Presentación

- **Nombre del estudiante:** Jamiel Santana.
- **Matricula:** 2019-8095
- Nombre del profesor: Geancarlos Sosa
- **Mat:** Seguridad de SO.
- **Tema:** Segundo parcial - OpenSCAP
- **Centro Educativo:** Instituto tecnológico de las Américas.

➢ Qué es OPCENSCAP y scap workbench:

- Primero para comenzar hay que saber que es openscap y que es scap workbench.

  - **OpenScap**: proporciona múltiples herramientas para ayudar a los administradores y auditores con la evaluación, medición y aplicación de las líneas de base de seguridad. El proyecto OpenSCAP proporciona una amplia variedad de guías de protección y líneas base de configuración desarrolladas por la comunidad de código abierto, lo que garantiza que puede elegir una directiva de seguridad que se adapte mejor a las necesidades de su organización, independientemente de su tamaño.

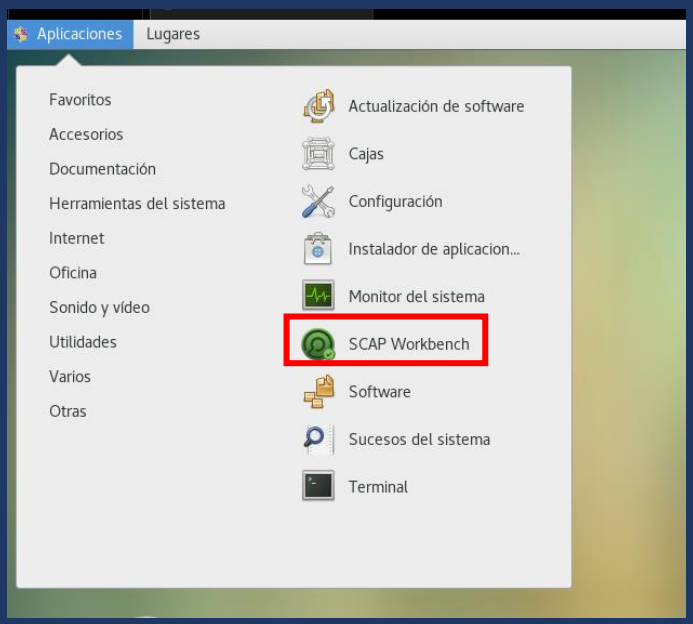
  - **Scap Workbench:** Esta herramienta permite a los usuarios realizar análisis de configuración y vulnerabilidad en un único sistema local o remoto, realizar la corrección del sistema de acuerdo con el archivo XCCDF o SDS dado.

➢ Instalación de Scap workbench en CentOS 7:

- Primero comenzaremos descargando la herramienta, junto con todas sus dependencias necesarias, para ello utilizaremos el comando: **yum install scap-workbench.**

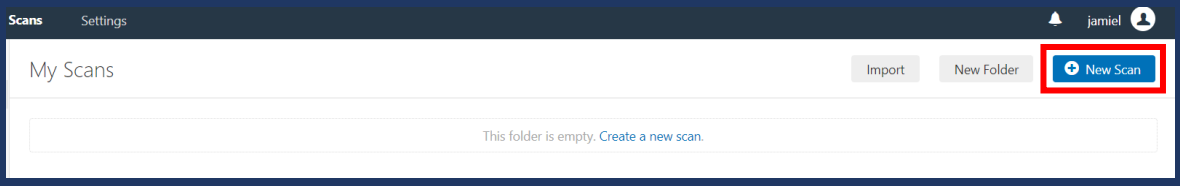
```
[root@localhost jamiel]# yum install scap-workbench
Complementos cargados:fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirror.ci.ifes.edu.br
 * extras: centos.ufes.br
 * updates: centos.ufes.br
Resolviendo dependencias
--> Ejecutando prueba de transacción
---> Paquete scap-workbench.x86_64 0:1.1.6-1.el7 debe ser instalado
--> Procesando dependencias: openscap-utils >= 1.2.0 para el paquete: scap-workbench-1.1.6-1.el7.x86_64
--> Procesando dependencias: openscap >= 1.2.13 para el paquete: scap-workbench-1.1.6-1.el7.x86_64
--> Procesando dependencias: scap-security-guide para el paquete: scap-workbench-1.1.6-1.el7.x86_64
```

- Ya finalizada la descarga como la herramienta se maneja mediante GUI, nos dirigimos hacia la interfaz gráfica de nuestro serv, damos click en el botón de inicio de nuestro CentOS e inmediatamente visualizaremos la herramienta.

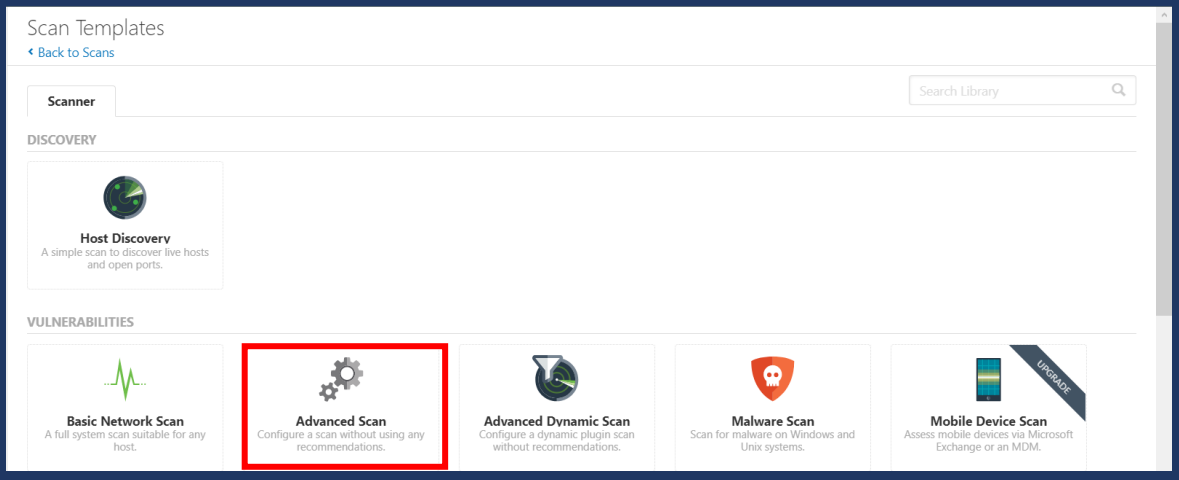


➢ Escaneo con Nessus a máquina cliente:

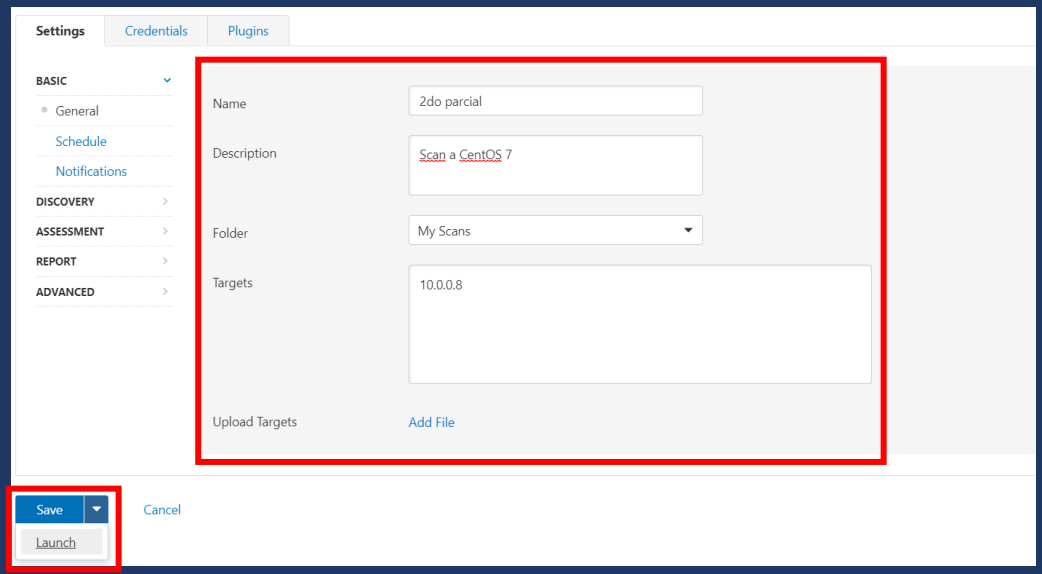
- Para nuestro Scan estaremos haciendo uso de Nessus el cuál fue instalado en mi máquina nativa después del proceso de registro, para realizar el escan haremos lo siguiente > en la pestaña de **my scan,** daremos click en el botón **new scan.**



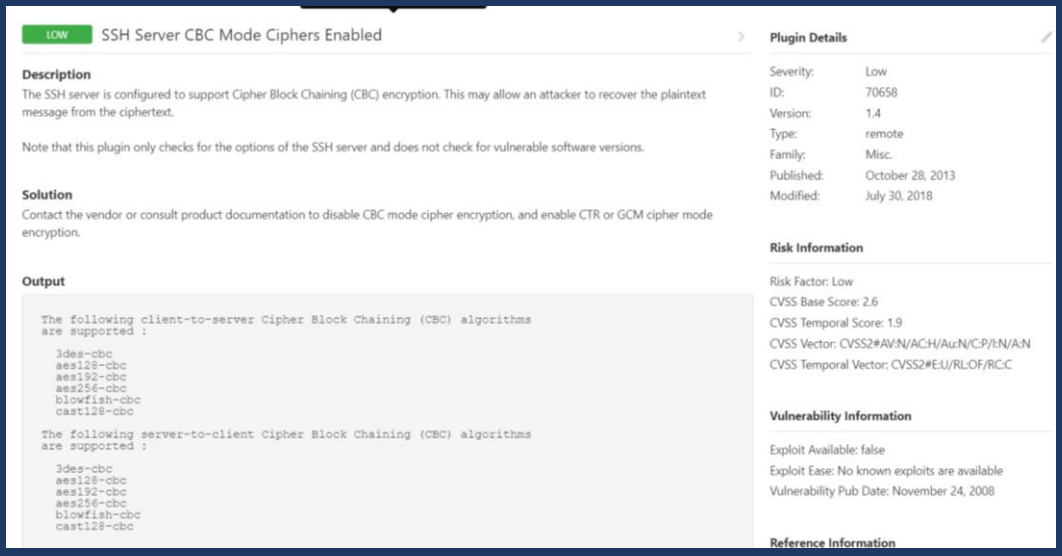
- En el apartado de los **Scan Templates** seleccionaremos el template de **Advanced Scan**



- Ya dentro del **template** rellenamos los campos solitados, y posteriormente damos click en la flecha junto a **save**, para luego hacer click en **launch,** para inicializar el scan inmediatamente.



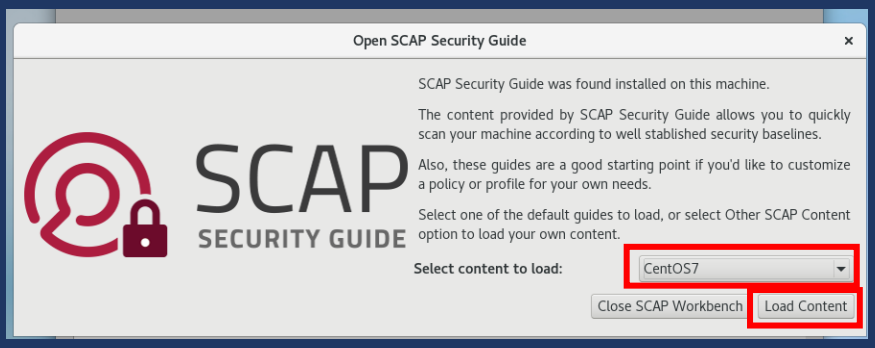
- Finalizado el scan solo vemos reportada una vulnerabilidad de nivel **low**, la cual tiene que ver con la encriptación de ssh, la resolveremos una vez realizado el scan con OPENSCAP.



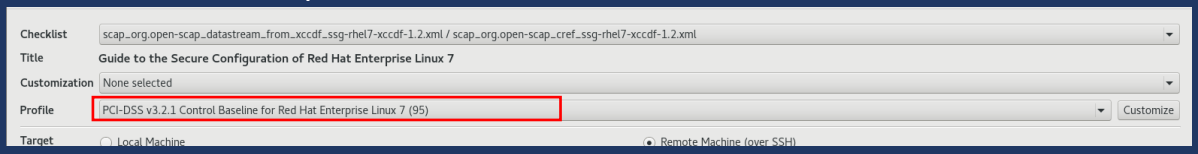
➢ Inicializar el SCAP workbench en el servidor y elegir el perfil de PCI-DSS.

- Para inicializar scap workbench, solo tenemos que dirigirnos a nuestro menú y buscar la herramienta llama **scap workbech.**

- Ya abierta nuestra herramienta, tendremos que escoger el contenido que nos va a cargar referente al SO, en nuestro caso CentOS 7, escogido esto damos click en cagar contenido.

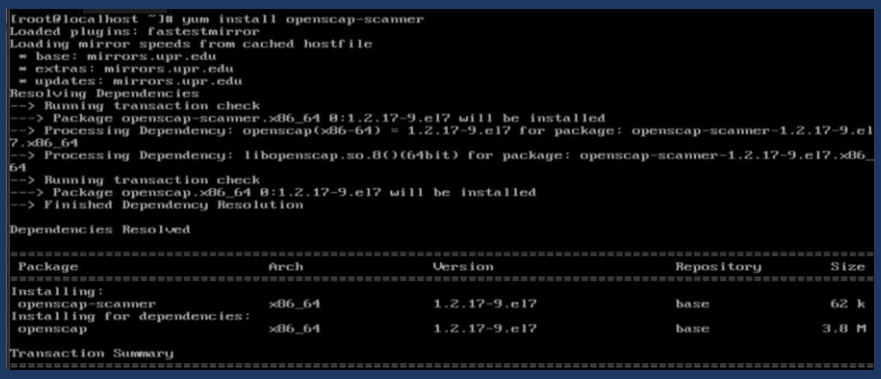


- Realizado esto se nos abrirá la ventana de conf y administración de SCAP, donde lo primero que haremos es elegir nuestro perfil, en nuestro caso seleccionaremos el perfil de PCI-DDS.

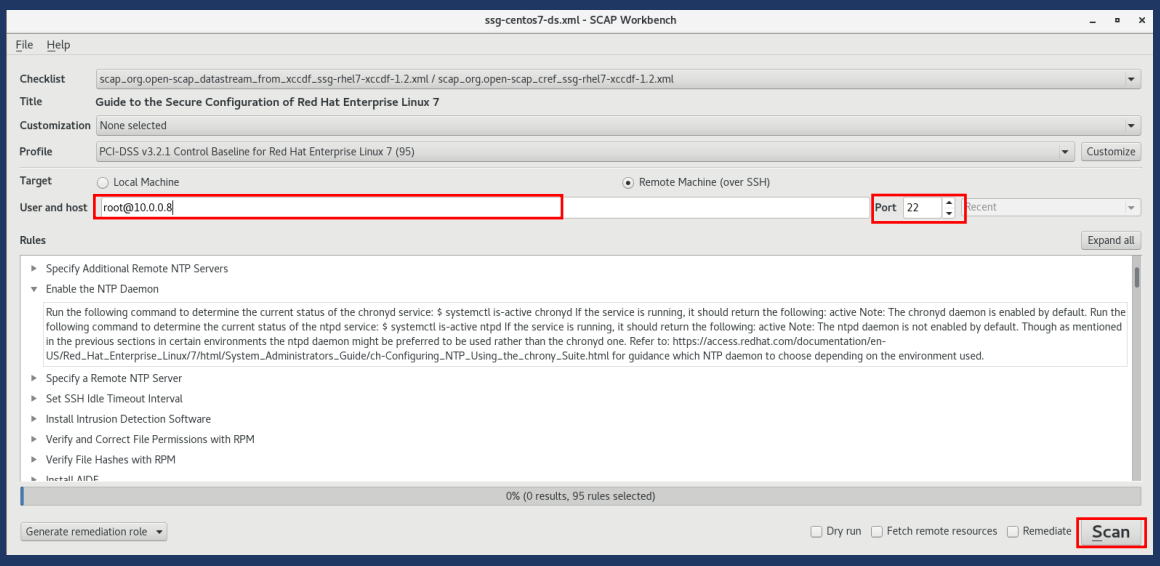


➢ Escanear el equipo cliente y Aplicar los parches de seguridad requeridos por el estándar PCI-DSS

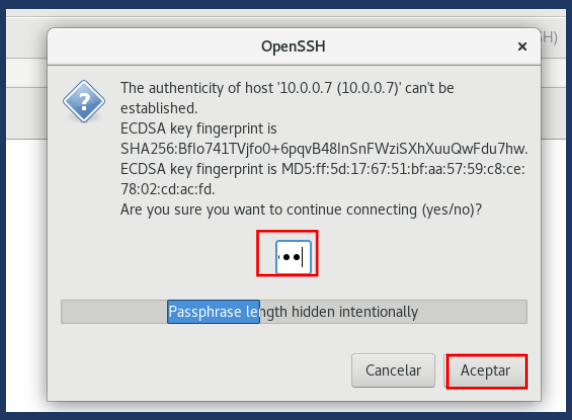
- Cabe recalcar que para que el scan pueda funcionar correctamente deberemos tener instalado en nuestra máquina cliente **openscap-scanner,** esto lo haremos simplemente ejecutando en la máquina cliente el comando **yum install openscap-scanner.**



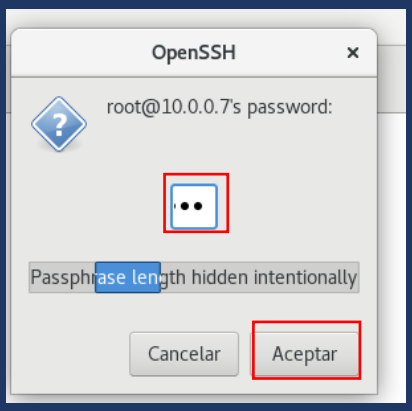
- Ya cargado el contenido, preparamos la configuración para realizar el scan a nuestra máquina cliente mediante SCAP, lo primero es seleccionar a quien se le realizará el scan si a la máquina local o a una máquina remota, en nuestro caso es a un cliente CentOS 7, por lo tanto seleccionamos la opción de remote machine, donde tendremos que tener en cuenta que la conexión se realiza por ssh, por lo tanto tendremos que proporcionar el user y la ip de la máquina externa.



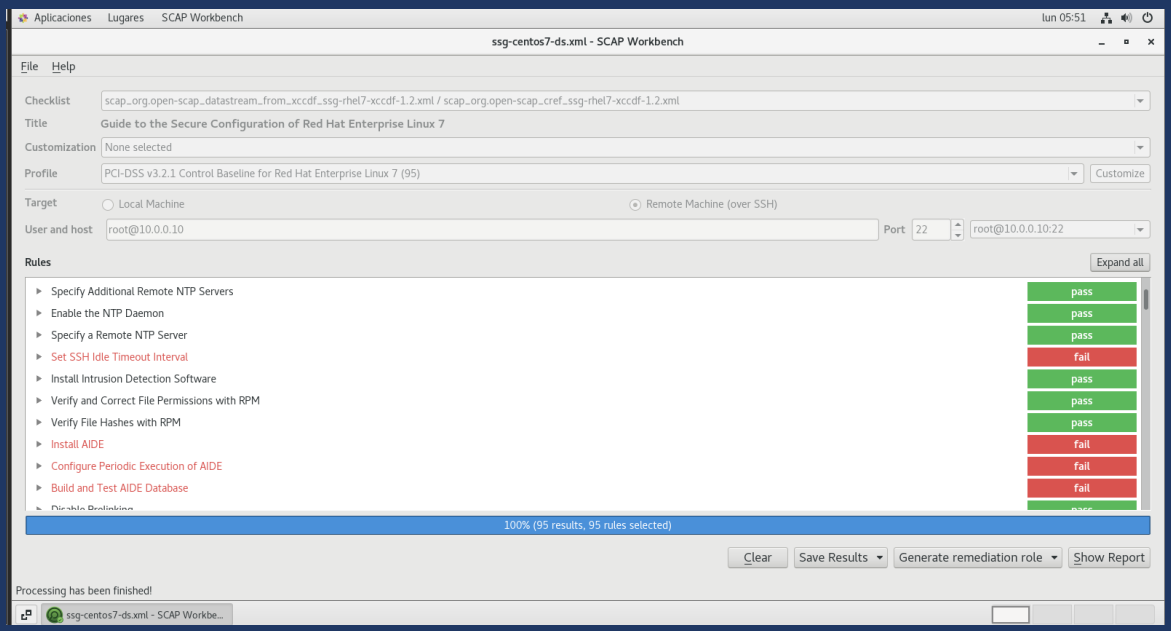
- Hecho click en scan, nos preguntará si queremos seguir con la conexión hacia el cliente escribimos yes, los caracteres están ocultos intencionadamente.



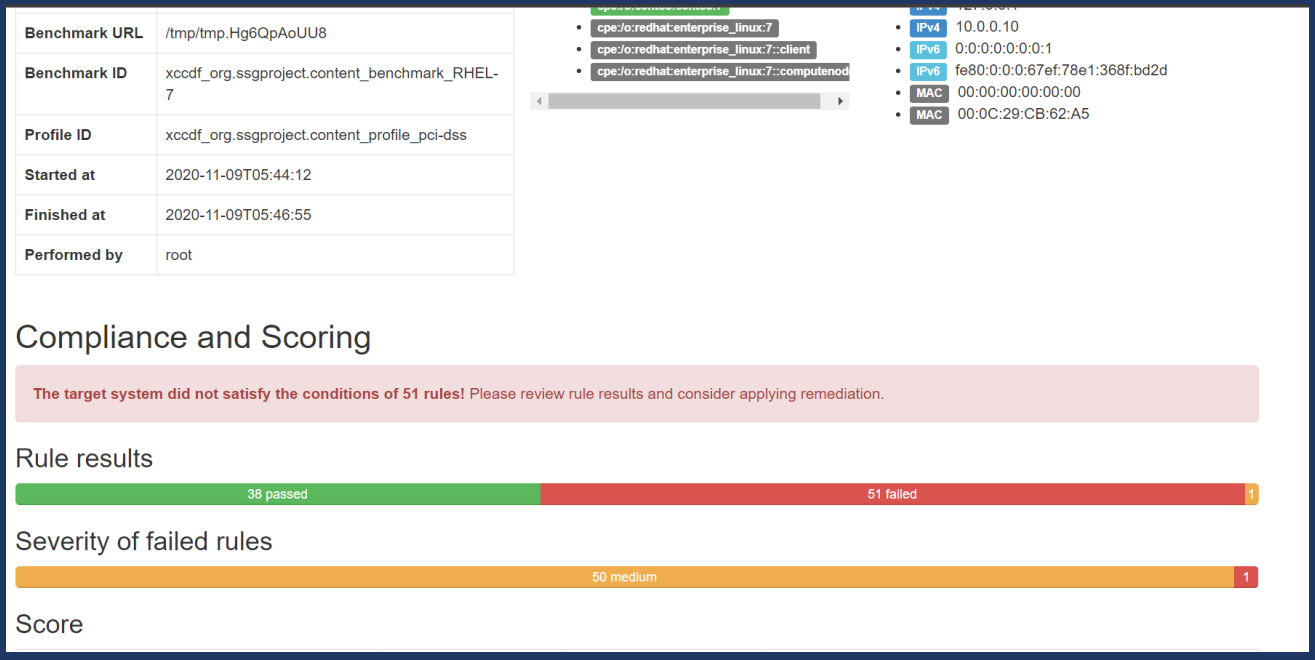
- Damos la credencial del user que hemos puesto.



- El scan comenzará a realizarse, donde nos estará lanzando los resultados del análisis mostrándonos las configuraciones que tenemos correctas con **pass** y las que tenemos que corregir con **fail.**

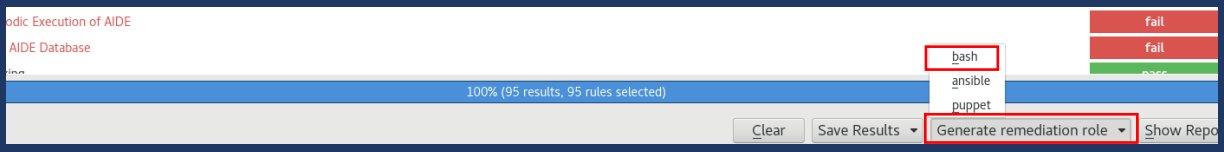


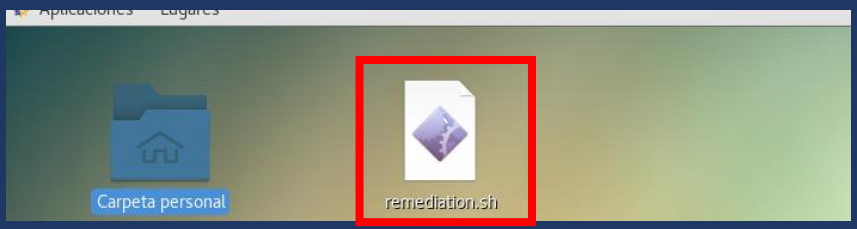
- para poder ver mejor los resultados del reporte daremos click en el botón **save result > HTML REPORT**, donde aquí tendremos un reporte completo del scan realizado. Ya abierto nuestro reporte nos saldrá el informe de la siguiente manera:



- si nos fijamos de 89 aspectos inspeccionados tenemos que corregir 51, aunque se vea un poco difícil no lo es para nada ya que **openscap** ofrece el script para solucionar todos los problemas encontrados.

- Para parchear todos estos problemas encontrados nos dirigimos a nuestro opnescap, **generate remediation role > bash,** hecho esto openscap nos va a generar un script con todo lo necesario para parchear todos los problemas encontrados, solo tendremos que pasar y ejecutar el script en la máquina cliente.





- ya generado nuestro scrip podemos pasarlo del lado del cliente con el comando **> scp archivo usuario@IP:ruta_máquina_cliente** ejecutado el comando damos la pass del user remoto que introducimos y vemos como el traspaso del archivo ha sido completado con éxito.

```
[jamiel@localhost ~]$ scp /home/jamiel/Escritorio/remediation.sh root@10.0.0.10:~/solution.sh
root@10.0.0.10's password:
remediation.sh                                100%  386KB  36.4MB/s   00:00
[jamiel@localhost ~]$
```

- como vemos en la imagen el script se ha copiado en nuestra máquina cliente con éxito, por lo tanto, procederemos a ejecutarlo con el comando **bash (nombre del archivo).** Comenzaremos a visualizar como se realizan las configuraciones e instalaciones necesarias según el estándar PCI-DDS.

```
[root@localhost ~]# ls
anaconda-ks.cfg  solution.sh
[root@localhost ~]# bash solution.sh
Remediating rule 1/51: 'xccdf_org.ssgproject.content_rule_sshd_set_idle_timeout'
Remediating rule 2/51: 'xccdf_org.ssgproject.content_rule_package_aide_installed'
Complementos cargados:fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirrors.upr.edu
 * extras: mirrors.upr.edu
 * updates: mirrors.upr.edu
Resolviendo dependencias
--> Ejecutando prueba de transacción
---> Paquete aide.x86_64 0:0.15.1-13.el7 debe ser instalado
--> Resolución de dependencias finalizada
```

- Terminada la ejecución del script, realizaremos otro scan con **openscap** para asegurarnos que la configuración se ha realizado correctamente, ya finalizada la ejecución del scan veremos que todos los problemas que faltaban por corregir se han parcheado correctamente.

Started at	2020-11-09T06:28:51
Finished at	2020-11-09T06:29:47
Performed by	root

Compliance and Scoring

There were no failed or uncertain rules. It seems that no action is necessary.

Rule results

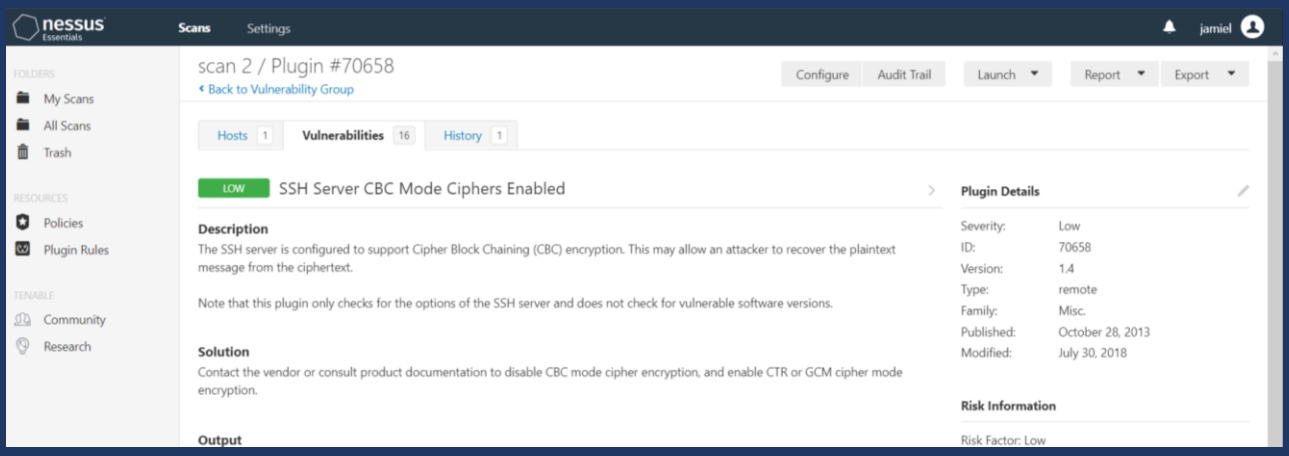
89 passed 1

Severity of failed rules

➢ Escanear nuevamente con Nessus y exportar el reporte de vulnerabilidades

- Ahora volveremos a ejecutar el **scan nessus** para verificar si la vulnerabilidad encontrada al principio se solucionó con lo que acabamos de aplicar o tenemos que parchearla manualmente o resolver por otra vía.

- Como vemos openscap no resolvió con la vulnerabilidad encontrada en Nessus.



- Por lo tanto, tendremos que parchear manualmente, esta vulnerabilidad encontrada en el servicio ssh, trata de que este servicio se encuentra admitiendo encriptación Cipher Block Chaining (CBC), lo cual es un cifrado muy débil y permite a los atacantes vean mensajes en texto plano.

- Las recomendaciones de Nessus es que habilitemos los cifrados más fuertes, esto lo haremos dirigiéndonos al archivo **/etc/ssh/sshd_config** allí agregaremos la siguiente línea **Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com,** guardamos y salimos del archivo de configuración y para finalizar reiniciamos el servicio ssh con el comando **systemctl restart sshd.**

```
# Ciphers and keying
Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
#RekeyLimit default none
```

```
jamiel@localhost:/home/jamiel
[root@localhost jamiel]# systemctl restart sshd
[root@localhost jamiel]#
```

- Hecho esto volveremos a realizar el scan para comprovar si la vulnerabilidad fue corregida, posterior a esto crearemos un reporte del informe de Nessus. Como vemos en la imagen realizado el reporte no encontraron vulnerabilidades.