MICRO SERVICIOS ORQUESTADORES DE COBRANZA Y CRÉDITO10.82.67.20 **Certificación-CargaEvidenciadeControles**

- **Gestion de Identidades y Privilegios Avanzado8800006**

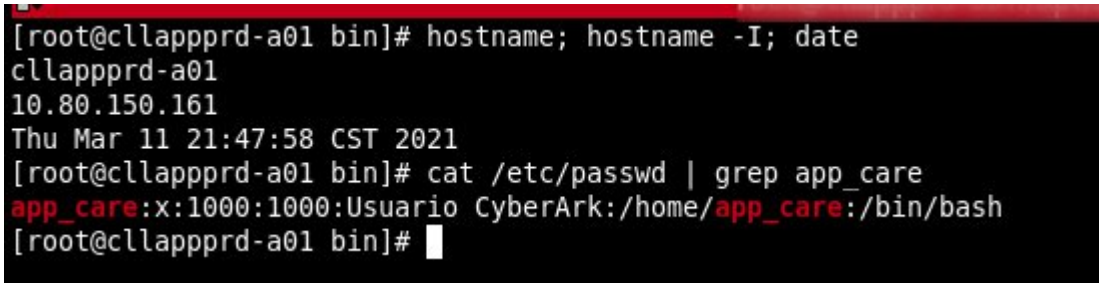
SRV-BAZ-CIT-201 Se deberá crear de el usuario app_care para Administración y Conciliación por parte del DSI CyAAL IT 5

¿En qué ayuda?

Garantizar accesos para administración y validación de puntos de seguridad y gestión de usuarios así como conexión en caso de contingencia

¿Como cumplirlo?

Generando los usuarios en el servidor. se valida con el Formato de listado de usuarios existentes



app_care_cllappprd-a01.png

en caso de que no este el usuario hay quedarlo de alta conforme al manual de app_care

y enviar un correo a CYAALIT-GS cyaalitgs@gruposalinas.com.mx adjuntando el formato de enrolamiento.

date;hostname;ip route get 1.2.3.4 | '{print $7}' awk '{print $7}';cat -n /etc/passwd | grep app_care

Usuario en S.O.	Área responsable	Tipo de usuario: (Aplicativo / Sistema)	Perfil / Grupo	El password puede ser modificado periódicamente?	Pueden ser aplicadas las políticas de passwords, inactividad, vigencia, longitud y complejidad?.	El usuario personalizado esta ligado a procesos y/o aplicaciones. (SI/No)	El usuario se encuentra en procesos batch	La contraseña esta inmersa en el código
b1014515	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b937777	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b181656	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b789393	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1038724	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1030520	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1025138	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1028173	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1032718	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1037337	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b10034978	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
scom	Servicios Cloud	Sistema	scom	SI	SI	NO	NO	NO
app_care	Servicios Cloud	Sistema	users	SI	SI	NO	NO	NO

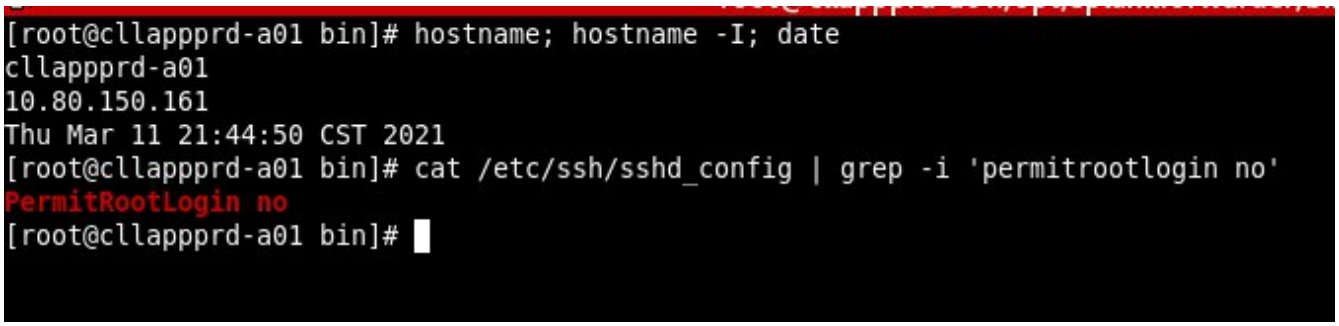
SRV-BAZ-CIT-218 Se deberá habilitar la Restricción de acceso al servidor con usuario root 5

¿En qué ayuda?

Evitar accesos directos con el superusuario

¿Como cumplirlo?

Adjuntando la imagen que muestre la configuración de este punto Verificar el servicio SSH si se tiene: PermitRootLogin NO Para mayor referencia consultar el manual de configuración ubicado en la ayuda de IEECOmcrsrvprd-a06_etc_passwd.txtmcrsrvprd-a06_etc_passwd.txt



date;hostname;ip route get 1.2.3.4 | awk '{print $7}';cat -n /etc/ssh/sshd_config | grep -i PermitRootLogin

Cambio de Parametro

sed -i 's/PermitRootLogin yes/PermitRootLogin No/g' /etc/ssh/sshd_config;

cuando se cambie a No validar si los nodos son productivos, si es son hay que notificar a cyberark de este cambio.

SRV-BAZ-CIT-219 Se deberá Configurar plantilla SUDO donde se defina los siguientes perfiles: Administración de usuarios Cambios de contraseña Cyberark Restricción SU 5

¿En qué ayuda?

Limitar privilegios a usuarios

¿Como cumplirlo?

Adjuntando la imagen que muestre la configuración de este punto Favor de consultar el archivo de grupos de comando a configurar ubicado en la ayuda de IEECO

Formato_Usuarios Privilegios SRV-BAZ-CIT-219.xlsx

Usuario en S.O.	Área responsable	Tipo de usuario: (Aplicativo / Sistema)	Perfil / Grupo	El password puede ser modificado periódicamente?	Pueden ser aplicadas las políticas de passwords, inactividad, vigencia, longitud y complejidad?.	El usuario personalizado esta ligado a procesos y/o aplicaciones. (SI/No)	El usuario se encuentra en procesos batch	La contraseña esta inmersa en el código
b1014515	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b937777	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b181656	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b789393	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1038724	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1030520	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1025138	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1028173	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1032718	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1037337	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b10034978	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
scom	Servicios Cloud	Sistema	scom	SI	SI	NO	NO	NO
app_care	Servicios Cloud	Sistema	users	SI	SI	NO	NO	NO

Cd

SRV-BAZ-CIT-202 Si el SO lo soporta ningún grupo/rol a excepción del administrativo y el correspondiente a DSI CyAAL deberá contar con permiso para la gestión de usuarios y privilegios. 5

¿En qué ayuda?

Eliminar el riesgo de movimientos a usuarios y/o privilegios del servidor no autorizados

¿Como cumplirlo?

Adjuntando el Formato de usuarios y privilegios ubicado en la ayuda de IEECO donde se deberá indicar los usuarios que pertenecen a cada grupo

Formato_UsuariosPrivilegiosSRV-BAZ-CIT-202.xlsx

Usuario en S.O.	Área responsable	Tipo de usuario: (Aplicativo / Sistema)	Perfil / Grupo	El password puede ser modificado periódicamente?	Pueden ser aplicadas las políticas de passwords, inactividad, vigencia, longitud y complejidad?.	El usuario personalizado esta ligado a procesos y/o aplicaciones. (SI/No)	El usuario se encuentra en procesos batch	La contraseña esta inmersa en el código
b1014515	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b937777	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b181656	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b789393	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1038724	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1030520	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1025138	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1028173	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1032718	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1037337	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b10034978	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
scom	Servicios Cloud	Sistema	scom	SI	SI	NO	NO	NO
app_care	Servicios Cloud	Sistema	users	SI	SI	NO	NO	NO

SRV-BAZ-CIT-217 El equipo deberá tener restricción de acceso por IP 5

¿En qué ayuda?

Controlar y limitar las conexiones autorizadas

¿Como cumplirlo?

Formato de listado de Ips permitidas Se deberán agregar al ACL las Ips de Cyberark 10.64.16.173 10.64.16.175 10.64.248.140 10.64.248.141 10.64.248.31 10.50.158.43 10.50.158.45 10.50.158.74

<<Formato Base para registro de Ips en ACLs>>

Dirección IP	Tipo de IP (Pc / Servidor)	Hostname	Nombre de usuario /	Nombre Completo del usuario	area responsable
10.X.X.X	Servidor	qtrurkemnprd-a03	b1014515	Antonio Rafael Notario Rodriguez	Servicios Cloud
			b937777	Juan Carlos Morales Morales	Servicios Cloud
			b181656	Genaro Morales Solano	Servicios Cloud
			b789393	Hector Rios Hernandez	Servicios Cloud
			b1038724	Hugo Espinosa Rosas	Servicios Cloud
			b1030520	Marcos Cayetano Lopez	Servicios Cloud
			b1025138	Angel Ivan Sanchez Godinez	Servicios Cloud
			b1028173	Paola Garcia Dominguez	Servicios Cloud
			b1032718	Raul Reyes Leon	Servicios Cloud
			b1037337	Luis Angel Duran Cervantes	Servicios Cloud
			b10034978	Luis Daniel Montiel Ramirez	Servicios Cloud

SRV-BAZ-CIT-216 En el equipo ningún usuario deberá contar con permisos de root 5

¿En qué ayuda?

Garantizar la Restricción de altos privilegios

¿Como cumplirlo?

El punto se valida con el listado de roles y privilegios

Usuario en S.O.	Área responsable	Tipo de usuario: (Aplicativo / Sistema)	Perfil / Grupo	El password puede ser modificado periódicamente?	Pueden ser aplicadas las políticas de passwords, inactividad, vigencia, longitud y complejidad?.	El usuario personalizado esta ligado a procesos y/o aplicaciones. (SI/No)	El usuario se encuentra en procesos batch	La contraseña esta inmersa en el código
b1014515	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b937777	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b181656	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b789393	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1038724	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1030520	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1025138	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1028173	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1032718	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1037337	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b10034978	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
scom	Servicios Cloud	Sistema	scom	SI	SI	NO	NO	NO
app_care	Servicios Cloud	Sistema	users	SI	SI	NO	NO	NO

SRV-BAZ-CIT-203 Se deberá proporcionar listado de usuarios indicando área, responsable y grupo asignado así como los grupos existentes en el servidor 5

¿En qué ayuda?

Identificar los usuarios y grupos existentes en el servidor.

¿Como cumplirlo?

Adjuntando el Formato de listado de usuarios existentes En Linux/Unix el listado de usuarios se obtiene del archivo /etc/passwd

No files in here

BUENO

SRV-BAZ-CIT-203

	Equipo / Tecnologia	Direccion IP / Equipo	Usuario	Safe	Plataforma	Verificado el
☐	Qtrurkemnprd-a03	10.53.168.23	app_care	BA_SERVCLOUD_R	BA_SER...	14/10/2021 04:...
☐	Qtrurkemnprd-a03	10.53.168.23	root	BA_SERVCLOUD_A	BA_SER...	14/10/2021 07:...

en caso de que no este el usuario hay crearlo conforme al manual de app_care

y enviar un correo a CYAALIT-GS cyaalitgs@gruposalinas.com.mx adjuntando el formato de enrolamiento.

---

date>>/home/b789393/etc_passwd.txt;hostname>>/home/b789393/etc_passwd.txt;ip route get 1.2.3.4 | awk '{print$7}' >>/home/b789393/etc_passwd.txt;cat /etc/passwd>>/home/b789393/etc_passwd.txt; mv /home/b789393/etc_passwd.txt $(hostname)_etc_passwd.txt

Gestion de Identidades y Privilegios Básico 1 1 0 0 0 *0 1*

SRV-BAZ-CIT-101 No deberán existir cuentas locales personalizadas. Todas las cuentas deben estar justificadas y deberán contar con los privilegios mínimos necesarios. 4

¿En qué ayuda?

Diferenciar y asignar accesos basados en privilegios específicos por rol.

¿Como cumplirlo?

Adjuntando el formato de usuarios ubicado en la ayuda de IEECO

subir el txt

Usuario en S.O.	Área responsable	Tipo de usuario: (Aplicativo / Sistema)	Perfil / Grupo	El password puede ser modificado periódicamente?	Pueden ser aplicadas las políticas de passwords, inactividad, vigencia, longitud y complejidad?.	El usuario personalizado esta ligado a procesos y/o aplicaciones. (SI/No)	El usuario se encuentra en procesos batch	La contraseña esta inmersa en el código
b1014515	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b937777	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b181656	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b789393	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1038724	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1030520	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1025138	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1028173	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1032718	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b1037337	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
b10034978	Servicios Cloud	Sistema	sysops	SI	SI	NO	NO	NO
scom	Servicios Cloud	Sistema	scom	SI	SI	NO	NO	NO
app_care	Servicios Cloud	Sistema	users	SI	SI	NO	NO	NO

·

· **Sistema Operativo Avanzado 2 2 0 0 0 *0 1***

SRV-BAZ-CSA-05 Asegurar que tiene instalado Splunk Universal Forwarder reportando a la consola central 1

¿En qué ayuda?

Centraliza el registro de eventos de Windows para alertamiento o futuras auditorías

¿Como cumplirlo?

Instalar el software Splunk Universal Forwarder y configurarlo para que reporte a Splunk Enviar una imagen donde el área de ImplementacionesDSI@totalsec.com.mx confirma que el equipo reporta a Splunk por medio de Splunk Universal Forwarder

/opt/splunkforwarder/bin

date;hostname; ip route get 1.2.3.4 | awk '{print $7}'; ./splunk list forward-server

admin:splunk password splunkadm123

```
[root@cllappprd-a01 bin]# hostname; hostname -I; date
cllappprd-a01
10.80.150.161
Thu Mar 11 21:40:54 CST 2021
[root@cllappprd-a01 bin]# ./splunk list forward-server
Active forwards:
        10.50.226.119:9997
Configured but inactive forwards:
        None
[root@cllappprd-a01 bin]#
```

SRV-BAZ-CSA-04 Asegurar que se llevan a cabo escaneos y cierre de vulnerabilidades de forma periódica 5

¿En qué ayuda?

Permite detectar de forma oportuna las vulnerabilidades conocidas del servidor

¿Como cumplirlo?

Adjunta evidencia de la salida de los escaneo sin vulnerabilidades críticas altas ni medias Paso 1: Solicitar permisos para que las siguientes IPs correspondientes a los sensores de Rapid7 alcancen la infraestructura a escanear dichos permisos deberán de ser any EKT Torres: 10.50.222.41 EKT KIO: 10.81.32.30 EKT Correo: 10.222.78.13 Afore BAZ: 10.54.53.214 Paso 2: Definir una ventana para realizar el escaneo Paso 3: Solicitar a su unidad de CSA la programación del escaneo. Paso 4: obtener y revisar los resultados en caso de ser necesario aplicar las correcciones necesarias. El control se cumplirá una vez hayan completado un escaneo con 0 vulnerabilidades críticas 0 vulnerabilidades altas y 0 vulnerabilidades medias.

Escaneo de Rapid 7 que se debe programar por parte de los responsables de la arquitectura.

· **Sistema Operativo Basico 3 3 0 0 0** ***2 5***

SRV-BAZ-CSA-19

ls Asegurar que solo se estan utilizando los puertos y servicios requeridos por el sistema 1

¿En qué ayuda?

Protege la confidencialidad de la información de los datos de administración del servidor.

¿Como cumplirlo?

Deshabilitar / Desinstalar todos los servicios que son considerados inseguros y no son necesarios para el sistema. Por ejemplo: - TeamViewer - VNC y sus derivados - Telnet Server - Servicios de correo - Etc. Cerrar todos los puertos no cifrados y / o no necesarios para el sistema. Por ejemplo - 5800 - 5938 - 25 - 110 - 143 - 995 - 993 - 465 - Etc. Enviar la salida de los siguientes comandos Linux:

netstat -noa systemctl list-unit-files --type service Windows: netstat -noa tasklist

Servicios

date >> /home/b789393/services.txt;hostname >> /home/b789393/services.txt;ip route get 1.2.3.4 | awk '{print $7}'>> /home/b789393/services.txt;systemctl list-unit-files >> /home/b789393/services.txt; mv /home/b789393/services.txt $(hostname)_services.txt

Netsatat (RHEL) o ss (Suse)

date >> /home/b789393/ss.txt;hostname >> /home/b789393/ss.txt;ip route get 1.2.3.4 | awk '{print $7}'>> /home/b789393/ss.txt;ss -tulpan >> /home/b789393/ss.txt; mv /home/b789393/ss.txt $(hostname)_ss.txt

mxroudmzapigee01-Release

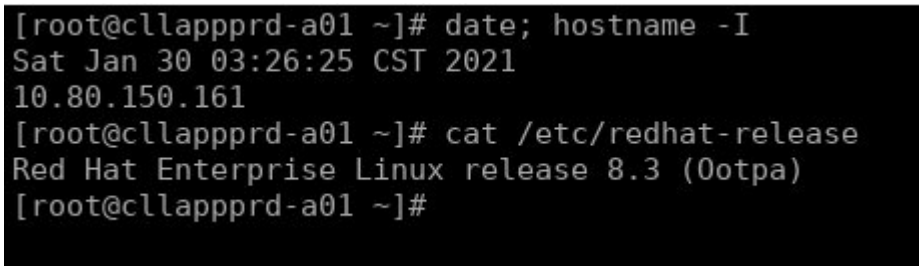
SRV-BAZ-CSA-17 Asegurar que cuenta con versiones de tecnología soportadas por el fabricante. Sólo se tomará como valida la versión actual la versión actual - 1 o la versión LTS Long Term Support 5

¿En qué ayuda?

Disminuye el riesgo de vulnerabilidades tipo 0-day vulnerabilidades recientes sin parches

¿Como cumplirlo?

Adjunta evidencia de las últimas versiones de sistema operativo utilizadas



date;hostname;ip route get 1.2.3.4 | awk '{print $7}';cat /etc/redhat-release

---

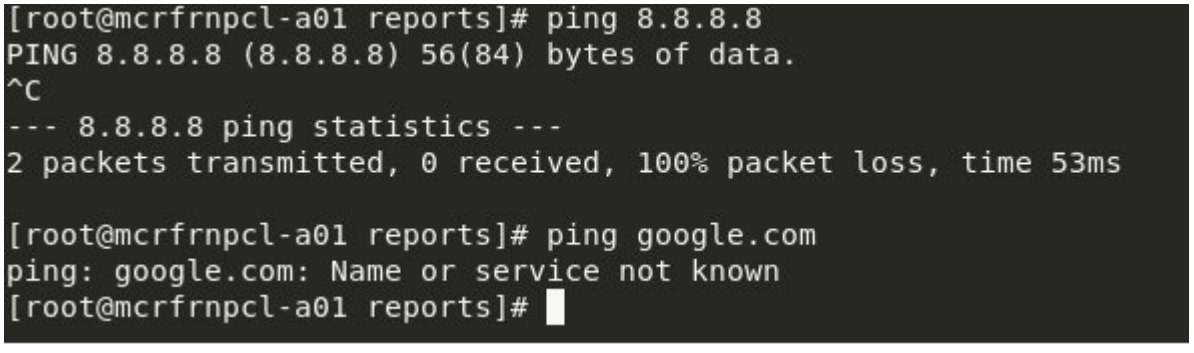
CSA **SRV-BAZ-CSA-18 Asegurar que no tiene salida a internet** 1

¿En qué ayuda?

Disminuye el riesgo de ataques de persistencia en los servidores

¿Como cumplirlo?

Deshabilitar la conexión a internet del equipo ya sea por firewall físico firewall local o declarando la no salida a internet en las rutas de la red. Ejecutar el comando ping 8.8.8.8 El resultado deberán ser todos los paquetes perdidos



date;hostname;ip route get 1.2.3.4 | awk '{print $7}';ping 8.8.8.8

SRV-BAZ-CSA-09 Asegurar que cumple con los controles de DSI y CIS Level 2 para la versión del Sistema Operativo 5

¿En qué ayuda?

Disminuye el riesgo de vulnerabilidades por mala configuración del servidor

¿Como cumplirlo?

Adjunta la salida del CIS con las plantillas definidas por DSI y los niveles de cumplimiento mínimos. De no contar con una plantilla de CIS para el Sistema Operativo por favor contactar a CSA de tu Unidad de Negocio: - DSI CSA Elektra csa-ekt@elektra.com.mx - DSI CSA TVA csa-tva@tvazteca.com.mx - DSI CSA Totalplay csa-tpe@totalplay.com.mx

/root/Assessor-CLI

Corres el CIS en cada equipo

SUSE

sudo sh ./Assessor-CLI.sh -b benchmarks/CIS_SUSE_Linux_Enterprise_15_Benchmark_v1.0.0-xccdf.xml -html -csv -p "Level 2 - Server"

LINUX 8

sudo sh ./Assessor-CLI.sh -b benchmarks/Totalsec_DSI-GS_Red_Hat_Enterprise_Linux_8_Benchmark_PROD_v1.0.0.1-xccdf.xml -html -csv -p "Level 2 - Server"

LINUX 7

sudo sh ./Assessor-CLI.sh -b benchmarks/Totalsec_DSI-GS_Red_Hat_Enterprise_Linux_7_Benchmark_PROD_v3.0.2-xccdf.xml -html -csv -p "Level 2 - Server"

Te lo deposita en reportes los archivos generados por los comandos