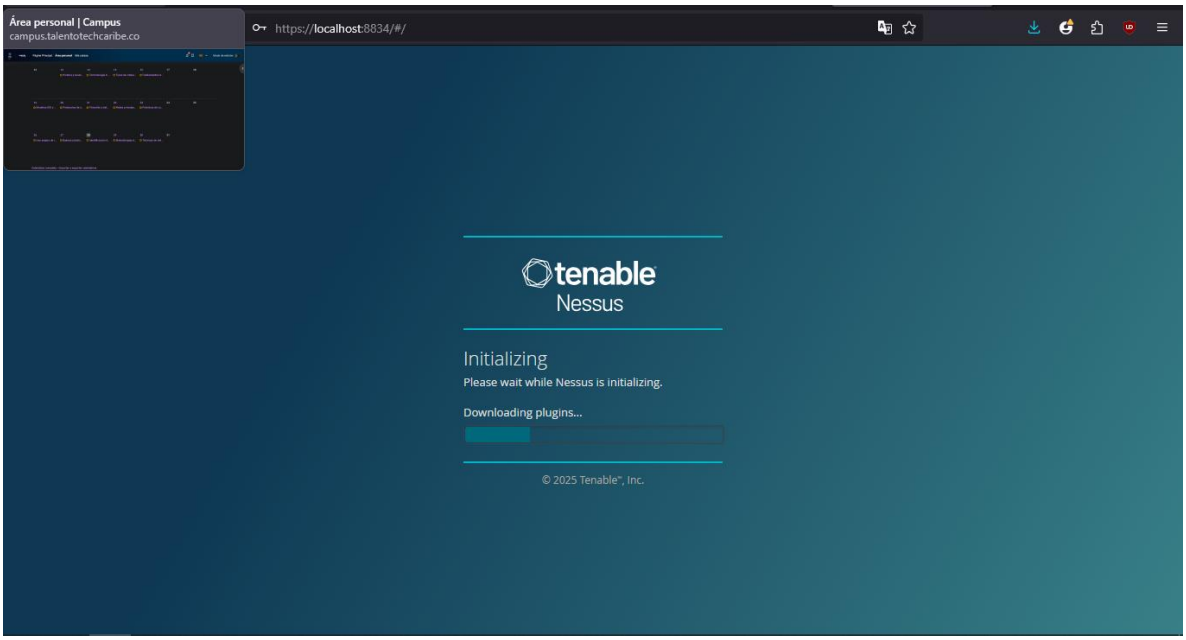
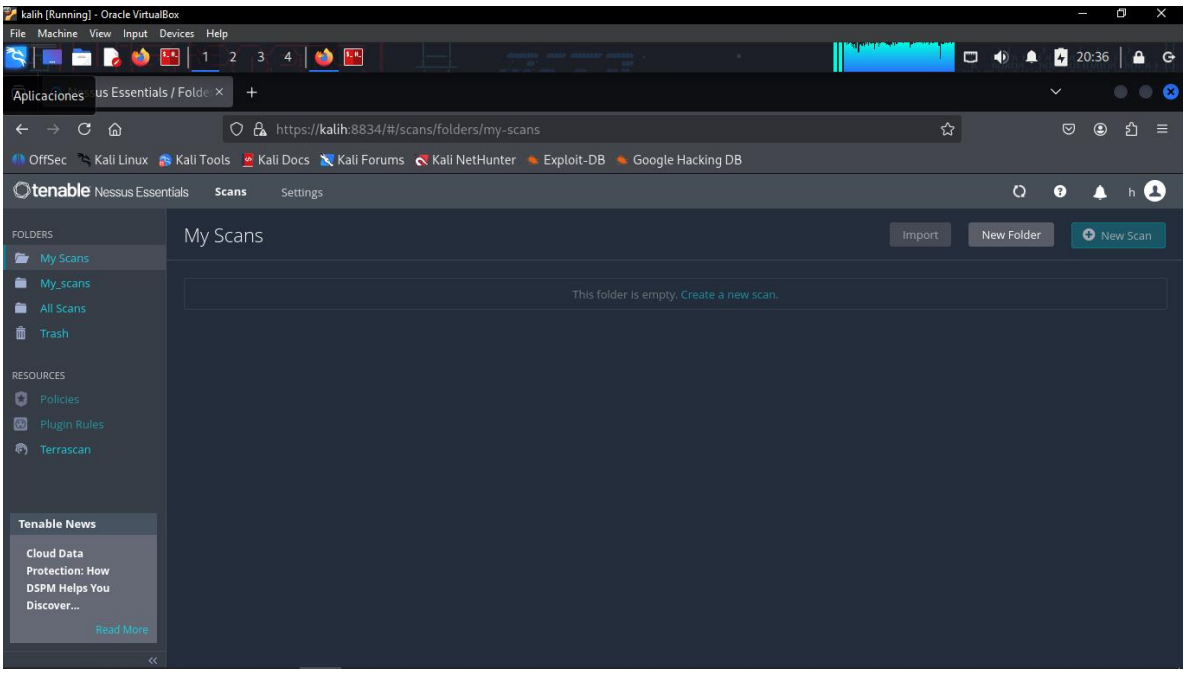
LABORATORIO 12

HECTOR DIAZ

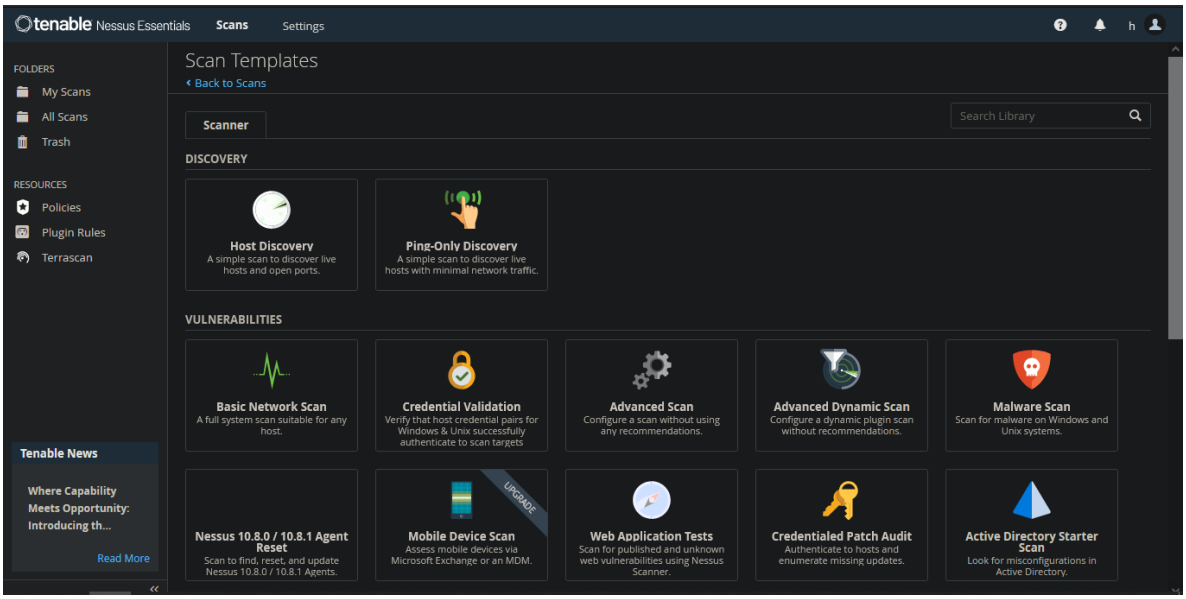
PASO 3: configuración de herramienta Nessus en windows



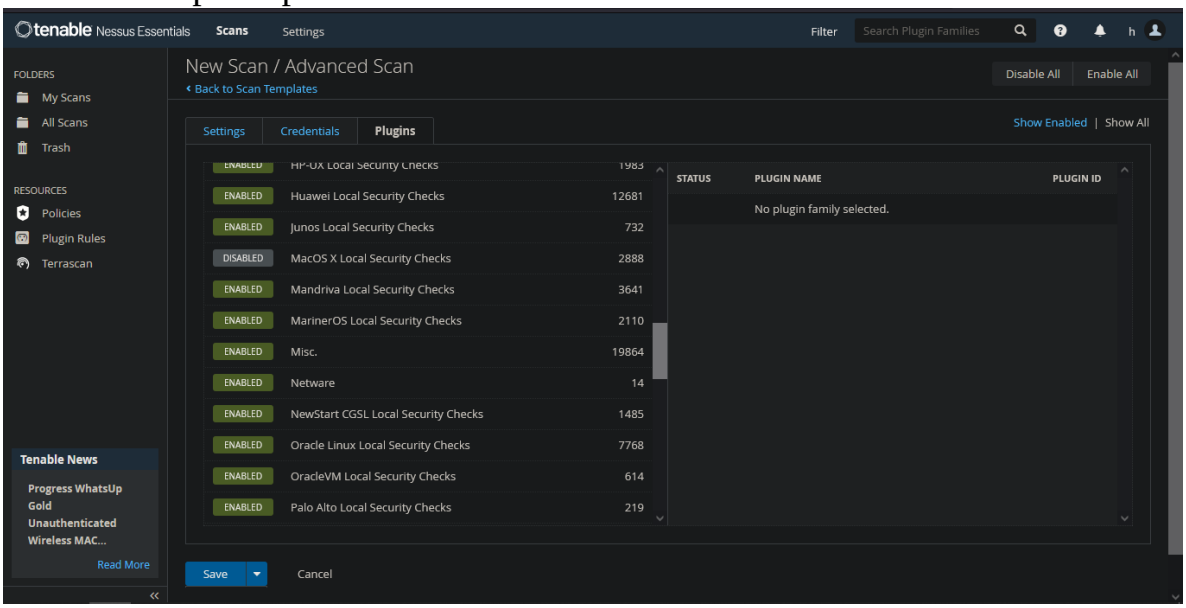
En Linux:



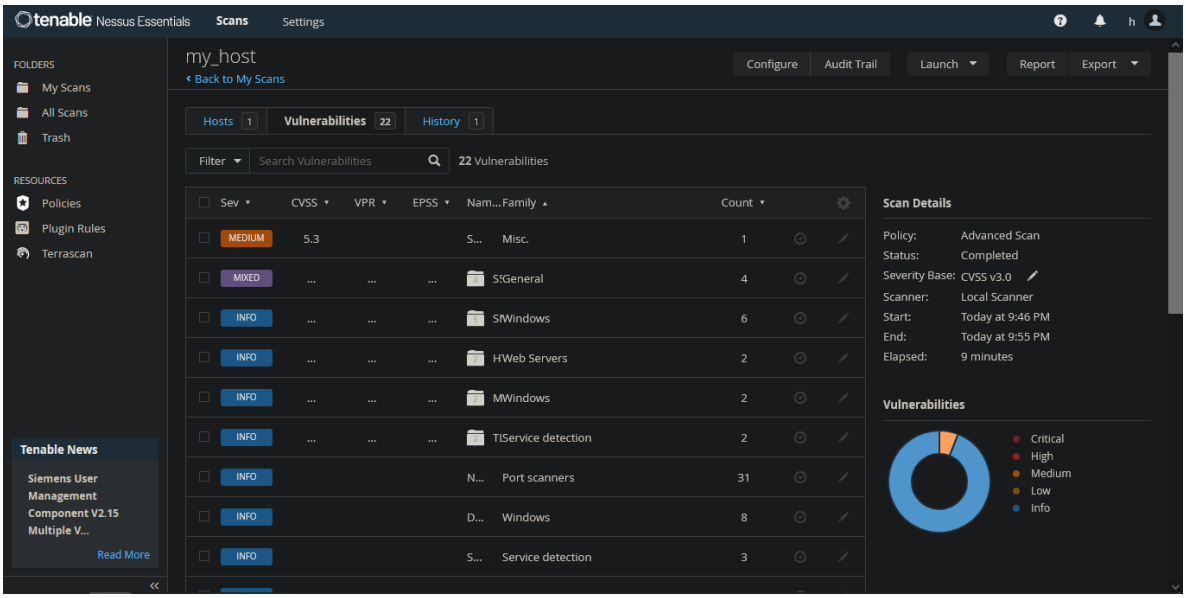
Configuración de Nessus para escaneos



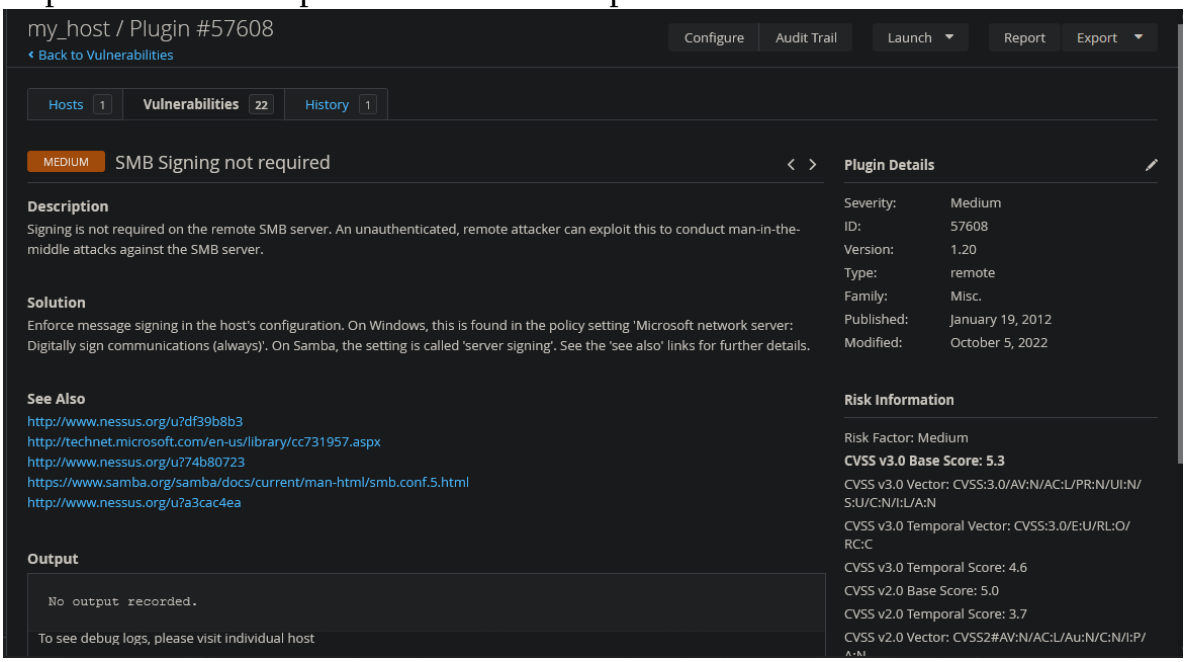
Creación de perfil personalizado en Nessus

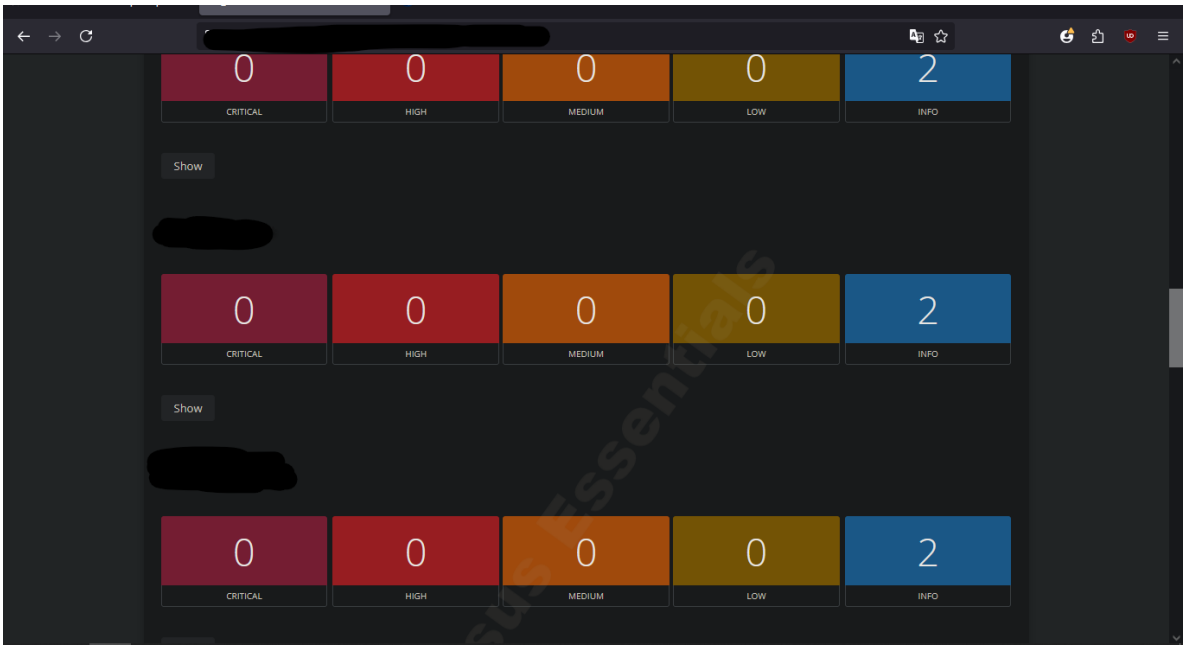


escaneo personalizado de vulnerabilidades a host



Explicar como interpretar los resultados preliminares





Parte 5: Posible soluciones de vulnerabilidades encontradas:

En el host propio se encontró dos vulnerabilidades de criticidad media, donde nos da una solución en Nessus, en el que se refiere al medio de autenticación en el que se aconseja métodos mas seguros para el servidor de samba.

Parte 6: Preparar un informe y recomendaciones para mitigar vulnerabilidades
Informe de vulnerabilidades con Nessus:
Se implementó la herramienta Nessus para escaneo de red, como identificación de dispositivos conectados a la red, y un escaneo de vulnerabilidades host.
En el escaneo de dispositivos se logró detectar 14 dispositivos en línea en los que uno llama la atención por tener diferentes puertos abiertos. Se identifica el host en un análisis, determinando que es nuestro host. Se realiza el escaneo de vulnerabilidades anteriormente, en el que nos arroja resultados con novedades, Estas novedades son 2 vulnerabilidades de criticidad media, en el que determinados que es con respecto al servidor SAMBA en el que se utiliza para la transferencia de archivos. Para la mitigación de vulnerabilidades es aconsejable seguir las recomendaciones de la herramienta samba donde nos da una solución en el que se pide mejorar la autenticación hacia el servidor.
Como recomendación adicional, se sugiere volver hacer un escaneo al host para confirmación de dichas vulnerabilidades.