INSTITUTO SUPERIOR TECNOLÓGICO "HUAQUILLAS"

Nessus

Manual Técnico

Tecnología
• **Tecnología Superior en Redes y Telecomunicaciones**

Autora:

Ing. Jessica Alejandro Becerra

Huaquillas – Ecuador

2020

Índice de contenido

Indice de contenido. 2

Ïndice de figuras..... 3

1.Introducción. 4

1.1. Objetivo general 5

1.2. Objetivos específicos 5

2. Contenido técnico 6

2.1. ¿Qué es Nessus? 6

2.1.1. Lo que no es Nessus 6

2.1.2. Cómo funciona Nessus 6

2.1.3. Instalación de Nessus y escaneo básico 7

3. Responsables. 17

4. Glosario. 18

5. Referencias..... 19

Índice de figuras

Figura 1. Página web de Nessus 7
Figura 2. Activación de Nessus 8
Figura 3. Selección de versión a descargar 8
Figura 4. Comando para instalar:dpkg-i 9
Figura 5. Command activación: /etc/init.d/nessusd start 9
Figura 6. Aviso de seguridad 9
Figura 7. Nessus Essentials 10
Figura 8. Relleno de parámetros 10
Figura 9. Registro de Nessus 11
Figura 10. Creación de Usuario y contraseña 11
Figura 11. Establecer políticas en Nessus 12
Figura 12. PLantilla "Escaneo de red básico" 12
Figura 13. Dirección Ip del host a analizar 13
Figura 14. Escanéo básico de red 13
Figura 15. "Mis escaneos" 14
Figura 16. Resultados de escaneo 14
Figura 17. Interpretación de resultados 15
Figura 18. generar reporte de resultados 15
Figura 19. Generar informe 16
Figura 20. Reporte final 16

1.Introducción.

Un administrador de redes debe ser consiente de los peligros a los cuales se expone constantemente las redes de datos, por ello es necesario analizar constantemente el tráfico de la red para identificar vulnerabilidades de cualquier índole tecnológico, que pueda existir dentro de la organización. Por ello es necesario contar con políticas de seguridad y utilitarios que ayuden a mejorar la seguridad en cualquier ambiente.

Nessus es una gran herramienta diseñada para automatizar las pruebas y el descubrimiento de problemas de seguridad conocidos. Por lo general, alguien, un grupo de hackers, una empresa de seguridad o un investigador descubre una forma específica de violar la seguridad de un producto de software. El descubrimiento puede ser accidental o dirigido directamente investigación; La vulnerabilidad, en varios niveles de detalle, se libera a la comunidad de seguridad.

Esta herramienta está diseñada para ayudar a identificar y resolver estos problemas conocidos, antes de que un hacker aproveche de ellos. Nessus es una herramienta con muchas capacidades.

1.1. Objetivo general

Identificar vulnerabilidades utilizando la herramienta Nessus, minimizando los riesgos a nivel de red.

1.2. Objetivos específicos

- Realizar una correcta instalación de Nessus
- Identificar las funciones que nos ofrece la herramienta
- Escanear la red de datos identificando posibles problemas.

2. Contenido técnico

2.1. ¿Qué es Nessus?

> Nessus es una herramienta de escaneo de seguridad remota, que escanea una computadora y genera una alerta si descubre cualquier vulnerabilidad que los piratas informáticos maliciosos puedan usar para acceder a cualquier computadora que haya conectado a una red. Lo hace ejecutando más de 1200 comprobaciones en una computadora determinada, probando para ver si alguno de estos ataques podría usarse para ingresar a la computadora o dañarla. (La redacción, 2018)

2.1.1. Lo que no es Nessus

Nessus no es una solución de seguridad completa, más bien es un componente de una buena estrategia de seguridad. Nessus no previene activamente los ataques, es solo una herramienta que verifica sus computadoras para encontrar vulnerabilidades que personas no autorizadas podrían explotar. El administrador del sistema debe parchear estas vulnerabilidades para crear una solución de seguridad.

2.1.2. Cómo funciona Nessus

Las herramientas de seguridad como Nessus acceden a diversos servicios (como un servidor web, servidor SMTP, servidor FTP, etc.) en un servidor remoto. La mayoría del tráfico de red de alto nivel, como el correo electrónico, las páginas web, etc., llega a un servidor a través de un protocolo de alto nivel que se transmite de manera confiable por un flujo TCP. Para evitar que diferentes flujos interfieran entre sí, una computadora divide su conexión física a la red en miles de rutas lógicas, llamadas puertos. Entonces, si desea hablar con un servidor web en una máquina determinada, debe conectarse al puerto # 80 (el puerto HTTP estándar), pero si desea conectarse a un servidor SMTP en esa misma máquina, debe conectarse al puerto # 25).

Cada computadora tiene miles de puertos, todos los cuales pueden o no tener servicios (es decir, un servidor para un protocolo específico de alto nivel) escuchándolos. Nessus funciona probando cada puerto en una computadora, determinando qué servicio está ejecutando y luego probando este servicio para asegurarse de que no haya vulnerabilidades en él que pueda ser utilizado por un hacker para llevar a cabo un ataque malicioso. Nessus se llama un "escáner remoto" porque no necesita ser instalado en una computadora para que pueda probar esa computadora. En cambio, puede instalarlo en una sola computadora y probar tantas computadoras como desee. (Lucio, 2020, pág. 20)

2.1.3. Instalación de Nessus y escaneo básico

1. Como primer paso dirigirse a la página web https://www.tenable.com/products/nessus-essentials, donde creará un usuario para poder descargar Nessus.

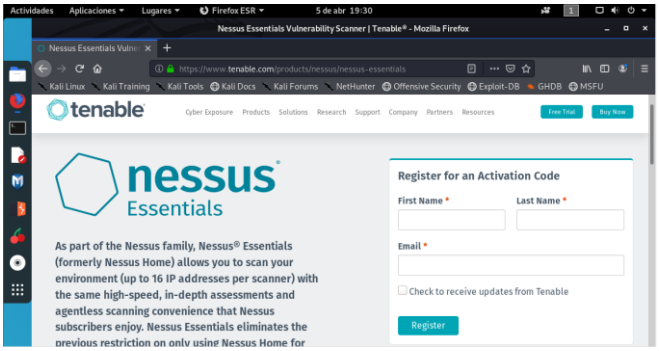

Figura 1. Página web de Nessus
Fuente: (Tenable, 2019)

2. Después automáticamente recibirá un mensaje en el correo, que contendrá el código de usuario y un enlace para descargar el instalador de Nessus

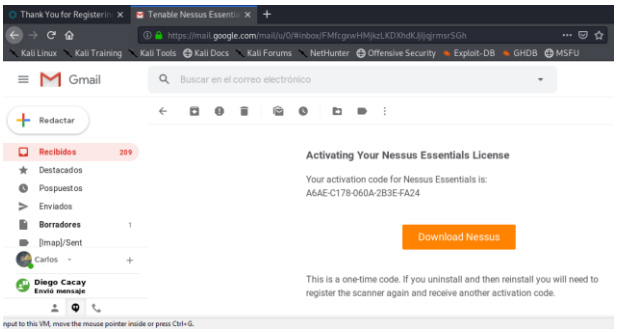

Figura 2. Activación de Nessus
Fuente: (Tenable, 2019)

3. Una vez dentro del enlace de descarga buscar la versión más adecuada para el equipo y su sistema operativo, en este caso se descargargo la versión para Kali Linux de 64bits.

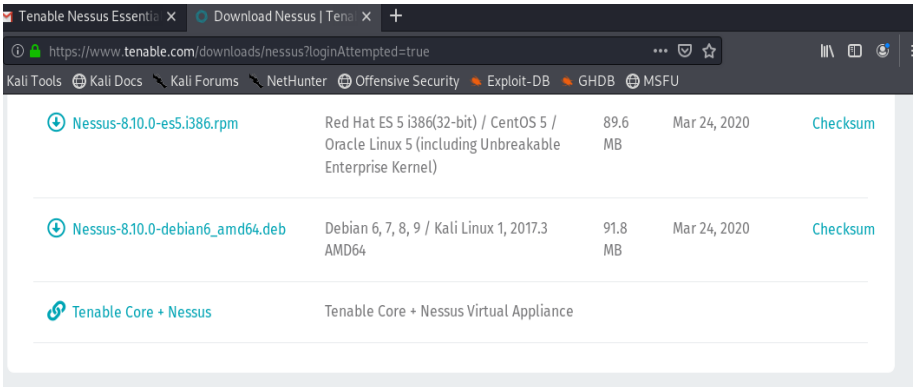

Figura 3. Selección de versión a descargar
Fuente: (Tenable, 2019)

4. Una vez completa la descarga, abrir una ventana “cmd”, donde se ingresará los siguientes comandos para iniciar la instalación y su activación.

Figura 4. Comando para instalar:dpkg-i
Fuente: (Tenable, 2019)

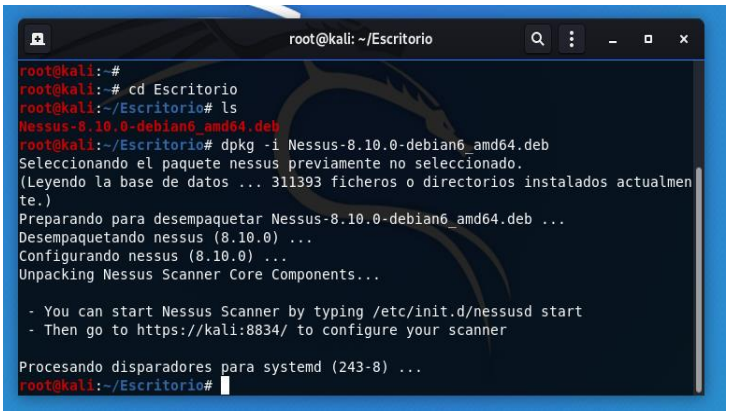

Figura 5. Command activación: /etc/init.d/nessusd start
Fuente: (Tenable, 2019)

5. Al finalizar dar clic al enlace web que se presenta, antes de entrar a la página web se desplegara un aviso de seguridad a lo cual se debe dar clic en “advanced y aceptar”.

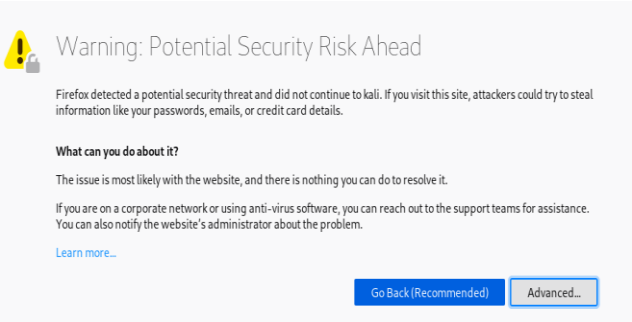

Figura 6. Aviso de seguridad
Fuente: (Tenable, 2019)

6. Al instante se presentará varias opciones de instalar Nessus a lo cual se dará clic en continuar en la primera opción.

Figura 7. Nessus Essentials
Fuente: (Tenable, 2019)

7. Después debe ingresar los datos que solicita y clic en continuar

Figura 8. Relleno de parámetros
Fuente: (Tenable, 2019)

8. Ahora pedirá ingresar el código de activación que al principio enviaron al correo.

Figura 9. Registro de Nessus
Fuente: (Tenable, 2019)

9. Por último, debe crear un nombre de usuario y una contraseña, y debe esperar a que inicie Nessus.

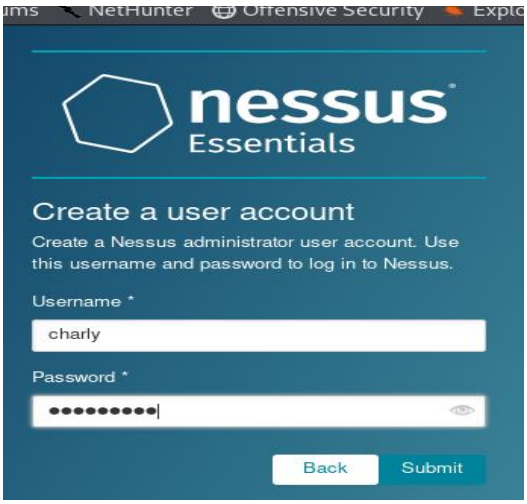

Figura 10. Creación de Usuario y contraseña
Fuente: (Tenable, 2019)

10. Una vez que se esté en la herramienta Nessus, se debe establecer las políticas para realizar los escaneos de vulnerabilidades. Existe la opción de crear nuevas políticas o por lo contrario utilizar plantillas que contienen cargadas las políticas.

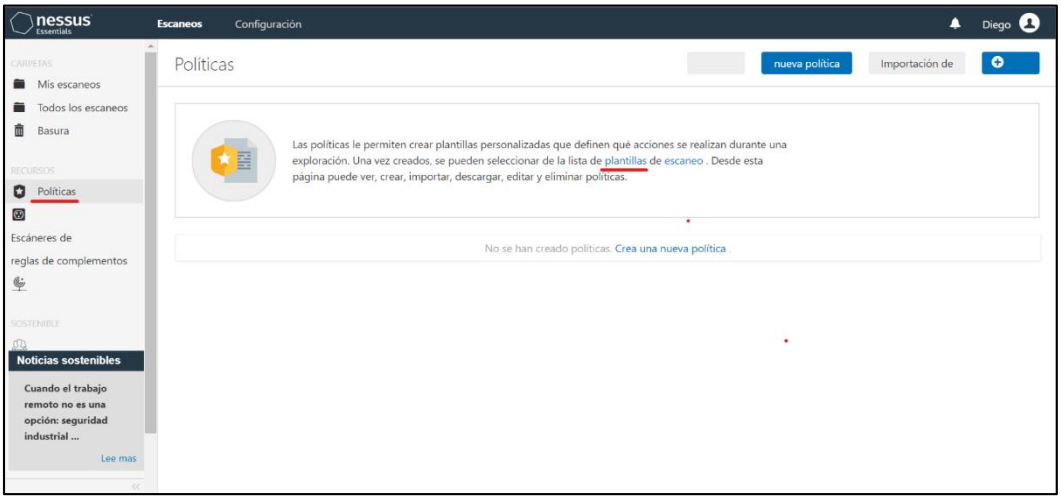

Figura 11. Establecer políticas en Nessus
Fuente: (Tenable, 2019)

11. A continuación, se presenta una serie de plantillas, entre ellas se encontrarán unas de pago, se debe escoger la plantilla que se apegue al tipo de escaneo que se necesita realizar, en este caso se escogió un escaneo de red básico.

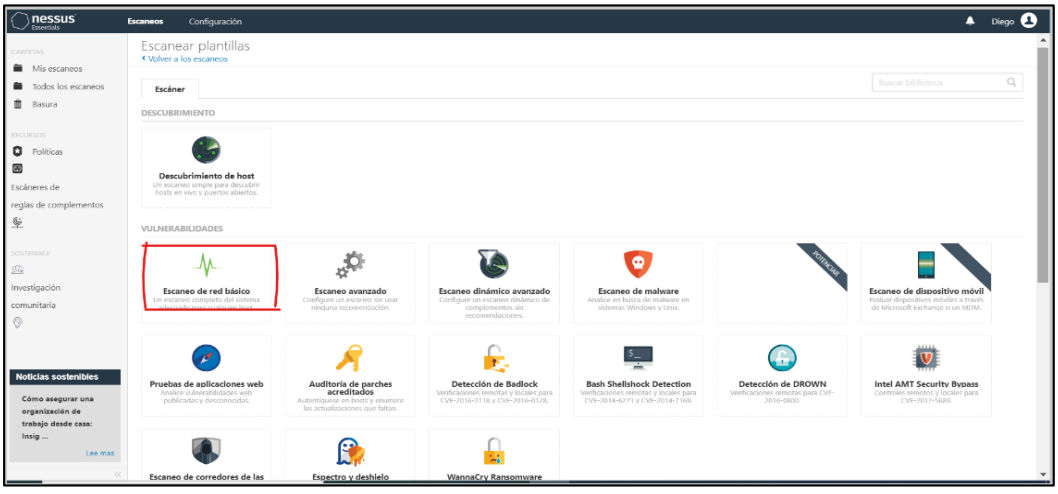

Figura 12. PLantilla "Escaneo de red básico"
Fuente: (Tenable, 2019)

12. Una vez allí, debe asignar un nombre y una descripción al escaneo que se debe realizar, luego ingresar la dirección Ip del host que se va a analizar o en su defecto poner un rango de direcciones Ip e incluso analizar toda la red.

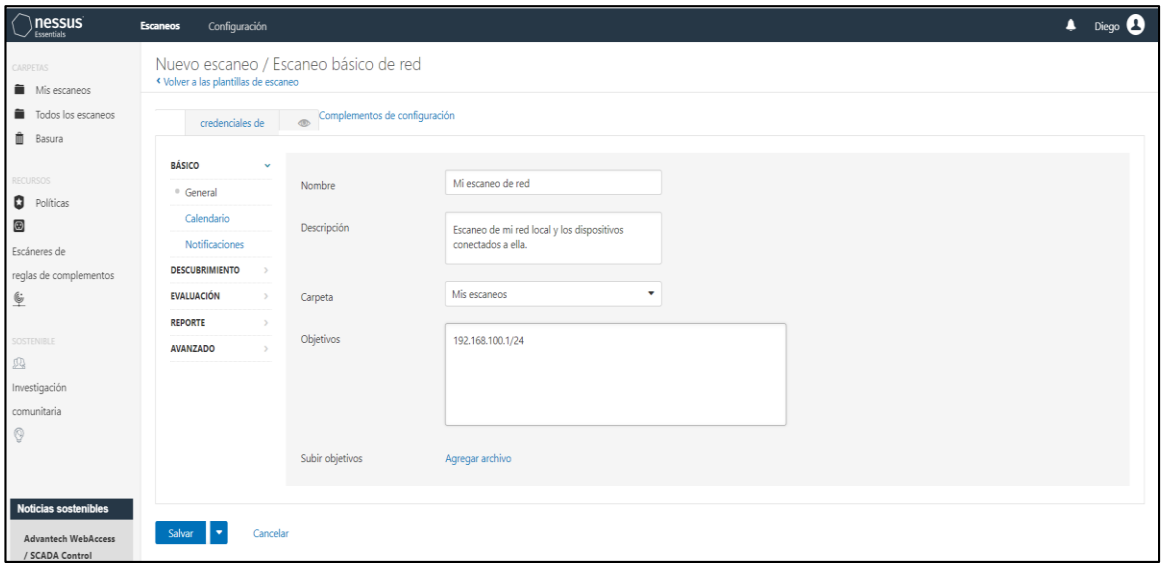

Figura 13. Dirección Ip del host a analizar
Fuente: (Tenable, 2019)

13. También se puede configurar otras opciones como descubrimiento, evaluación, reporte y avanzado, que permite al usuario configurar ciertos parámetros previos al escaneo. Una vez configurados o dejados por defecto, cual sea el caso dar clic en salvar.

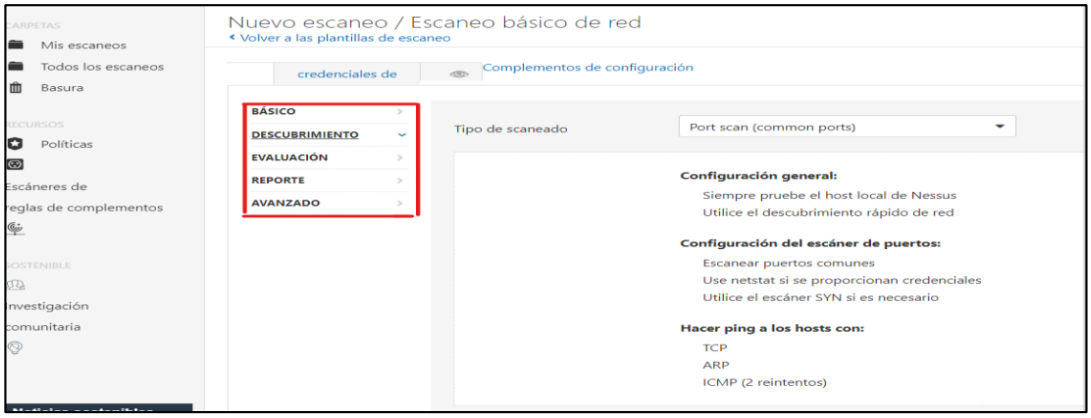

Figura 14. Escanéo básico de red
Fuente: (Tenable, 2019)

Dentro de la carpeta “Mis escaneos” se crea el escaneo con las políticas que se configuró, solo debe dar clic en “lanzamiento” para empezar con el análisis de vulnerabilidades.

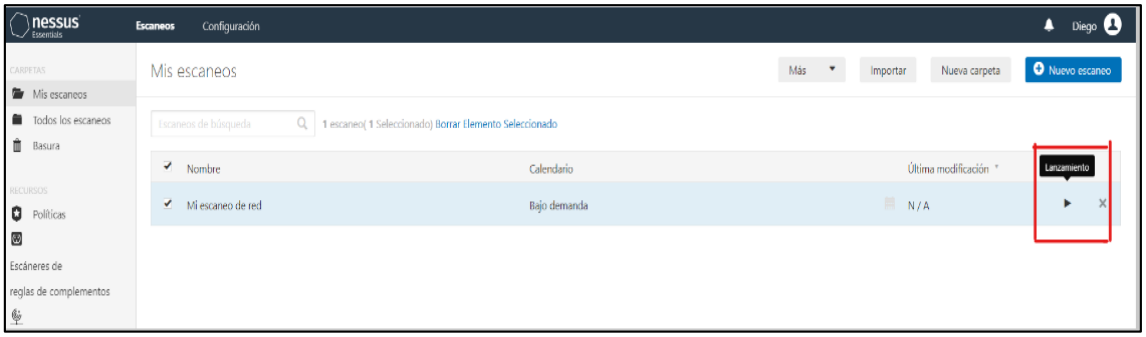

Figura 15. "Mis escaneos"
Fuente: (Tenable, 2019)

14. Luego de esperar que la herramienta Nessus termine de hacer el escaneo muestra los resultados, donde se listan por la dirección ip del host, además muestra la cantidad total de vulnerabilidades y la intensidad o estado de las mismas.

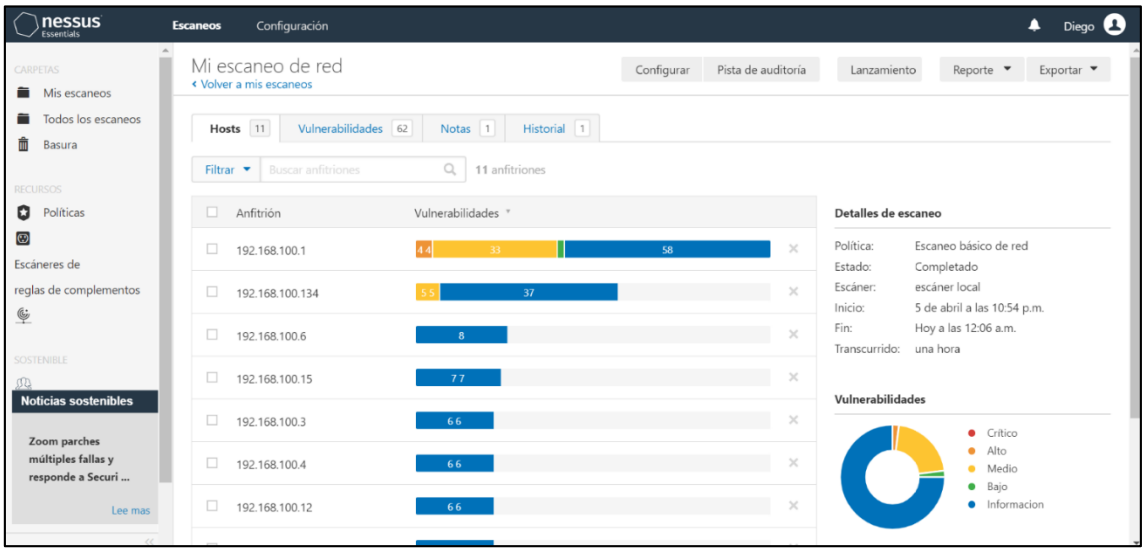

Figura 16. Resultados de escaneo
Fuente: (Tenable, 2019)

15. Basta con dar un clic en cualquiera de las direcciones ip analizadas para ver con detalle cual es la vulnerabilidad y a que familia pertenece.

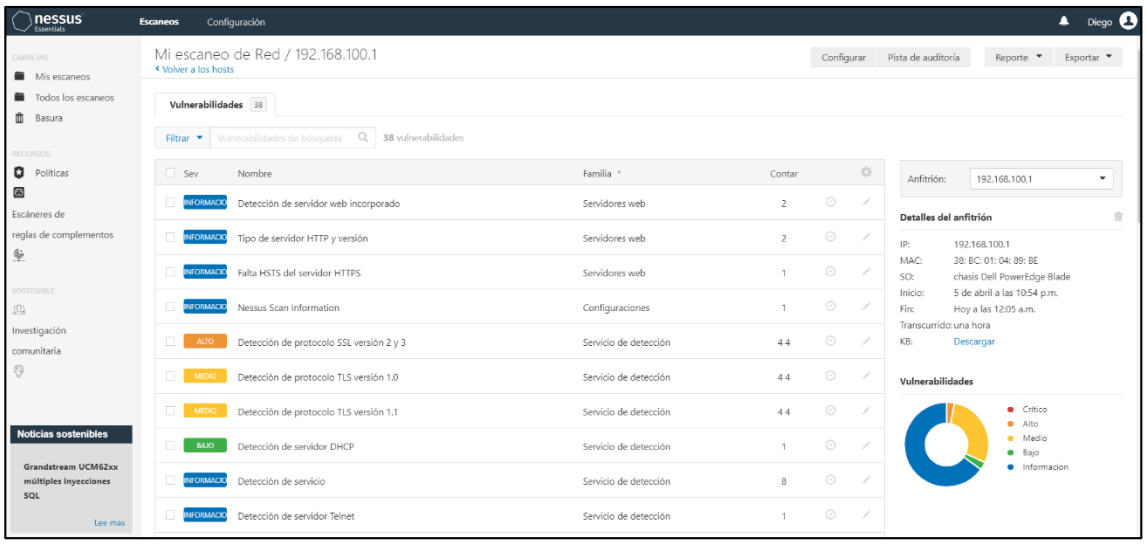

Figura 17. Interpretación de resultados
Fuente: (Tenable, 2019)

16. Una vez realizado el análisis se puede generar un reporte en formato HTML, como se ve a continuación.

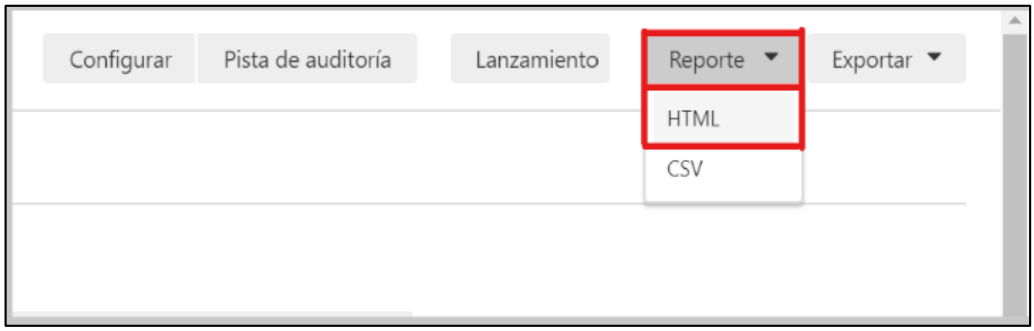

Figura 18. generar reporte de resultados
Fuente: (Tenable, 2019)

17. Una vez allí se escoge la opción “Resumen ejecutivo” y luego clic en “Generar Informe”

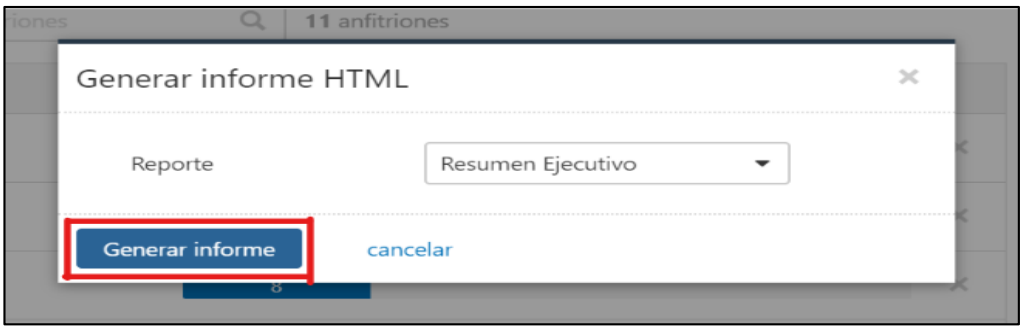

Figura 19. Generar informe
Fuente: (Tenable, 2019)

18. Luego se genera y descarga un archivo con el reporte, donde se tendrá detallado y organizado los resultados del análisis.

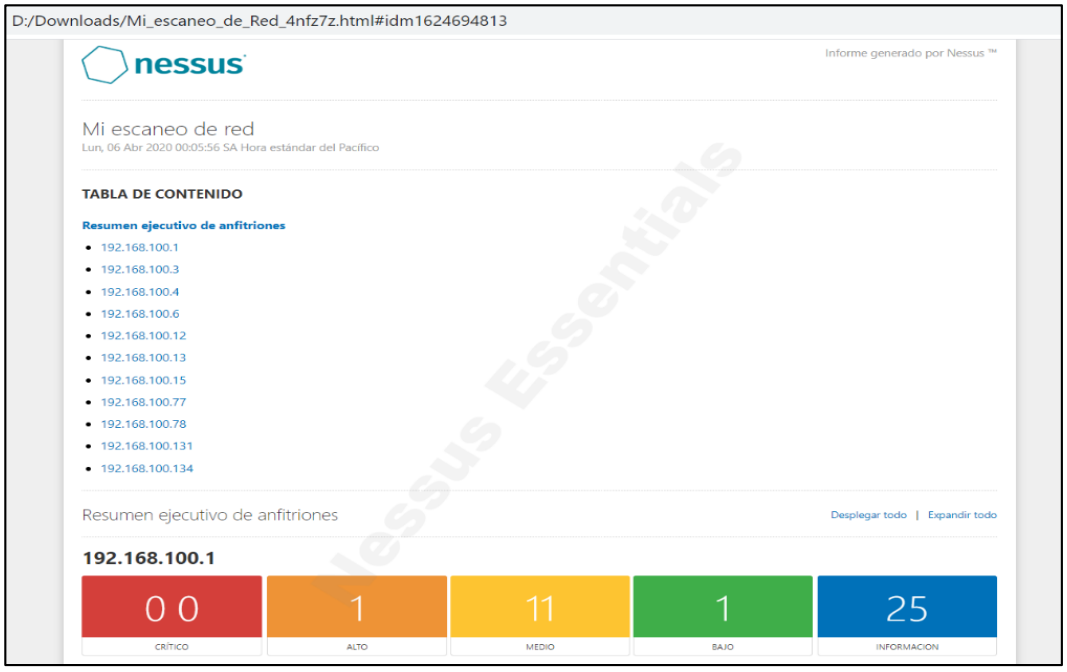

Figura 20. Reporte final
Fuente: (Tenable, 2019)

3. Responsables.

Ingeniera en sistemas

Formación:

- Universidad del Azuay - Certificación en Administración de Base de Datos y Herramientas Ofimáticas

Experiencia:

- Docente en educación tecnológica por 7 años - Asesora en proyectos de titulación - Coordinación académica del Instituto Huaquillas por 3 años - Coordinación de vinculación por 1 año.

Responsable:

Ing. Jessica Alejandro Becerra

Revisado y Aprobado por:

Ing. Jorge David Herrera Sarango

4. Glosario.

IP: (Internet Protocol) Protocolo de Internet

5. Referencias

La redacción. (06 de 04 de 2018). *Las mejores 19 herramientas de hacking y penetración para Kali Linux*. Obtenido de LabLinux: https://laboratoriolinux.es/index.php/-noticias-mundo-linux-/software/20398-las-mejores-19-herramientas-de-hacking-y-penetracion-para-kali-linux-2.html

Lucio, A. (2020). Análisis para detectar amenazas y vulnerabilidades en la red del ISTB de la ciudad de Babahoyo. *Examen complexivo*. Babahoyo, Los Ríos, Ecuador: Universidad Técnica de Babahoyo.

NESSUS. org. (22 de febreo de 2017). Obtenido de https://www.cs.cmu.edu/~dwendlan/personal/nessus.html

OpenVAS.org. (s.f.). *OpenVAS - Open Vulnerability Assessment Scanner.* Obtenido de openvas.org: https://www.openvas.org/

Tenable. (04 de 11 de 2019). *tenable*. Obtenido de https://es-la.tenable.com/