**EJERCICIOS GESTIÓN DE VULNERABILIDADES CON NESSUS**

Prerrequisitos

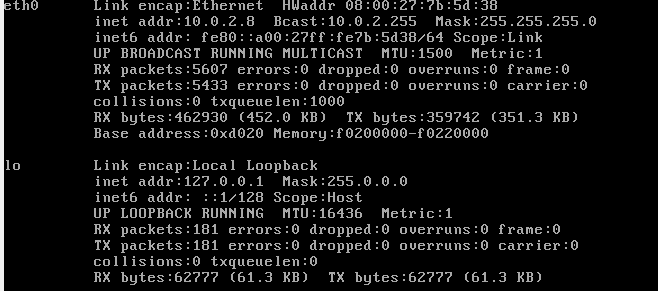
* Kali Linux
* Metasploitable2

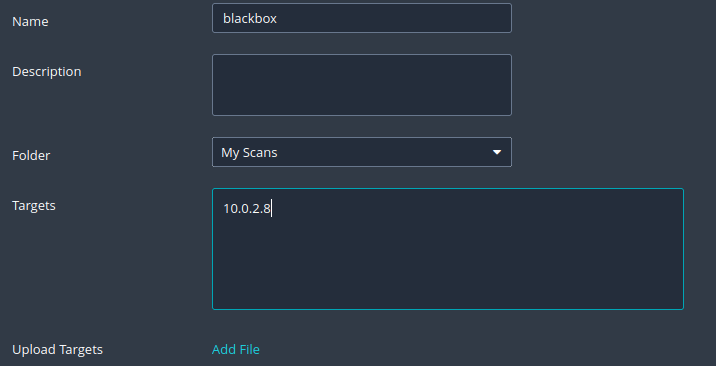
**Ejercicio 1 - Nessus Black Box**

*Realizar un análisis de vulnerabilidades sobre la máquina Metasploitable2 en modo Black Box.*

* Tipo: Basic Network Scan.
* Credenciales: Sin credenciales
* Creando informe PDF ejecutivo y PDF personalizado:
* Metasploitable2\_black\_executive.pdf
* Metasploitable2\_black\_custom.pdf

Para iniciar se comprueba el ip de la maquina metasploitable y luego realizar el escaneo básico con Nessus. Esto es un laboratorio entiendo en un entorno real se podría usar la página web u otro dato para saber la IP del dispositivo.



Se procede a realizar el escaneo básico solo con la IP. 10.0.2.8

* Creando informe PDF ejecutivo y PDF personalizado:
* Metasploitable2\_black\_executive.pdf
* Metasploitable2\_black\_custom.pdf

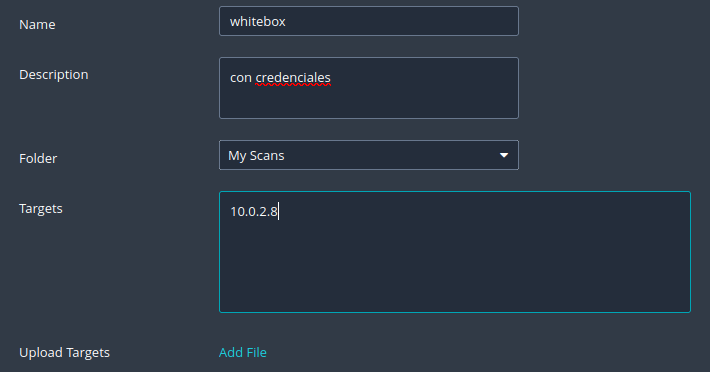
Creado y subido

**Ejercicio 1 - Nessus White Box**

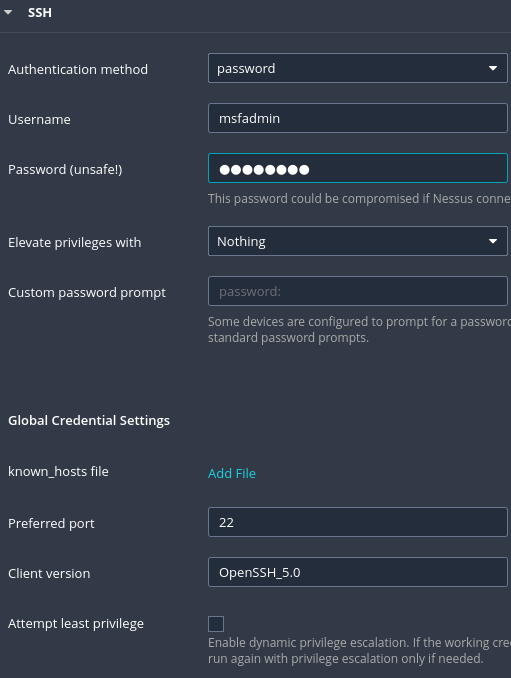
*Realizar un análisis de vulnerabilidades sobre la máquina Metasploitable2 en modo White Box.*

* Tipo: Basic Network Scan.
* Credenciales: msfadmin/msfadmin

Se procede igual hasta iniciar el escaneo, abajo la configuracion en Nessus con las credenciales y se exporta los reportes una vez terminado el escaneo.



En el grafico se abajo se ve la configuracion determinada para el whitebox con las credenciales solicitdas.



* Creando informe PDF ejecutivo y PDF personalizado:
* Metasploitable2\_black\_executive.pdf
* Metasploitable2\_black\_custom.pdf

Creados y subidos.

**Ejercicio 3 - Caso Real**

*Imagina que un cliente te solicita información por correo detallada de alguna de las vulnerabilidades de tus informes. En base a esto, desarrolla una explicación detallada de la vulnerabilidad que elijas.*

Estimados Señores,

Hacemos referencia a su correo anterior con relación a su consulta acerca de vulnerabilidades criticas de su servidor. Si bien hemos hallado varias vulnerabilidades criticas en nuestro escaneo, quisiera comentarle en particular una que es urgente sea mitigada, teniendo en cuenta el volumen de ataques recibos.

Hemos detectado entre otras, que el software de servidor web es obsoleto, esta es es una vulnerabilidad de alto riesgo que es una de las que se encuentran con mayor frecuencia en las redes de todo el mundo y normalmente pasa desapercibido debido a la falta de alertas y es muy fácil de resolver. Según la versión que utilizan en su compañía, el servidor web remoto está obsoleto y su vendedor o proveedor ya no lo mantiene. La falta de soporte implica que no se lanzarán nuevos parches de seguridad para él, es decir, que, con la aparición de nuevas vulnerabilidades, sus equipos no estarán protegidos contra estos debido a que es obsoleto.

Esta vulnerabilidad posee algunas opciones de solución, como quitar el servidor web si ya no es necesario. De lo contrario, actualice a una versión compatible si es posible o cambie a otro servidor. Le remito el screen de nuestro escáner.



Quedo atenta,

Saludos,