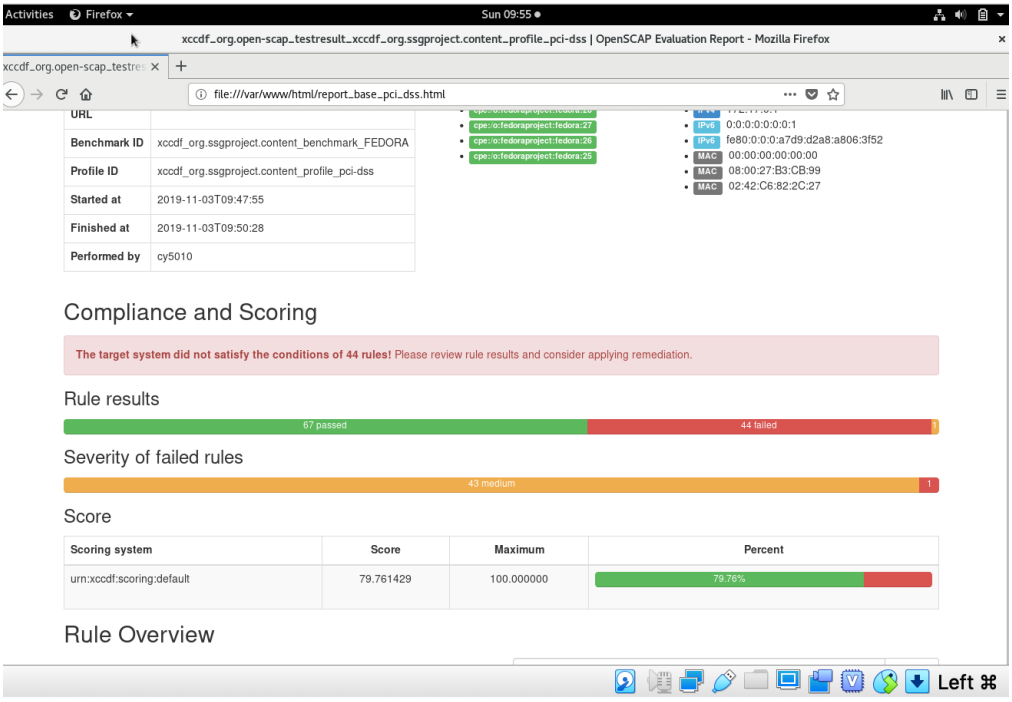
Hence we can see that oscap, has remediated a lot of checks, which failed in initial check, like :

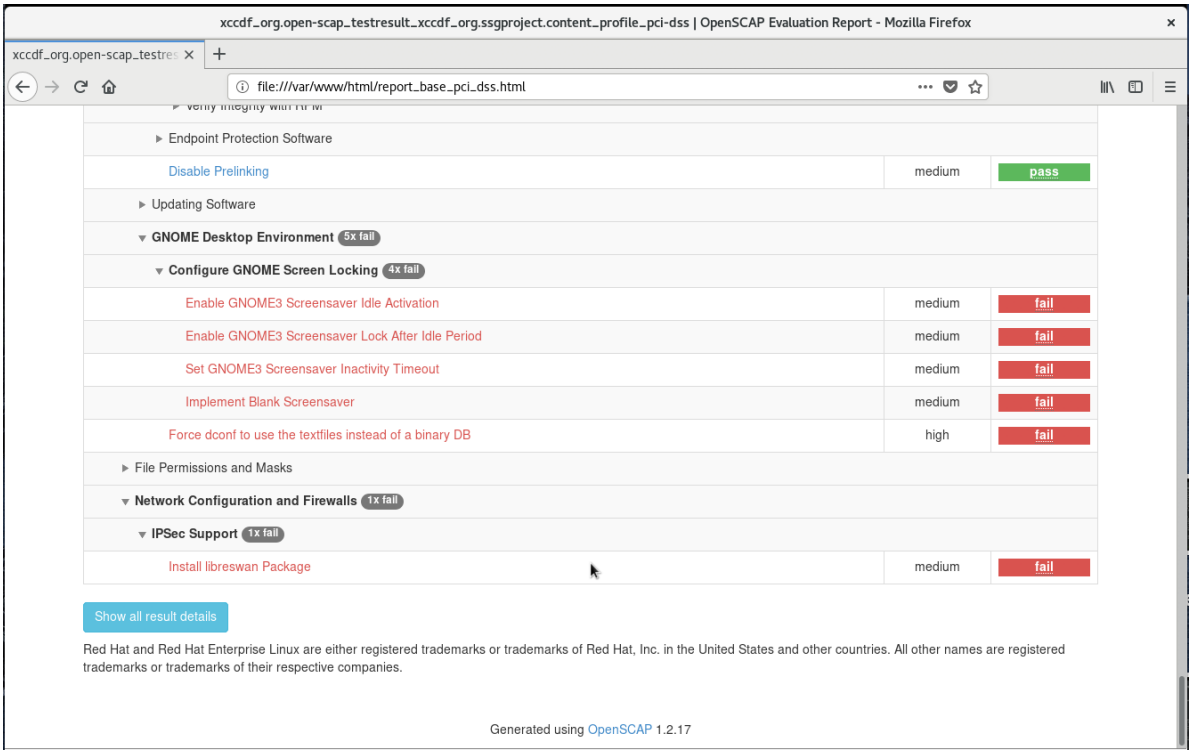
1. Disable SSH root login
2. Specify a remote NTP server
3. Configure audit space_left action on low disk_space and many more.

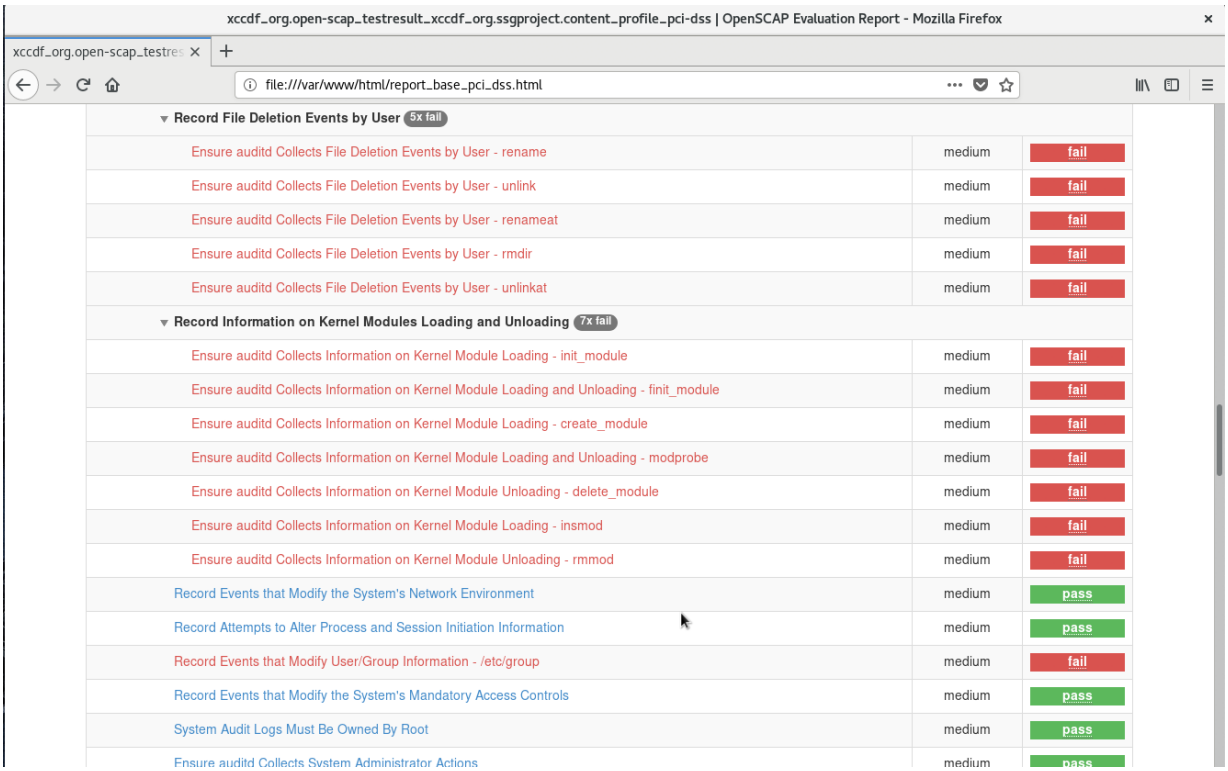
Scanning for PCI-DSS :

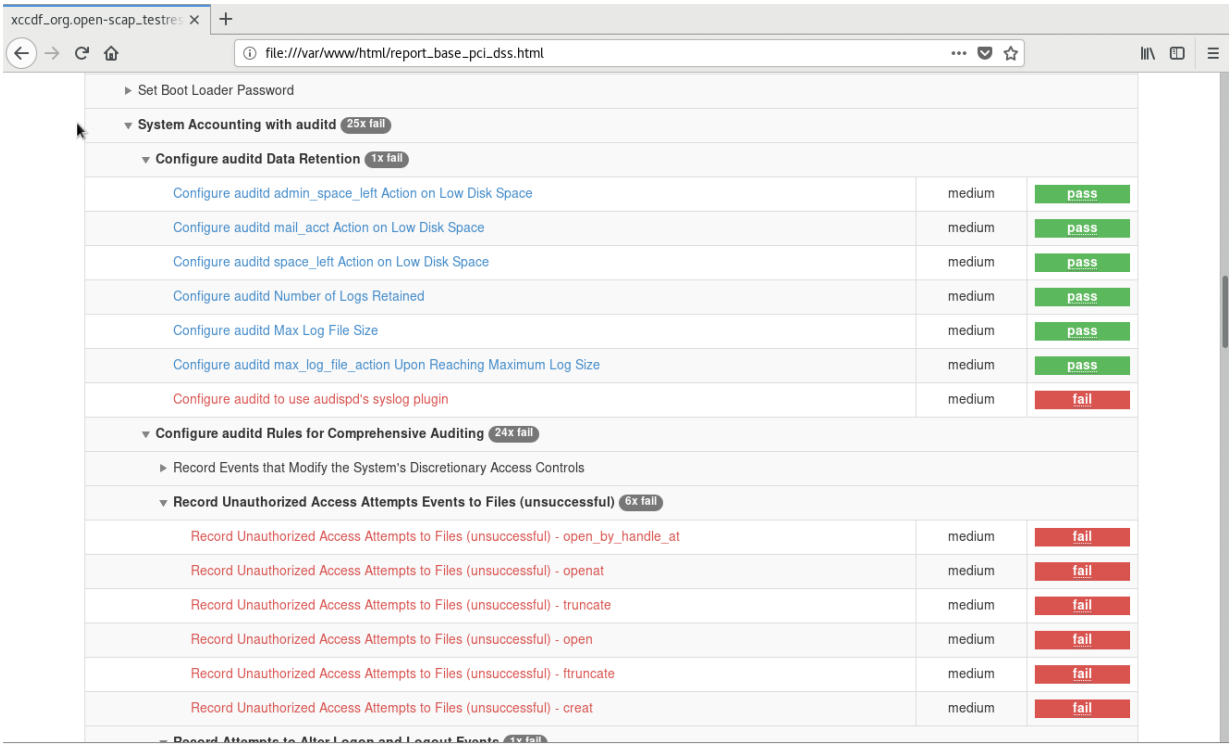


PCI-DSS scan report :

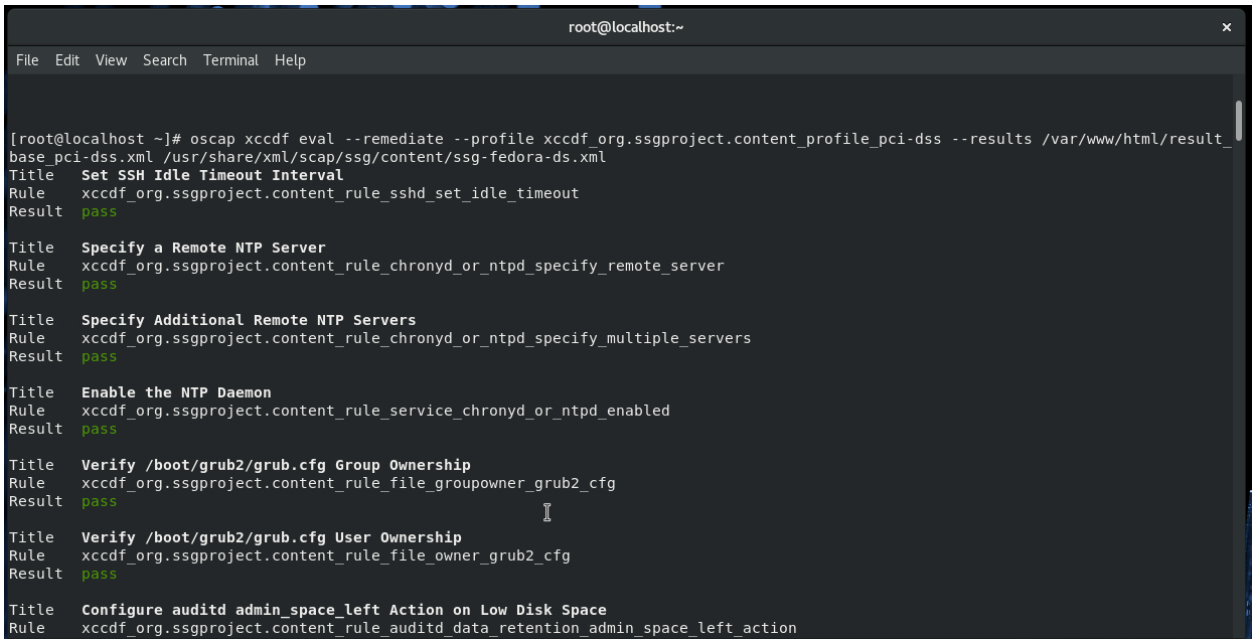



xccdf_org.open-scap_testresult_xccdf_org.ssgproject.content_profile_pci-dss | OpenSCAP Evaluation Report - Mozilla Firefox
file:///var/www/html/report_base_pci_dss.html
Endpoint Protection Software
Disable Prelinking medium pass
Updating Software
GNOME Desktop Environment 5x fail
Configure GNOME Screen Locking 4x fail
Enable GNOME3 Screensaver Idle Activation medium fail
Enable GNOME3 Screensaver Lock After Idle Period medium fail
Set GNOME3 Screensaver Inactivity Timeout medium fail
Implement Blank Screensaver medium fail
Force dconf to use the textfiles instead of a binary DB high fail
File Permissions and Masks
Network Configuration and Firewalls 1x fail
IPSec Support 1x fail
Install libreswan Package medium fail
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 1.2.17

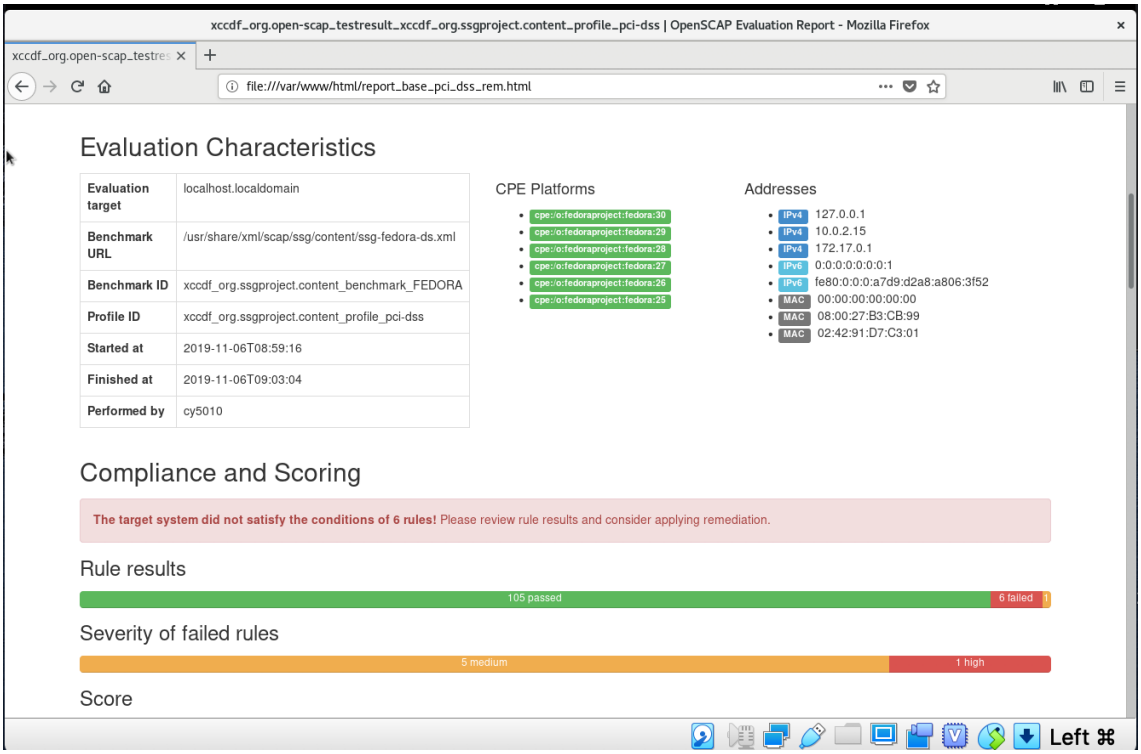

xccdf_org.open-scap_testresult_xccdf_org.ssgproject.content_profile_pci-dss | OpenSCAP Evaluation Report - Mozilla Firefox
file:///var/www/html/report_base_pci_dss.html
Record File Deletion Events by User 5x fail
Ensure auditd Collects File Deletion Events by User - rename medium fail
Ensure auditd Collects File Deletion Events by User - unlink medium fail
Ensure auditd Collects File Deletion Events by User - renameat medium fail
Ensure auditd Collects File Deletion Events by User - rmdir medium fail
Ensure auditd Collects File Deletion Events by User - unlinkat medium fail
Record Information on Kernel Modules Loading and Unloading 7x fail
Ensure auditd Collects Information on Kernel Module Loading - init_module medium fail
Ensure auditd Collects Information on Kernel Module Loading and Unloading - finit_module medium fail
Ensure auditd Collects Information on Kernel Module Loading - create_module medium fail
Ensure auditd Collects Information on Kernel Module Loading and Unloading - modprobe medium fail
Ensure auditd Collects Information on Kernel Module Unloading - delete_module medium fail
Ensure auditd Collects Information on Kernel Module Loading - insmod medium fail
Ensure auditd Collects Information on Kernel Module Unloading - rmmod medium fail
Record Events that Modify the System's Network Environment medium pass
Record Attempts to Alter Process and Session Initiation Information medium pass
Record Events that Modify User/Group Information - /etc/group medium fail
Record Events that Modify the System's Mandatory Access Controls medium pass
System Audit Logs Must Be Owned By Root medium pass
Ensure auditd Collects System Administrator Actions medium pass

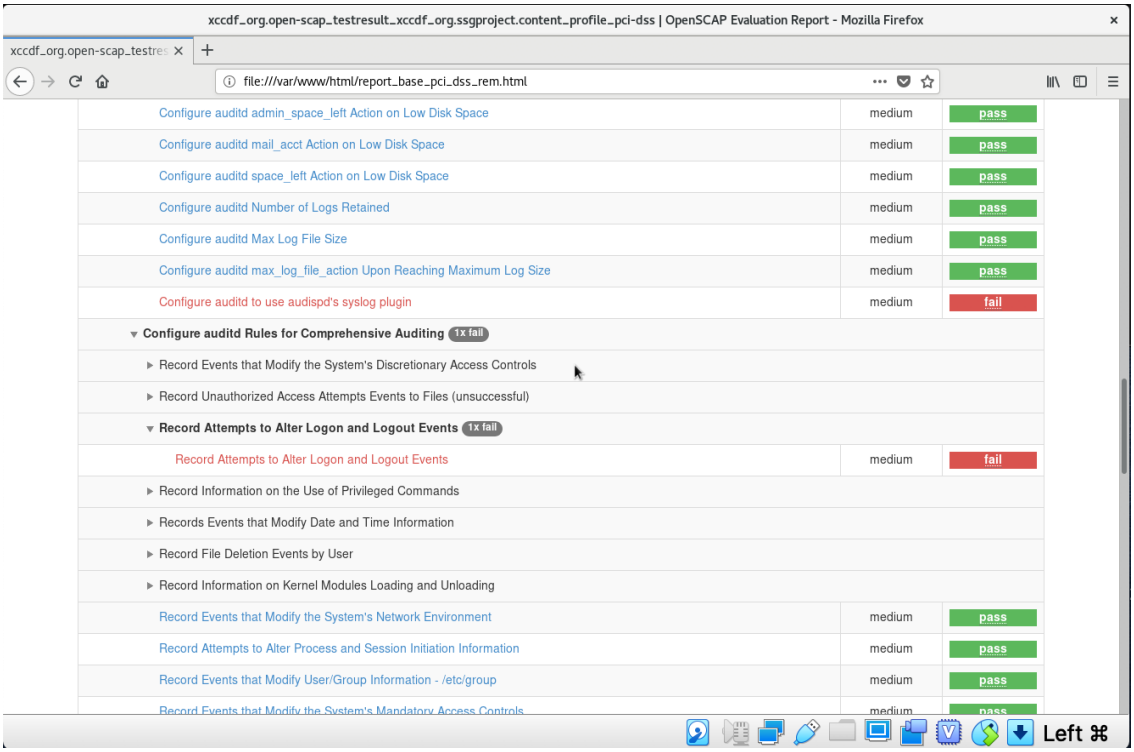


Remediation for PCI-DSS :



PCI-DSS scan report after remediation :

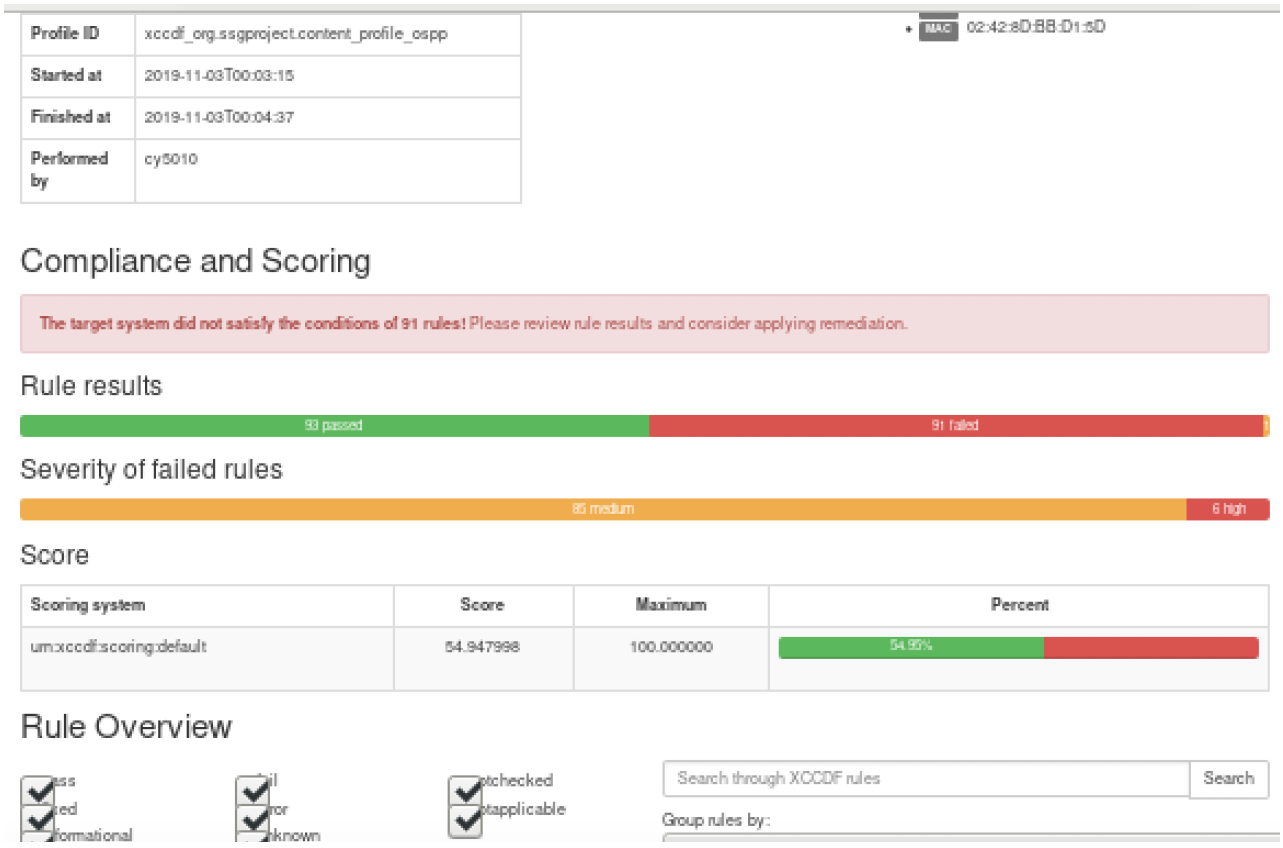




Scanning for OSPP :

```
[root@localhost ~]# oscap xccdf eval --profile xccdf_org.ssgproject.content_profile_ospp --results /var/www/html/result_base_ospp.xml
 --report /var/www/html/result_base_ospp.html /usr/share/xml/scap/ssg/content/ssg-fedora-ds.xml
Title   Disable SSH Support for User Known Hosts
Rule    xccdf_org.ssgproject.content_rule_sshd_disable_user_known_hosts
Result  fail

Title   Enable SSH Warning Banner
Rule    xccdf_org.ssgproject.content_rule_sshd_enable_warning_banner
Result  fail

Title   Disable SSH Access via Empty Passwords
Rule    xccdf_org.ssgproject.content_rule_sshd_disable_empty_passwords
Result  pass

Title   Disable SSH Support for .rhosts Files
Rule    xccdf_org.ssgproject.content_rule_sshd_disable_rhosts
Result  pass

Title   Disable Host-Based Authentication
Rule    xccdf_org.ssgproject.content_rule_disable_host_auth
Result  pass
```

OSPP scan report :



Profile ID	xccdf_org.ssgproject.content_profile_ospp
Started at	2019-11-03T00:03:15
Finished at	2019-11-03T00:04:37
Performed by	cy5010

MAC 02:42:8D:BB:D1:5D

Compliance and Scoring

The target system did not satisfy the conditions of 91 rules! Please review rule results and consider applying remediation.

Rule results

93 passed | 91 failed

Severity of failed rules

85 medium | 6 high

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	54.947998	100.000000	54.95%

Rule Overview

Search through XCCDF rules | Search

Group rules by:

Title	Severity	Result
Guide to the Secure Configuration of Fedora 91x fail 1x notchecked		
Services 4x fail		
SSH Server 3x fail		
Configure OpenSSH Server if Necessary 3x fail		
Disable SSH Support for User Known Hosts	medium	fail
Enable SSH Warning Banner	medium	fail
Disable SSH Access via Empty Passwords	high	pass
Disable SSH Support for .rhosts Files	medium	pass
Disable Host-Based Authentication	medium	pass
Disable GSSAPI Authentication	medium	fail
Disable SSH Root Login	medium	pass
Disable Kerberos Authentication	medium	pass
Mail Server Software		
Base Services 1x fail		
Uninstall Automatic Bug Reporting Tool (abrt)	medium	fail
System Security Services Daemon		
System Settings 87x fail 1x notchecked		
Set Boot Loader Password 1x fail		
Set Boot Loader Password in grub2	high	fail
Record Unsuccessul Permission Changes to Files - lremovexattr	medium	fail
Record Unauthorized Access Attempts to Files (unsuccessful) - openat	medium	pass
Record Unsuccessul Permission Changes to Files - setxattr	medium	fail
Ensure auditd Unauthorized Access Attempts To open_by_handle_at Are Ordered Correctly	medium	fail
Record Unsuccessul Permission Changes to Files - lsetxattr	medium	fail
Record Unsuccessul Permission Changes to Files - removexattr	medium	fail
Record Unauthorized Creation Attempts to Files - open_by_handle_at O_CREAT	medium	fail
Record Unauthorized Access Attempts to Files (unsuccessful) - truncate	medium	pass
Record Unauthorized Modification Attempts to Files - open_by_handle_at O_TRUNC	medium	fail
Record Unsuccessul Permission Changes to Files - chmod	medium	fail
Record Unauthorized Modification Attempts to Files - open O_TRUNC	medium	fail
Record Unsuccessul Ownership Changes to Files - chown	medium	fail
Record Unauthorized Access Attempts to Files (unsuccessful) - open	medium	pass
Record Unauthorized Access Attempts to Files (unsuccessful) - ftruncate	medium	pass
Ensure auditd Rules For Unauthorized Attempts To openat Are Ordered Correctly	medium	fail
Record Unsuccessul Delete Attempts to Files - unlinkat	medium	fail
Record Unsuccessul Ownership Changes to Files - fchownat	medium	fail
Record Unauthorized Access Attempts to Files (unsuccessful) - creat	medium	pass
Record Unauthorized Modification Attempts to Files - openat O_TRUNC	medium	fail

Record Any Attempts to Run restorecon	medium	fail
Record Any Attempts to Run semanage	medium	fail
▸ Record Information on Kernel Modules Loading and Unloading		
Record Events that Modify User/Group Information via open syscall - /etc/gshadow	medium	fail
Record Events that Modify User/Group Information via open syscall - /etc/shadow	medium	fail
Record Attempts to Alter Process and Session Initiation Information	medium	pass
Record Events that Modify User/Group Information via open syscall - /etc/passwd	medium	fail
Record Events that Modify User/Group Information - /etc/group	medium	pass
Record Events that Modify the System's Mandatory Access Controls	medium	pass
Record Events that Modify User/Group Information via open_by_handle_at syscall - /etc/shadow	medium	fail
Record Events that Modify User/Group Information via openat syscall - /etc/passwd	medium	fail
Record Events that Modify User/Group Information via openat syscall - /etc/group	medium	fail
Record Events that Modify User/Group Information via open_by_handle_at syscall - /etc/group	medium	fail
Ensure auditd Collects System Administrator Actions	medium	pass
Record Events that Modify User/Group Information via open syscall - /etc/group	medium	fail
Record Events that Modify User/Group Information - /etc/shadow	medium	pass
Record Events that Modify User/Group Information via open_by_handle_at syscall - /etc/passwd	medium	fail
Record Events that Modify User/Group Information via openat syscall - /etc/shadow	medium	fail
Record Events that Modify User/Group Information via open_by_handle_at syscall - /etc/gshadow	medium	fail

OSPP scan report after remediation :

Evaluation target	localhost.localdomain
Benchmark URL	/usr/share/xml/scap/ssg/content/ssg-fedora-ds.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_FEDORA
Profile ID	xccdf_org.ssgproject.content_profile_ospp
Started at	2019-11-03T00:26:27
Finished at	2019-11-03T00:27:50
Performed by	cy5010

CPE Platforms

- cpe:/o:fedoraproject:fedora:30
- cpe:/o:fedoraproject:fedora:29
- cpe:/o:fedoraproject:fedora:28
- cpe:/o:fedoraproject:fedora:27
- cpe:/o:fedoraproject:fedora:26
- cpe:/o:fedoraproject:fedora:25

Addresses

- IPv4 127.0.0.1
- IPv4 10.0.2.15
- IPv4 172.17.0.1
- IPv6 0:0:0:0:0:0:0:1
- IPv6 fe80:0:0:0:a7d9:d2a8:a806:3f52
- MAC 00:00:00:00:00:00
- MAC 08:00:27:B3:CB:99
- MAC 02:42:8D:BB:D1:5D

Compliance and Scoring

The target system did not satisfy the conditions of 20 rules! Please review rule results and consider applying remediation.

Rule results

164 passed | 20 failed

Severity of failed rules

15 medium | 5 high

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	87.994339	100.000000	87.99%

Rule Overview

Search through XCCDF rules | Search

Group rules by: Default

Title	Severity	Result
Guide to the Secure Configuration of Fedora 20x fail 1x notchecked		
▸ Services		
▾ System Settings 20x fail 1x notchecked		
▾ Set Boot Loader Password 1x fail		
Set Boot Loader Password in grub2	high	fail
Set the UEFI Boot Loader Password	medium	pass

Set the UEFI Boot Loader Password	medium	pass
▾ System Accounting with auditd 11x fail		
▾ Configure auditd Data Retention 1x fail		
Encrypt Audit Records Sent With audispd Plugin	medium	pass
Configure audispd Plugin To Send Logs To Remote Server	medium	pass
Configure auditd to use audispd's syslog plugin	medium	fail
▾ Configure auditd Rules for Comprehensive Auditing 10x fail		
▸ Record Events that Modify the System's Discretionary Access Controls		
▾ Record Unauthorized Access Attempts Events to Files (unsuccessful) 9x fail		
Record Unsuccessul Ownership Changes to Files - fchown	medium	pass
Record Unauthorized Creation Attempts to Files - open O_CREAT	medium	fail
Record Unsuccessul Delete Attempts to Files - rename	medium	pass
Record Unauthorized Creation Attempts to Files - openat O_CREAT	medium	fail
Record Unsuccessul Permission Changes to Files - fchmod	medium	pass
Record Unsuccessul Delete Attempts to Files - renameat	medium	pass
Record Unsuccessul Permission Changes to Files - fsetxattr	medium	pass
Record Unsuccessul Delete Attempts to Files - unlink	medium	pass
Record Unauthorized Access Attempts to Files (unsuccessful) - open_by_handle_at	medium	pass
Record Unsuccessul Permission Changes to Files - lremovexattr	medium	pass
Record Unauthorized Access Attempts to Files (unsuccessful) - openat	medium	pass
Record Unsuccessul Permission Changes to Files - setxattr	medium	pass
Ensure auditd Unauthorized Access Attempts To open_by_handle_at Are Ordered Correctly	medium	fail
Record Unsuccessul Permission Changes to Files - lsetxattr	medium	pass
Record Unsuccessul Permission Changes to Files - removexattr	medium	pass
Record Unauthorized Creation Attempts to Files - open_by_handle_at O_CREAT	medium	fail
Record Unauthorized Access Attempts to Files (unsuccessful) - truncate	medium	pass
Record Unauthorized Modification Attempts to Files - open_by_handle_at O_TRUNC	medium	fail
Record Unsuccessul Permission Changes to Files - chmod	medium	pass
Record Unauthorized Modification Attempts to Files - open O_TRUNC	medium	fail
Record Unsuccessul Ownership Changes to Files - chown	medium	pass
Record Unauthorized Access Attempts to Files (unsuccessful) - open	medium	pass
Record Unauthorized Access Attempts to Files (unsuccessful) - ftruncate	medium	pass
Ensure auditd Rules For Unauthorized Attempts To openat Are Ordered Correctly	medium	fail

Record Unsuccessul Delete Attempts to Files - unlinkat	medium	pass
Record Unsuccessul Ownership Changes to Files - fchownat	medium	pass
Record Unauthorized Access Attempts to Files (unsuccessful) - creat	medium	pass
Record Unauthorized Modification Attempts to Files - openat O_TRUNC	medium	fail
Ensure auditd Rules For Unauthorized Attempts To open Are Ordered Correctly	medium	fail
Record Unsuccessul Ownership Changes to Files - lchown	medium	pass
Record Unsuccessul Permission Changes to Files - fchmodat	medium	pass
Record Unsuccessul Permission Changes to Files - fremovexattr	medium	pass
▾ **Record Attempts to Alter Logon and Logout Events** 1x fail		
Record Attempts to Alter Logon and Logout Events - lastlog	medium	pass
Record Attempts to Alter Logon and Logout Events - tallylog	medium	pass
Record Attempts to Alter Logon and Logout Events - faillock	medium	fail
▸ Record Information on the Use of Privileged Commands		
▸ Record File Deletion Events by User		
▸ Record Execution Attempts to Run SELinux Privileged Commands		
▸ Record Information on Kernel Modules Loading and Unloading		
Record Events that Modify User\Group Information via open syscall - /etc/gshadow	medium	pass
Record Events that Modify User\Group Information via open syscall - /etc/shadow	medium	pass
Record Attempts to Alter Process and Session Initiation Information	medium	pass
Record Events that Modify User\Group Information via open syscall - /etc/passwd	medium	pass
Record Events that Modify User\Group Information - /etc/group	medium	pass
Record Events that Modify the System's Mandatory Access Controls	medium	pass
Record Events that Modify User\Group Information via open_by_handle_at syscall - /etc/shadow	medium	pass
Record Events that Modify User\Group Information via openat syscall - /etc/passwd	medium	pass
Record Events that Modify User\Group Information via openat syscall - /etc/group	medium	pass
Record Events that Modify User\Group Information via open_by_handle_at syscall - /etc/group	medium	pass
Ensure auditd Collects System Administrator Actions	medium	pass
Record Events that Modify User\Group Information via open syscall - /etc/group	medium	pass
Record Events that Modify User\Group Information - /etc/shadow	medium	pass
Record Events that Modify User\Group Information via open_by_handle_at syscall - /etc/passwd	medium	pass
Record Events that Modify User\Group Information via openat syscall - /etc/shadow	medium	pass
Record Events that Modify User\Group Information via open_by_handle_at syscall - /etc/gshadow	medium	pass
Record Events that Modify User\Group Information via openat syscall - /etc/gshadow	medium	pass

Configure SELinux Policy	high	pass
Ensure No Daemons are Unconfined by SELinux	medium	pass
Ensure SELinux State is Enforcing	high	pass
▸ Account and Access Control		
▾ **Installing and Maintaining Software** 4x fail 1x notchecked		
▾ **System and Software Integrity** 4x fail 1x notchecked		
▾ **System Cryptographic Policies** 1x fail 1x notchecked		
Configure OpenSSL library to use System Crypto Policy	medium	pass
Configure Libreswan to use System Crypto Policy	medium	pass
Configure SSH to use System Crypto Policy	medium	pass
Configure Kerberos to use System Crypto Policy	medium	pass
Configure System Cryptography Policy	high	fail
Configure BIND to use System Crypto Policy	medium	notchecked
▾ **Software Integrity Checking** 1x fail		
▾ **Verify Integrity with RPM** 1x fail		
Verify File Hashes with RPM	high	fail
▾ **Federal Information Processing Standard (FIPS)** 1x fail		
Enable FIPS Mode	high	fail
▾ **Operating System Vendor Support and Certification** 1x fail		
The Installed Operating System Is Vendor Supported	high	fail
▸ Updating Software		
▸ GNOME Desktop Environment		
▾ **File Permissions and Masks** 2x fail		
▾ **Restrict Partition Mount Options** 2x fail		
Add noexec Option to /dev/shm	medium	pass
Add nosuid Option to /dev/shm	medium	fail
Add nodev Option to /dev/shm	medium	fail
▸ Restrict Programs from Dangerous Execution Patterns		
▾ **Network Configuration and Firewalls** 1x fail		
▾ **firewalld** 1x fail		
▸ Inspect and Activate Default firewalld Rules		
▾ **Strengthen the Default Ruleset** 1x fail		
Set Default firewalld Zone for Incoming Packets	medium	fail

Part 3 - Docker Container Preparation and Scanning Fedora Docker Container :

Scanning Fedora Docker Container :

After running the xccdf scan on Fedora container, we found four vulnerabilities, AIDE and Libreswan were not installed, Build and Test AIDE Database test failed and Verification of file permission with RPM failed.

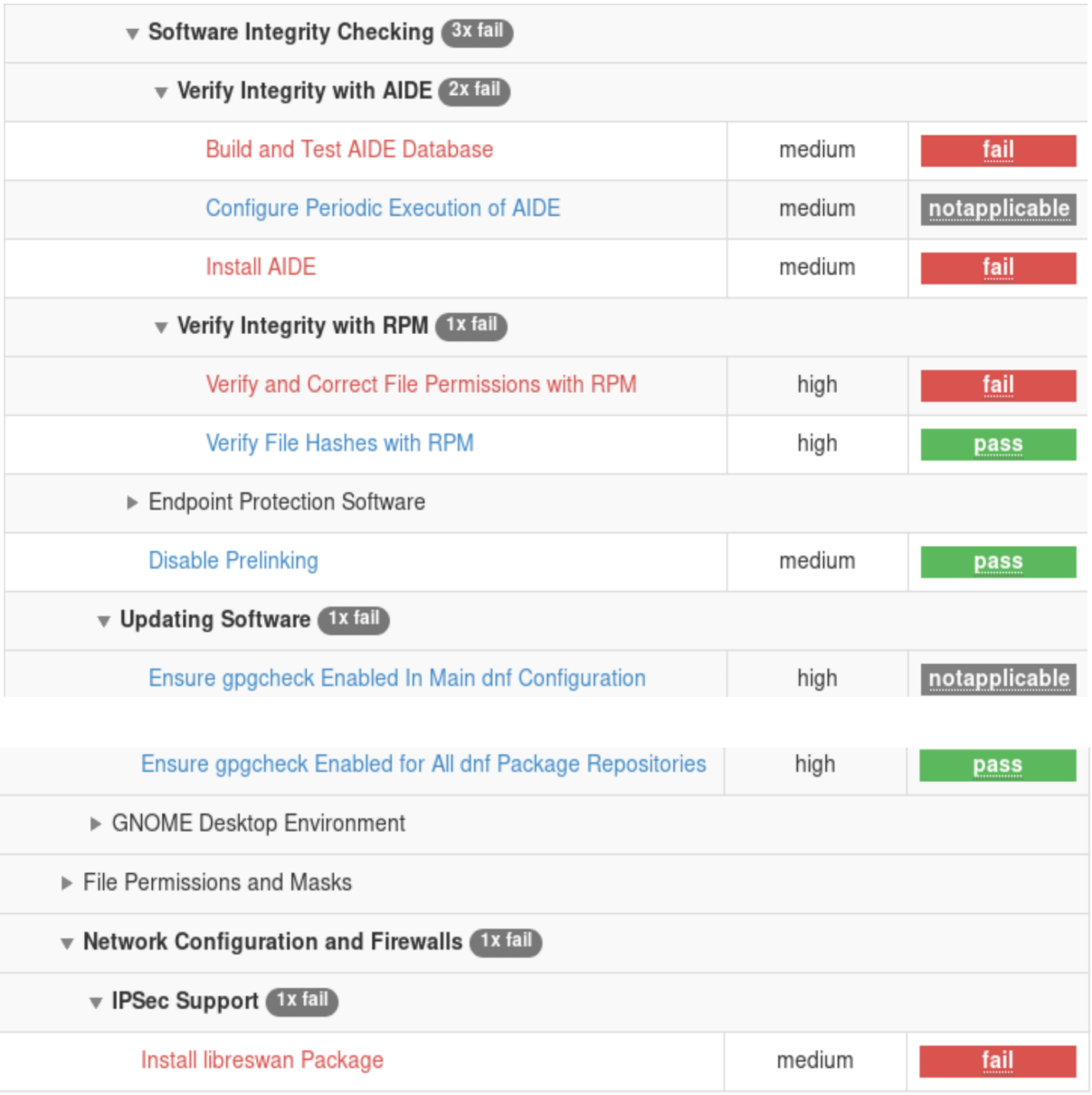
Benchmark URL	/usr/share/xml/scap/ssg/content/ssg-fedora-xccdf.xml
Profile ID	pci-dss
Started at	2019-11-03T01:01:04
Finished at	2019-11-03T01:01:12
Performed by	cy5010

CPE Platforms

- cpe:/o:fedoraproject:fedora:26
- cpe:/o:fedoraproject:fedora:30
- cpe:/o:fedoraproject:fedora:29
- cpe:/o:fedoraproject:fedora:28
- cpe:/o:fedoraproject:fedora:27
- cpe:/o:fedoraproject:fedora:25

Addresses

- IPv4 127.0.0.1
- IPv4 10.0.2.15

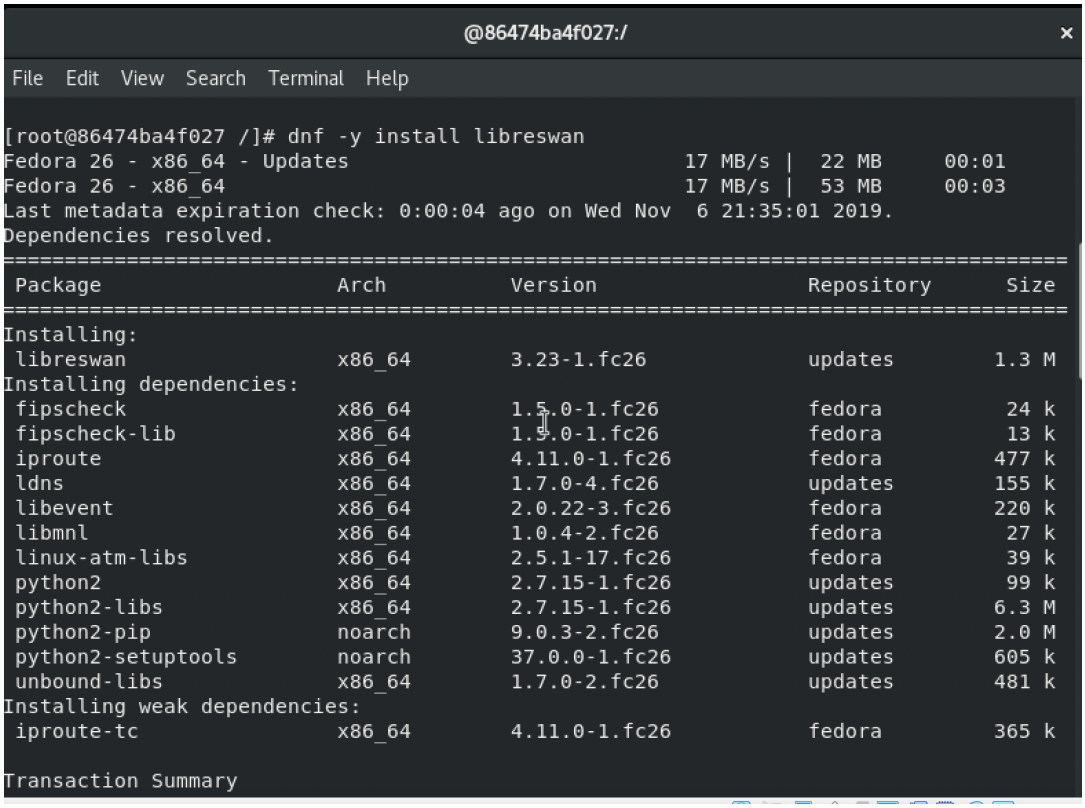


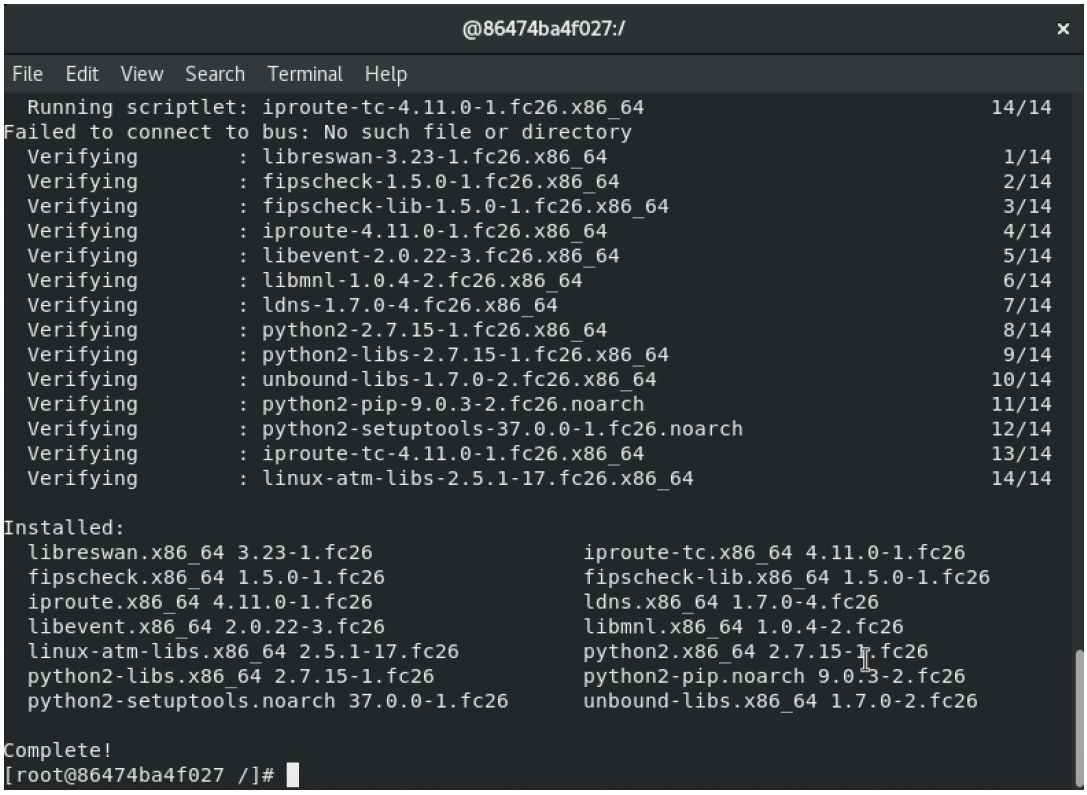
We chose to remediate two vulnerabilities, installing Libreswan and AIDE.

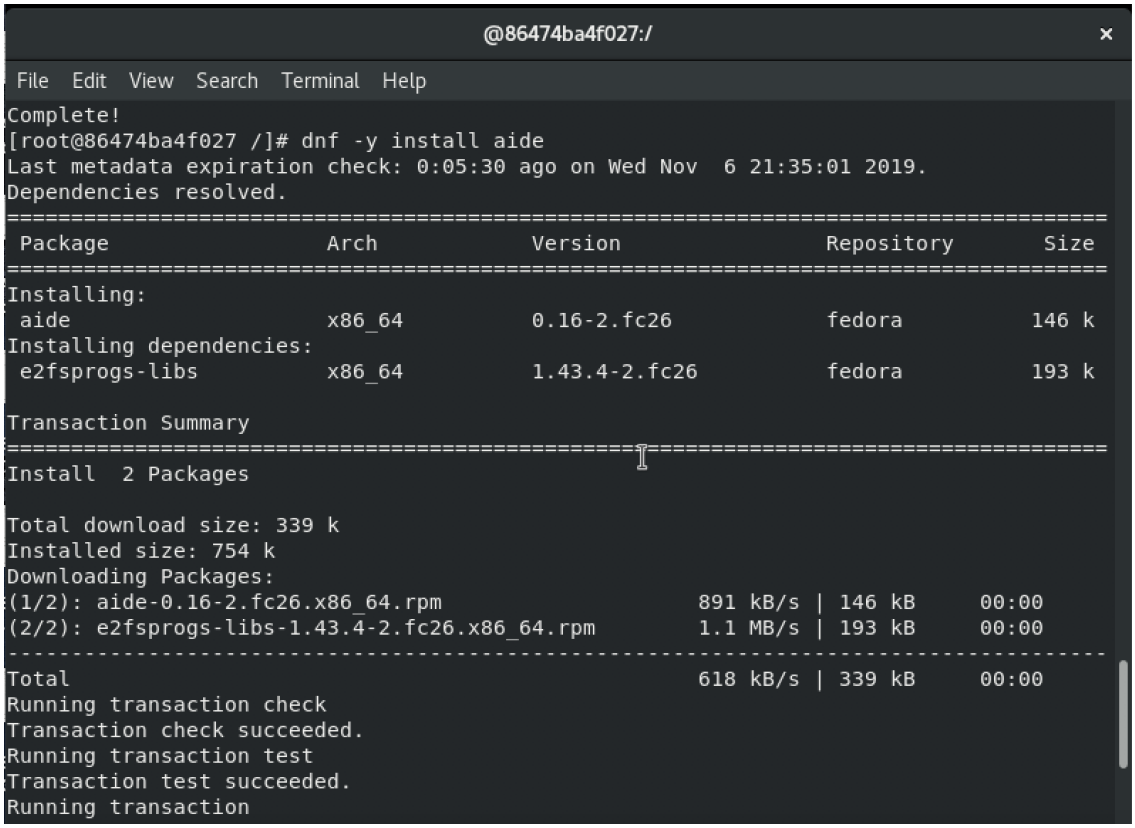
We executed the bash in the container and ran the commands:

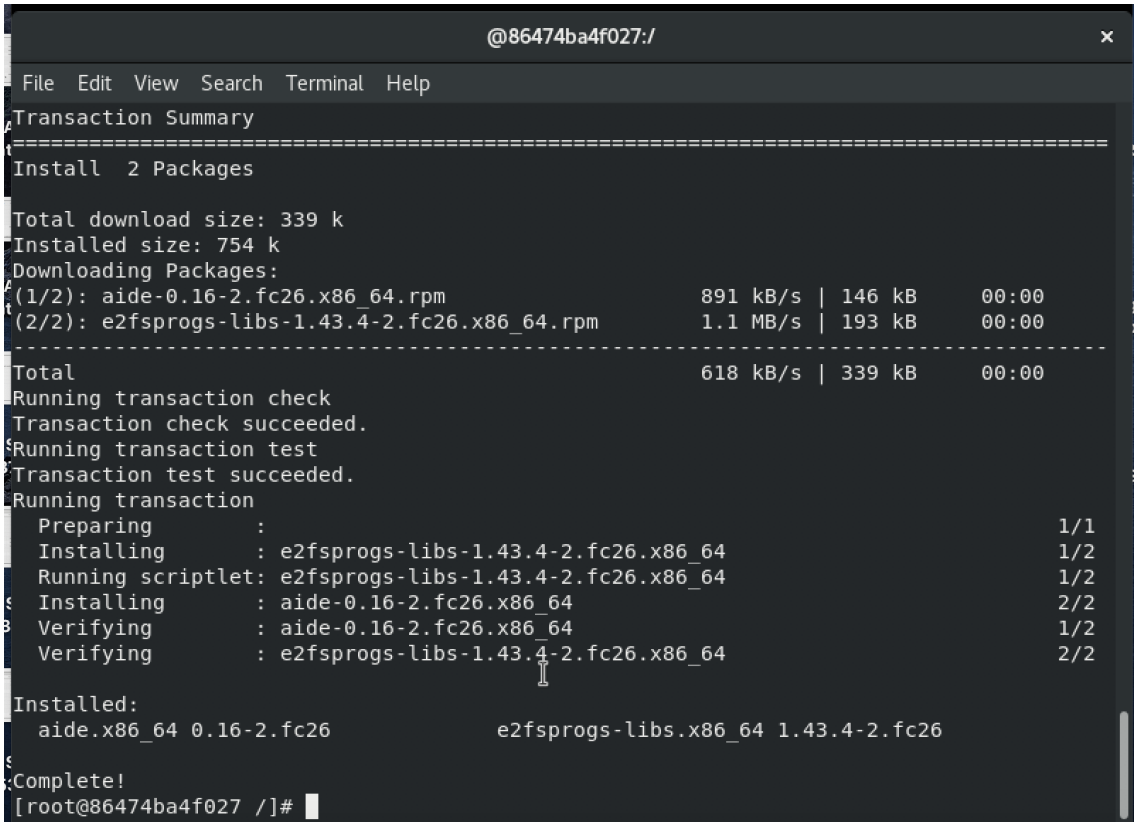
dnf -y install aide
dnf -y install libreswan

to install AIDE and Libreswan on Fedora container and remediated the vulnerabilities.


@86474ba4f027:/
File Edit View Search Terminal Help
[root@86474ba4f027 /]# dnf -y install libreswan
Fedora 26 - x86_64 - Updates 17 MB/s | 22 MB 00:01
Fedora 26 - x86_64 17 MB/s | 53 MB 00:03
Last metadata expiration check: 0:00:04 ago on Wed Nov 6 21:35:01 2019.
Dependencies resolved.
Package Arch Version Repository Size
Installing:
libreswan x86_64 3.23-1.fc26 updates 1.3 M
Installing dependencies:
fipscheck x86_64 1.5.0-1.fc26 fedora 24 k
fipscheck-lib x86_64 1.5.0-1.fc26 fedora 13 k
iproute x86_64 4.11.0-1.fc26 fedora 477 k
ldns x86_64 1.7.0-4.fc26 updates 155 k
libevent x86_64 2.0.22-3.fc26 fedora 220 k
libmnl x86_64 1.0.4-2.fc26 fedora 27 k
linux-atm-libs x86_64 2.5.1-17.fc26 fedora 39 k
python2 x86_64 2.7.15-1.fc26 updates 99 k
python2-libs x86_64 2.7.15-1.fc26 updates 6.3 M
python2-pip noarch 9.0.3-2.fc26 updates 2.0 M
python2-setuptools noarch 37.0.0-1.fc26 updates 605 k
unbound-libs x86_64 1.7.0-2.fc26 updates 481 k
Installing weak dependencies:
iproute-tc x86_64 4.11.0-1.fc26 fedora 365 k
Transaction Summary


@86474ba4f027:/
File Edit View Search Terminal Help
Running scriptlet: iproute-tc-4.11.0-1.fc26.x86_64 14/14
Failed to connect to bus: No such file or directory
Verifying : libreswan-3.23-1.fc26.x86_64 1/14
Verifying : fipscheck-1.5.0-1.fc26.x86_64 2/14
Verifying : fipscheck-lib-1.5.0-1.fc26.x86_64 3/14
Verifying : iproute-4.11.0-1.fc26.x86_64 4/14
Verifying : libevent-2.0.22-3.fc26.x86_64 5/14
Verifying : libmnl-1.0.4-2.fc26.x86_64 6/14
Verifying : ldns-1.7.0-4.fc26.x86_64 7/14
Verifying : python2-2.7.15-1.fc26.x86_64 8/14
Verifying : python2-libs-2.7.15-1.fc26.x86_64 9/14
Verifying : unbound-libs-1.7.0-2.fc26.x86_64 10/14
Verifying : python2-pip-9.0.3-2.fc26.noarch 11/14
Verifying : python2-setuptools-37.0.0-1.fc26.noarch 12/14
Verifying : iproute-tc-4.11.0-1.fc26.x86_64 13/14
Verifying : linux-atm-libs-2.5.1-17.fc26.x86_64 14/14
Installed:
libreswan.x86_64 3.23-1.fc26
iproute-tc.x86_64 4.11.0-1.fc26
fipscheck.x86_64 1.5.0-1.fc26
fipscheck-lib.x86_64 1.5.0-1.fc26
iproute.x86_64 4.11.0-1.fc26
ldns.x86_64 1.7.0-4.fc26
libevent.x86_64 2.0.22-3.fc26
libmnl.x86_64 1.0.4-2.fc26
linux-atm-libs.x86_64 2.5.1-17.fc26
python2.x86_64 2.7.15-1.fc26
python2-libs.x86_64 2.7.15-1.fc26
python2-pip.noarch 9.0.3-2.fc26
python2-setuptools.noarch 37.0.0-1.fc26
unbound-libs.x86_64 1.7.0-2.fc26
Complete!
[root@86474ba4f027 /]#


@86474ba4f027:/
File Edit View Search Terminal Help
Complete!
[root@86474ba4f027 /]# dnf -y install aide
Last metadata expiration check: 0:05:30 ago on Wed Nov 6 21:35:01 2019.
Dependencies resolved.
Package Arch Version Repository Size
Installing:
aide x86_64 0.16-2.fc26 fedora 146 k
Installing dependencies:
e2fsprogs-libs x86_64 1.43.4-2.fc26 fedora 193 k
Transaction Summary
Install 2 Packages
Total download size: 339 k
Installed size: 754 k
Downloading Packages:
(1/2): aide-0.16-2.fc26.x86_64.rpm 891 kB/s | 146 kB 00:00
(2/2): e2fsprogs-libs-1.43.4-2.fc26.x86_64.rpm 1.1 MB/s | 193 kB 00:00
Total 618 kB/s | 339 kB 00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction


@86474ba4f027:/
File Edit View Search Terminal Help
Transaction Summary
Install 2 Packages
Total download size: 339 k
Installed size: 754 k
Downloading Packages:
(1/2): aide-0.16-2.fc26.x86_64.rpm 891 kB/s | 146 kB 00:00
(2/2): e2fsprogs-libs-1.43.4-2.fc26.x86_64.rpm 1.1 MB/s | 193 kB 00:00
Total 618 kB/s | 339 kB 00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing : 1/1
Installing : e2fsprogs-libs-1.43.4-2.fc26.x86_64 1/2
Running scriptlet: e2fsprogs-libs-1.43.4-2.fc26.x86_64 1/2
Installing : aide-0.16-2.fc26.x86_64 2/2
Verifying : aide-0.16-2.fc26.x86_64 1/2
Verifying : e2fsprogs-libs-1.43.4-2.fc26.x86_64 2/2
Installed:
aide.x86_64 0.16-2.fc26 e2fsprogs-libs.x86_64 1.43.4-2.fc26
Complete!
[root@86474ba4f027 /]#

Scanning Fedora Docker Container After Remediation :

Evaluation target	localhost.localdomain
Benchmark URL	/usr/share/xml/scap/ssg/content/ssg-fedora-xccdf.xml
Profile ID	pci-dss
Started at	2019-11-03T01:26:23
Finished at	2019-11-03T01:26:34
Performed by	cy5010

CPE Platforms

- cpe:/o:fedoraproject:fedora:26
- cpe:/o:fedoraproject:fedora:30
- cpe:/o:fedoraproject:fedora:29
- cpe:/o:fedoraproject:fedora:28
- cpe:/o:fedoraproject:fedora:27
- cpe:/o:fedoraproject:fedora:25

- MAC DE:1E:AC:0F:9F:F0

Compliance and Scoring

The target system did not satisfy the conditions of 3 rules! Please review rule results and consider applying remediation.

Rule results

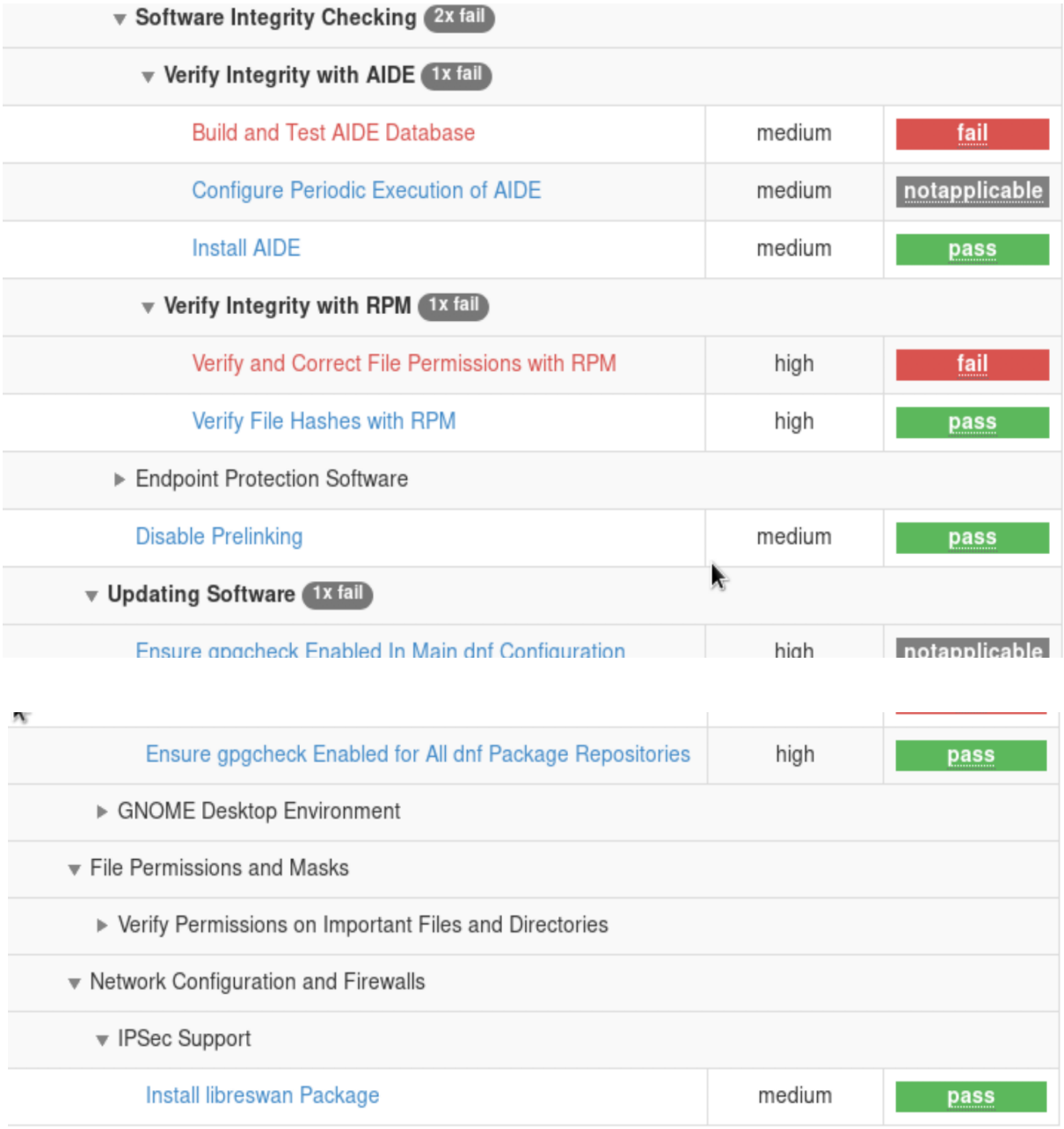
17 passed | 3 failed | 1

Severity of failed rules

1 medium | 2 high

Score

Scoring system	Score	Maximum	Percent



▼ Software Integrity Checking 2x fail		
▼ Verify Integrity with AIDE 1x fail		
Build and Test AIDE Database	medium	fail
Configure Periodic Execution of AIDE	medium	notapplicable
Install AIDE	medium	pass
▼ Verify Integrity with RPM 1x fail		
Verify and Correct File Permissions with RPM	high	fail
Verify File Hashes with RPM	high	pass
▶ Endpoint Protection Software		
Disable Prelinking	medium	pass
▼ Updating Software 1x fail		
Ensure gpgcheck Enabled In Main dnf Configuration	high	notapplicable
Ensure gpgcheck Enabled for All dnf Package Repositories	high	pass
▶ GNOME Desktop Environment		
▼ File Permissions and Masks		
▶ Verify Permissions on Important Files and Directories		
▼ Network Configuration and Firewalls		
▼ IPSec Support		
Install libreswan Package	medium	pass

Scanning CentOS Docker Container :

After running the xccdf scan on CentOS container, we found four vulnerabilities, AIDE and Libreswan were not installed, Build and Test AIDE Database test failed and Verification of file permission with RPM failed.

Evaluation Characteristics

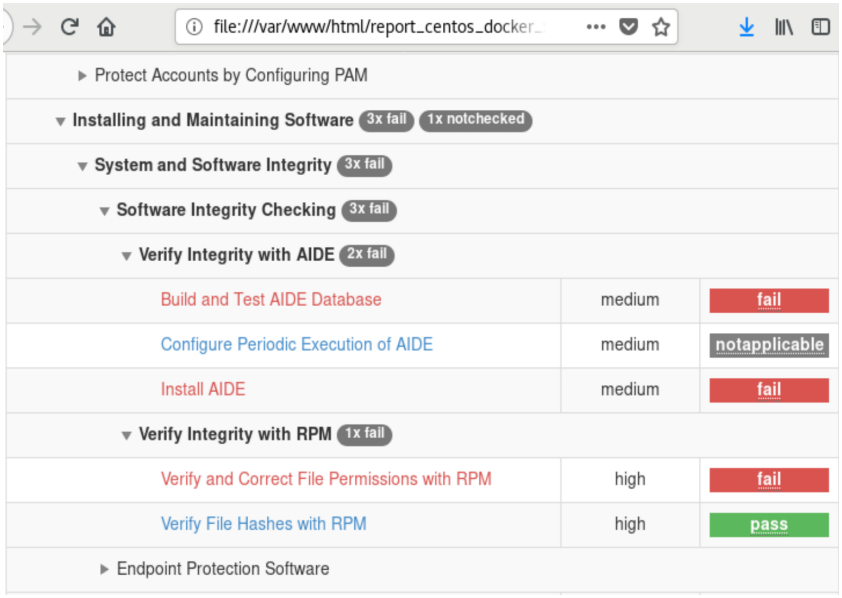
Evaluation target	localhost.localdomain
Benchmark URL	/usr/share/xml/scap/ssg/content/ssg-centos7-xccdf.xml
Profile ID	pci-dss
Started at	2019-11-03T01:35:14
Finished at	2019-11-03T01:35:21
Performed by	cy5010

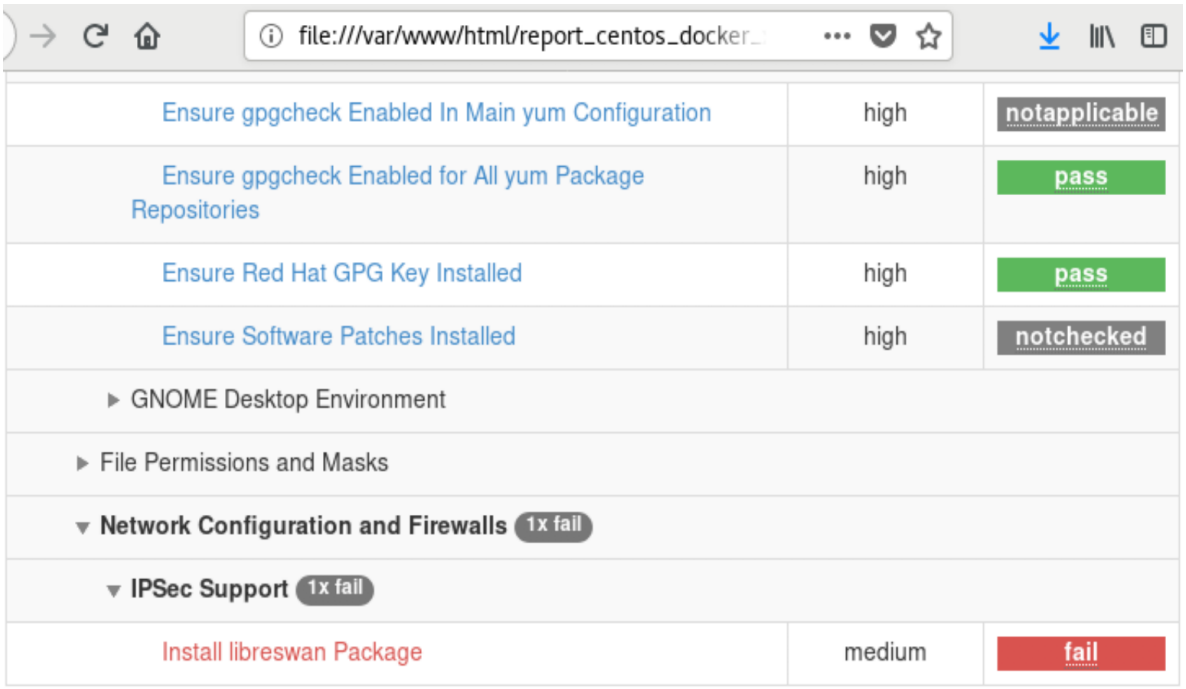
CPE Platforms

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

Addresses

We chose to remediate two vulnerabilities, installing Libreswan and AIDE.





We executed the bash in the container and ran the commands:

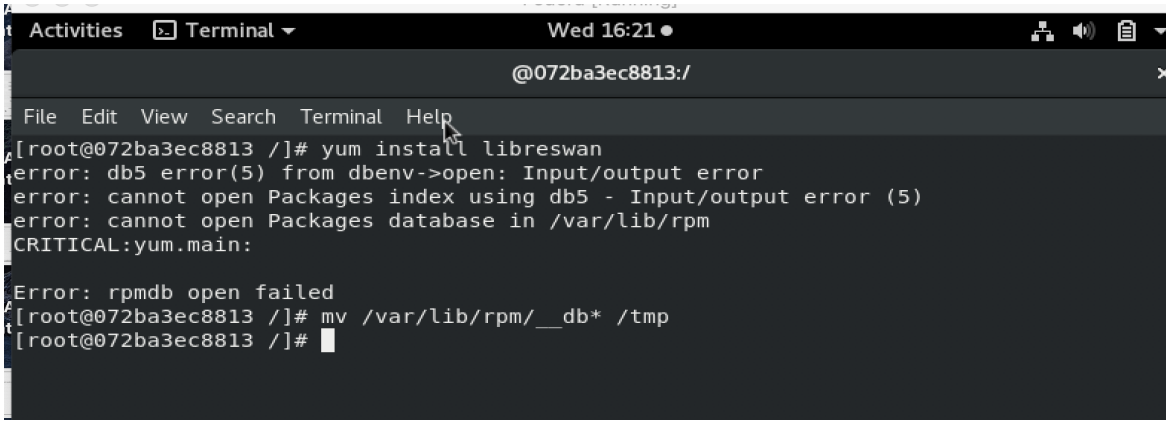
yum install aide
yum install libreswan

to install AIDE and Libreswan on CentOS container and remediated the vulnerabilities.

But the commands gave error: “rpmdb open failed” indicating broken yum. To fix yum, we moved the rpm db to another temporary location (for backup) and then ran the commands:

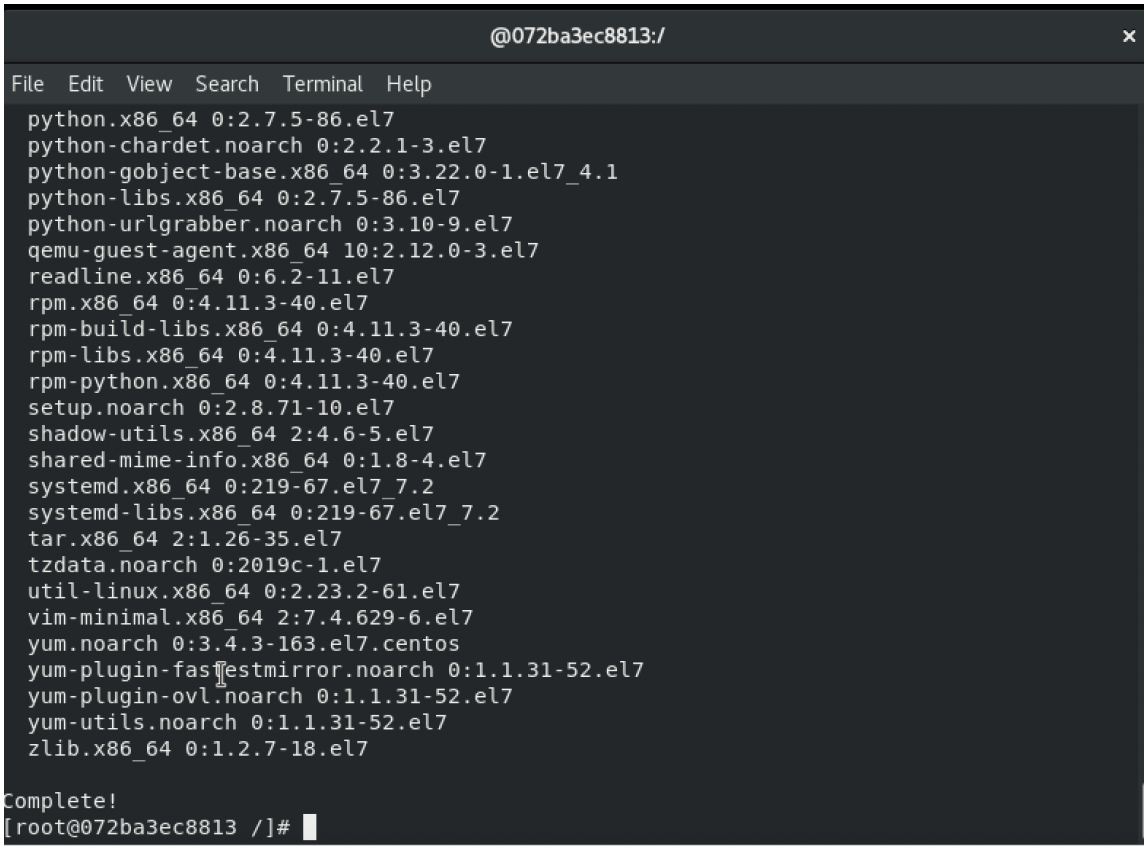
yum clean all
yum update

These commands fixed yum repos and allowed the usage of yum to install AIDE and Libreswan.



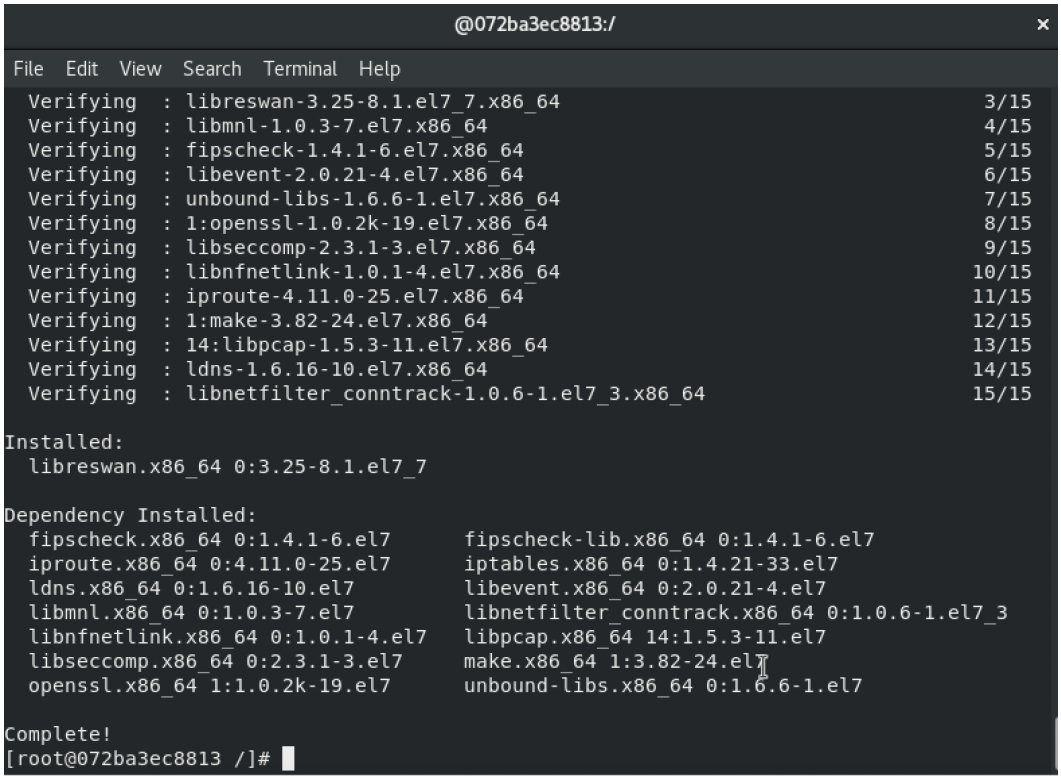
```
CRITICAL:yum.main:

Error: rpmdb open failed
[root@072ba3ec8813 /]# mv /var/lib/rpm/__db* /tmp
[root@072ba3ec8813 /]# yum clean all
Loaded plugins: fastestmirror, ovl
Cleaning repos: base extras updates
Cleaning up everything
Maybe you want: rm -rf /var/cache/yum, to also free up space taken by orphaned data fr
om disabled or removed repos
[root@072ba3ec8813 /]#
```

```
Maybe you want: rm -rf /var/cache/yum, to also free up space taken by orphaned data fr
om disabled or removed repos
[root@072ba3ec8813 /]# yum update
Loaded plugins: fastestmirror, ovl
base                                                     | 3.6 kB  00:00:00
extras                                                   | 2.9 kB  00:00:00
updates                                                  | 2.9 kB  00:00:00
(1/4): base/7/x86_64/group_gz                            | 165 kB  00:00:00
(2/4): extras/7/x86_64/primary_db                        | 153 kB  00:00:00
(3/4): updates/7/x86_64/primary_db                       | 2.8 MB  00:00:00
(4/4): base/7/x86_64/primary_db                          | 6.0 MB  00:01:32
Determining fastest mirrors
 * base: mirrors.tripadvisor.com
 * extras: mirrors.tripadvisor.com
 * updates: mirror.metrocast.net
Resolving Dependencies
--> Running transaction check
---> Package acl.x86_64 0:2.2.51-12.el7 will be updated
---> Package acl.x86_64 0:2.2.51-14.el7 will be an update
---> Package audit-libs.x86_64 0:2.7.6-3.el7 will be updated
---> Package audit-libs.x86_64 0:2.8.5-4.el7 will be an update
---> Package bash.x86_64 0:4.2.46-29.el7_4 will be updated
---> Package bash.x86_64 0:4.2.46-33.el7 will be an update
---> Package bind-license.noarch 32:9.9.4-51.el7 will be updated
---> Package bind-license.noarch 32:9.11.4-9.P2.el7 will be an update
---> Package binutils.x86_64 0:2.25.1-32.base.el7_4.1 will be updated
---> Package binutils.x86_64 0:2.27-41.base.el7_7.1 will be an update
```

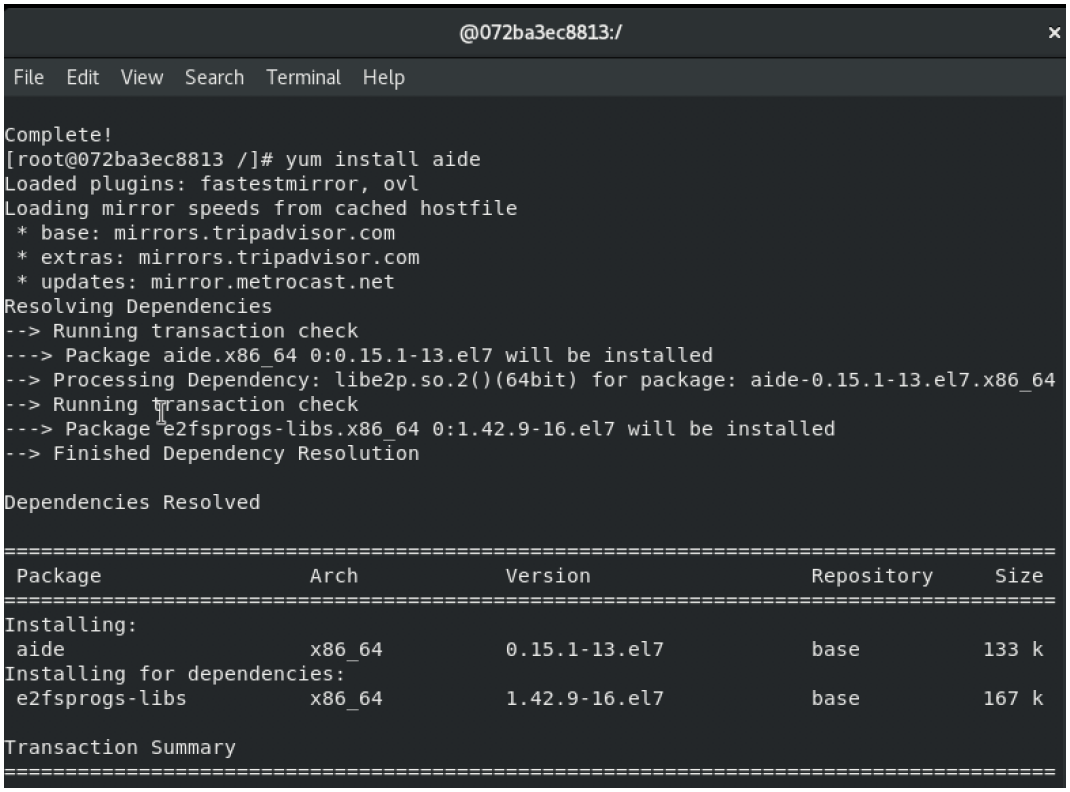


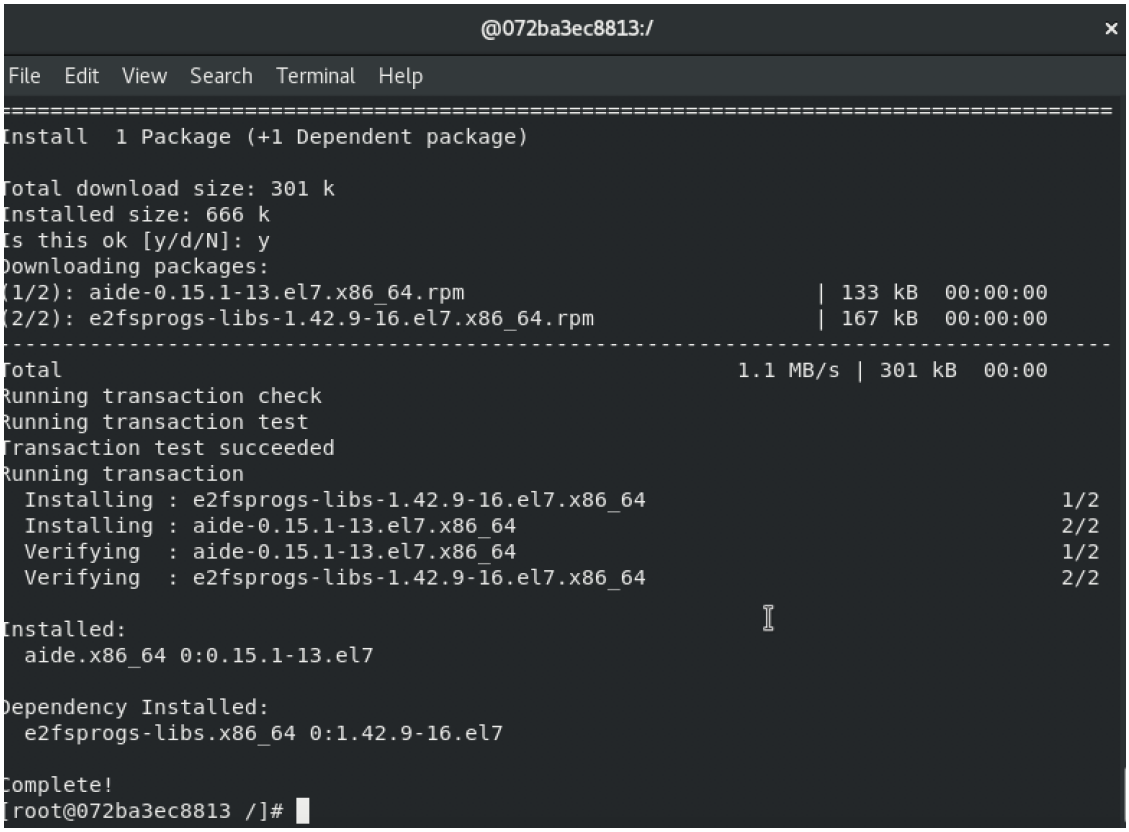
After fixing yum, we tried to install Libreswan again:

```
Complete!
[root@072ba3ec8813 /]# yum install libreswan
Loaded plugins: fastestmirror, ovl
Loading mirror speeds from cached hostfile
 * base: mirrors.tripadvisor.com
 * extras: mirrors.tripadvisor.com
 * updates: mirror.metrocast.net
Resolving Dependencies
--> Running transaction check
---> Package libreswan.x86_64 0:3.25-8.1.el7_7 will be installed
--> Processing Dependency: unbound-libs >= 1.6.6 for package: libreswan-3.25-8.1.el7_7
.x86_64
--> Processing Dependency: iproute >= 2.6.8 for package: libreswan-3.25-8.1.el7_7.x86_
64
--> Processing Dependency: fipscheck(x86-64) for package: libreswan-3.25-8.1.el7_7.x86
_64
--> Processing Dependency: libunbound.so.2()(64bit) for package: libreswan-3.25-8.1.el
7_7.x86_64
--> Processing Dependency: libseccomp.so.2()(64bit) for package: libreswan-3.25-8.1.el
7_7.x86_64
--> Processing Dependency: libldns.so.1()(64bit) for package: libreswan-3.25-8.1.el7_7
.x86_64
--> Processing Dependency: libfipscheck.so.1()(64bit) for package: libreswan-3.25-8.1.
el7_7.x86_64
--> Processing Dependency: libevent_pthreads-2.0.so.5()(64bit) for package: libreswan-
3.25-8.1.el7_7.x86_64
--> Processing Dependency: libevent-2.0.so.5()(64bit) for package: libreswan-3.25-8.1.
```

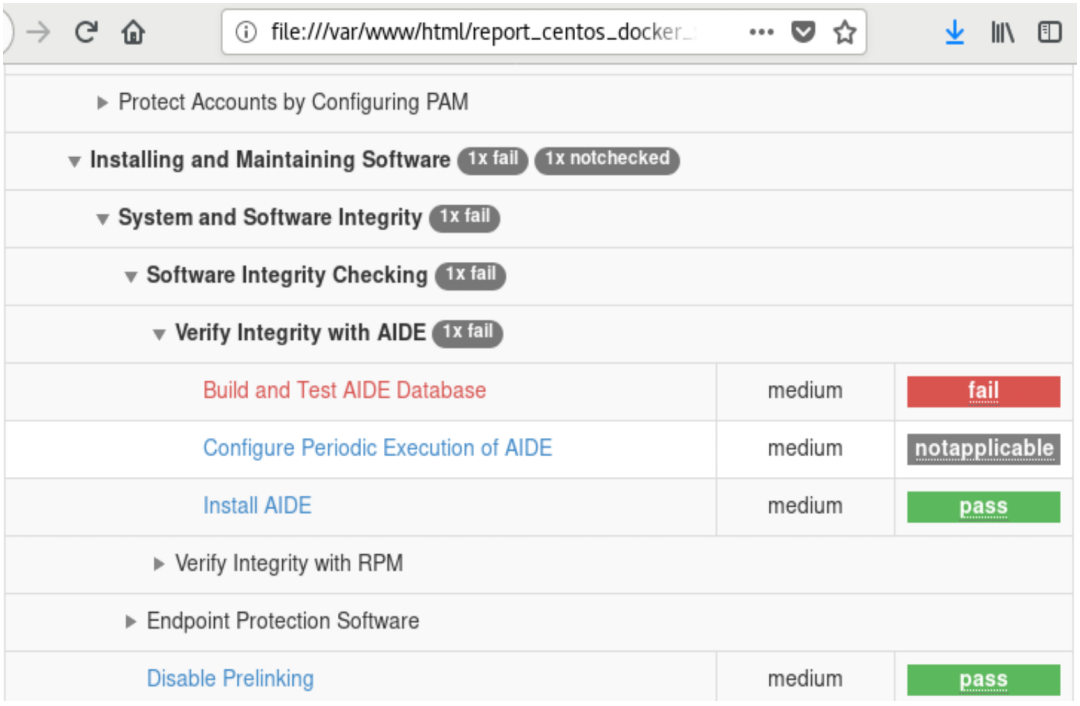


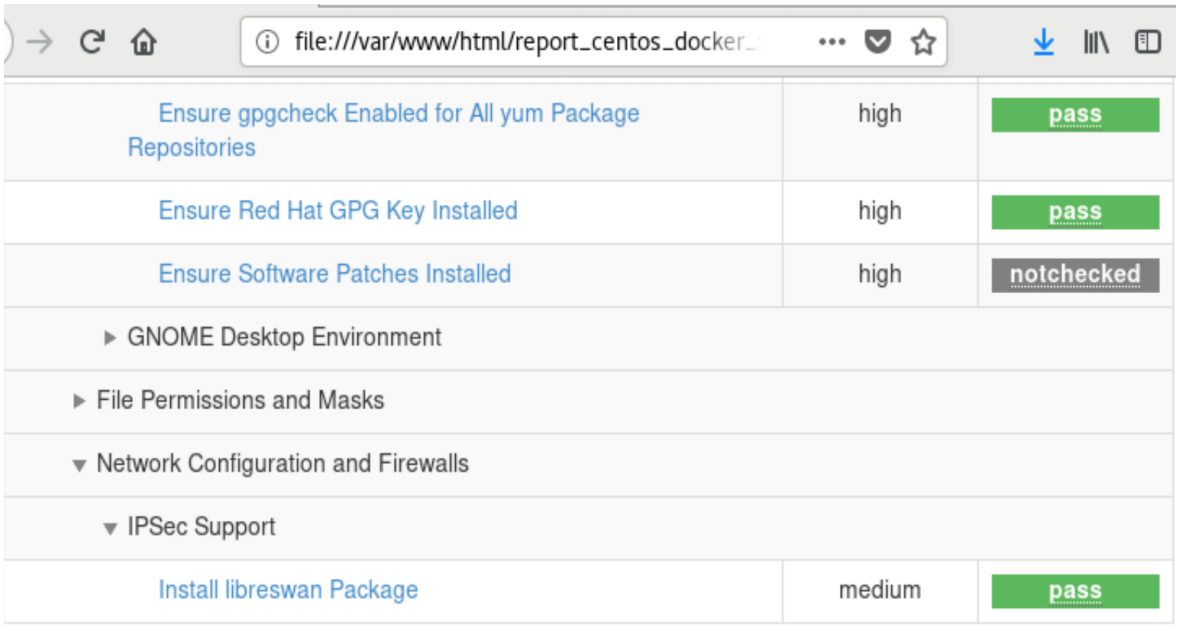
After successfully installing Libreswan in CentOS container, we installed AIDE:





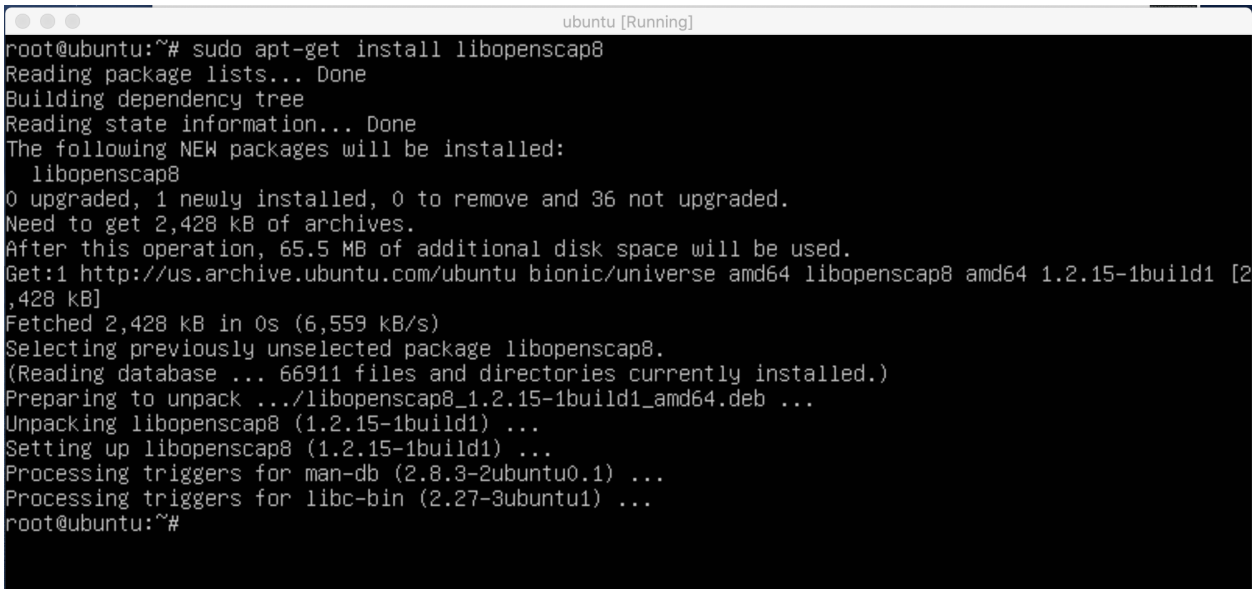
Scanning CentOS Docker Container After Remediation :



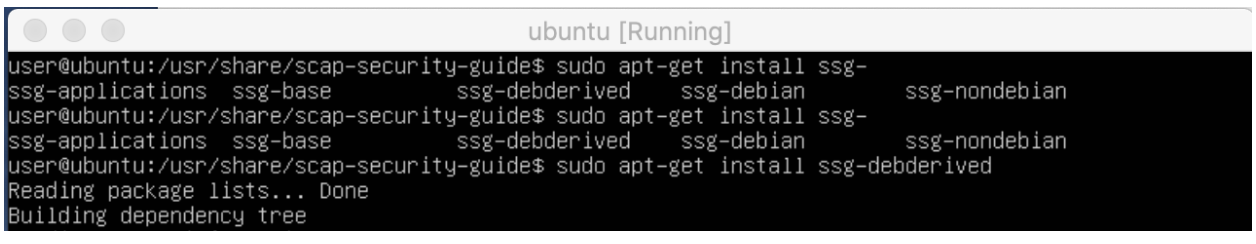


Extra Credit :

First we install open scap on ubuntu VM :



Additionally we also installed openscap-security-guide by using `apt install ssg-debderived`

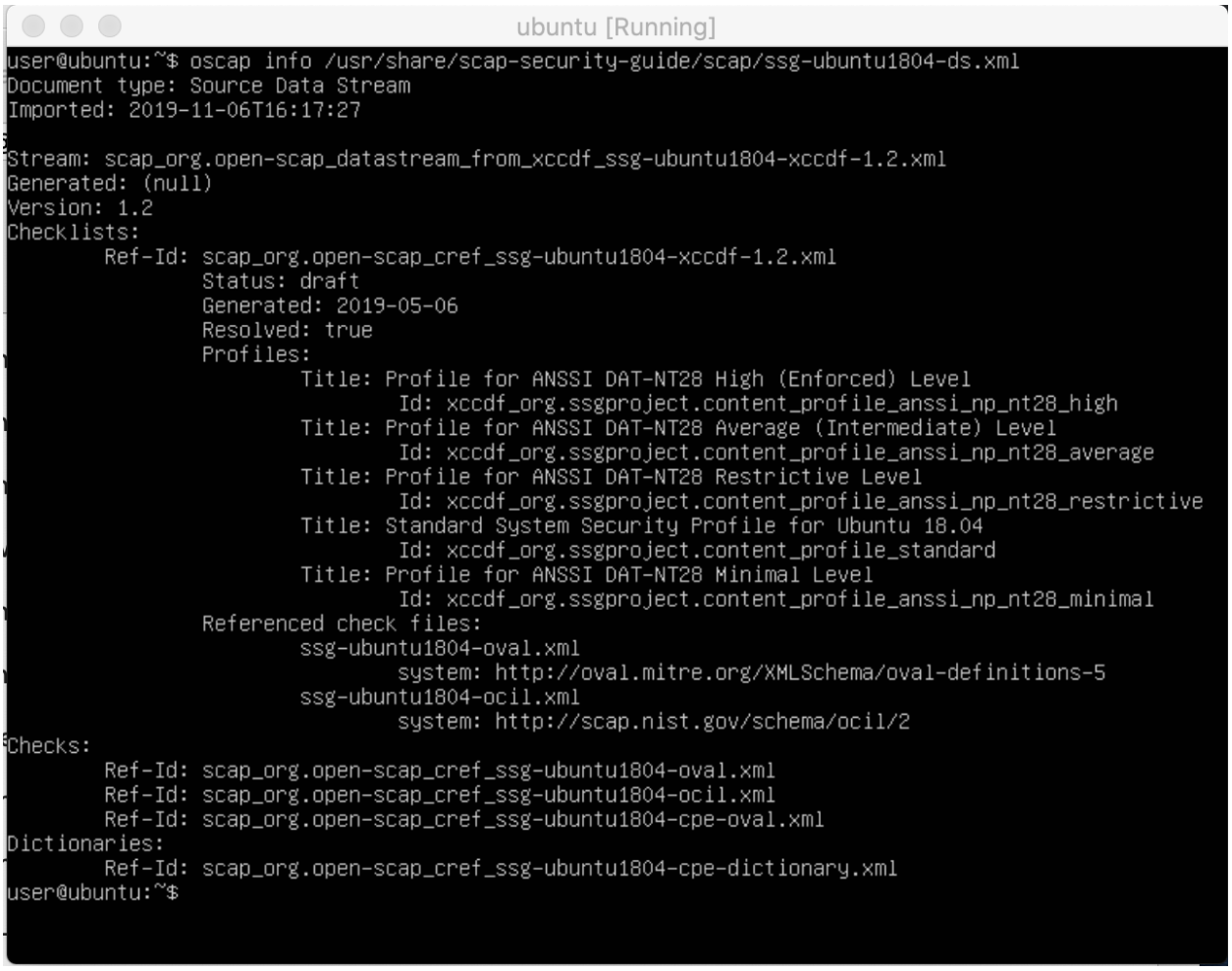


Now we find the profiles available with ubuntu 18 xccdf file :

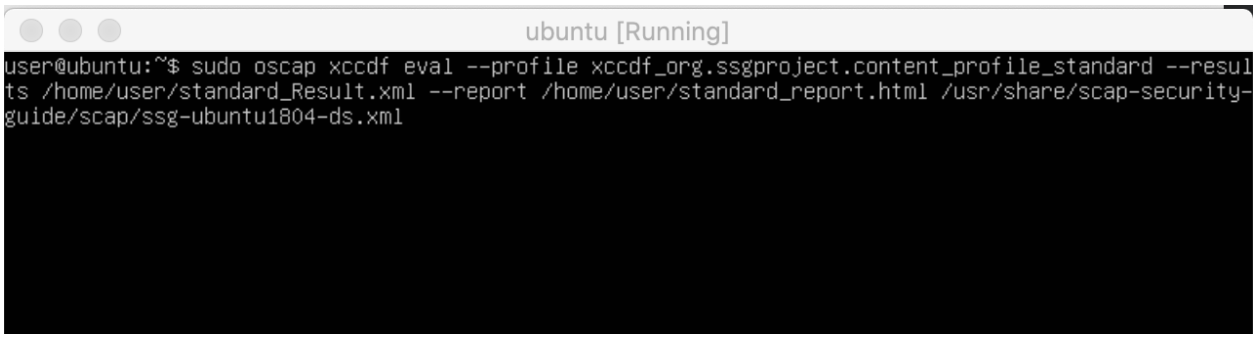
Here we have a lot of profiles to work with like :

- Common
- Minimal ANSSI DAT-NT28
- Average ANSSI DAT-NT28
- Restrictive ANSSI DAT-NT28
- High (Enforced) ANSSI DAT-NT28

Now we will check the ubuntu1804-ds.xml file for the scan profiles :

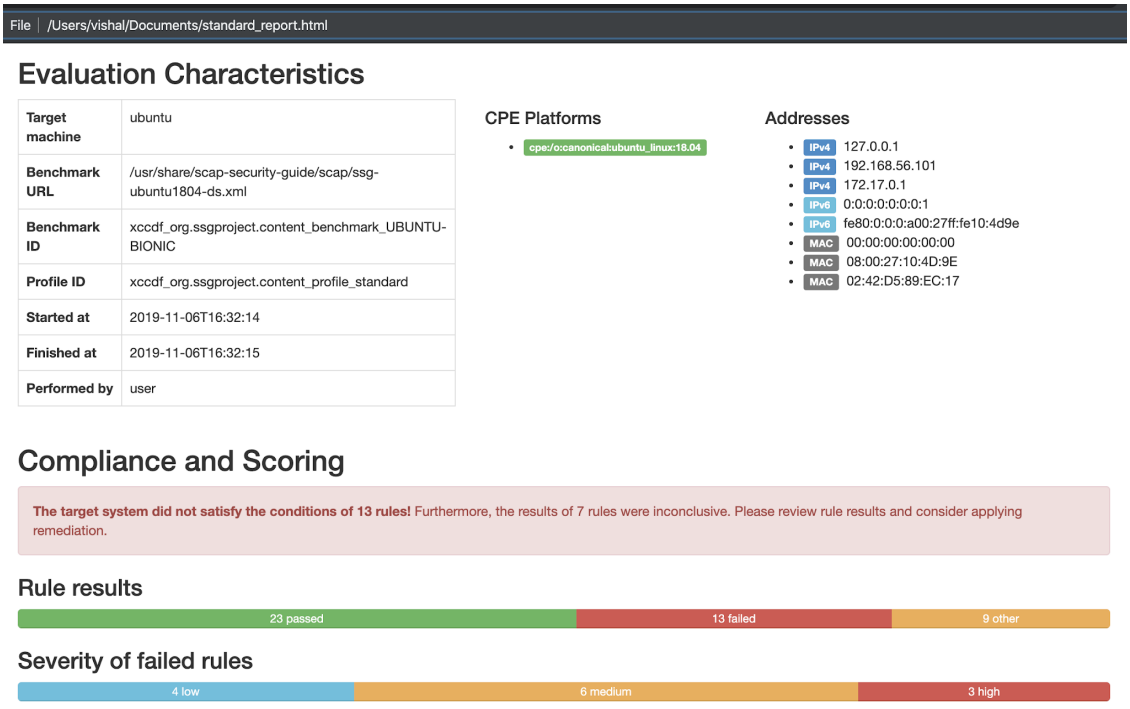


We will now run the scan for standard profile :



```
Title   Disallow creating symlinks to a file you not own
Rule    xccdf_org.ssgproject.content_rule_sysctl_fs_protected_symlinks
Result  pass

Title   Disallow creating symlinks to a file you not own
Rule    xccdf_org.ssgproject.content_rule_sysctl_fs_protected_hardlinks
Result  pass

Title   Enable Randomized Layout of Virtual Address Space
Rule    xccdf_org.ssgproject.content_rule_sysctl_kernel_randomize_va_space
Result  fail

Title   Disable Core Dumps for SUID programs
Rule    xccdf_org.ssgproject.content_rule_sysctl_fs_suid_dumpable
Result  fail

OpenSCAP Error: Probe with PID=1213 has been killed with signal 11 [../../../../../src/OVAL/probes/S
EAP/sch_pipe.c:173]
Item corresponding to object 'oval:ssg-obj_package_cron_installed:obj:1' from test 'oval:ssg-test_pa
ckage_cron_installed:tst:1' has an unknown flag. This may indicate a bug in OpenSCAP. [../../../../s
rc/OVAL/results/oval_resultTest.c:914]
Probe with PID=1236 has been killed with signal 11 [../../../../../src/OVAL/probes/SEAP/sch_pipe.c:1
73]
Item corresponding to object 'oval:ssg-obj_package_telnetd-ssl_removed:obj:1' from test 'oval:ssg-te
st_package_telnetd-ssl_removed:tst:1' has an unknown flag. This may indicate a bug in OpenSCAP. [../
../../../src/OVAL/results/oval_resultTest.c:914]
Probe with PID=1282 has been killed with signal 11 [../../../../../src/OVAL/probes/SEAP/sch_pipe.c:1
73]
Item corresponding to object 'oval:ssg-obj_package_inetutils-telnetd_removed:obj:1' from test 'oval:
ssg-test_package_inetutils-telnetd_removed:tst:1' has an unknown flag. This may indicate a bug in Op
enSCAP. [../../../../src/OVAL/results/oval_resultTest.c:914]
Probe with PID=1288 has been killed with signal 11 [../../../../../src/OVAL/probes/SEAP/sch_pipe.c:1
73]
Item corresponding to object 'oval:ssg-obj_package_rsyslog_installed:obj:1' from test 'oval:ssg-test
_package_rsyslog_installed:tst:1' has an unknown flag. This may indicate a bug in OpenSCAP. [../../.
./../src/OVAL/results/oval_resultTest.c:914]
user@ubuntu:~$
```

Here is the report of the scan :



File | /Users/vishal/Documents/standard_report.html

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	26.250000	100.000000	26.25%

Rule Overview

pass fail notchecked
fixed error notapplicable
informational unknown

Search through XCCDF rules Search

Group rules by: Default

Title	Severity	Result
Guide to the Secure Configuration of Ubuntu 18.04 13x fail 7x error 2x notchecked		
Services 2x fail 4x error 1x notchecked		
Cron and At Daemons 2x error		
Enable cron Service	medium	error
Install the cron service	medium	error
SSH Server		
Network Time Protocol 2x fail 1x notchecked		
Install the ntp service	high	fail
Enable the NTP Daemon	high	fail
Enable systemd_timesyncd Service	high	notchecked

File | /Users/vishal/Documents/standard_report.html

Enable systemd_timesyncd Service	high	notchecked
Deprecated services 2x error		
Uninstall the ntpdate package	low	pass
Uninstall the telnet server	high	pass
Uninstall the ssl compliant telnet server	high	error
Uninstall the inet-based telnet server	high	error
Uninstall the nis package	low	pass
System Settings 11x fail 3x error 1x notchecked		
System Accounting with auditd 2x fail		
Enable auditd Service	high	fail
install the auditd service	medium	fail
Configure Syslog 2x fail 3x error 1x notchecked		
Ensure All Logs are Rotated by logrotate 1x fail		
Ensure Logrotate Runs Periodically	medium	fail
Ensure Proper Configuration of Log Files 1x fail 1x error 1x notchecked		
Ensure System Log Files Have Correct Permissions	medium	error
Ensure Log Files Are Owned By Appropriate Group	medium	notchecked
Ensure Log Files Are Owned By Appropriate User	medium	fail
Enable rsyslog Service	medium	error

File | /Users/vishal/Documents/standard_report.html

▼ **Installing and Maintaining Software** 5x fail		
▼ **Disk Partitioning** 5x fail		
Ensure /tmp Located On Separate Partition	low	fail
Ensure /var Located On Separate Partition	low	fail
Ensure /var/log Located On Separate Partition	medium	fail
Ensure /home Located On Separate Partition	low	fail
Ensure /var/log/audit Located On Separate Partition	low	fail
▼ **File Permissions and Masks** 2x fail		
▶ Verify Permissions on Important Files and Directories		
▼ **Restrict Programs from Dangerous Execution Patterns** 2x fail		
▼ **Enable ExecShield** 1x fail		
Enable Randomized Layout of Virtual Address Space	medium	fail
▼ **Disable Core Dumps** 1x fail		
Disable Core Dumps for SUID programs	medium	fail

Show all result details

Generated using OpenSCAP 1.2.15

Next we run oval scan using the ssg-ubuntu1804-oval.xml :

```
user@ubuntu:~$ sudo oscap oval eval --results oval_results.xml --report oval-report.html /usr/share/
scap-security-guide/scap/ssg-ubuntu1804-oval.xml | head -n15
E: The package cache file is corrupted, it has the wrong hash
W: oscap:       Entity name 'value' from state (id: 'oval:ssg-state_sshd_not_required:ste:1') not fo
und in item (id: '1037281').
W: oscap:         Entity name 'value' from state (id: 'oval:ssg-state_sshd_requirement_unset:ste:1')
 not found in item (id: '1037281').
W: oscap:       Entity name 'value' from state (id: 'oval:ssg-state_sshd_required:ste:1') not found
in item (id: '1037281').
Definition oval:ssg-system_info_architecture_x86_64:def:1: true
Definition oval:ssg-system_info_architecture_x86:def:1: false
Definition oval:ssg-system_info_architecture_ppc_64:def:1: false
Definition oval:ssg-system_info_architecture_aarch_64:def:1: false
Definition oval:ssg-system_info_architecture_64bit:def:1: true
Definition oval:ssg-system_boot_mode_is_uefi:def:1: false
Definition oval:ssg-sysctl_vm_mmap_min_addr:def:1: true
Definition oval:ssg-sysctl_static_vm_mmap_min_addr:def:1: true
Definition oval:ssg-sysctl_static_net_ipv6_conf_all_disable_ipv6:def:1: false
Definition oval:ssg-sysctl_static_net_ipv4_ip_forward:def:1: false
Definition oval:ssg-sysctl_static_kernel_sysrq:def:1: false
Definition oval:ssg-sysctl_static_kernel_randomize_va_space:def:1: false
Definition oval:ssg-sysctl_static_kernel_pid_max:def:1: false
Definition oval:ssg-sysctl_static_kernel_perf_event_paranoid:def:1: false
Definition oval:ssg-sysctl_static_kernel_perf_event_max_sample_rate:def:1: false
W: oscap:       Can't receive message: 103, Software caused connection abort.
E: The package cache file is corrupted, it has the wrong hash
W: oscap:       Can't receive message: 103, Software caused connection abort.
E: The package cache file is corrupted, it has the wrong hash
W: oscap:     Can't receive message: 103, Software caused connection abort.
E: The package cache file is corrupted, it has the wrong hash
W: oscap:     Can't receive message: 103, Software caused connection abort.
E: The package cache file is corrupted, it has the wrong hash
W: oscap:     Can't receive message: 103, Software caused connection abort.
E: probe_partition: An error ocured while receiving SEAP message. errno=103, Software caused connect
ion abort.
user@ubuntu:~$
```

We tried another scan after downloading the oval scan file from https://oval.cisecurity.org/repository/download/5.11.2/vulnerability/ubuntu_1804.xml :

```
user@ubuntu:~/scap-security-guide-0.1.47$ cd
user@ubuntu:~$ wget https://oval.cisecurity.org/repository/download/5.11.2/vulnerability/ubuntu_1804
.xml
--2019-11-06 23:11:13--  https://oval.cisecurity.org/repository/download/5.11.2/vulnerability/ubuntu
_1804.xml
Resolving oval.cisecurity.org (oval.cisecurity.org)... 52.1.106.207, 52.1.223.65
Connecting to oval.cisecurity.org (oval.cisecurity.org)|52.1.106.207|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 672 [application/octet-stream]
Saving to: ‘ubuntu_1804.xml’

ubuntu_1804.xml          100%[===================================>]     672  --.-KB/s    in 0s

2019-11-06 23:11:13 (140 MB/s) - ‘ubuntu_1804.xml’ saved [672/672]
```

After the scan we got the following result :

```
Connecting to oval.cisecurity.org (oval.cisecurity.org)|52.1.106.207|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 672 [application/octet-stream]
Saving to: ‘ubuntu_1804.xml’

ubuntu_1804.xml          100%[===================================>]     672  --.-KB/s    in 0s

2019-11-06 23:11:13 (140 MB/s) - ‘ubuntu_1804.xml’ saved [672/672]

user@ubuntu:~$ oscap oval eval --results ./oval_results.xml --report ./oval_report.html ubuntu_1804.
xml
Evaluation done.
```

OVAL Results Generator Information

Schema Version	Product Name	Product Version	Date	Time
5.11.2	cpe:/a:open-scap:oscap	1.2.15	2019-11-06	23:11:48
#×	#✓	#Error	#Unknown	#Other
0	0	0	0	0

OVAL Definition Generator Information

Schema Version	Product Name	Product Version	Date	Time
5.11.2	CIS OVAL Repository	0.1	2019-11-06	08:49:51
#Definitions	#Tests	#Objects	#States	#Variables
0 Total	0	0	0	0

System Information

Host Name	ubuntu
Operating System	Linux
Operating System Version	#67-Ubuntu SMP Thu Aug 22 16:55:30 UTC 2019
Architecture	x86_64
Interfaces	Interface Name: lo IP Address: 127.0.0.1 MAC Address: 00:00:00:00:00:00 Interface Name: enp0s3 IP Address: 10.0.2.15 MAC Address: 08:00:27:10:4D:9E Interface Name: docker0 IP Address: 172.17.0.1 MAC Address: 02:42:31:6C:16:D1 Interface Name: lo IP Address: ::1 MAC Address: 00:00:00:00:00:00 Interface Name: enp0s3 IP Address: fe80::a00:27ff:fe10:4d9e MAC Address: 08:00:27:10:4D:9E

OVAL System Characteristics Generator Information

Schema Version	Product Name	Product Version	Date	Time
5.11.2	cpe:/a:open-scap:oscap	0.1	2019-11-06	23:11:48

OVAL Definition Results

× ✓ Error Unknown Other

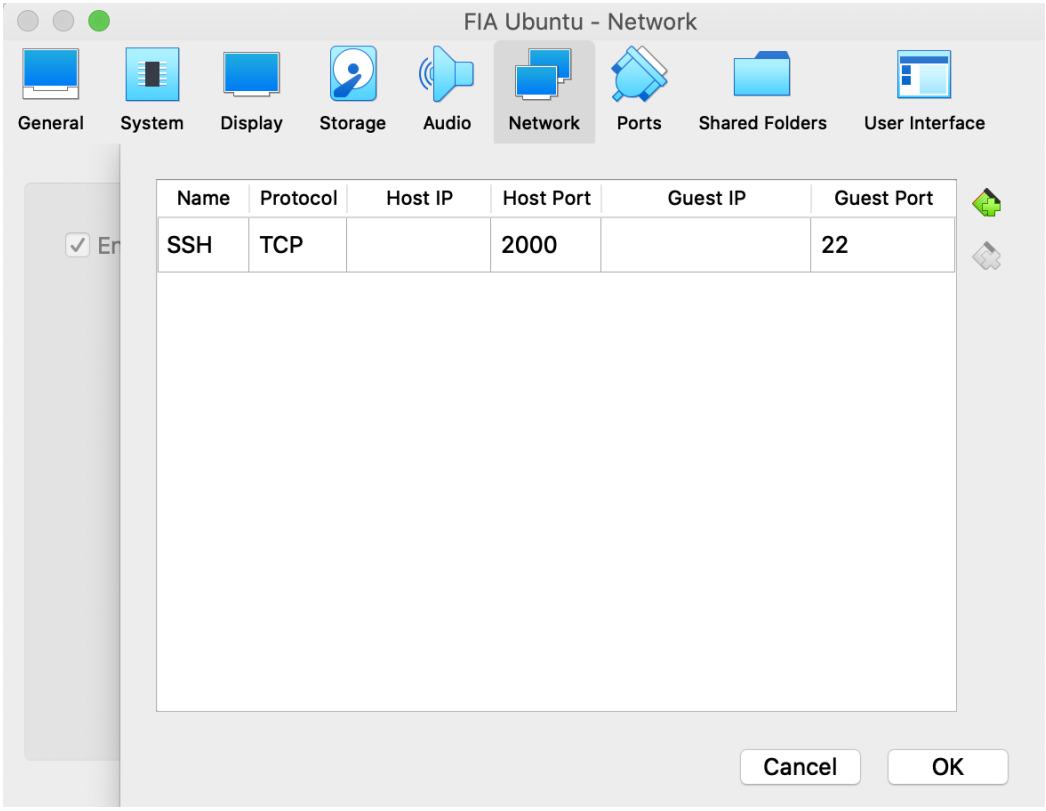
ID	Result	Class	Reference ID	Title

Scap-Workbench in Host Machine to scan Ubuntu VM:

After scanning the ubuntu VM using xccdf and oval, we tried to remediate the Ubuntu VM vulnerabilities flagged by openscap scan. Following are the steps taken to remediate the VM:

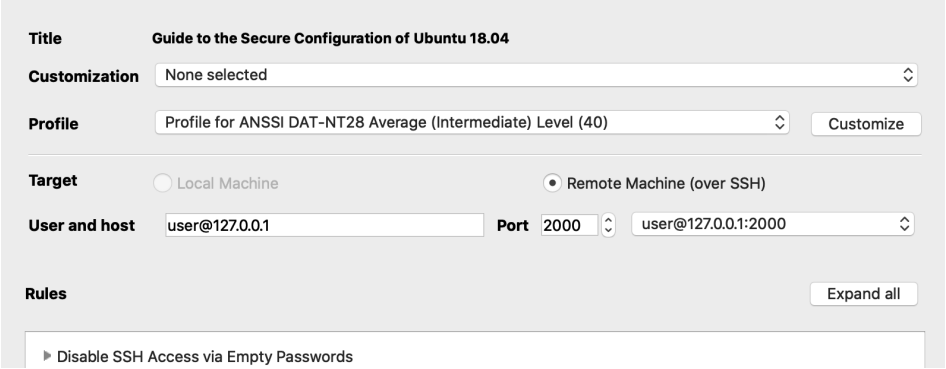
1. **Installation and setup of Scap-Workbench:**
   We installed the scap-workbench from the specified site and after installation, loaded the SCAP content with the file *ssg-ubuntu1804-ds.xml*. After loading the content we configured the VM as follows:

   In VirtualBox, we changed the network settings of Ubuntu VM. In Network Adapter 1(NAT), we enabled port forwarding with the following configuration to allow the SSH connection for scap-workbench remediation:

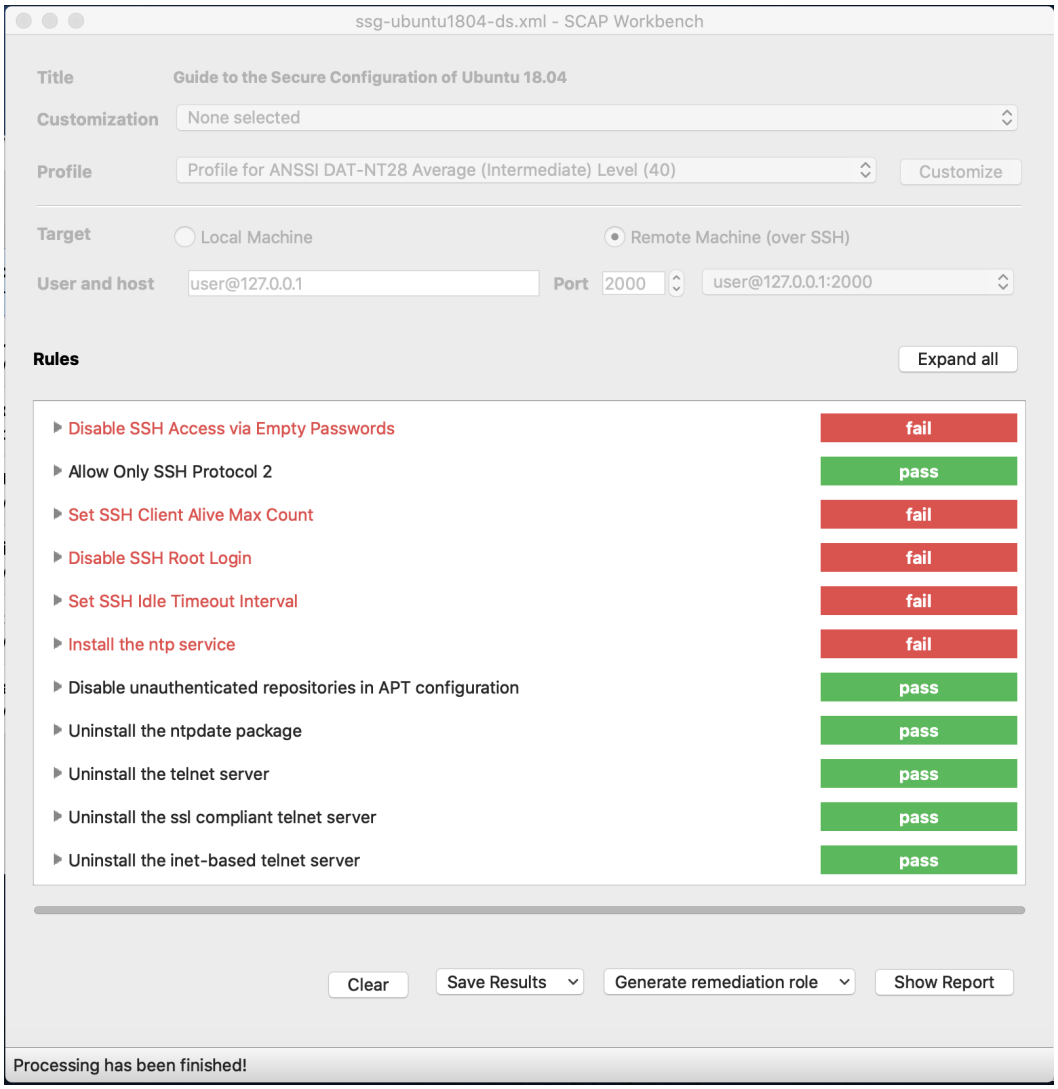


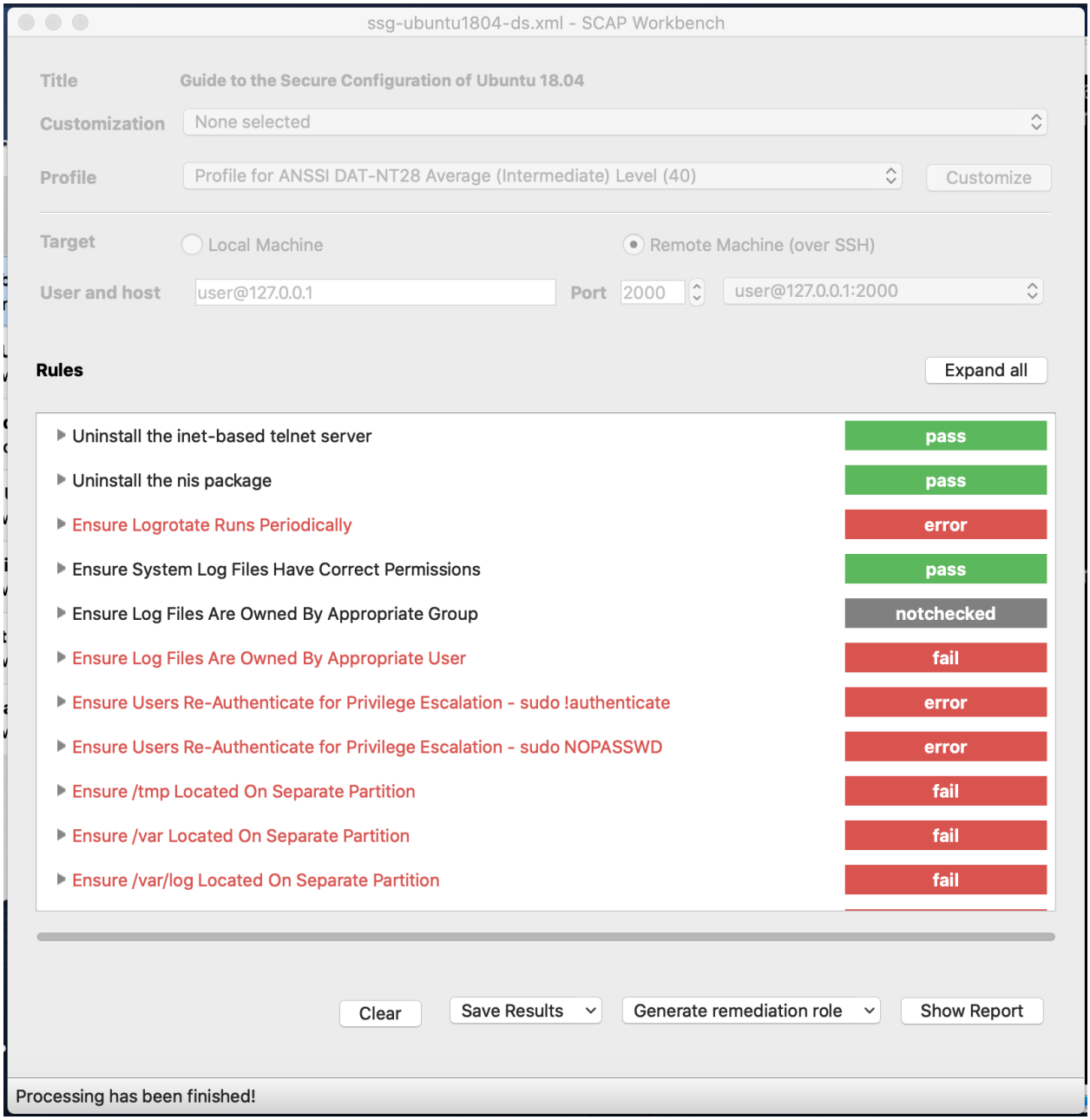
2. **Remediating the Ubuntu VM using scap-workbench:**

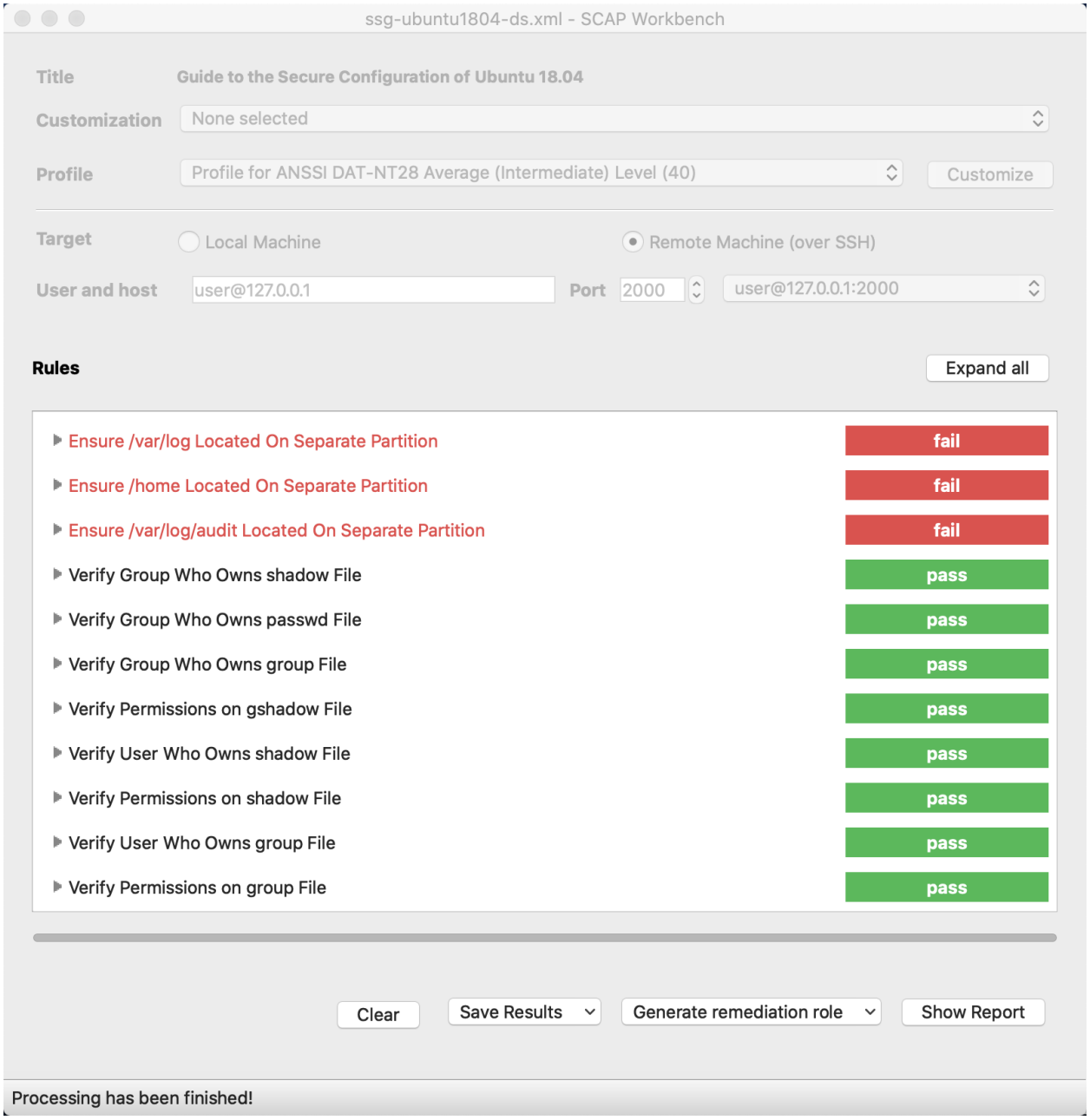
   After configuring network configuration for SSH, we gave the following details in the scap-workbench:

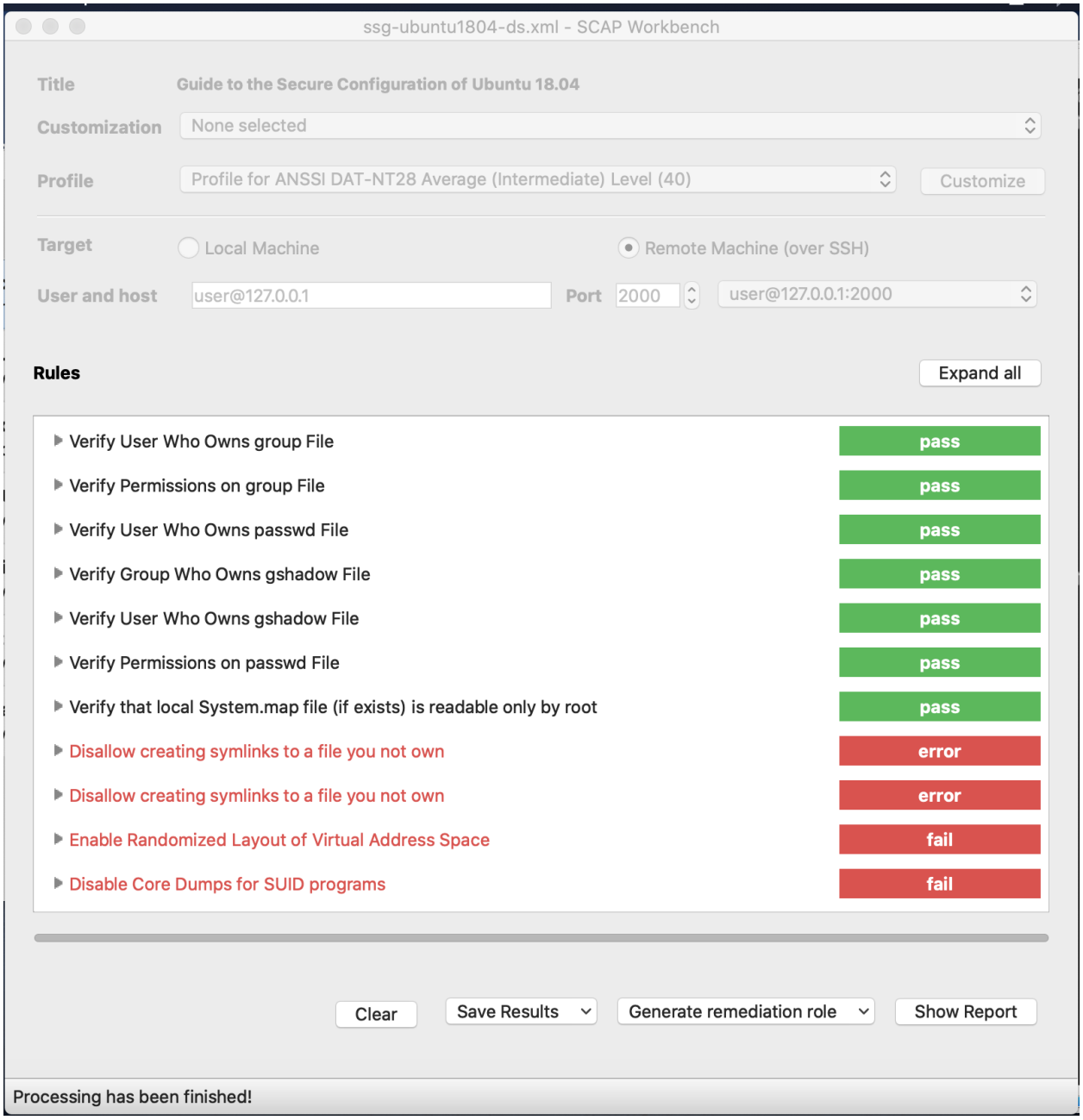


Since we gave port for Host as 2000, the port number here mentioned is 2000 and user@localhost is the user and host combination for SSH. After providing the details, we scanned the Ubuntu VM with remediate option and got the following report:




ssg-ubuntu1804-ds.xml - SCAP Workbench
Title
Guide to the Secure Configuration of Ubuntu 18.04
Customization
None selected
Profile
Profile for ANSSI DAT-NT28 Average (Intermediate) Level (40)
Customize
Target
Local Machine
Remote Machine (over SSH)
User and host
user@127.0.0.1
Port
2000
user@127.0.0.1:2000
Rules
Expand all
Uninstall the inet-based telnet server
pass
Uninstall the nis package
pass
Ensure Logrotate Runs Periodically
error
Ensure System Log Files Have Correct Permissions
pass
Ensure Log Files Are Owned By Appropriate Group
notchecked
Ensure Log Files Are Owned By Appropriate User
fail
Ensure Users Re-Authenticate for Privilege Escalation - sudo !authenticate
error
Ensure Users Re-Authenticate for Privilege Escalation - sudo NOPASSWD
error
Ensure /tmp Located On Separate Partition
fail
Ensure /var Located On Separate Partition
fail
Ensure /var/log Located On Separate Partition
fail
Clear
Save Results
Generate remediation role
Show Report
Processing has been finished!


ssg-ubuntu1804-ds.xml - SCAP Workbench
Title
Guide to the Secure Configuration of Ubuntu 18.04
Customization
None selected
Profile
Profile for ANSSI DAT-NT28 Average (Intermediate) Level (40)
Customize
Target
Local Machine
Remote Machine (over SSH)
User and host
user@127.0.0.1
Port
2000
user@127.0.0.1:2000
Rules
Expand all
Ensure /var/log Located On Separate Partition
fail
Ensure /home Located On Separate Partition
fail
Ensure /var/log/audit Located On Separate Partition
fail
Verify Group Who Owns shadow File
pass
Verify Group Who Owns passwd File
pass
Verify Group Who Owns group File
pass
Verify Permissions on gshadow File
pass
Verify User Who Owns shadow File
pass
Verify Permissions on shadow File
pass
Verify User Who Owns group File
pass
Verify Permissions on group File
pass
Clear
Save Results
Generate remediation role
Show Report
Processing has been finished!


ssg-ubuntu1804-ds.xml - SCAP Workbench
Title
Guide to the Secure Configuration of Ubuntu 18.04
Customization
None selected
Profile
Profile for ANSSI DAT-NT28 Average (Intermediate) Level (40)
Customize
Target
Local Machine
Remote Machine (over SSH)
User and host
user@127.0.0.1
Port
2000
user@127.0.0.1:2000
Rules
Expand all
Verify User Who Owns group File
pass
Verify Permissions on group File
pass
Verify User Who Owns passwd File
pass
Verify Group Who Owns gshadow File
pass
Verify User Who Owns gshadow File
pass
Verify Permissions on passwd File
pass
Verify that local System.map file (if exists) is readable only by root
pass
Disallow creating symlinks to a file you not own
error
Disallow creating symlinks to a file you not own
error
Enable Randomized Layout of Virtual Address Space
fail
Disable Core Dumps for SUID programs
fail
Clear
Save Results
Generate remediation role
Show Report
Processing has been finished!

We saved the results in html and viewed the report in browser for more details:

Evaluation Characteristics

Target machine	ubuntu
Benchmark URL	/tmp/tmp.mUOzE3oQTV
Benchmark ID	xccdf_org.ssgproject.content_benchmark_UBUNTU-BIONI
Profile ID	xccdf_org.ssgproject.content_profile_anssi_np_nt28_averag
Started at	2019-11-06T20:36:37
Finished at	2019-11-06T20:36:37
Performed by	user

CPE Platforms

- cpe:/o:canonical:ubuntu_linux:18.04

Addresses

- IPv4 127.0.0.1
- IPv4 10.0.2.15
- IPv4 172.17.0.1
- IPv6 0:0:0:0:0:0:0:1
- IPv6 fe80:0:0:0:a00:27ff:fe10:4d9e
- MAC 00:00:00:00:00:00
- MAC 08:00:27:10:4D:9E
- MAC 02:42:14:28:9E:F0

Compliance and Scoring

The target system did not satisfy the conditions of 13 rules! Furthermore, the results of 5 rules were inconclusive. Please review rule results and consider applying remediation.

Rule results

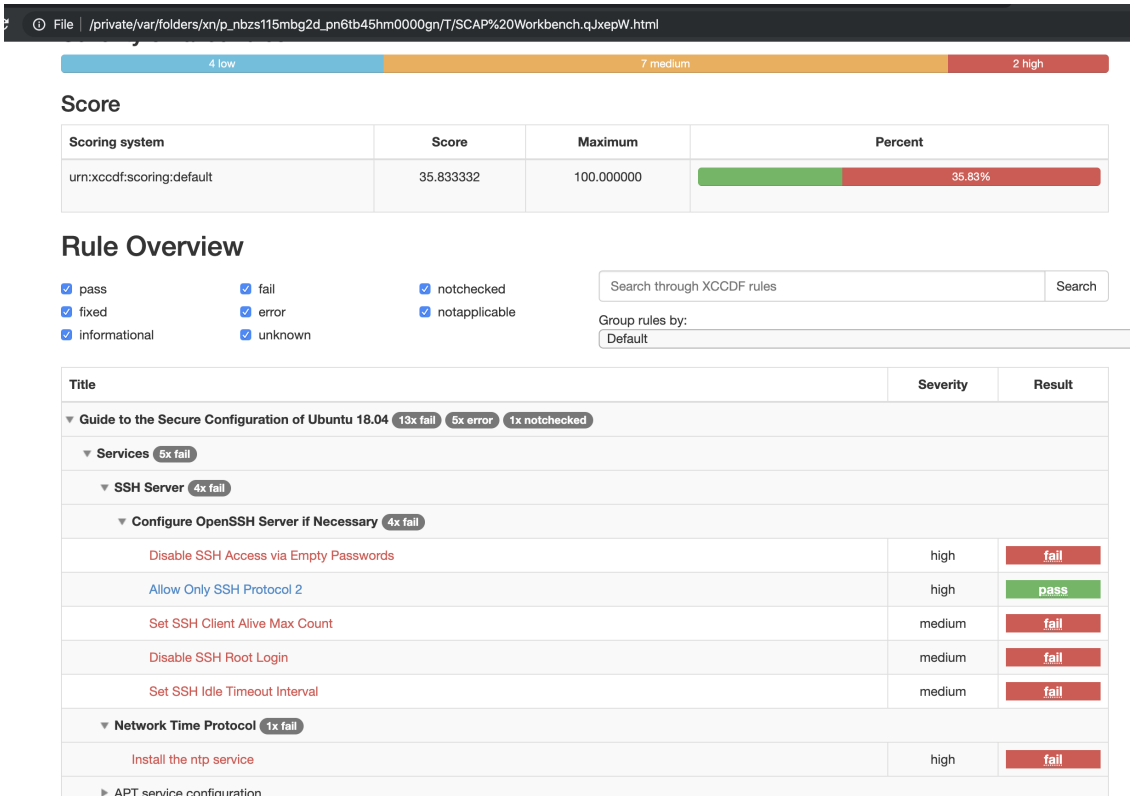
21 passed | 13 failed | 6 other

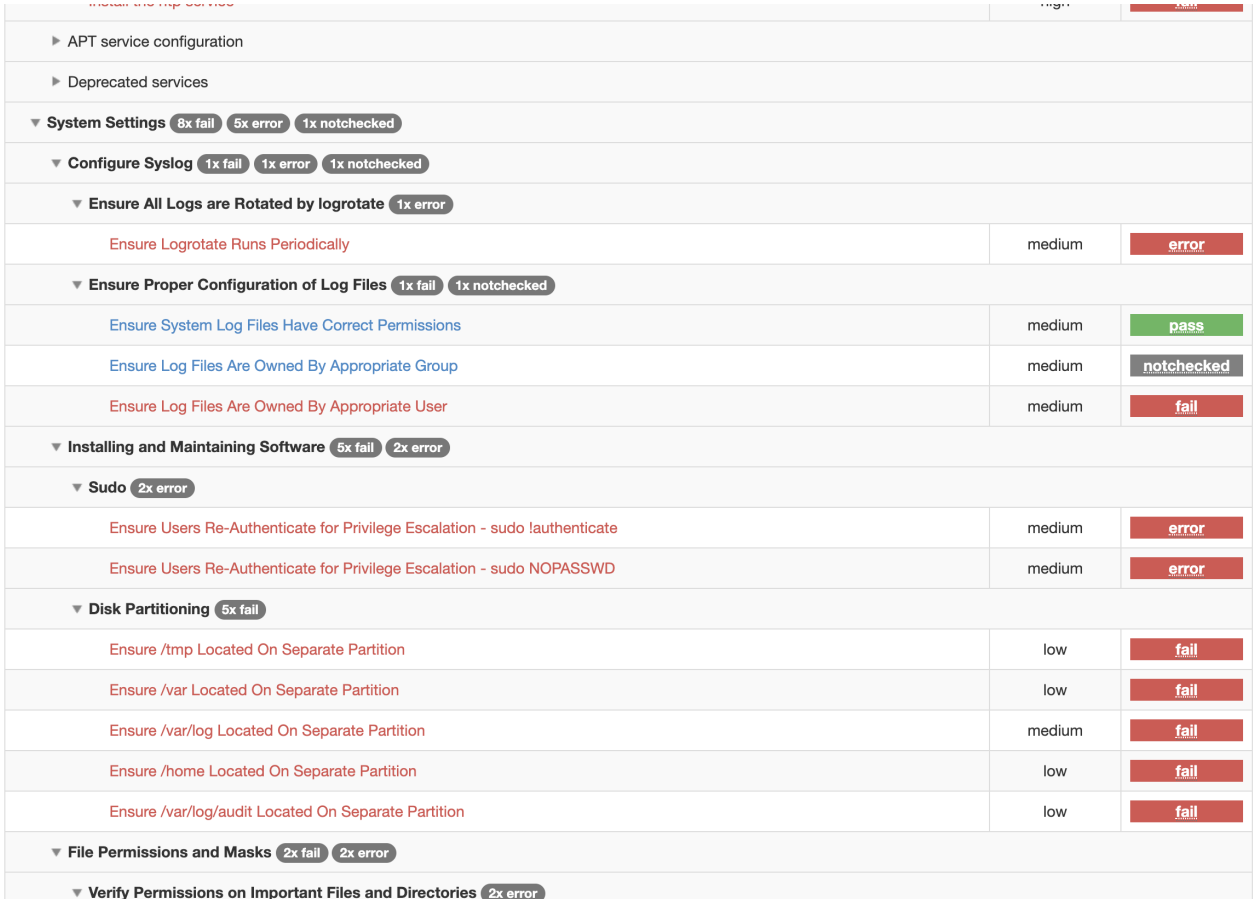
Severity of failed rules

4 low | 7 medium | 2 high

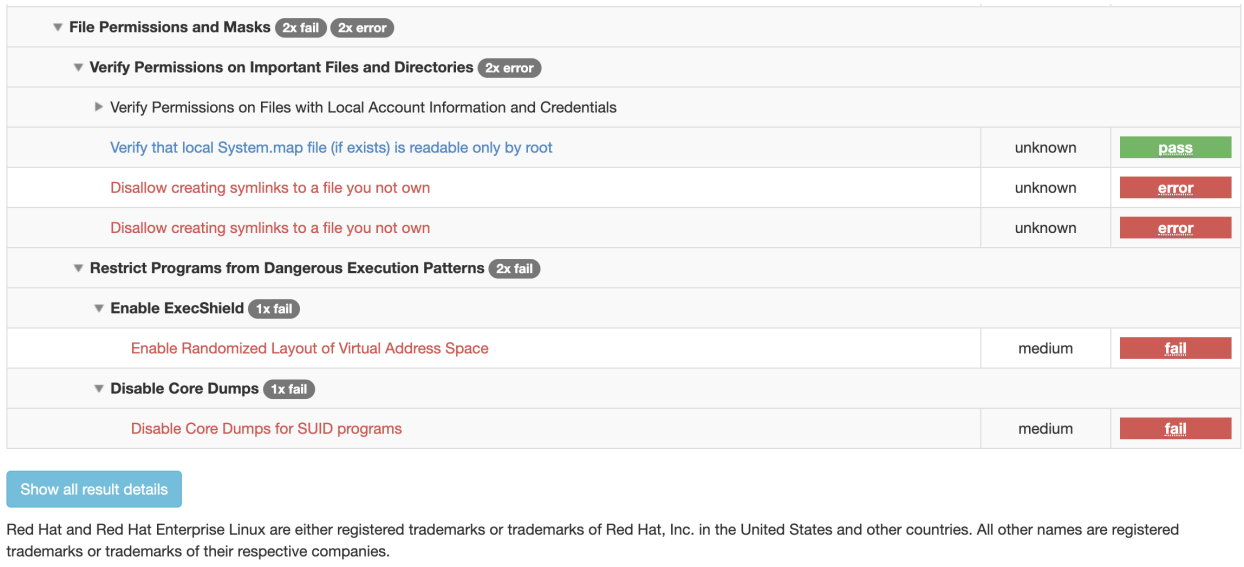
Score

Scoring system	Score	Maximum	Percent





▸ APT service configuration		
▸ Deprecated services		
▾ **System Settings** 8x fail 5x error 1x notchecked		
▾ **Configure Syslog** 1x fail 1x error 1x notchecked		
▾ **Ensure All Logs are Rotated by logrotate** 1x error		
Ensure Logrotate Runs Periodically	medium	error
▾ **Ensure Proper Configuration of Log Files** 1x fail 1x notchecked		
Ensure System Log Files Have Correct Permissions	medium	pass
Ensure Log Files Are Owned By Appropriate Group	medium	notchecked
Ensure Log Files Are Owned By Appropriate User	medium	fail
▾ **Installing and Maintaining Software** 5x fail 2x error		
▾ **Sudo** 2x error		
Ensure Users Re-Authenticate for Privilege Escalation - sudo !authenticate	medium	error
Ensure Users Re-Authenticate for Privilege Escalation - sudo NOPASSWD	medium	error
▾ **Disk Partitioning** 5x fail		
Ensure /tmp Located On Separate Partition	low	fail
Ensure /var Located On Separate Partition	low	fail
Ensure /var/log Located On Separate Partition	medium	fail
Ensure /home Located On Separate Partition	low	fail
Ensure /var/log/audit Located On Separate Partition	low	fail
▾ **File Permissions and Masks** 2x fail 2x error		
▾ **Verify Permissions on Important Files and Directories** 2x error		



▾ **File Permissions and Masks** 2x fail 2x error		
▾ **Verify Permissions on Important Files and Directories** 2x error		
▸ Verify Permissions on Files with Local Account Information and Credentials		
Verify that local System.map file (if exists) is readable only by root	unknown	pass
Disallow creating symlinks to a file you not own	unknown	error
Disallow creating symlinks to a file you not own	unknown	error
▾ **Restrict Programs from Dangerous Execution Patterns** 2x fail		
▾ **Enable ExecShield** 1x fail		
Enable Randomized Layout of Virtual Address Space	medium	fail
▾ **Disable Core Dumps** 1x fail		
Disable Core Dumps for SUID programs	medium	fail

Show all result details

After remediating the Ubuntu VM, we noticed that the Deprecated Services (under SSH Server Services) tests that failed before remediating Ubuntu using scap-workbench were passed after remediating the VM:

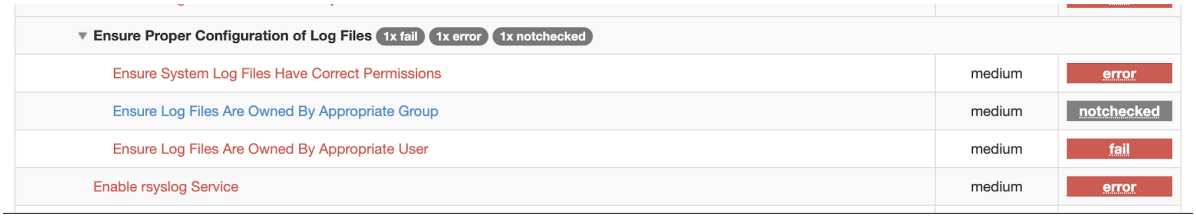
Before remediation:

Enable systemd_timesyncd Service	high	notchecked
▼ Deprecated services 2x error		
Uninstall the ntpdate package	low	pass
Uninstall the telnet server	high	pass
Uninstall the ssl compliant telnet server	high	error
Uninstall the inet-based telnet server	high	error
Uninstall the nis package	low	pass

After remediation:

▼ Deprecated services		
Uninstall the ntpdate package	low	pass
Uninstall the telnet server	high	pass
Uninstall the ssl compliant telnet server	high	pass
Uninstall the inet-based telnet server	high	pass
Uninstall the nis package	low	pass
▼ System Settings 8x fail 5x error 1x notchecked		
▼ Configure Syslog 1x fail 1x error 1x notchecked		

The test "*Ensure System Log Files Have Correct Permissions*" failed before:



▼ Ensure Proper Configuration of Log Files 1x fail 1x error 1x notchecked		
Ensure System Log Files Have Correct Permissions	medium	error
Ensure Log Files Are Owned By Appropriate Group	medium	notchecked
Ensure Log Files Are Owned By Appropriate User	medium	fail
Enable rsyslog Service	medium	error

After remediation, the test was passed:

▼ Deprecated services		
Uninstall the ntpdate package	low	pass
Uninstall the telnet server	high	pass
Uninstall the ssl compliant telnet server	high	pass
Uninstall the inet-based telnet server	high	pass
Uninstall the nis package	low	pass
▼ System Settings 8x fail 5x error 1x notchecked		
▼ Configure Syslog 1x fail 1x error 1x notchecked		

References:

[1]https://medium.com/@pierangelo1982/setting-ssh-connection-to-ubuntu-on-virtualbox-af243f737b8b
[2]https://wiki.workassis.com/virtualbox-ssh-between-host-and-guest/