





Me llamo Diego

- ♦ Soy funcionario TIC
- Llevo tiempo engrasando y automatizando procesos

Y voy a hablar sobre algo que no es nuevo, pero...



¿De qué voy a hablar?









MANTENIBILIDAD ESCALABILIDAD LEGIBILIDAD TRAZABILIDAD

¿De dónde surge la idea?

- Auditoría del ENS sobre un sistema de la familia RHEL
- ¿Cómo afrontamos la auditoría?



Objetivo: sistema auditado y bastionado











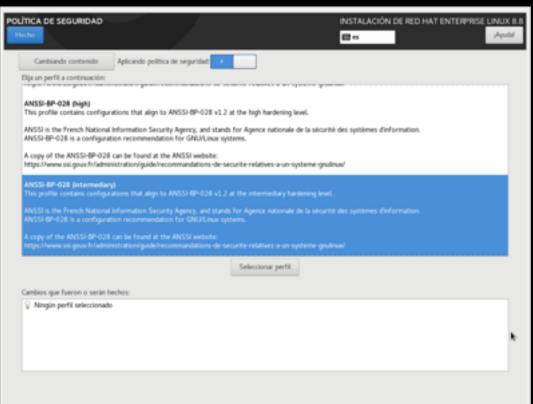
Tracklist #1 Fichero de políticas de seguridad

Tracklist #2 **Enfoque imperativo** (shellscripts)

Tracklist #3 **Enfoque declarativo** → Ansible

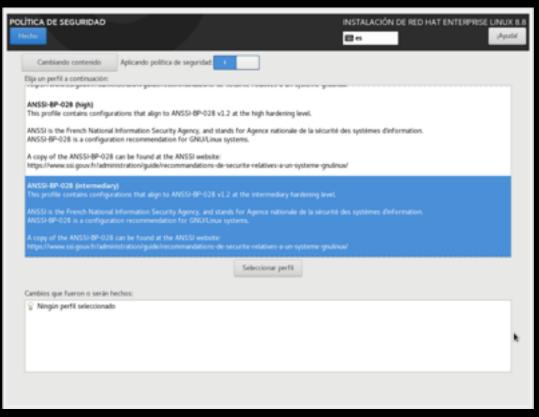
Fichero de políticas de seguridad





Fichero de políticas de seguridad







```
1 k7xml version="1.0"7>
        ds:data-stream-collection xmlms:cat="urm:casis:namen:tc:entity:xmlmn:xml:catalog" xmlmn:cpe-dict="http://cpe.mitre.org/dictionary/2.0" xmlmn:cpe-lang="http
           <ds:data-stream id="scap_org.open-scap_datastream_from_sccdf_sng-old-xccdf_xml" scap-version="1.3" use-case="OTHER">
                 <ds:component-ref id-"scap_org.open-scap_cref_ssg-ol8-cpe-dictionary.xml" xlink:href="#scap_org.open-scap_comp_ssg-ol8-cpe-dictionary.xml">
                        -(cat:uri name="ssg-ol8-cpe-oval.mml" uri="#scap_org.open-scap_cref_ssg-ol8-cpe-oval.mml"/>
              (/ds:component-ref)
(/ds:dictionaries)
              odsschecklists)
                                    mt-ref 10-"scap_org.open-scap_cref_ssg-o38-xcc0f.xml" xlink:href-"#scap_org.open-scap_comp_ssg-o18-xcc0f.xml">
                        ccat;uri name="ssg.olf.ocil.xml" uri="fscap.org.open-scap_cref_ssg.olf.ocil.xml"/>
ccat;uri name="ssg.olf.ope.ocil.xml" uri="fscap.org.open-scap_cref_ssg.olf.ope.ocil.xml"/>
                         ccatturl name="security-oval-com.oracle.elsa-olf.onf.bo2" url="fscap_org.open-scap_cref_security-oval-com.oracle.elsa-olf.onf.bo2"/>
                 </dischecklists>
                 <ds:component-ref id="scap_org.open-scap_cref_ssg-olf-oval.xml" xlink:href="fscap_org.open-scap_comp_ssg-olf-oval.xml"/>
                 <ds:component-ref id="scap_org.open-scap_cref_ssg-ol8-ocil.xml" xlink:href="#scap_org.open-scap_comp_ssg-ol8-ocil.xml"/>
                  cds:component-ref id="scap_org.open-scap_cref_ssg-old-cpe-oval.xml" xlink:href="%scap_org.open-scap_comp_ssg-old-cpe-oval.xml"/>
                 <ds:component-ref id="scap org.open-scap cref security-sval-com.oracle.elsa-ol8.xml.bo2" slink:href="https://linux.oracle.com/security/sval/com.oracle.</p>
           -ds:component id-"scap_org.open-scap_comp_ssg-ol8-cpe-dictionary.xml" timestamp="2024-01-30714:04:56">
                     orpe-dict:title xml:lang="en-us":Oracle Linux 8c/ope-dict:title>
                     ccpe-dict:check href="ssg-el8-cpe-oval.xml" system="http://oval.mitre.org/XMLSchema/oval-definitions-5"loval:ssg-installed_05_is_el8_family:def:1c/c
                             ent Ed-"scap_org.open-scap_comp_ssg-ol8-xccdf_xml" timestamp="2024-01-30714:04:54">
              cocdf-1.2:Benchmark 16~scc0f_org.ssgsroject.content benchmark_OL-8" resolved-"true" style="SCAP_1.2" xsi:schemalocation="http://checklists.mist.gov/xc
                 cxcodf-1.2:status date="2024-01-30">draftc/xccdf-1.2:status>
                  cxcodf-1.2:descriptionsThis guide presents a catalog of security-relevant
       content structured in the efftensible Configuration Checklist Description Format (MCCDF)
       in order to support security automation. The SCAP content is
       is available in the chtml:codesocrap-security-guidec/html:codes package which is developed at
              dital:a href-"https://www.open-scap.org/security-policies/scap-security-guide":https://www.open-scap.org/security-policies/scap-security-guidec/httpl://www.open-scap.org/security-policies/scap-security-guidec/https://www.open-scap.org/security-policies/scap-security-guidec/https://www.open-scap.org/security-policies/scap-security-guidec/https://www.open-scap.org/security-policies/scap-security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/https://www.open-scap.org/security-guidec/h
       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
```

Enfoque imperativo (shellscripts)

```
echo " ANTES DE COMENZAR SE CREARÁ UN BACKUP DE LA CARPETA PAM.D EN EL DIRECTORIO /etc/pam.d backup[fecha/hora]"
    echo " NO DETENGA EL SCRIPT, NI HAGA NADA HASTA QUE EL SCRIPT FINALICE"
    echo " EN CASO DE DETENCIÓN DEL SCRIPT; VUELVA A EJECUTARLO ANTES DE REINICIAR HASTA QUE FINALICE EL PROCESO CORRECTAMENTE
    read -p "Pulse ENTER para continuar o Ctrl + C para cancelar...."
    tiempo=$( date +"%d-%b-%y-%H:%M:%S" )
11 mkdir /etc/pam.d bakup $tiempo
12 cp -r /etc/pam.d/* /etc/pam.d bakup $tiempo
14 var1=$(cat /etc/pam.d/password-auth | grep "pam faillock.so")
15 if [ -z "$var1" ]
17 sudo sed -i '8i auth
                                required
                                                            pam_faillock.so preauth silent audit deny=8 even_deny_root unlock_time=3600 /etc/pam.d/password-auth
18 sudo sed -1 '101 auth
                                [default=die]
                                                            pam faillock.so authfail deny-8 even deny root unlock time-3600' /etc/pam.d/password-auth
19 sudo sed -i '15i account
                              required
                                                            pam_faillock.so' /etc/pam.d/password-auth
                                                           pam pwhistory.so debug use authtok remember-25 retry-8' /etc/pam.d/password-auth
20 sudo sed -i '23i password requisite
21 sudo sed -i -e 's/pam_pwquality.so try_first_pass local_users_only */pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=/' /etc/pam.d/password-auth
26 var2=$(cat /etc/pam.d/system-auth | grep "pam_faillock.so")
27 if [ -z "$var2" ]
                                                            pam_faillock.so preauth silent audit deny=8 even_deny_root unlock_time=3600' /etc/pam.d/system-auth
    sudo sed -1 '91 auth
                                required
                                [default=die]
    sudo sed -i '11i auth
                                                            pam_faillock.so authfail deny=8 even_deny_root unlock_time=3600' /etc/pam.d/system-auth
31 sudo sed -i '16i account
                                required
                                                            pam faillock.so' /etc/pam.d/system-auth
32 sudo sed -i '24i password requisite
                                                            pam pwhistory.so debug use authtok remember-25 retry-8 /etc/pam.d/system-auth
33 sudo sed -i -e 's/pam pwquality.so try first pass local users only */pam pwquality.so try first pass local users only retry=3 authtok type=/' /etc/pam.d/system-auth
    echo "Ya se encuentra configurado /etc/pam.d/system-auth"
    echo " >>>>>>EL PROCESO A FINALIZADO CORRECTAMENTE<<<<<<<
    read -p "Pulse ENTER y el sistema se reiniciará automáticamente en 1 minuto, guarde los archivos que tenga abiertos antes de continuar......"
```

Enfoque declarativo



```
- name: Configurar pam faillock.so
       become: true
       community.general.pamd:
        backup: true
        name: "{{ item }}"
         type: auth
         control: required
         module path: pam deny.so
         state: after
         new_type: auth
        new control: required
         new_module_path: pam_faillock.so
        module_arguments: "preauth silent audit deny=8 even_deny_root unlock_time={{ UNLOCK_TIME }}"

    password-auth

    system-auth

        - Reiniciar host
     - name: Actualización pam_faillock.so
       become: true
       community.general.pamd:
        backup: true
         name: '{{ item }}'
        type: auth
        control: required
        module path: pam faillock.so
        module_arguments: "preauth silent audit deny-8 even_deny_root unlock_time-{{ UNLOCK_TIME }}"
        - password-auth

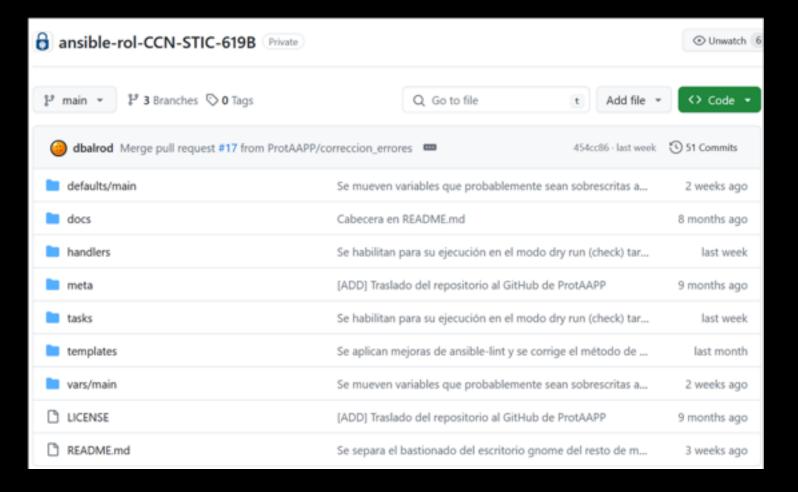
    system-auth

    Reiniciar_host

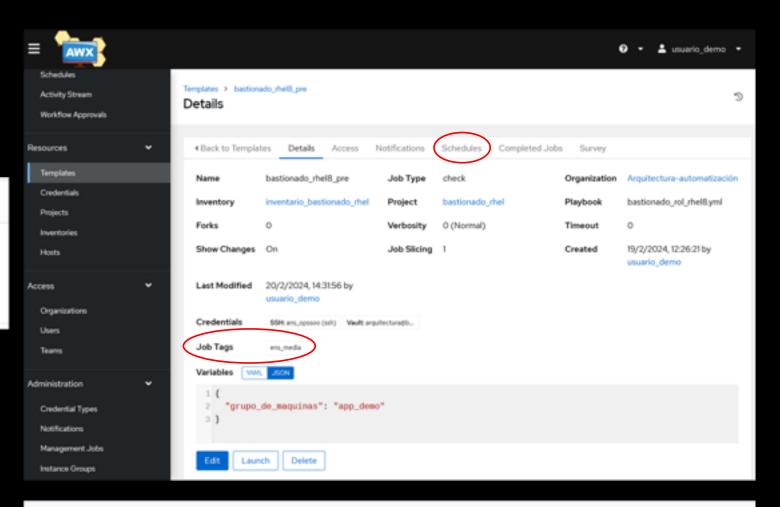
34
```

¿Qué se ha hecho?





Caso de uso



ansible-playbook my_playbook_con_rol_CCN-STIC-619B.yml -i hosts_categoria_media_ENS --tag ens_media

Caso de éxito

Cumplimiento (41,22%)

41,22%



Porcentaje de elementos en relación al control configurados adecuadamente. No es necesario realizar ninguna acción.



Porcentaje de elementos en relación al control cuya configuración no es la esperada pero no es considerada incorrecta. Es necesaria la revisión del informe técnico.



Porcentaje de elementos en relación al control con discrepancias detectadas. Implica la revisión del informe técnico y la aplicación de medidas correctoras para su subsanación.

Resultados

Contraseña de root:

Permisos sobre partición de inicio:

Contraseña de Grub: Parámetros GNOME:

Usuarios con UID 0:

Usuarios con UID U.

Bloqueo de cuenta: Shells de usuarios:

Permisos sobre home:

Registro de actividad - Configuración auditd:

Banner:

Usuarios sin contraseñas:

Volcados de núcleo:

Registro de actividad - Reglas de auditoria:

Complejidad de contraseñas:

Servicios:

Caducidad de contraseñas:

Contraseña configurada

Los parámetros no están configurados

Contraseña no configurada

El sistema Operativo no tiene entorno Gráfico GNOME

No existen usuarios con UIDO

Los parámetros no están configurados

Revisar por auditor

Parámetros configurados correctamente

Parámetros configurados correctamente

Revisar por auditor

No existen usuarios sin contraseña

Los parâmetros no están configurados correctamente

Revisar por auditor

Los parámetros no están configurados

Revisar por auditor

Los parámetros no están configurados correctamente





Caso de éxito

Cumplimiento (41,22%)

41,22%



Porcentaje de elementos en relación al control configurados adecuadamente. No es necesario realizar ninguna acción.



Porcentaje de elementos en relación al control cuya configuración no es la esperada pero no es considerada incorrecta. Es necesaria la revisión del informe técnico.



Porcentaje de elementos en relación al control con discrepancias detectadas. Implica la revisión del informe técnico y la aplicación de medidas correctoras para su subsanación.

Resultados

Contraseña de root:

Permisos sobre partición de inicio:

Contraseña de Grub:

Parámetros GNOME:

Usuarios con UID 0:

Bloqueo de cuenta:

Shells de usuarios:

Permisos sobre home:

Registro de actividad - Configuración auditd:

Banner:

Usuarios sin contraseñas:

Volcados de núcleo:

Registro de actividad - Reglas de auditoría:

Complejidad de contraseñas:

Servicios:

Caducidad de contraseñas:

Contraseña configurada

Los parámetros no están configurados

Contraseña no configurada

El sistema Operativo no tiene entorno Gráfico GNOME

No existen usuarios con UIDO

Los parámetros no están configurados

Revisar por auditor

Parámetros configurados correctamente

Parámetros configurados correctamente

Revisar por audito

No existen usuarios sin contraseña

Los parâmetros no están configurados correctamente

Revisar por auditor

Los parámetros no están configurados

Revisar por auditor

Los parâmetros no están configurados correctamente

Cumplimiento (100%)

100%



Porcentaje de elementos en relación al control configurados adecuadamente. No es necesario realizar ninguna acción.



Porcentaje de elementos en relación al control cuya configuración no es la esperada pero no es considerada incorrecta. Es necesaria la revisión del informe técnico.



Porcentaje de elementos en relación al control con discrepancias detectadas. Implica la revisión del informe técnico y la aplicación de medidas correctoras para su subsanación.

Resultados

Contraseña de root:

Permisos sobre partición de inicio:

Contraseña de Grub:

Parámetros GNOME:

Usuarios con UID 0:

Bloqueo de cuenta:

Shells de usuarios:

Permisos sobre home:

Registro de actividad - Configuración auditd:

Banner:

Usuarios sin contraseñas:

Volcados de núcleo:

iditoria:

Contraseña configurada

Parâmetros configurados correctamente

Contraseña configurada

El sistema Operativo no tiene entorno Gráfico GNOME

No existen usuarios con UIDO

Parámetros configurados correctamente

Revisar por auditor

Parámetros configurados correctamente

Parámetros configurados correctamente

Tiene un banner configurado

No existen usuarios sin contraseña

Parámetros configurados correctamente

Revisar por auditor

Parámetros configurados correctamente

Revisar por audito

Parámetros configurados correctamente





¿Quién es nuestro superhéroe?



Conclusiones

- ♦ La Idempotencia permite:
 - Auditoría continua y bastionado continuo
 - Legibilidad y trazabilidad
- Rol de Ansible con modelo de gestión de software libre
 - Mantenibilidad y escalabilidad
 - **→** KI77
 - → Fail Fast
 - → Pareto



Ansible es la herramienta pero lo importante son los procesos

DEMO



MUCHAS CRACIAS



Highway to RHEL [AC/BC]

Auditoría, fortificación y remediación perpetua automatizada de sistemas mediante Infraestructure as Code (IaC)

https://github.com/ProtAAPP/ansible-rol-CCN-STIC-619B.git

