

Actividad práctica numero 10:

Formato: Individual.

Asignatura: Seguridad en Sistemas Computacionales

Código: SSC 5501

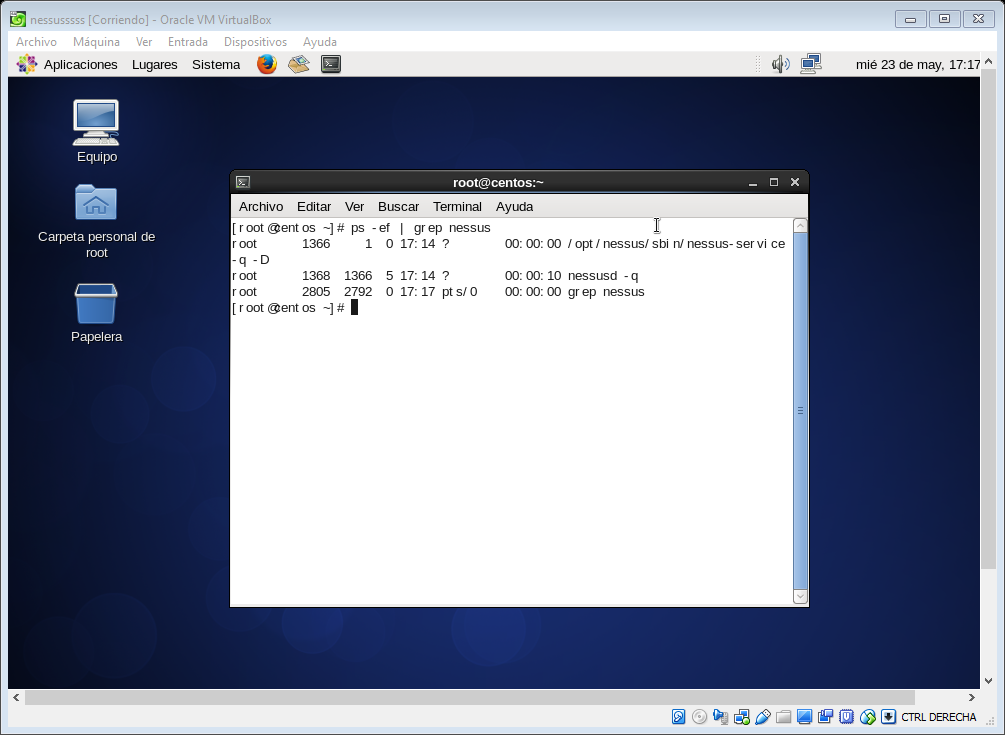
**Objetivo:**

**Realizar diferentes tipos de análisis de vulnerabilidades con la herramienta Nessus.**

1.- Instale la maquina virtual provista por su profesor con la interfaz de red en modo puente, ingrese con el usuario de Sistema Operativo "root", contraseña “duoc.2015”.

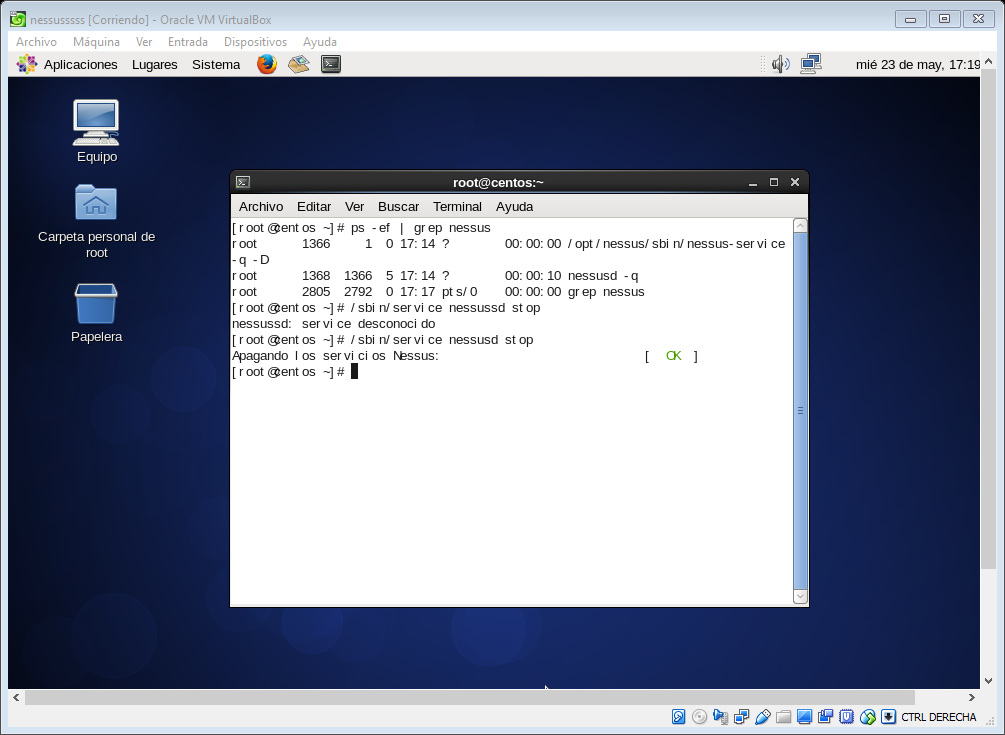
2.- Confirme que el servicio nessus está operativo con el siguiente comando:

# ps –ef | grep nessus



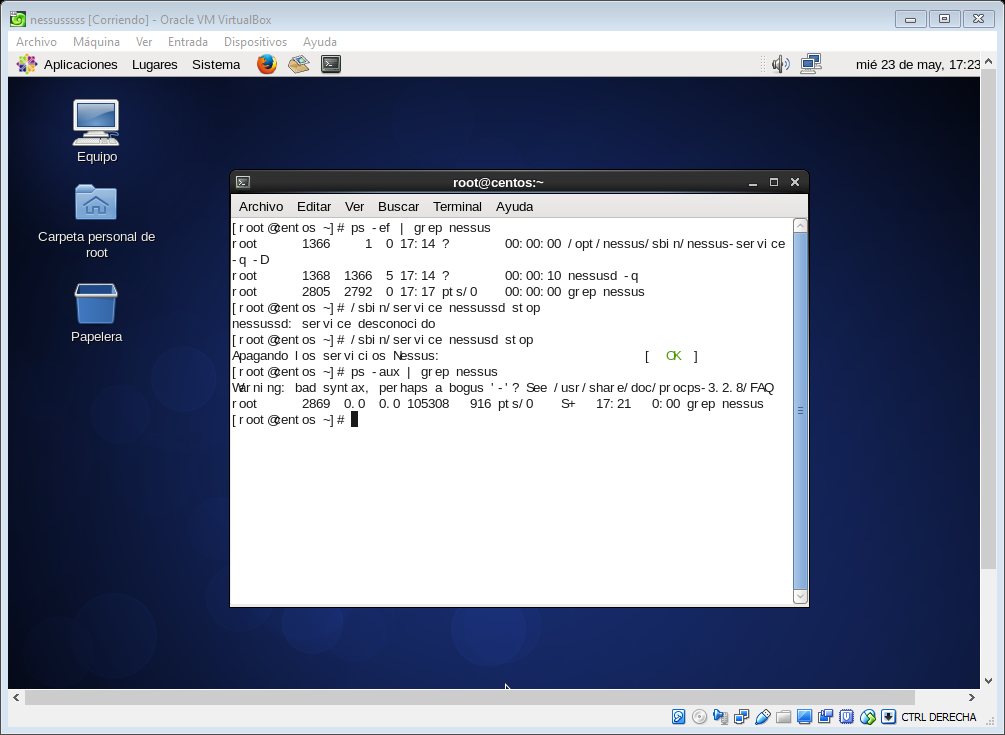
3.- Detenga el servicio Nessus con el comando:

**# /sbin/service nessusd stop**

****

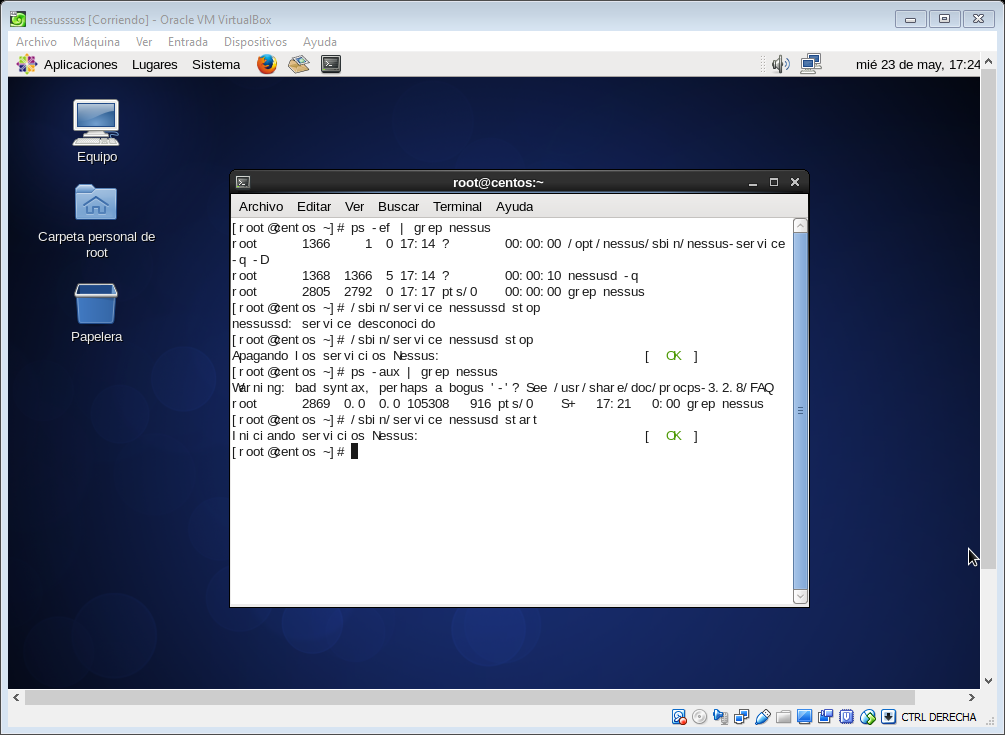
4.- Compruebe que el servicio NO se está ejecutando con el comando:

**# ps -aux | grep nessus**

****

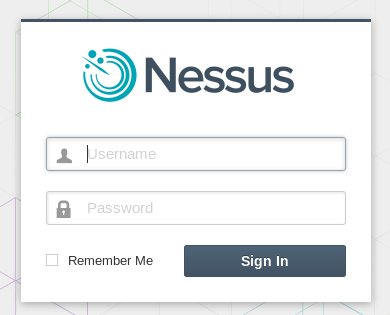
5.- Para subir el servicio nuevamente utilice el comando:

**# /sbin/service nessusd start**

****

6.- Conéctese a la administración con el browser instalado en su máquina virtual a la dirección:

[https://localhost:8834](https://IPmaquinavirtual:8834)



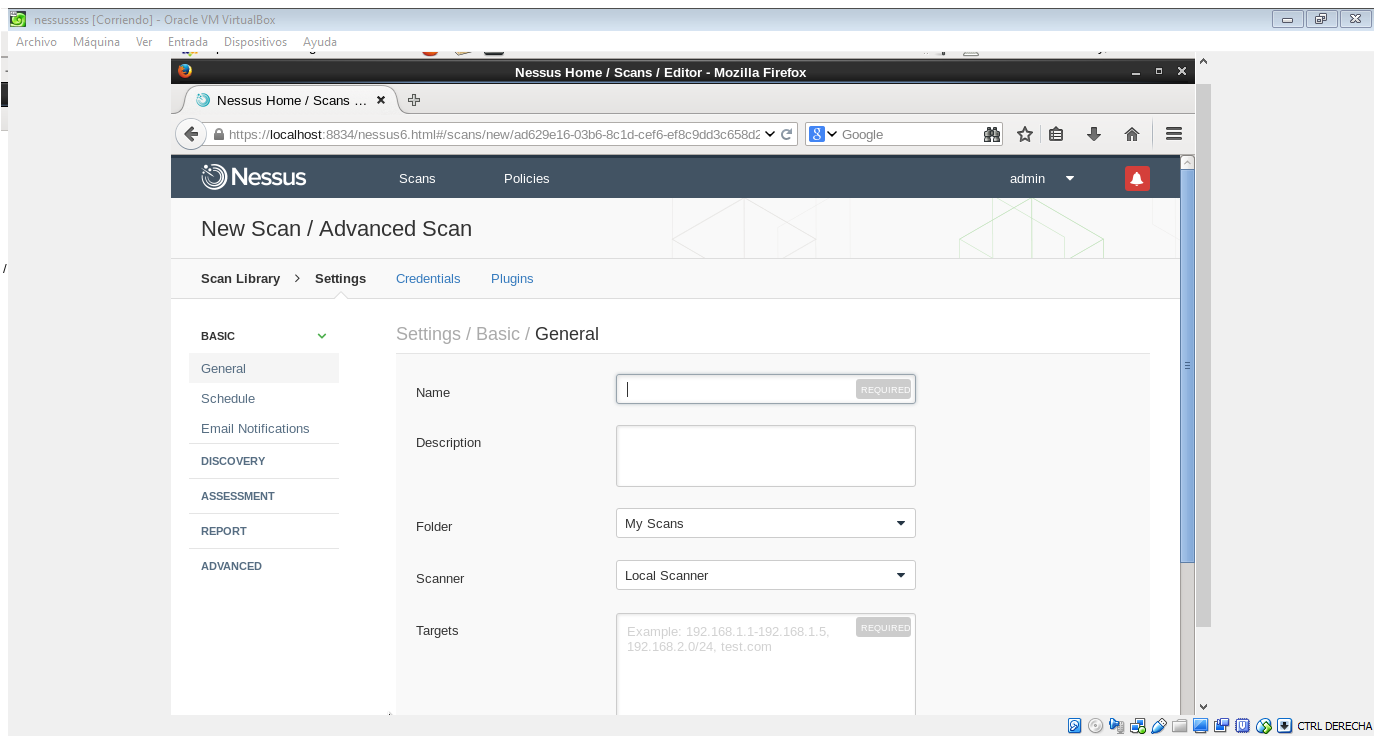
7.- Utilice las siguientes credenciales para la administración:

**- usuario: admin**

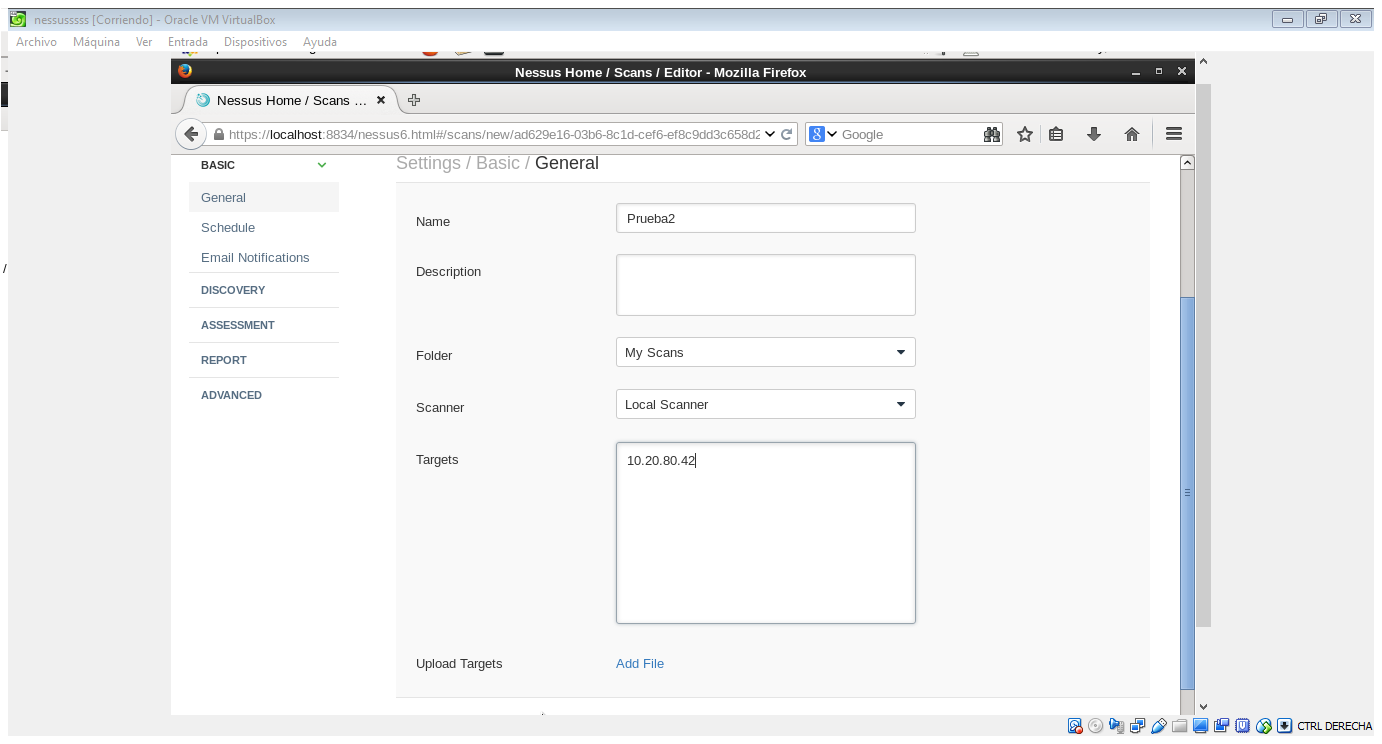
**- password: admin**

8.- Haga click en “New Scan” para crear una nueva política de análisis

9.- Seleccione el perfil “Advanced Scan”



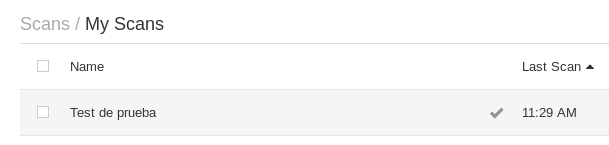
10.- Escriba un nombre para el análisis y en la opción “Target” la dirección IP provista por su profesor

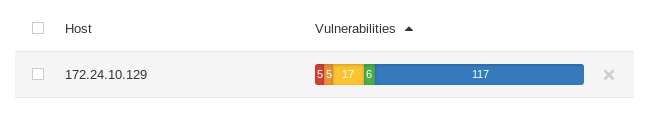


11.- Vaya al final de la página y haga click en “Save”

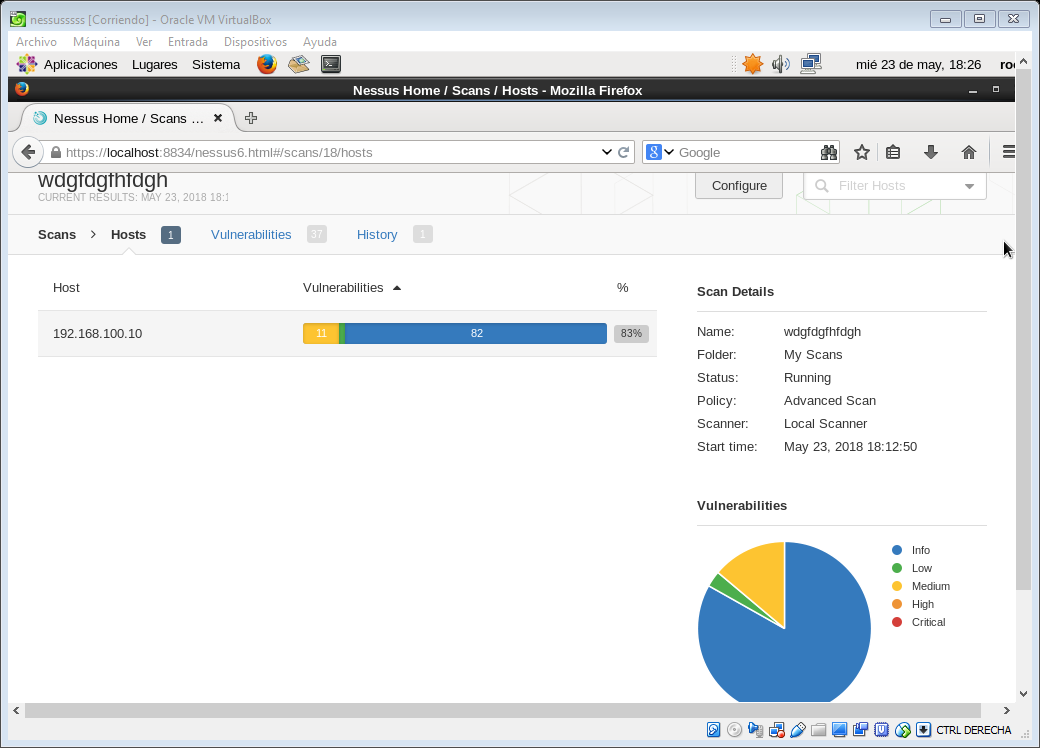
12.- Confirme que se inició el análisis de seguridad

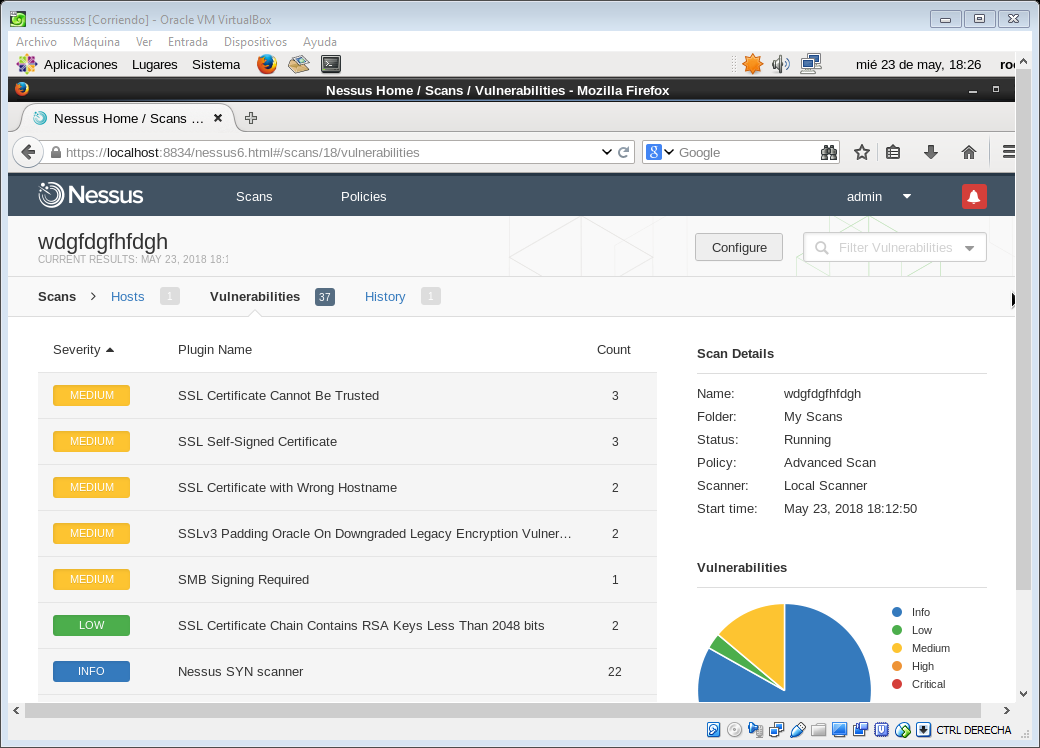
13.- Una vez finalizado el análisis, haga click en la barra del Test y revise las vulnerabilidades encontradas





14.- Haga click sobre la barra del análisis para ver el detalle de las vulnerabilidades



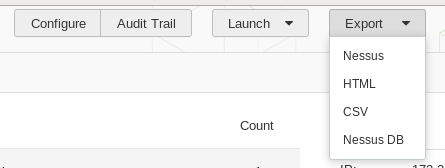


15.- Revise cuantas vulnerabilidades hay de cada tipo y complete el siguiente cuadro

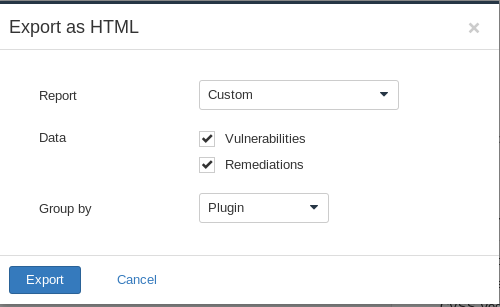
|  |  |
| --- | --- |
| **Nivel de Riesgo** | **Cantidad** |
| Critical | 0 |
| High | 0 |
| Medium | 11 |
| Low | 2 |
| Info | 82 |

**Generación de reporte:**

1.- Seleccione la opción de reportes en HTML para obtener un detalle de las vulnerabilidades encontradas



2.- Configure el reporte según la imagen mostrada en la figura y haga click en “Export”



3.- Observe el reporte generado y responda:

- ¿Qué tipo de vulnerabilidades encontró? ¿A qué tipo de servicios corresponden?

- ¿Qué otro indicador, además del grafico de color entrega Nessus respecto de las vulnerabilidades encontradas?

4.- Seleccione alguna vulnerabilidad de riesgo “CRITICAL” y complete el cuadro mostrado a continuación:

|  |  |
| --- | --- |
| Descripción |  |
| Solución |  |
| Factor de riesgo |  |
| Factor CVSS |  |
| Código CVE |  |
| Fecha de publicación |  |
| Número de plugin de Nessus |  |

5.- Repita el proceso completo de análisis con la nueva dirección IP dada por su profesor

¿Qué diferencias puede comentar respecto del reporte anterior?