

2 DE DICIEMBRE DE 2024

BASTIONADO DE SISTEMAS

FUNDAMENTOS DE LAS SEGURIDAD EN EL SOFTWARE Y EN LOS
COMPONENTES

ENRIQUE GARCIA CUADRADO
PAULA DANIELA SANCHEZ RODRIGUEZ

Universidad de Alcalá de Henares

PARTE I. BASTIONADO MANUAL

Guías de Configuración Segura para CentOS 7

1. ¿Cómo está estructurado el contenido de la guía?

El contenido está estructurado en secciones según los temas de configuración de seguridad. Incluye una tabla de contenidos con categorías como configuración inicial, servicios, red, acceso y autenticación, registro y auditoría, etc. Cada sección detalla recomendaciones específicas para cada caso concreto.

2. Qué niveles de seguridad se definen?

Nivel 1: Para servidores y estaciones de trabajo, enfocado en configuraciones prácticas y prudentes que no inutilizan el sistema más allá de lo aceptable.

Nivel 2: Extiende el nivel 1 y está diseñado para entornos donde la seguridad es lo más importante. Estas configuraciones pueden impactar en el rendimiento o en la utilidad del sistema.

3. ¿Cuál es la estructura de una verificación de seguridad? Elige un ejemplo y extrae su contenido

Cada verificación incluye:

- **Título:** Describe la recomendación.
- **Descripción:** Explica el propósito y detalles del control.
- **Justificación (Rationale):** Expone los motivos de seguridad.
- **Procedimientos de Auditoría y Remediación:** Detalla cómo validar y corregir la configuración.
- **Referencias:** Recursos adicionales para contextualización.

Ejemplo:

- **Título:** Ensure cramfs kernel module is not available
- **Descripción:** Este módulo es un sistema de archivos comprimido solo lectura. Si no es necesario, se debe deshabilitar.
- **Justificación:** Reducir el ataque local deshabilitando módulos no esenciales.
- **Auditoría:** Usar scripts o comandos para verificar si el módulo está deshabilitado o no cargado en el kernel.
- **Remediación:** Crear entradas en `/etc/modprobe.d/` para denegar su carga y descargar el módulo si está activo.

4. ¿Cuál es el número aproximado de verificaciones o controles que define el documento?

La guía incluye más de 300 recomendaciones principales y más de 900 controles distribuidos en diferentes áreas de seguridad.

5. Aplicar los controles que pueda de la guía sobre la máquina virtual de CentOS (si son aplicables) y hacer un informe con los resultados presentando además una estimación de cuánto tardáis en verificar el cumplimiento de cada control.

Informe de Auditoría de Controles de Seguridad

Nombre del Sistema: CentOS Linux 7
Fecha: 02/12/2024

Detalles de los Controles

1.1.1.1: Asegurar que el módulo cramfs no esté disponible

Resultado Auditoría:

Al ejecutar "modprobe -n -v cramfs", inicialmente se detectó que el módulo estaba disponible:

```
insmod /lib/modules/3.10.0-1160.el7.x86_64/kernel/fs/cramfs/cramfs.ko.xz
```

Después de aplicar las configuraciones de remediación y verificar nuevamente, el resultado mostró que el módulo no se cargará:

```
install /bin/false
```

El comando "lsmod | grep cramfs" confirmó que el módulo no estaba cargado en el sistema.

Remediación Aplicada:

Se utilizó el siguiente comando para bloquear el módulo cramfs:

```
sudo echo "install cramfs /bin/false" >> /etc/modprobe.d/cramfs.conf
```

Para asegurarse de que no se pueda cargar, también se añadió a la lista negra:

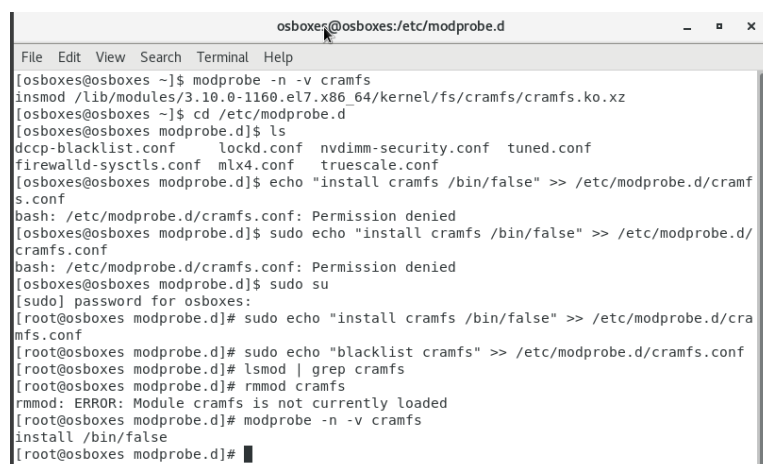
```
sudo echo "blacklist cramfs" >> /etc/modprobe.d/cramfs.conf
```

Finalmente, se intentó eliminarlo del kernel con "rmmod cramfs", aunque no estaba cargado.

Estado: Cumple

Notas: El módulo ha sido correctamente bloqueado y no está disponible para cargar en el sistema.

Evidencia:



```
osboxes@osboxes: /etc/modprobe.d
File Edit View Search Terminal Help
[osboxes@osboxes ~]$ modprobe -n -v cramfs
insmod /lib/modules/3.10.0-1160.el7.x86_64/kernel/fs/cramfs/cramfs.ko.xz
[osboxes@osboxes ~]$ cd /etc/modprobe.d
[osboxes@osboxes modprobe.d]$ ls
dcbp-blacklist.conf  lockd.conf  nvdim-security.conf  tuned.conf
firewalld-sysctls.conf  mlx4.conf  truescale.conf
[osboxes@osboxes modprobe.d]$ echo "install cramfs /bin/false" >> /etc/modprobe.d/cramfs.conf
bash: /etc/modprobe.d/cramfs.conf: Permission denied
[osboxes@osboxes modprobe.d]$ sudo echo "install cramfs /bin/false" >> /etc/modprobe.d/cramfs.conf
bash: /etc/modprobe.d/cramfs.conf: Permission denied
[osboxes@osboxes modprobe.d]$ sudo su
[sudo] password for osboxes:
[root@osboxes modprobe.d]# sudo echo "install cramfs /bin/false" >> /etc/modprobe.d/cramfs.conf
[root@osboxes modprobe.d]# sudo echo "blacklist cramfs" >> /etc/modprobe.d/cramfs.conf
[root@osboxes modprobe.d]# lsmod | grep cramfs
[root@osboxes modprobe.d]# rmmod cramfs
rmmod: ERROR: Module cramfs is not currently loaded
[root@osboxes modprobe.d]# modprobe -n -v cramfs
install /bin/false
[root@osboxes modprobe.d]#
```

1.1.2.1.2: Configurar nodev en la partición /tmp

Resultado Auditoría: findmnt no muestra nada, lo que indica que la opción nodev está activa.

Estado: Cumple.

Evidencia:

```
[root@osboxes /]# findmnt -nk /tmp | grep -v nodev
[root@osboxes /]#
```

1.2.2: Asegurarse de que gpgcheck está activa globalmente

Resultado Auditoría: La salida muestra el gpgcheck=1 por lo que si esta activada

Estado: Cumple.

Evidencia:

```
[root@osboxes /]# grep -P -- '^h*gpgcheck\b' /etc/yum.conf
gpgcheck=1
[root@osboxes /]#
```

1.6.2: Configurar el banner de advertencia para inicios de sesión locales correctamente

Resultado Auditoría:

Se ejecuto el comando “cat /etc/issue” y el resultado obtenido, no incluye un mensaje de advertencia adecuado, por lo que no cumple con el control.

```
[root@osboxes /]# cat /etc/issue
\5
Kernel \r on an \m
```

Remediación Aplicada:

Se editó el archivo para que contenga un mensaje de advertencia adecuado que informe a los usuarios sobre las condiciones de uso del sistema y se verifican los cambios

Estado: Cumple.

Evidencia:

```
[root@osboxes /]# nano /etc/issue
[root@osboxes /]# cat /etc/issue
*****
ATENCIÓN: Este sistema es de uso exclusivo para personal autorizado.
*****
```

2.1.1: Asegurar que se utilice sincronización de tiempo

Resultado Auditoría:

Se ejecuto el comando “rpm -q chrony” y el resultado obtenido, demuestra que está instalado en el sistema.

Estado: Cumple.

Evidencia:

```
[root@osboxes /]# systemctl is-active chronyd
active
```

2.2.4: Asegurar que el servicio de servidor DNS no esté en uso

Resultado Auditoría:

Se ejecuto el comando “rpm -q bind” y el resultado obtenido, demuestra que no está instalado en el sistema.

Estado: Cumple.

Evidencia:

Se verifico si el servicio está activo

```
[root@osboxes /]# rpm -q bind
package bind is not installed
[root@osboxes /]# systemctl is-active named.service 2>/dev/null | grep '^active'
```

2.2.4: Asegurar que el servicio firewalld esté habilitado y en ejecución

Resultado Auditoría:

Se ejecuto el comando “systemctl is-enabled firewalld” para verificar si el servicio firewalld está habilitado.

Se ejecuto el comando “firewall-cmd --state” para verificar si el servicio firewalld está ejecutándose.

Estado: Cumple.

Evidencia:

Se verifico que el servicio está activo y en ejecución.

```
[root@osboxes /]# systemctl is-enabled firewalld
enabled
[root@osboxes /]# firewall-cmd --state
running
```

Conclusión

De los 8 controles revisados, el sistema cumple con **7 controles**. El control **3.3.3** requiere remediación para cumplir con las recomendaciones de la guía CIS.

6. ¿Qué tiempo estimáis para realizar la validación completa? ¿Qué podemos concluir sobre el proceso?

La estimación que hacemos para una validación completa de las más de 900 verificaciones puede llevar diferentes tiempos dependiendo del método que se use.

Utilizando herramientas de automatización como OpenSCAP, el proceso puede hacerse en aproximadamente un día si se hace minuciosamente. Esto incluye la configuración inicial de las herramientas, la ejecución del análisis y la interpretación de los resultados para identificar las configuraciones críticas que requieren cambios.

En cambio, si hacemos la validación manualmente sería mucho más tiempo, ya que se necesitaría entre 5 y 10 minutos por control. Esto equivale a un total de entre 100 y 200 horas, o de 2 a 4 semanas de trabajo.

Con esto podemos concluir que es necesario el uso de herramientas automatizadas a la hora de hacer estos análisis para poder ahorrar tiempo y emplearlo de forma útil.

PARTE II. VERIFICACIONES AUTOMATIZADAS UTILIZANDO SCAP

ANÁLISIS DE SISTEMAS FEDORA USANDO OSCAP:

Auditoria de un Servidor Fedora

```
osboxes@vbox:~$ oscap -V
OpenSCAP command line tool (oscap) 1.4.0
Copyright 2009--2023 Red Hat Inc., Durham, North Carolina.

==== Supported specifications ====
SCAP Version: 1.3
XCCDF Version: 1.2
OVAL Version: 5.11.1
CPE Version: 2.3
Asset Identification Version: 1.1
Asset Reporting Format Version: 1.1

==== Capabilities added by auto-loaded plugins ====
No plugins have been auto-loaded...

==== Paths ====
Schema files: /usr/share/openscap/schemas
Default CPE files: /usr/share/openscap/cpe

==== Inbuilt CPE names ====
Linux - cpe:/o:linux:linux_kernel:-
```

```
==== Inbuilt CPE names ====
Linux - cpe:/o:linux:linux_kernel:-

==== Supported OVAL objects and associated OpenSCAP probes ====
OVAL family   OVAL object   OpenSCAP probe
-----
independent   environmentvariable   probe_environmentvariable
independent   environmentvariable58   probe_environmentvariable58
independent   family               probe_family
independent   filehash58           probe_filehash58 (SHA-224, SHA-256, SHA-384, SHA-512)
independent   sql                   probe_sql
independent   sql57                 probe_sql57
independent   system_info           probe_system_info
independent   textfilecontent       probe_textfilecontent
independent   textfilecontent54     probe_textfilecontent54
independent   variable              probe_variable
independent   xmlfilecontent        probe_xmlfilecontent
independent   yamlfilecontent       probe_yamlfilecontent
linux         dpkginfo              probe_dpkginfo
linux         iflisteners            probe_iflisteners
linux         inetlisteningserver   probe_inetlisteningserver
linux         partition              probe_partition
linux         rpminfo                probe_rpminfo
linux         rpmverify              probe_rpmverify
linux         rpmverifyfile          probe_rpmverifyfile
linux         rpmverifypackage       probe_rpmverifypackage
linux         selinuxboolean         probe_selinuxboolean
linux         selinuxsecuritycontext   probe_selinuxsecuritycontext
linux         systemdunitdependency   probe_systemdunitdependency
linux         systemdunitproperty    probe_systemdunitproperty
linux         fwupdsecattr           probe_fwupdsecattr
unix          dnscache               probe_dnscache
unix          file                    probe_file
unix          fileextendedattribute   probe_fileextendedattribute
unix          interface              probe_interface
unix          password                probe_password
unix          process                 probe_process
unix          process58               probe_process58
unix          routingtable            probe_routingtable
unix          runlevel                probe_runlevel
unix          shadow                  probe_shadow
unix          symlink                 probe_symlink
unix          sysctl                  probe_sysctl
unix          uname                   probe_uname
```

¿Qué versiones de las especificaciones anteriores (XCCDF, OVAL, CPE, CVSS, CVE, AI, ARF) se están empleando?

OpenSCAP utiliza varias especificaciones estándar, incluyendo SCAP en su versión 1.3, XCCDF en la versión 1.2, OVAL en la versión 5.11.1, CPE en la versión 2.3, AI en la versión 1.1 y ARF en la versión 1.1.

¿Qué tipo de sistemas (software, sistemas operativos) están soportados por la herramienta?

La herramienta soporta principalmente sistemas operativos Linux, como CentOS, RHEL, Fedora, Debian y otros basados en Unix, con arquitectura x86_64. Además, permite auditar servicios de red, configuraciones del kernel, integridad de archivos, autenticación y permisos, incluyendo verificaciones sobre servicios en escucha, parámetros de SELinux, paquetes RPM, y configuraciones de usuarios y grupos.

¿Dónde se encuentran los ficheros CPE que definen estos vocabularios?

Los ficheros CPE necesarios para identificar plataformas y sistemas se encuentran en las rutas `/usr/share/openscap/schemas` para los esquemas SCAP y `/usr/share/openscap/cpe` para los ficheros CPE predeterminados.

¿Qué información se muestra sobre OVAL?

La herramienta muestra los objetos soportados junto con los probes asociados que realizan las evaluaciones. Por ejemplo, incluye verificaciones para variables de entorno, integridad de archivos, procesos del sistema, servicios en escucha, particiones y configuraciones específicas del kernel. Los probes asociados como `probe_environmentvariable`, `probe_rpmverifyfile` y `probe_selinuxboolean` permiten validar estos aspectos de manera automatizada.

Información del sistema

```
osboxes@vbox: /usr/share/xml/scap/ssg/content$ ^C
osboxes@vbox: /usr/share/xml/scap/ssg/content$ oscap info /usr/share/xml/scap/ssg/content/ssg-fedora-ds.xml
Document type: Source Data Stream
Imported: 2024-08-11T20:00:00

Stream: scap_org.open-scap_datastream_from_xccdf_ssg-fedora-xccdf.xml
Generated: (null)
Version: 1.3
Checklists:
  Ref-Id: scap_org.open-scap_cref_ssg-fedora-xccdf.xml
  Status: draft
  Generated: 2024-08-13
  Resolved: true
  Profiles:
    Title: CUSP - Common User Security Profile for Fedora Workstation
    Id: xccdf_org.ssgproject.content_profile_cusp_fedora
    Title: DSPP - Protection Profile for General Purpose Operating Systems
    Id: xccdf_org.ssgproject.content_profile_ospp
    Title: PCI-DSS v3.2.1 Control Baseline for Fedora
    Id: xccdf_org.ssgproject.content_profile_pci-dss
    Title: Standard System Security Profile for Fedora
    Id: xccdf_org.ssgproject.content_profile_standard
  Referenced check files:
    ssg-fedora-oval.xml
    system: http://oval.mitre.org/XMLSchema/oval-definitions-5
    ssg-fedora-ocil.xml
    system: http://scap.nist.gov/schema/ocil/2
Checks:
  Ref-Id: scap_org.open-scap_cref_ssg-fedora-oval.xml
  Ref-Id: scap_org.open-scap_cref_ssg-fedora-ocil.xml
  Ref-Id: scap_org.open-scap_cref_ssg-fedora-cpe-oval.xml
Dictionaries:
  Ref-Id: scap_org.open-scap_cref_ssg-fedora-cpe-dictionary.xml
osboxes@vbox: /usr/share/xml/scap/ssg/content$
```

La salida del comando `oscap info` da información sobre el archivo de contenido SCAP especificado. El fichero `ssg-fedora-ds.xml` contiene varios elementos como los metadatos del archivo, el tipo de documento (Source Data Stream) y la fecha de importación. Define perfiles de seguridad específicos para diferentes propósitos, como el perfil estándar para Fedora o el perfil PCI-DSS v3.2.1. También referencia archivos que contienen las reglas y verificaciones, como los archivos OVAL y OCIL, junto con esquemas estándar de SCAP y CPE. La última parte organiza los checks necesarios para auditar sistemas fedora siguiendo diferentes estándares.

Escaneo del Sistema

```
Rule      xccdf_org.ssgproject.content_rule_accounts_maximum_age_login_defs
Result    fail

Title     Set Password Minimum Age
Rule      xccdf_org.ssgproject.content_rule_accounts_minimum_age_login_defs
Result    fail

Title     Set Password Warning Age
Rule      xccdf_org.ssgproject.content_rule_accounts_password_warn_age_login_defs
Result    pass

Title     Verify All Account Password Hashes are Shadowed
Rule      xccdf_org.ssgproject.content_rule_accounts_password_all_shadowed
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     Prevent Login to Accounts With Empty Password
Rule      xccdf_org.ssgproject.content_rule_no_empty_passwords
Result    fail

Title     Verify No netrc Files Exist
Rule      xccdf_org.ssgproject.content_rule_no_netrc_files
Result    pass

Title     Verify Only Root Has UID 0
Rule      xccdf_org.ssgproject.content_rule_accounts_no_uid_except_zero
Result    pass

Title     Direct root Logins Not Allowed
Rule      xccdf_org.ssgproject.content_rule_no_direct_root_logins
Result    fail

Title     Restrict Serial Port Root Logins
Rule      xccdf_org.ssgproject.content_rule_restrict_serial_port_logins
Result    pass

Title     Restrict Virtual Console Root Logins
Rule      xccdf_org.ssgproject.content_rule_securetty_root_login_console_only
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
Result    pass

Title     Verify firewalld Enabled
Rule      xccdf_org.ssgproject.content_rule_service_firewalld_enabled
```

```
Title     Record attempts to alter time through adjtimex
Rule      xccdf_org.ssgproject.content_rule_audit_rules_time_adjtimex
Result    fail

Title     Record Attempts to Alter Time Through clock_settime
Rule      xccdf_org.ssgproject.content_rule_audit_rules_time_clock_settime
Result    fail

Title     Record attempts to alter time through settimeofday
Rule      xccdf_org.ssgproject.content_rule_audit_rules_time_settimeofday
Result    fail

Title     Record Attempts to Alter Time Through stime
Rule      xccdf_org.ssgproject.content_rule_audit_rules_time_stime
Result    fail

Title     Record Attempts to Alter the localtime File
Rule      xccdf_org.ssgproject.content_rule_audit_rules_time_watch_localtime
Result    fail

Title     Configure auditd to use audispd's syslog plugin
Rule      xccdf_org.ssgproject.content_rule_auditd_audispd_syslog_plugin_activated
Result    fail

Title     Configure auditd mail_acct Action on Low Disk Space
Rule      xccdf_org.ssgproject.content_rule_auditd_data_retention_action_mail_acct
Result    pass

Title     Configure auditd admin_space_left Action on Low Disk Space
Rule      xccdf_org.ssgproject.content_rule_auditd_data_retention_admin_space_left_action
Result    fail

Title     Configure auditd Max Log File Size
Rule      xccdf_org.ssgproject.content_rule_auditd_data_retention_max_log_file
Result    pass

Title     Configure auditd max_log_file_action Upon Reaching Maximum Log Size
Rule      xccdf_org.ssgproject.content_rule_auditd_data_retention_max_log_file_action
Result    pass

Title     Configure auditd Number of Logs Retained
Rule      xccdf_org.ssgproject.content_rule_auditd_data_retention_num_logs
Result    pass

Title     Configure auditd space_left Action on Low Disk Space
Rule      xccdf_org.ssgproject.content_rule_auditd_data_retention_space_left_action
Result    fail
```

Han fallado un total de 42 reglas de la lista predefinida:

1. **Verify and Correct File Permissions with RPMZ** verifica y corrige permisos de archivos instalados mediante RPM.
2. **Build and Test AIDE Database** configura y verifica el sistema AIDE para detectar cambios no autorizados en los archivos.
3. **Ensure PAM Displays Last Logon/Access Notification** configura PAM para mostrar la última fecha y hora de acceso en los inicios de sesión.
4. **Set Password Maximum Age** establece un límite de días máximo para que las contraseñas expiren.
5. **Set Password Minimum Age** define un mínimo de días antes de que una contraseña pueda cambiarse.
6. **Prevent Login to Accounts With Empty Passwords** evita que cuentas con contraseñas vacías puedan iniciar sesión.
7. **Direct root Logins Not Allowed** prohíbe que el usuario root inicie sesión directamente.
8. **Set Default Firewall Zone for Incoming Packets** configura una zona predeterminada para manejar paquetes entrantes con firewalld.
9. **Disable Kernel Support for USB via Bootloader Configuration** desactiva el soporte de USB desde el cargador de arranque para limitar ataques físicos.
10. **Disable SSH Root Login** desactiva el acceso SSH al usuario root para mayor seguridad.
11. **Enable Auditing for Processes Which Start Prior to the Audit Daemon** habilita la auditoría para procesos que inician antes del demonio auditd.
12. **Make the auditd Configuration Immutable** protege la configuración de auditd contra modificaciones.
13. **Record Events That Modify the System's Mandatory Access Controls** audita eventos que cambien los controles obligatorios de acceso al sistema.
14. **Ensure auditd Collects Information on Exporting to Media (successful)** audita operaciones de exportación de datos a dispositivos de almacenamiento.
15. **Record Events That Modify the System's Network Environment** registra modificaciones en la configuración de red del sistema.
16. **Record Attempts to Alter Process and Session Initiation Information** audita intentos de alterar la información de procesos o sesiones.
17. **Ensure auditd Collects System Administrator Actions** audita acciones realizadas por administradores del sistema.
18. **Record Events That Modify User/Group Information** audita cambios en usuarios o grupos del sistema.
19. **Record Events That Modify the System's Discretionary Access Controls (chmod)** audita cambios en permisos de archivos con chmod.

20. **Record Events That Modify the System's Discretionary Access Controls (fchmod)** audita cambios en permisos de archivos con fchmod.
21. **Record Events That Modify the System's Discretionary Access Controls (chown)** audita cambios de propiedad en archivos con chown.
22. **Record Events That Modify the System's Discretionary Access Controls (fchown)** audita cambios de propiedad en archivos con fchown.
23. **Record Events That Modify the System's Discretionary Access Controls (lchown)** audita cambios de propiedad en archivos con lchown.
24. **Ensure auditd Collects File Deletion Events by User** audita eventos donde usuarios eliminan archivos.
25. **Ensure auditd Collects Unauthorized Access Attempts to Files (unsuccessful)** registra intentos fallidos de acceso no autorizado a archivos.
26. **Ensure auditd Collects Information on Kernel Module Loading and Unloading** audita operaciones de carga y descarga de módulos del kernel.
27. **Record Attempts to Alter Logon and Logout Events** audita intentos de modificar eventos de inicio y cierre de sesión.
28. **Record Attempts to Alter Time Through adjtimex** audita modificaciones del tiempo del sistema usando adjtimex.
29. **Record Attempts to Alter Time Through clock_settime** registra cambios en el tiempo del sistema mediante clock_settime.
30. **Record Attempts to Alter Time Through settimeofday** monitorea cambios en el tiempo del sistema usando settimeofday.
31. **Record Attempts to Alter Time Through stime** audita cambios en el tiempo del sistema mediante stime.
32. **Record Attempts to Alter the localtime File** audita modificaciones en el archivo localtime.
33. **Configure auditd to use audispd's syslog plugin** asegura que auditd use el complemento syslog para registrar eventos.
34. **Configure auditd admin_space_left Action on Low Disk Space** configura auditd para actuar cuando queda poco espacio en disco.
35. **Configure auditd space_left Action on Low Disk Space** define la acción de auditd cuando el espacio en disco es crítico.
36. **Configure auditd Max Log File Size** establece un tamaño máximo para los archivos de registro de auditd.
37. **Configure auditd max_log_file_action Upon Reaching Maximum Log Size** configura auditd para actuar cuando el tamaño del archivo de registro es máximo.
38. **Configure auditd Number of Logs Retained** define cuántos registros antiguos de auditd deben mantenerse.
39. **Ensure auditd Collects Information About Discretionary Access Changes** audita modificaciones en atributos discrecionales de acceso, como setxattr.

- 40. **Ensure auditd Collects Privileged Command Executions** audita comandos ejecutados con privilegios elevados.
- 41. **Enable Cryptographic Policies in SSH** configura políticas de criptografía en SSH para mayor seguridad.
- 42. **Record Attempts to Export Sensitive Data** audita intentos de exportar datos sensibles desde el sistema.

Generación de informes y visualización

Una vez realizado el informe en formato HTML con el comando `oscap xccdf generate report` hemos tenido que copiarlo a una máquina donde si tengamos interfaz gráfica y podamos ver el archivo en un navegador. Esto lo hemos hecho mediante una copia por conexión SSH tal y como aprendimos el otro día en clase.

```
(kali㉿kali)-[~]  
$ scp -P 22 osboxes@10.0.2.15:/home/osboxes/scan-xccdf-rht_ccp-report.html /home/kali/  
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.  
ED25519 key fingerprint is SHA256:VDgH9ZENvqJqfcoqMUjRJydu7t561Fy57eioalonof4.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])?  
yes  
Warning: Permanently added '10.0.2.15' (ED25519) to the list of known hosts.  
osboxes@10.0.2.15's password:  
scan-xccdf-rht_ccp-report.html 100% 1546KB 60.8MB/s 00:00ers and b
```

El informe generado es este:

Guide to the Secure Configuration of Fedora

with profile **Standard System Security Profile for Fedora**

— This profile contains rules to ensure standard security baseline of a Fedora system.
Regardless of your system's workload all of these checks should pass.

The SCAP Security Guide Project
<https://www.open-scap.org/security-policies/scap-security-guide>

This guide presents a catalog of security-relevant configuration settings for Fedora. It is a rendering of content structured in the eXtensible Configuration Checklist Description Format (XCCDF) in order to support security automation. The SCAP content is available in the **scap-security-guide** package which is developed at <https://www.open-scap.org/security-policies/scap-security-guide>.

Providing system administrators with such guidance informs them how to securely configure systems under their control in a variety of network roles. Policy makers and baseline creators can use this catalog of settings, with its associated references to higher-level security control catalogs, in order to assist them in security baseline creation. This guide is a *catalog*, not a *checklist*, and satisfaction of every item is not likely to be possible or sensible in many operational scenarios. However, the XCCDF format enables granular selection and adjustment of settings, and their association with OVAL and OCIL content provides an automated checking capability. Transformations of this document, and its associated automated checking content, are capable of providing baselines that meet a diverse set of policy objectives. Some example XCCDF *Profiles*, which are selections of items that form checklists and can be used as baselines, are available with this guide. They can be processed, in an automated fashion, with tools that support the Security Content Automation Protocol (SCAP). The DISA STIG, which provides required settings for US Department of Defense systems, is one example of a baseline created from this guidance.

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

Evaluation Characteristics

Evaluation target	vbox
Benchmark URL	ssg-fedora-ds.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_FEDORA
Benchmark version	0.1.74
Profile ID	xccdf_org.ssgproject.content_profile_standard
Started at	2024-11-25T16:36:19-05:00
Finished at	2024-11-25T16:36:42-05:00
Performed by	osboxes
Test system	cpe:/a:redhat:openscap:1.4.0

CPE Platforms

- cpe:/o:fedoraproject:fedora:39
- cpe:/o:fedoraproject:fedora:40
- cpe:/o:fedoraproject:fedora:41
- cpe:/o:fedoraproject:fedora:42
- cpe:/o:fedoraproject:fedora:43
- cpe:/o:fedoraproject:fedora:44
- cpe:/o:fedoraproject:fedora:45

Addresses

- IPv4 127.0.0.1
- IPv4 10.0.2.15
- IPv6 0:0:0:0:0:0:1
- IPv6 fd00:0:0:0:a00:27ff:feb7:3b8a
- IPv6 fe80:0:0:0:a00:27ff:feb7:3b8a
- MAC 00:00:00:00:00:00
- MAC 08:00:27:B7:3B:8A

Compliance and Scoring

The target system did not satisfy the conditions of 45 rules! Please review rule results and consider applying remediation.

Rule results



Severity of failed rules



Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	43.606152	100.000000	<div><div></div></div> 43.61%

Rule Overview

☒ pass☒ fail☒ notchecked
☒ fixed☒ error☒ notapplicable
☒ informational☒ unknown

Group rules by:

Title	Severity	Result
▼ Guide to the Secure Configuration of Fedora 45x fail		
▼ System Settings 9x fail		
▼ Installing and Maintaining Software 2x fail		
▼ System and Software Integrity 2x fail		
▼ Software Integrity Checking 2x fail		
▼ Verify Integrity with RPM 1x fail		
Verify File Hashes with RPM	high	pass
Verify and Correct File Permissions with RPM	high	fail
▼ Verify Integrity with AIDE 1x fail		
Build and Test AIDE Database	medium	fail
▶ System Cryptographic Policies		
▶ Updating Software		
▼ Account and Access Control 5x fail		
▼ Protect Accounts by Configuring PAM 1x fail		
Ensure PAM Displays Last Logon/Access Notification	low	fail
▼ Protect Accounts by Restricting Password-Based Login 4x fail		
▶ Set Account Expiration Parameters		
▼ Set Password Expiration Parameters 2x fail		
Set Password Maximum Age	medium	fail
Set Password Minimum Age	medium	fail
Set Password Warning Age	medium	pass
▼ Verify Proper Storage and Existence of Password Hashes 1x fail		

El informe indica que el sistema presenta un nivel de cumplimiento bajo con los estándares de seguridad establecidos ya que de las reglas evaluadas, 29 han sido aprobadas y 45 han fallado. Entre las que han fallado se incluyen 39 de gravedad media, 3 de gravedad alta y 1 de gravedad baja, lo que resalta la presencia de riesgos significativos que requieren atención prioritaria.

Las principales áreas de los problemas están relacionadas con configuraciones básicas del sistema, como permisos de archivos, políticas de contraseñas, la configuración del firewall y la falta de herramientas para monitorear cambios no autorizados, como AIDE.

Además, hay problemas específicos en el control de acceso de usuarios, como la presencia de contraseñas vacías o configuraciones inseguras en los inicios de sesión.

Con una puntuación general de 43.61 sobre 100, el sistema necesita ajustes para mejorar su seguridad.

Set Password Maximum Age

Rule ID	xccdf_org.ssgproject.content_rule_accounts_maximum_age_login_defs																													
Result	fail																													
Multi-check rule	no																													
OVAL Definition ID	oval:ssg-accounts_maximum_age_login_defs:def:1																													
Time	2024-11-25T16:36:33-05:00																													
Severity	medium																													
References:	<table><tr><td>cis-csc</td><td>1, 12, 15, 16, 5</td></tr><tr><td>cjis</td><td>5.6.2.1</td></tr><tr><td>cobit5</td><td>DSS05.04, DSS05.05, DSS05.07, DSS05.10, DSS06.03, DSS06.10</td></tr><tr><td>cui</td><td>3.5.6</td></tr><tr><td>disa</td><td>CCI-000199</td></tr><tr><td>isa-62443-2009</td><td>4.3.3.2.2, 4.3.3.5.1, 4.3.3.5.2, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.2, 4.3.3.7.4</td></tr><tr><td>isa-62443-2013</td><td>SR 1.1, SR 1.10, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 2.1</td></tr><tr><td>ism</td><td>0418, 1055, 1402</td></tr><tr><td>iso27001-2013</td><td>A.18.1.4, A.7.1.1, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3</td></tr><tr><td>nist</td><td>IA-5(f), IA-5(1)(d), CM-6(a)</td></tr><tr><td>nist-csf</td><td>PR.AC-1, PR.AC-6, PR.AC-7</td></tr><tr><td>pcidss</td><td>Req-8.2.4</td></tr><tr><td>os-srg</td><td>SRG-OS-000076-GPOS-00044</td></tr><tr><td>pcidss4</td><td>8.3.9</td></tr></table>		cis-csc	1, 12, 15, 16, 5	cjis	5.6.2.1	cobit5	DSS05.04, DSS05.05, DSS05.07, DSS05.10, DSS06.03, DSS06.10	cui	3.5.6	disa	CCI-000199	isa-62443-2009	4.3.3.2.2, 4.3.3.5.1, 4.3.3.5.2, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.2, 4.3.3.7.4	isa-62443-2013	SR 1.1, SR 1.10, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 2.1	ism	0418, 1055, 1402	iso27001-2013	A.18.1.4, A.7.1.1, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3	nist	IA-5(f), IA-5(1)(d), CM-6(a)	nist-csf	PR.AC-1, PR.AC-6, PR.AC-7	pcidss	Req-8.2.4	os-srg	SRG-OS-000076-GPOS-00044	pcidss4	8.3.9
cis-csc	1, 12, 15, 16, 5																													
cjis	5.6.2.1																													
cobit5	DSS05.04, DSS05.05, DSS05.07, DSS05.10, DSS06.03, DSS06.10																													
cui	3.5.6																													
disa	CCI-000199																													
isa-62443-2009	4.3.3.2.2, 4.3.3.5.1, 4.3.3.5.2, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.2, 4.3.3.7.4																													
isa-62443-2013	SR 1.1, SR 1.10, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 2.1																													
ism	0418, 1055, 1402																													
iso27001-2013	A.18.1.4, A.7.1.1, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3																													
nist	IA-5(f), IA-5(1)(d), CM-6(a)																													
nist-csf	PR.AC-1, PR.AC-6, PR.AC-7																													
pcidss	Req-8.2.4																													
os-srg	SRG-OS-000076-GPOS-00044																													
pcidss4	8.3.9																													
Description	<p>To specify password maximum age for new accounts, edit the file <code>/etc/login.defs</code> and add or correct the following line:</p> <div>PASS_MAX_DAYS 90</div> <p>A value of 180 days is sufficient for many environments. The DoD requirement is 60. The profile requirement is 90.</p>																													
Rationale	<p>Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system passwords could be compromised.</p> <p>Setting the password maximum age ensures users are required to periodically change their passwords. Requiring shorter password lifetimes increases the risk of users writing down the password in a convenient location subject to physical compromise.</p>																													
<div>Remediation Shell script</div>																														
<div>Remediation Ansible snippet</div>																														

Se puede ver en detalle cada regla con un panel que permite ver varios aspectos: la gravedad de la regla (en este caso, media), referencias normativas asociadas (como NIST, ISO27001, y PCI DSS), una descripción de cómo solucionar el problema editando el archivo mencionado, y la justificación para aplicar el cambio. También da opciones automatizadas para corregir la configuración usando scripts.

Solución de problemas

Lo primero fue hacer el script que remedia los errores de configuración del sistema con el comando oscan cxxdf generate fix

```
osboxes@localhost:~$ ls
hola.txt remediation-script.sh scan-ccxdf-rht_ccp-report.html
```

Una vez teniendo esto, lo ejecutamos:

```
osboxes@localhost:~$ sudo ./remediation-script.sh
Remediating rule 1/76: 'ccxdf_org.ssgproject.content_rule_rpm_verify_hashes'
Remediating rule 2/76: 'ccxdf_org.ssgproject.content_rule_rpm_verify_permissions'
Remediating rule 3/76: 'ccxdf_org.ssgproject.content_rule_aide_build_database'
Fedora 40 - x86_64 - Updates                                86 kB/s | 25 kB    00:00
Fedora 40 - x86_64 - Updates                                2.7 MB/s | 4.1 MB  00:01
Last metadata expiration check: 0:00:02 ago on Sun 01 Dec 2024 02:35:31 PM EST.
Dependencies resolved.
=====
Package                               Architecture      Version           Repository        Size
=====
Installing:
aide                                   x86_64            0.18.6-4.fc40     fedora            144 k
=====
Transaction Summary
=====
Install 1 Package

Total download size: 144 k
Installed size: 352 k
Downloading Packages:
aide-0.18.6-4.fc40.x86_64.rpm                                499 kB/s | 144 kB  00:00
-----
Total                                                     193 kB/s | 144 kB  00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing                :
  Installing               : aide-0.18.6-4.fc40.x86_64
  Running scriptlet        : aide-0.18.6-4.fc40.x86_64
Installed:
  aide-0.18.6-4.fc40.x86_64
Complete!

fix for info rule 'ccxdf_org.ssgproject.content_rule_no_mount_files' IS MISSING!
Remediating rule 21/76: 'ccxdf_org.ssgproject.content_rule_accounts_no_uid_except_zero'
Remediating rule 22/76: 'ccxdf_org.ssgproject.content_rule_no_direct_root_logins'
Remediating rule 23/76: 'ccxdf_org.ssgproject.content_rule_restrict_serial_port_logins'
Remediating rule 24/76: 'ccxdf_org.ssgproject.content_rule_securetty_root_login_console_only'
Remediating rule 25/76: 'ccxdf_org.ssgproject.content_rule_accounts_root_path_dirs_no_write'
FIX FOR THIS RULE 'ccxdf_org.ssgproject.content_rule_accounts_root_path_dirs_no_write' IS MISSING!
Remediating rule 26/76: 'ccxdf_org.ssgproject.content_rule_service_firewalld_enabled'
Remediating rule 27/76: 'ccxdf_org.ssgproject.content_rule_set_firewalld_default_zone'
FIX FOR THIS RULE 'ccxdf_org.ssgproject.content_rule_set_firewalld_default_zone' IS MISSING!
Remediating rule 28/76: 'ccxdf_org.ssgproject.content_rule_file_ownership_binary_dirs'
FIX FOR THIS RULE 'ccxdf_org.ssgproject.content_rule_file_ownership_binary_dirs' IS MISSING!
Remediating rule 29/76: 'ccxdf_org.ssgproject.content_rule_file_ownership_library_dirs'
Remediating rule 30/76: 'ccxdf_org.ssgproject.content_rule_file_permissions_binary_dirs'
FIX FOR THIS RULE 'ccxdf_org.ssgproject.content_rule_file_permissions_binary_dirs' IS MISSING!
Remediating rule 31/76: 'ccxdf_org.ssgproject.content_rule_file_permissions_library_dirs'
Remediating rule 32/76: 'ccxdf_org.ssgproject.content_rule_grub2_nousb_argument'
Remediating rule 33/76: 'ccxdf_org.ssgproject.content_rule_service_chronyd_or_ntpd_enabled'
Remediating rule 34/76: 'ccxdf_org.ssgproject.content_rule_chronyd_or_ntpd_specify_remote_server'
Remediating rule 35/76: 'ccxdf_org.ssgproject.content_rule_sshd_disable_empty_passwords'
Remediating rule 36/76: 'ccxdf_org.ssgproject.content_rule_sshd_disable_root_login'
Remediating rule 37/76: 'ccxdf_org.ssgproject.content_rule_service_auidtd_enabled'
Remediating rule 38/76: 'ccxdf_org.ssgproject.content_rule_grub2_audit_argument'
Remediating rule 39/76: 'ccxdf_org.ssgproject.content_rule_audit_rules_immutable'
Remediating rule 40/76: 'ccxdf_org.ssgproject.content_rule_audit_rules_mac_modification'
Remediating rule 41/76: 'ccxdf_org.ssgproject.content_rule_audit_rules_media_export'
Remediating rule 42/76: 'ccxdf_org.ssgproject.content_rule_audit_rules_networkconfig_modification'
Remediating rule 43/76: 'ccxdf_org.ssgproject.content_rule_audit_rules_session_events'
Remediating rule 44/76: 'ccxdf_org.ssgproject.content_rule_audit_rules_sysadmin_actions'
Remediating rule 45/76: 'ccxdf_org.ssgproject.content_rule_audit_rules_usergroup_modification'
FIX FOR THIS RULE 'ccxdf_org.ssgproject.content_rule_audit_rules_usergroup_modification' IS MISSING!
Remediating rule 46/76: 'ccxdf_org.ssgproject.content_rule_file_ownership_var_log_audit'
Remediating rule 47/76: 'ccxdf_org.ssgproject.content_rule_audit_rules_dac_modification_chmod'
Remediating rule 48/76: 'ccxdf_org.ssgproject.content_rule_audit_rules_dac_modification_chown'
Remediating rule 49/76: 'ccxdf_org.ssgproject.content_rule_audit_rules_dac_modification_fchmod'
Remediating rule 50/76: 'ccxdf_org.ssgproject.content_rule_audit_rules_dac_modification_fchmodat'
Remediating rule 51/76: 'ccxdf_org.ssgproject.content_rule_audit_rules_dac_modification_fchown'
Remediating rule 52/76: 'ccxdf_org.ssgproject.content_rule_audit_rules_dac_modification_fchownat'
Remediating rule 53/76: 'ccxdf_org.ssgproject.content_rule_audit_rules_dac_modification_fremovexattr'
Remediating rule 54/76: 'ccxdf_org.ssgproject.content_rule_audit_rules_dac_modification_fsetxattr'
Remediating rule 55/76: 'ccxdf_org.ssgproject.content_rule_audit_rules_dac_modification_lchown'
Remediating rule 56/76: 'ccxdf_org.ssgproject.content_rule_audit_rules_dac_modification_lremovexattr'
Remediating rule 57/76: 'ccxdf_org.ssgproject.content_rule_audit_rules_dac_modification_lsetxattr'
Remediating rule 58/76: 'ccxdf_org.ssgproject.content_rule_audit_rules_dac_modification_removexattr'
Remediating rule 59/76: 'ccxdf_org.ssgproject.content_rule_audit_rules_dac_modification_setxattr'
```

Tras remediar las vulnerabilidades, repetimos la validación contra la política, generamos el archivo xml y de él generamos de nuevo el html para poder ver mejor los resultados.

Lo copiamos mediante SSH a nuestra máquina con interfaz y el resultado es:

Evaluation Characteristics

Evaluation target	localhost
Benchmark URL	/usr/share/xml/scap/ssg/content/ssg-fedora-ds.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_FEDORA
Benchmark version	0.1.74
Profile ID	xccdf_org.ssgproject.content_profile_standard
Started at	2024-12-01T14:47:58-05:00
Finished at	2024-12-01T14:48:19-05:00
Performed by	osboxes
Test system	cpe:/a:redhat:openscap:1.4.0

CPE Platforms

- cpe:/o:fedoraproject:fedora:39
- cpe:/o:fedoraproject:fedora:40
- cpe:/o:fedoraproject:fedora:41
- cpe:/o:fedoraproject:fedora:42
- cpe:/o:fedoraproject:fedora:43
- cpe:/o:fedoraproject:fedora:44
- cpe:/o:fedoraproject:fedora:45

Addresses

- IPv4 127.0.0.1
- IPv4 10.0.2.15
- IPv6 0:0:0:0:0:0:1
- IPv6 fe80:0:0:0:a00:27ff:feb7:3b8a
- MAC 00:00:00:00:00:00
- MAC 08:00:27:B7:3B:8A

Compliance and Scoring

The target system did not satisfy the conditions of 34 rules! Furthermore, the results of 2 rules were inconclusive. Please review rule results and consider applying remediation.

Rule results



Severity of failed rules



Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	52.476852	100.000000	52.48%

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 Fedora 34x fail 2x error		
▼ System Settings 3x fail		
▼ Installing and Maintaining Software 1x fail		

En el nuevo informe generado tras la aplicación del script se observa una mejora en el cumplimiento de las reglas. Inicialmente, el sistema tenía 29 reglas aprobadas y 45 fallidas, con una puntuación de cumplimiento del 43.61%. Después de aplicar el script de mejoras, el sistema pasó a tener 38 reglas aprobadas, 34 fallidas y 2 marcadas como no concluidas, alcanzando una puntuación del 52.48%. Esto representa un avance, pero todavía existen áreas críticas que requieren cambios.

Los fallos restantes probablemente estén relacionados con configuraciones más complejas o aspectos que el script no puede abordar de forma automatizada, por lo que como conclusión podemos decir que el uso de herramientas como OpenSCAP es eficaz para abordar problemas comunes de seguridad, pero no puede garantizar que se cumplan todas las reglas por lo que no ofrece una seguridad total.

