Utilizar Nessus para escanear las vulnerabilidades de su servidor

Ya teniendo listo nuestro **Nessus** le haremos un SCAN a nuestro servidor web para ver que resultados nos da sobre nuestro servidor y así de esta marena buscarle una solución a los errores mostrados. En el caso de este proyecto estaremos resolviendo solo los problemas (medium, hight y critical).

En mi caso en el informe tuve hallazgos medios y hight, los cuales fueron los siguientes. Click aquí para ver el informe

Ahora vamos a presentar la solución a cada uno de los problemas.

TLS Version 1.0 Protocol Detection

Este es un problema que se da mucho en los servidores web que no tienen un buen hardening implementado, y es causado debido a que el servicio remoto acepta conexiones cifradas mediante TLS 1.0. TLS 1.0 tiene una serie de defectos de diseño criptográfico. Las implementaciones modernas de TLS 1.0 mitigan estos problemas, pero las versiones más recientes de TLS, como la 1.2 y la 1.3, están diseñadas contra estos fallos y deberían utilizarse siempre que sea posible.

Solución

Simplemente tendremos que dirigirnos a nuestro archivo **ssl.conf** que en mi caso y seguramente en el de ustedes este archivo se encuentre en la ruta **/etc/httpd/conf.d/ssl.conf** abrimos este archivo en mi caso con nano

```
nano /etc/httpd/conf.d/ssl.conf
```