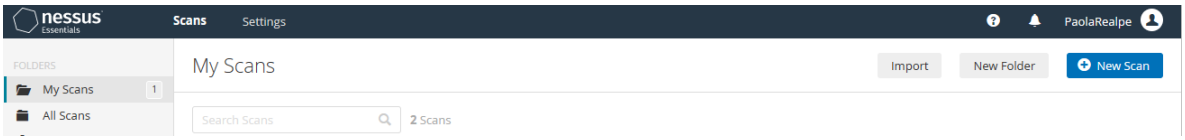
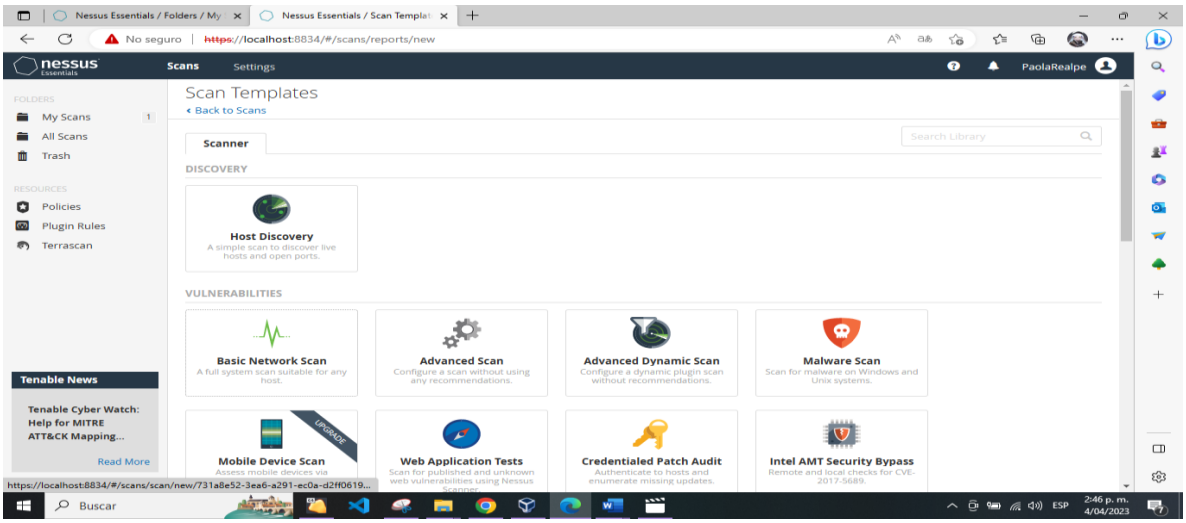
A. Descripción del proceso desarrollado para la instalación y el escaneo de un sitio web

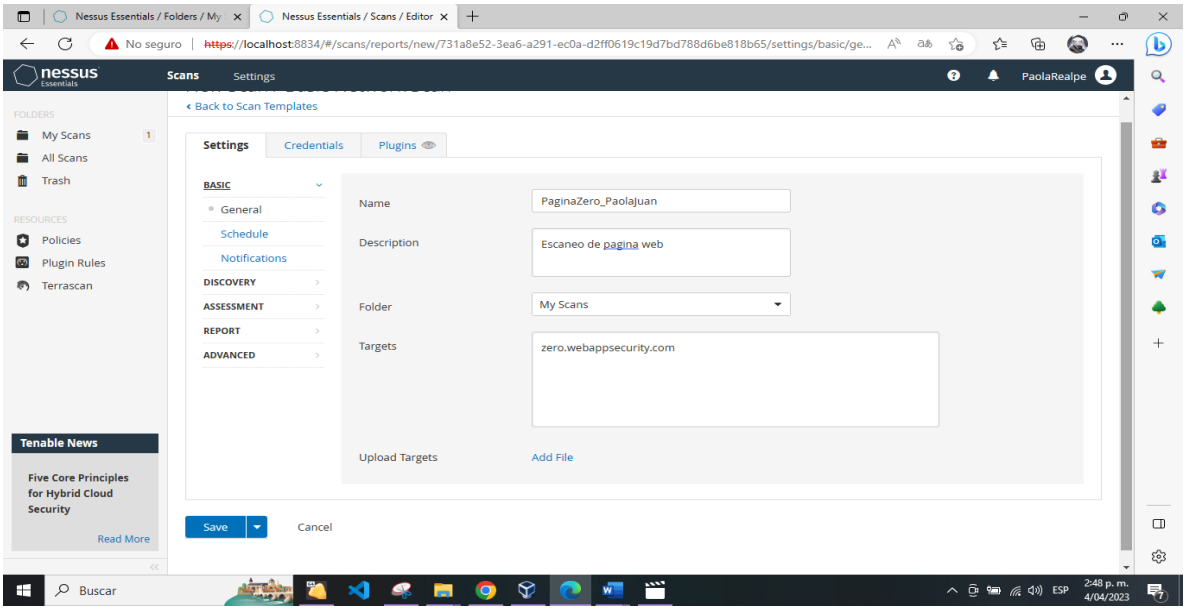
Ahora se va a realizar un escaneo de sitios web por lo que nos vamos a la opción de New Scan



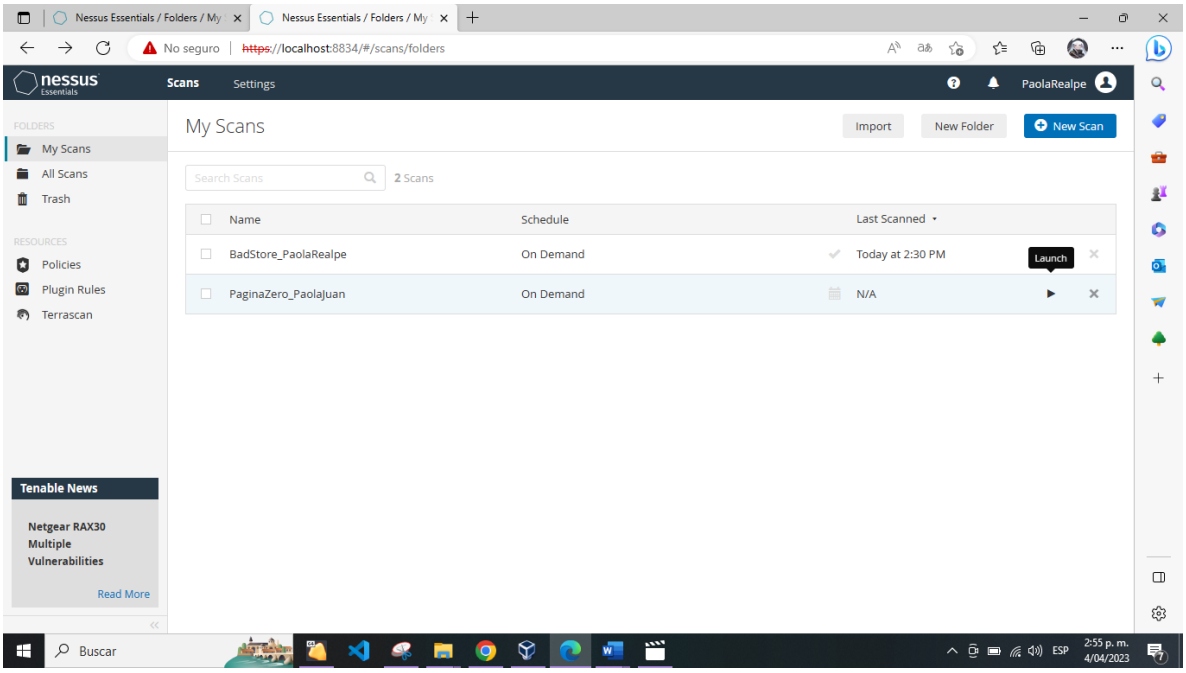
Seleccionamos Basic Network Scan o un escaneo de red básico, que se utiliza para analizar la seguridad de los sistemas activos en una red



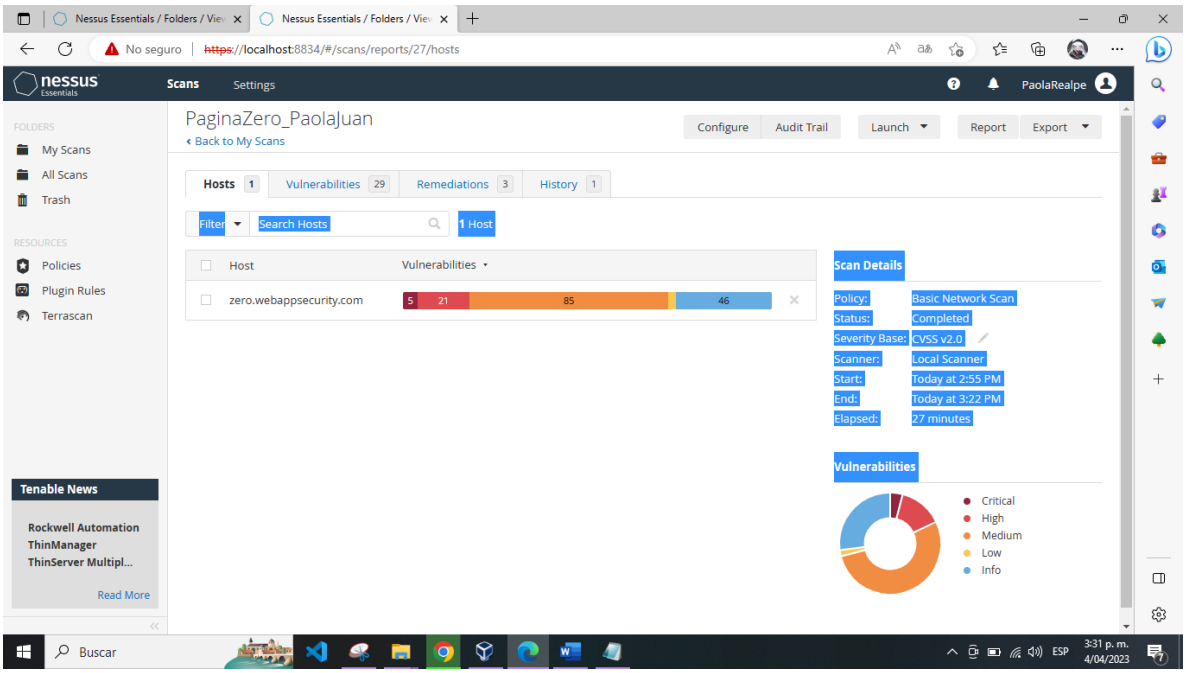
Se agrega un nombre que en este caso es **PaginaZero_PaolaJuan**, luego se escribe una descripción y en la Target se agrega el enlace url de la página web que se quiere analizar, para por último darle clic en **Save**



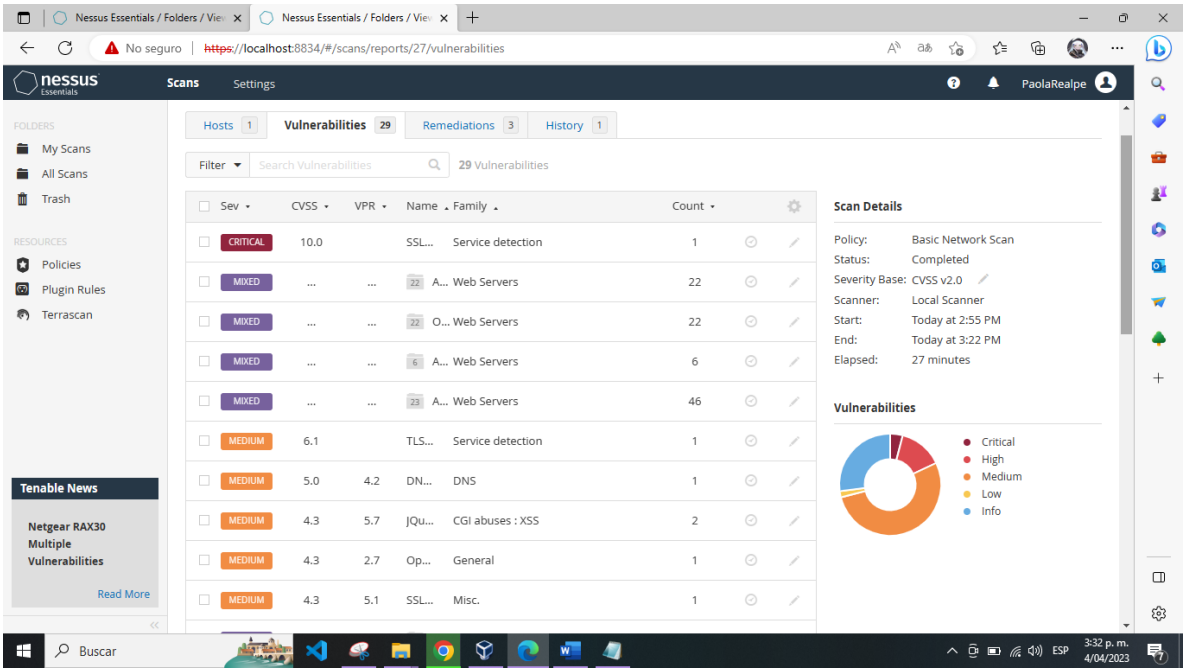
Ahora iniciamos el escaneo dando clic al icono de Start y esperamos unos minutos para que se termine el proceso

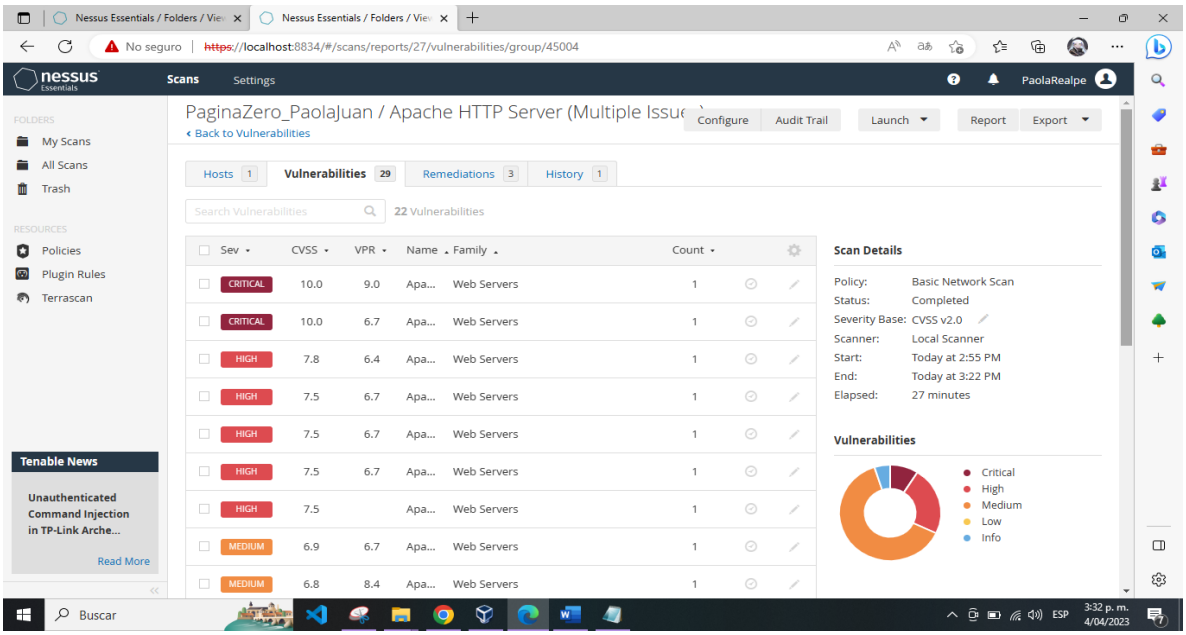


Cuando termine de analizar podemos dar clic en el scan y observar las vulnerabilidades encontradas, esta vez hay de tipo crítico y alto; es decir más peligrosas que en el anterior escaneo

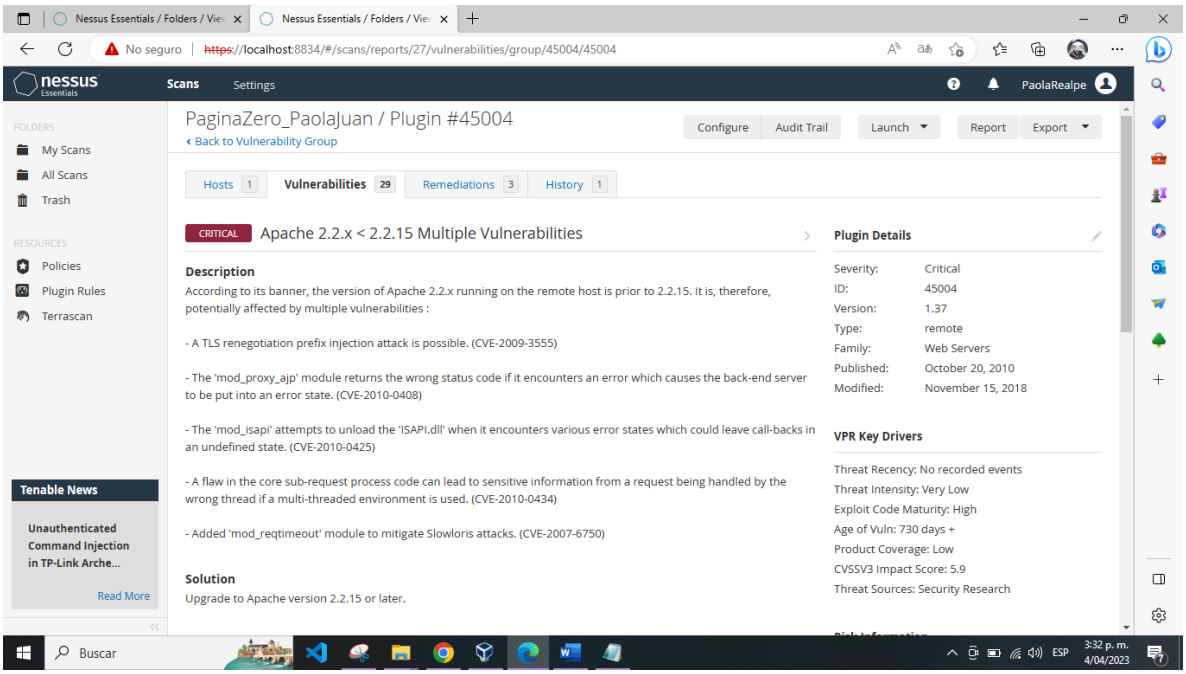


Para poder observarlas mejor le damos clic a la pestaña de vulnerabilidades y también podemos abrir los archivos de **Mixed**



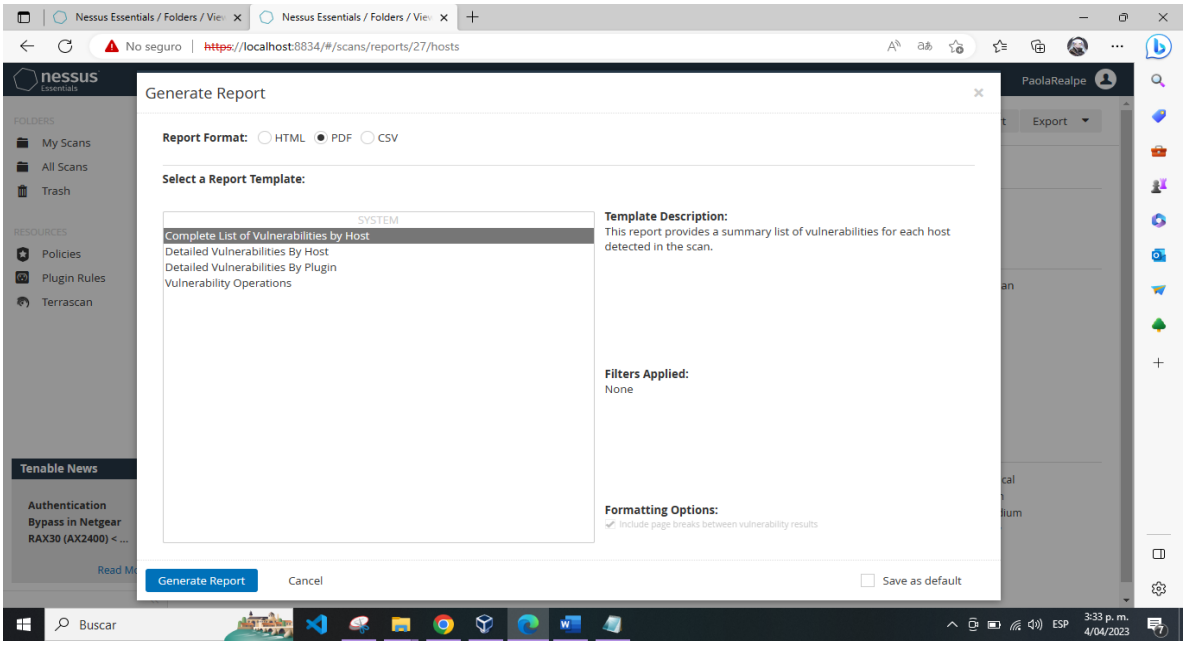


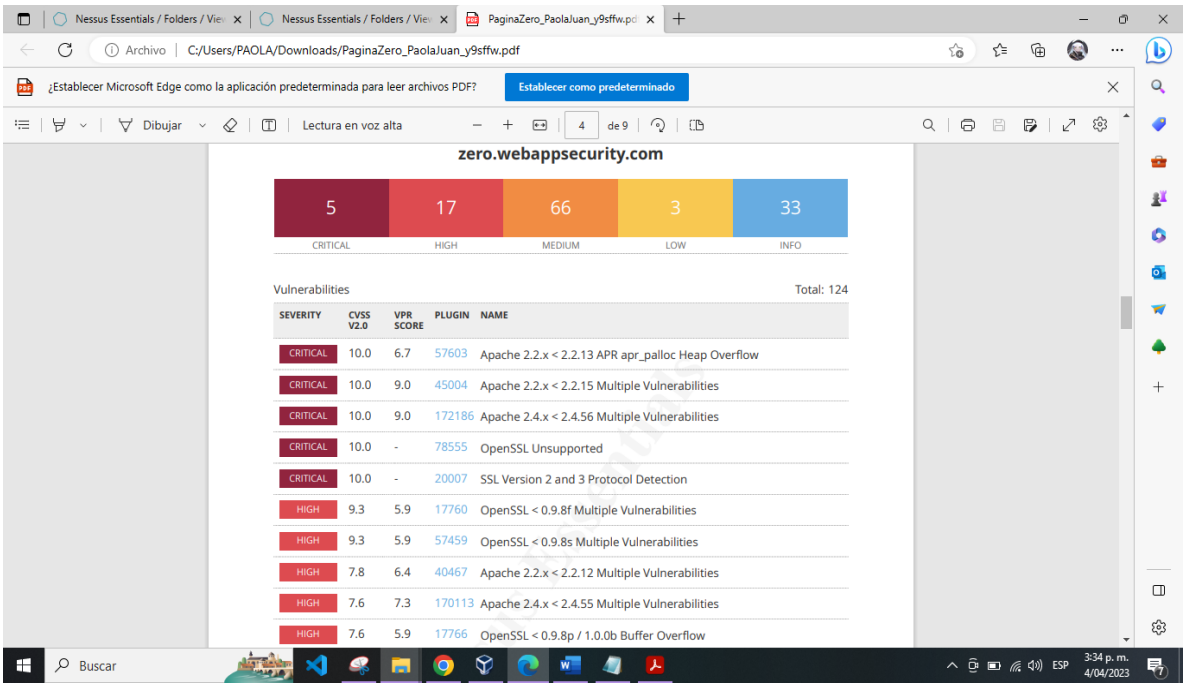
Para ver todo el contenido recolectado sobre la vulnerabilidad, junto con las posibles soluciones podemos dar clic en la primera que aparece y luego el programa de Nessus nos muestra esa información

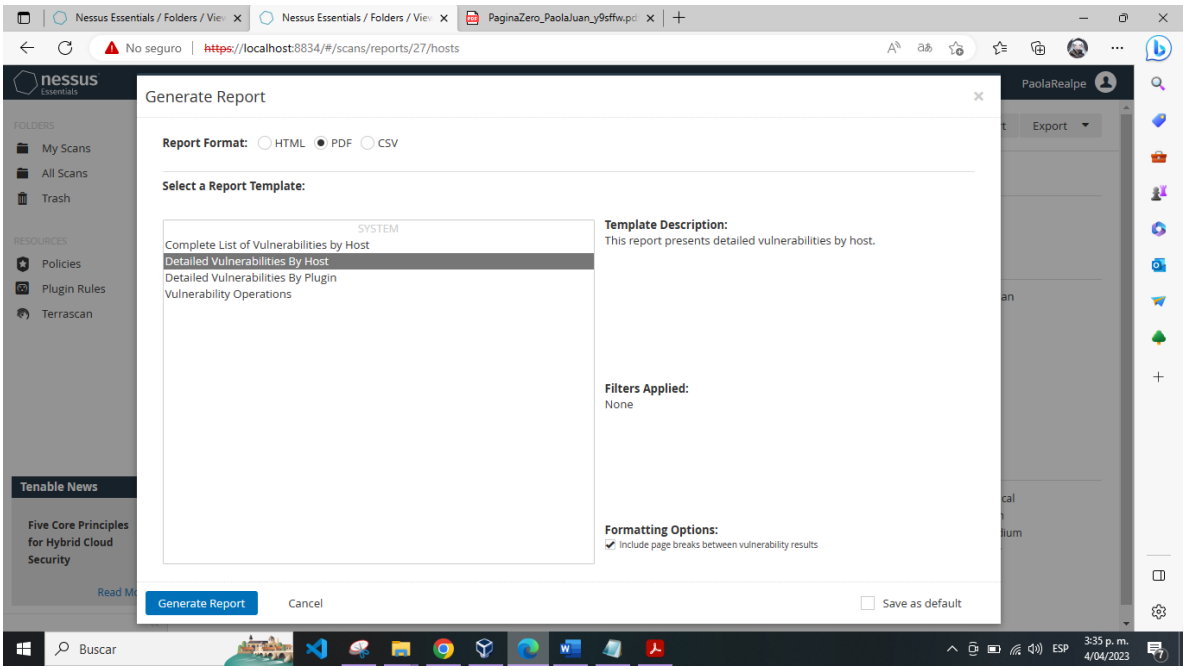


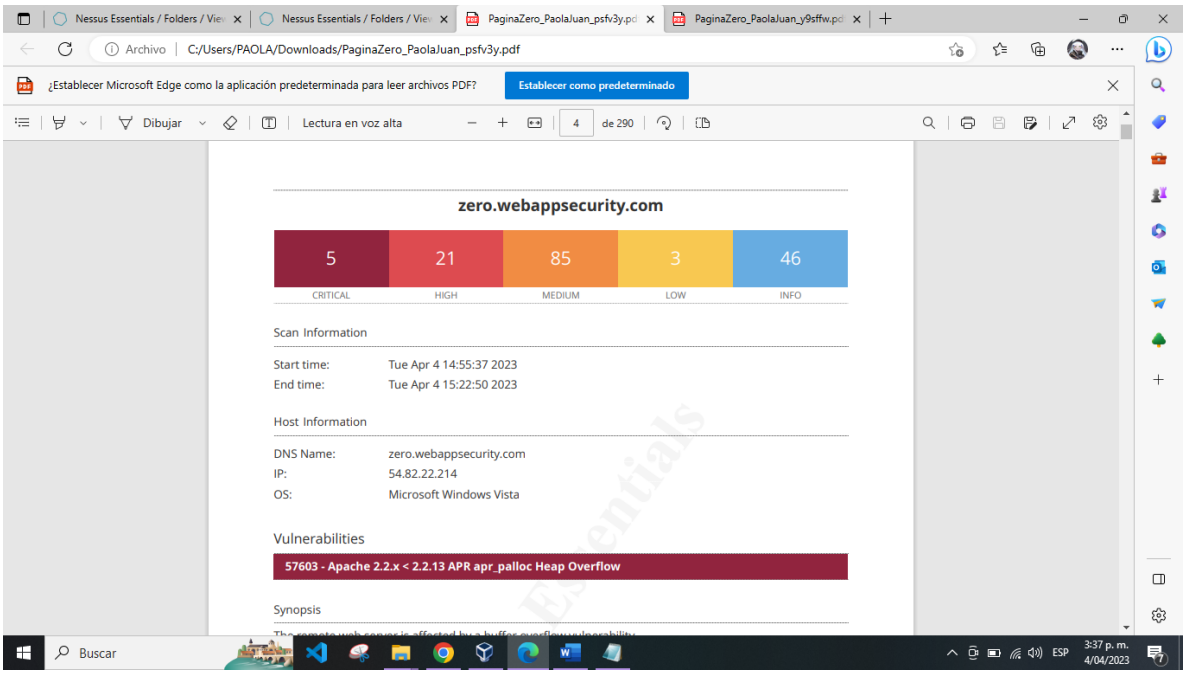
Para generar el reporte nos ubicamos en la opción de la parte superior llamada **Report** y realizamos los dos.

El primero con **Complete List** y el segundo con **Detalled Vulnerabilities**




Nessus Essentials / Folders / Vie
Nessus Essentials / Folders / Vie
PaginaZero_PaolaJuan_y9sffw.pd
Archivo | C:/Users/PAOLA/Downloads/PaginaZero_PaolaJuan_y9sffw.pdf
¿Establecer Microsoft Edge como la aplicación predeterminada para leer archivos PDF?
Establecer como predeterminado
Dibujar
Lectura en voz alta
4
de 9
zero.webappsecurity.com
5
17
66
3
33
CRITICAL
HIGH
MEDIUM
LOW
INFO
Vulnerabilities
Total: 124
SEVERITY
CVSS V2.0
VPR SCORE
PLUGIN
NAME
CRITICAL 10.0 6.7 57603 Apache 2.2.x < 2.2.13 APR apr_palloc Heap Overflow
CRITICAL 10.0 9.0 45004 Apache 2.2.x < 2.2.15 Multiple Vulnerabilities
CRITICAL 10.0 9.0 172186 Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
CRITICAL 10.0 - 78555 OpenSSL Unsupported
CRITICAL 10.0 - 20007 SSL Version 2 and 3 Protocol Detection
HIGH 9.3 5.9 17760 OpenSSL < 0.9.8f Multiple Vulnerabilities
HIGH 9.3 5.9 57459 OpenSSL < 0.9.8s Multiple Vulnerabilities
HIGH 7.8 6.4 40467 Apache 2.2.x < 2.2.12 Multiple Vulnerabilities
HIGH 7.6 7.3 170113 Apache 2.4.x < 2.4.55 Multiple Vulnerabilities
HIGH 7.6 5.9 17766 OpenSSL < 0.9.8p / 1.0.0b Buffer Overflow
Buscar
ESP
3:34 p. m.
4/04/2023


Nessus Essentials / Folders / Vie
Nessus Essentials / Folders / Vie
PaginaZero_PaolaJuan_y9sffw.pd
No seguro | https://localhost:8834/#/scans/reports/27/hosts
nessus
Essentials
PaolaRealpe
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Export
Generate Report
Report Format: HTML PDF CSV
Select a Report Template:
SYSTEM
Complete List of Vulnerabilities by Host
Detailed Vulnerabilities By Host
Detailed Vulnerabilities By Plugin
Vulnerability Operations
Template Description:
This report presents detailed vulnerabilities by host.
Filters Applied:
None
Formatting Options:
Include page breaks between vulnerability results
Generate Report
Cancel
Save as default
Tenable News
Five Core Principles for Hybrid Cloud Security
Buscar
ESP
3:35 p. m.
4/04/2023



B.Describa con sus propias palabras las vulnerabilidades encontradas en cada caso y describa con sus palabras teniendo en cuenta la documentación que sugiere nessus, como se debería solucionar o qué medidas se deben tomar para resolver la vulnerabilidad

CRITICAL - SSL Version 2 and 3 Protocol Detection (Detección de protocolos SSL versión 2)

Esta vulnerabilidad de nivel crítico que se encontró en la página web de Zero, afirma que el servicio remoto está aceptando conexiones cifradas por SSL 2.0 o la versión 3.0, las cuales cuentan con muchos problemas criptográficos debido a que no están en las versiones mas recientes; algunos de estos son:

- Esquemas inseguros que reanudan sesiones, donde un ciberdelincuente puede atacar con una intercepción en las comunicaciones haciéndose pasar como un usuario legitimo para poder leer, modificar o inyectar mensajes de comunicación, suplantando la identidad de otras personas, a este tipo de ataque también se lo conoce como Man in the Middle.
- Aplicación del SSL y TLS, a pesar de que se conoce que posee un medio seguro en versiones altas, se debe tener en cuenta que muchos de los navegadores web lo aplican como una forma insegura, por lo que el ciberdelincuente puede degradar la conexión.
- Aplicación de SSL 3 que no es apto para las comunicaciones seguras, según NIST debido a que no aplica una criptografía fuerte y confiable

SOLUCION NESSUS

Según Nessus las soluciones que se recomiendan es deshabilitar el SSL 2.0 y la versión 3.0 del mismo, debido a que presentan grandes vulnerabilidades, ya que son versiones

obsoletas de los protocolos de seguridad que suelen aplicarse en la capa de transporte para cifrar las comunicaciones, por lo que un tercero puede aprovecharse de ello para conseguir información confidencial o privada.

A cambio también sugiere utilizar el protocolo de seguridad TLS en la versión 1.2 o superior, también conocido como seguridad de capa de sockets y transporte, el cual cumple con la función de brindar una comunicación entre los sistemas informáticos de forma segura, además de utilizar conjuntos de cifrados que eviten los ataques de tipo Man in the Middle

SOLUCION INTEGRANTES DEL GRUPO

En base a la información dada, también se pueden tomar otras medidas para evitar los ataques a las capas, como es acceder a sitios web con certificado, actualizar continuamente el software, hacer uso de contraseñas seguras, evitar la conexión a redes abiertas, entre otros.

CRITICAL - Apache 2.2.x < 2.2.15 Multiple Vulnerabilities (Apache 2.2.x < 2.2.15 Múltiples vulnerabilidades)

Esta vulnerabilidad de nivel crítico que se encontró en la página web de Zero, indica que la versión de Apache 2.2 que actualmente se esta ejecutando por medio de un host remoto, es una versión inferior a la 2.2.15, por lo que no cuenta con las actualizaciones o los parches necesarios para prevenir múltiples vulnerabilidades, por lo que está expuesta para un ataque por hackers, como:

- Ataque de inyección de prefijo TLS, en el cual el atacante se aprovecha de la capacidad de renegociación de sesión para inyectar datos en la conexión antes de la autentificación para robar o modificar información y perjudicar la seguridad en la conexión entre un cliente y servidor
- Modulo mod proxy ajp, está devolviendo de forma incorrecta el código de estado, por lo que suele aparecer en back-end errores y problemas
- Error en el código de procesos de subsolicitud central en un entorno determinado que puede provocar que la información confidencial se maneje por un proceso incorrecto o equivocado
- Modulo mod_reqtimeout el cual se encarga de la mitigación de ataques por Slowloris que aprovechan las conexiones prolongadas del servidor, para agotar los recursos del mismo

SOLUCION NESSUS

La solución que brinda Nessus para esta vulnerabilidad es la actualización de Apache al 2.2.15 o una versión superior, que cuente con mejores medidas de seguridad y los parches necesarios para evitar los errores y posibles ataques de inyección.

SOLUCION INTEGRANTES DE GRUPO

Otras medidas que se pueden tomar es implementar una validación de los datos de entrada de los usuarios, emplear parámetros o consultas parametrizadas, limitar los privilegios, actualización de los componentes y el software, uso de herramientas de seguridad, etc

HIGH - Apache Tomcat Web Server SEoL (7.0.x) (Servidor web Apache Tomcat SEoL (7.0.x)

El servidor que se emplea es Apache 7.0, por lo que se conocer que nos mantenido o actualizado activamente por la Apache Software Foundation, en otras palabras, no aplican nuevas actualizaciones de seguridad, parches o correcciones de errores y vulnerabilidades, lo que puede llegar a afectar el rendimiento y la estabilidad del servidor.

SOLUCION NESSUS

La solución que brinda Nessus para esta vulnerabilidad es eliminar este servidor en tal caso de que no sea necesario y cambiar de servidor, en caso de que no pueda realizarse entonces actualizarlo a una versión de Apache más nueva que brinde mejores medidas de seguridad.

SOLUCION INTEGRANTES DEL GRUPO

Otras medidas que se pueden tomar es la implementación de configuraciones adicionales en el servidor para limitar el acceso a los recursos críticos, procesos de autentificación robusta, etc.