

A dark stage with several spotlights shining down from above. In the center, there is a drum set on a raised platform. To the left and right of the drum set are two tall, dark, rectangular structures that look like server racks or storage units. The overall atmosphere is dramatic and high-tech.

Highway to RHEL (AC/BC)

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

Sobre mí



Me llamo Diego

- ◆ **Soy funcionario TIC**
- ◆ **Llevo tiempo engrasando y automatizando procesos**

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



@diegobr



¿De qué voy a hablar?



AC⚡BC

IDEM⚡POTENCIA

**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

siempre



Tracklist #1

Fichero de políticas
de seguridad



Tracklist #2

Enfoque imperativo
(shellscripts)



Tracklist #3

Enfoque declarativo
→ Ansible

Fichero de políticas de seguridad



POLÍTICA DE SEGURIDAD INSTALACIÓN DE RED HAT ENTERPRISE LINUX 8.8

[Hecho](#) es [Ayuda](#)

[Cambiando contenido](#) [Aplicando política de seguridad](#) ☒

Elija un perfil a continuación:

ANSSI-BP-028 (high)
This profile contains configurations that align to ANSSI-BP-028 v1.2 at the high hardening level.

ANSSI is the French National Information Security Agency, and stands for Agence nationale de la sécurité des systèmes d'information. ANSSI-BP-028 is a configuration recommendation for GNU/Linux systems.

A copy of the ANSSI-BP-028 can be found at the ANSSI website:
<https://www.ssi.gouv.fr/administration/guide/recommandations-de-securite-relatives-a-un-systeme-gnu/linux/>

ANSSI-BP-028 (intermediary)
This profile contains configurations that align to ANSSI-BP-028 v1.2 at the intermediary hardening level.

ANSSI is the French National Information Security Agency, and stands for Agence nationale de la sécurité des systèmes d'information. ANSSI-BP-028 is a configuration recommendation for GNU/Linux systems.

A copy of the ANSSI-BP-028 can be found at the ANSSI website:
<https://www.ssi.gouv.fr/administration/guide/recommandations-de-securite-relatives-a-un-systeme-gnu/linux/>

[Seleccionar perfil](#)

Cambios que fueron o serán hechos:

Ningún perfil seleccionado

Fichero de políticas de seguridad



POLÍTICA DE SEGURIDAD INSTALACIÓN DE RED HAT ENTERPRISE LINUX 8.8

Hecho es Ayuda

Elija un perfil a continuación:

ANSSI-BP-028 (high)
This profile contains configurations that align to ANSSI-BP-028 v1.2 at the high hardening level.

ANSSI is the French National Information Security Agency, and stands for Agence nationale de la sécurité des systèmes d'information. ANSSI-BP-028 is a configuration recommendation for GNU/Linux systems.

A copy of the ANSSI-BP-028 can be found at the ANSSI website:
<https://www.ssi.gov.fr/administration/guide/recommandations-de-securite-relatives-a-un-systeme-gnu/linux/>

ANSSI-BP-028 (intermediary)
This profile contains configurations that align to ANSSI-BP-028 v1.2 at the intermediary hardening level.

ANSSI is the French National Information Security Agency, and stands for Agence nationale de la sécurité des systèmes d'information. ANSSI-BP-028 is a configuration recommendation for GNU/Linux systems.

A copy of the ANSSI-BP-028 can be found at the ANSSI website:
<https://www.ssi.gov.fr/administration/guide/recommandations-de-securite-relatives-a-un-systeme-gnu/linux/>

Cambios que fueron o serán hechos:

Ningún perfil seleccionado

```
1 <?xml version="1.0"?>
2 <ds:data-stream-collection xmlns:cat="urn:nasis:names:tc:entity:xmlns:xml:catalog" xmlns:cpe-dict="http://cpe.mitre.org/dictionary/2.0" xmlns:cpe-lang="http
3 <ds:data-stream id="scap_org.open-scap_datastream_from_xccdf_ssg-018-xccdf.xml" scap-version="1.3" use-case="OTHER">
4   <ds:dictionary>
5     <ds:component-ref id="scap_org.open-scap_cref_ssg-018-cpe-dictionary.xml" xlink:href="#scap_org.open-scap_comp_ssg-018-cpe-dictionary.xml">
6       <cat:catalog>
7         <cat:url name="sg-018-cpe-oval.xml" uri="#scap_org.open-scap_cref_ssg-018-cpe-oval.xml"/>
8       </cat:catalog>
9     </ds:component-ref>
10  </ds:dictionary>
11  <ds:checklists>
12    <ds:component-ref id="scap_org.open-scap_cref_ssg-018-xccdf.xml" xlink:href="#scap_org.open-scap_comp_ssg-018-xccdf.xml">
13      <cat:catalog>
14        <cat:url name="sg-018-oval.xml" uri="#scap_org.open-scap_cref_ssg-018-oval.xml"/>
15        <cat:url name="sg-018-ocil.xml" uri="#scap_org.open-scap_cref_ssg-018-ocil.xml"/>
16        <cat:url name="sg-018-cpe-oval.xml" uri="#scap_org.open-scap_cref_ssg-018-cpe-oval.xml"/>
17        <cat:url name="security-oval-com.oracle.elsa-018.xml.bz2" uri="#scap_org.open-scap_cref_security-oval-com.oracle.elsa-018.xml.bz2"/>
18      </cat:catalog>
19    </ds:component-ref>
20  </ds:checklists>
21  <ds:checks>
22    <ds:component-ref id="scap_org.open-scap_cref_ssg-018-oval.xml" xlink:href="#scap_org.open-scap_comp_ssg-018-oval.xml"/>
23    <ds:component-ref id="scap_org.open-scap_cref_ssg-018-ocil.xml" xlink:href="#scap_org.open-scap_comp_ssg-018-ocil.xml"/>
24    <ds:component-ref id="scap_org.open-scap_cref_ssg-018-cpe-oval.xml" xlink:href="#scap_org.open-scap_comp_ssg-018-cpe-oval.xml"/>
25    <ds:component-ref id="scap_org.open-scap_cref_security-oval-com.oracle.elsa-018.xml.bz2" xlink:href="https://linux.oracle.com/security/oval/com.oracle
26  </ds:checks>
27 </ds:data-stream>
28 <ds:component id="scap_org.open-scap_comp_ssg-018-cpe-dictionary.xml" timestamp="2024-01-30T14:04:56">
29   <cpe-dict:cpe-list xsi:schemaLocation="http://cpe.mitre.org/dictionary/2.0 http://cpe.mitre.org/files/cpe-dictionary_2.1.xsd">
30     <cpe-dict:cpe-item name="cpe:/o:oracle:linux:8">
31       <cpe-dict:title xml:lang="en-us">Oracle Linux 8</cpe-dict:title>
32       <cpe-dict:check href="sg-018-cpe-oval.xml" system="http://oval.mitre.org/XMLSchema/oval-definitions-5" oval:sg-installed_OS_is_8_family:define/c
33     </cpe-dict:cpe-item>
34   </cpe-dict:cpe-list>
35 </ds:component>
36 <ds:component id="scap_org.open-scap_comp_ssg-018-xccdf.xml" timestamp="2024-01-30T14:04:56">
37   <xccdf:1.2:benchmark id="xccdf_org.ssgproject.content_benchmark_DS-8" resolved="true" style="SCAP_1.2" xsi:schemaLocation="http://checklists.nist.gov/xcc
38   <xccdf:1.2:status date="2024-01-30">draft</xccdf:1.2:status>
39   <xccdf:1.2:title>Guide to the Secure Configuration of Oracle Linux 8</xccdf:1.2:title>
40   <xccdf:1.2:description>This guide presents a catalog of security-relevant
41 configuration settings for Oracle Linux 8. It is a rendering of
42 content structured in the assessable Configuration Checklist Description Format (XCCDF)
43 in order to support security automation. The SCAP content is
44 is available in the chml:codescap-security-guide/html:codes package which is developed at
45
46   <html:a href="https://www.open-scap.org/security-policies/scap-security-guide">https://www.open-scap.org/security-policies/scap-security-guide/html:as
47   </html:a></html:br>
48 Providing system administrators with such guidance informs them how to securely
49 configure systems under their control in a variety of network roles. Policy
50 makers and baseline creators can use this catalog of settings, with its
```

Enfoque imperativo (shellscripts)

```
1 #!/bin/bash
2 echo "-----"
3 echo "--BLOQUEO DE CUENTAS POR INTENTOS FALLIDOS--"
4 echo "-----"
5 echo -e "\n"
6 echo " ANTES DE COMENZAR SE CREARÁ UN BACKUP DE LA CARPETA PAM.D EN EL DIRECTORIO /etc/pam.d_backup[fecha/hora]"
7 echo " NO DETENGA EL SCRIPT, NI HAGA NADA HASTA QUE EL SCRIPT FINALICE"
8 echo " EN CASO DE DETENCIÓN DEL SCRIPT; VUELVA A EJECUTARLO ANTES DE REINICIAR HASTA QUE FINALICE EL PROCESO CORRECTAMENTE"
9 read -p "Pulse ENTER para continuar o Ctrl + C para cancelar....."
10 tiempo=$( date +"%d-%b-%y-%H:%M:%S" )
11 mkdir /etc/pam.d_backup_${tiempo}
12 cp -r /etc/pam.d/* /etc/pam.d_backup_${tiempo}
13
14 var1=$(cat /etc/pam.d/password-auth |grep "pam_faillock.so")
15 if [ -z "$var1" ]
16 then
17 sudo sed -i '8i auth          required          pam_faillock.so preauth silent audit deny=8 even_deny_root unlock_time=3600' /etc/pam.d/password-auth
18 sudo sed -i '10i auth         [default=deny]      pam_faillock.so authfail deny=8 even_deny_root unlock_time=3600' /etc/pam.d/password-auth
19 sudo sed -i '15i account      required          pam_faillock.so' /etc/pam.d/password-auth
20 sudo sed -i '23i password     requisite         pam_pwhistory.so debug use_authok remember=25 retry=8' /etc/pam.d/password-auth
21 sudo sed -i -e 's/pam_pwquality.so try_first_pass local_users_only */pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=/' /etc/pam.d/password-auth
22
23 else
24 echo "Ya se encuentra configurado /etc/pam.d/password-auth"
25 fi
26 var2=$(cat /etc/pam.d/system-auth |grep "pam_faillock.so")
27 if [ -z "$var2" ]
28 then
29 sudo sed -i '9i auth          required          pam_faillock.so preauth silent audit deny=8 even_deny_root unlock_time=3600' /etc/pam.d/system-auth
30 sudo sed -i '11i auth         [default=deny]      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_authok 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
34 else
35 echo "Ya se encuentra configurado /etc/pam.d/system-auth"
36 fi
37
38 echo " >>>>>>>EL PROCESO A FINALIZADO CORRECTAMENTE<<<<<<<"
39 read -p "Pulse ENTER y el sistema se reiniciará automáticamente en 1 minuto, guarde los archivos que tenga abiertos antes de continuar....."
40 shutdown -r
```


Enfoque declarativo



```
1 - name: Configurar pam_faillock.so
2   become: true
3   community.general.pamd:
4     backup: true
5     name: "{{ item }}"
6     type: auth
7     control: required
8     module_path: pam_deny.so
9     state: after
10    new_type: auth
11    new_control: required
12    new_module_path: pam_faillock.so
13    module_arguments: "preauth silent audit deny=8 even_deny_root unlock_time={{ UNLOCK_TIME }}"
14  loop:
15    - password-auth
16    - system-auth
17  notify:
18    - Reiniciar_host
19
20 - name: Actualización pam_faillock.so
21   become: true
22   community.general.pamd:
23     backup: true
24     name: '{{ item }}'
25     type: auth
26     control: required
27     module_path: pam_faillock.so
28     module_arguments: "preauth silent audit deny=8 even_deny_root unlock_time={{ UNLOCK_TIME }}"
29  loop:
30    - password-auth
31    - system-auth
32  notify:
33    - Reiniciar_host
34
```

¿Qué se ha hecho?



ansible-rol-CCN-STIC-619B Private			Unwatch 6
main	3 Branches	0 Tags	Go to file t Add file <> Code
dbalrod	Merge pull request #17 from ProtAAPP/correccion_erroses		454cc86 · last week 51 Commits
defaults/main	Se mueven variables que probablemente sean sobrescritas a...	2 weeks ago	
docs	Cabecera en README.md	8 months ago	
handlers	Se habilitan para su ejecución en el modo dry run (check) tar...	last week	
meta	[ADD] Traslado del repositorio al GitHub de ProtAAPP	9 months ago	
tasks	Se habilitan para su ejecución en el modo dry run (check) tar...	last week	
templates	Se aplican mejoras de ansible-lint y se corrige el método de ...	last month	
vars/main	Se mueven variables que probablemente sean sobrescritas a...	2 weeks ago	
LICENSE	[ADD] Traslado del repositorio al GitHub de ProtAAPP	9 months ago	
README.md	Se separa el bastionado del escritorio gnome del resto de m...	3 weeks ago	

Caso de uso

```
bastionado_rol_rhel8.yml 176 bytes
1 - name: CCN-STIC-6198 Configuración segura de CentOS 8
2   hosts: "{{ grupo_de_maquinas }}"
3   vars_files:
4     - ./vars/banner.yml
5   roles:
6     - role: ansible-rol-CCN-STIC-6198
```

The screenshot shows the AWX web interface. On the left is a sidebar with navigation options: Schedules, Activity Stream, Workflow Approvals, Resources (Templates, Credentials, Projects, Inventories, Hosts), Access (Organizations, Users, Teams), and Administration (Credential Types, Notifications, Management Jobs, Instance Groups). The main panel displays the 'Details' of a job template named 'bastionado_rhel8_pre'. The 'Schedules' tab is selected and circled in red. Below the tabs, a table lists the template's properties: Name, Job Type, Organization, Inventory, Project, Forks, Verbose, Show Changes, Job Slicing, Last Modified, Credentials, Job Tags, and Variables. The 'Job Tags' field is also circled in red and contains the value 'ens_media'. At the bottom, there are buttons for 'Edit', 'Launch', and 'Delete'. The variables section shows a JSON object with 'grupo_de_maquinas' set to 'app_demo'.

Name	Job Type	Organization
bastionado_rhel8_pre	check	Arquitectura-automatización

Inventory	Project	Playbook
inventario_bastionado_rhel	bastionado_rhel	bastionado_rol_rhel8.yml

Forks	Verbosity	Timeout
0	0 (Normal)	0

Show Changes	Job Slicing	Created
On	1	19/2/2024, 12:26:21 by usuario_demo

Last Modified	Credentials	Job Tags
20/2/2024, 14:31:56 by usuario_demo	SSH ansible (ssh)	ens_media




```
1 {
2   "grupo_de_maquinas": "app_demo"
3 }
```

```
ansible-playbook my_playbook_con_rol_CCN-STIC-6198.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:	Contraseña configurada
Permisos sobre partición de inicio:	Los parámetros no están configurados
Contraseña de Grub:	Contraseña no configurada
Parámetros GNOME:	El sistema Operativo no tiene entorno Gráfico GNOME
Usuarios con UID 0:	No existen usuarios con UID 0
Bloqueo de cuenta:	Los parámetros no están configurados
Shells de usuarios:	Revisar por auditor
Permisos sobre home:	Parámetros configurados correctamente
Registro de actividad - Configuración auditd:	Parámetros configurados correctamente
Banner:	Revisar por auditor
Usuarios sin contraseñas:	No existen usuarios sin contraseña
Volcados de núcleo:	Los parámetros no están configurados correctamente
Registro de actividad - Reglas de auditoría:	Revisar por auditor
Complejidad de contraseñas:	Los parámetros no están configurados
Servicios:	Revisar por auditor
Caducidad de contraseñas:	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:	Contraseña configurada
Permisos sobre partición de inicio:	Los parámetros no están configurados
Contraseña de Grub:	Contraseña no configurada
Parámetros GNOME:	El sistema Operativo no tiene entorno Gráfico GNOME
Usuarios con UID 0:	No existen usuarios con UID 0
Bloqueo de cuenta:	Los parámetros no están configurados
Shells de usuarios:	Revisar por auditor
Permisos sobre home:	Parámetros configurados correctamente
Registro de actividad - Configuración auditd:	Parámetros configurados correctamente
Banner:	Revisar por auditor
Usuarios sin contraseñas:	No existen usuarios sin contraseña
Volcados de núcleo:	Los parámetros no están configurados correctamente
Registro de actividad - Reglas de auditoría:	Revisar por auditor
Complejidad de contraseñas:	Los parámetros no están configurados
Servicios:	Revisar por auditor
Caducidad de contraseñas:	Los parámetros 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:	Contraseña configurada
Permisos sobre partición de inicio:	Parámetros configurados correctamente
Contraseña de Grub:	Contraseña configurada
Parámetros GNOME:	El sistema Operativo no tiene entorno Gráfico GNOME
Usuarios con UID 0:	No existen usuarios con UID 0
Bloqueo de cuenta:	Parámetros configurados correctamente
Shells de usuarios:	Revisar por auditor
Permisos sobre home:	Parámetros configurados correctamente
Registro de actividad - Configuración auditd:	Parámetros configurados correctamente
Banner:	Tiene un banner configurado
Usuarios sin contraseñas:	No existen usuarios sin contraseña
Volcados de núcleo:	Parámetros configurados correctamente
Registro de actividad - Reglas de auditoría:	Revisar por auditor
Complejidad de contraseñas:	Parámetros configurados correctamente
Servicios:	Revisar por auditor
Caducidad de contraseñas:	Parámetros configurados correctamente



¿Quién es nuestro superhéroe?



IDEM ⚡ POTENCIA

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 GRACIAS

AC/BC



Highway to RHEL (AC/BC)

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

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



@diegobr

