

## **Actividad 1 – Detección y Prevención de Ataques de Acceso**

### **Seguridad Informática II**

### **Ingeniería en Desarrollo de Software**

**Tutor: Jessica Hernández Romero**

**Alumno: Kathya Viridiana Chávez Domínguez**

**Fecha: 29/09/2024**

## Índice

Introducción .....	3
Descripción .....	4
Justificación.....	5
Desarrollo .....	6
Incidencias encontradas .....	6
Reporte .....	15
Análisis e identificación de mejoras .....	20
Conclusión.....	22
Referencias .....	23

## Introducción

La detección y prevención de ataques de acceso se vuelve cada vez más difícil a medida que las organizaciones expanden su presencia en la nube, conectan más dispositivos a internet y adoptan un modelo de trabajo híbrido. Estos factores incrementan las oportunidades para que actores malintencionados exploten vulnerabilidades y se aprovechen de la fragmentación en las herramientas de seguridad con diferentes tipos de tácticas. Una estrategia efectiva para la detección de amenazas debe ser capaz de detener un ataque antes de que se convierta en un riesgo.

A través de esta actividad, conoceremos la importancia de identificar y detener diferentes ataques de acceso, considerando los riesgos que suponen tanto para los usuarios como para las empresas. Para lograrlo, utilizaremos un software que nos permita detectar y prevenir ataques al sistema. Finalmente, analizaremos e identificaremos áreas de mejora para optimizar la seguridad, aplicando buenas prácticas que nos ayuden a detectar cualquier tipo de amenaza.

## Descripción

En esta ocasión, se busca implementar técnicas de protección ante ataques de explotación y acceso no autorizado a sistemas, llevando a cabo auditorías de red mediante el uso de herramientas tecnológicas, ya sean especializadas o que cuenten con funcionalidad de auditoría.

Para ello, es fundamental analizar los siguientes factores que resaltan la importancia de la seguridad:

- ✓ Prevenir los ataques de acceso
- ✓ Prevenir accesos a las redes
- ✓ Monitoreo completo de la red

Para lograrlo, será necesario instalar y utilizar un software que permita detectar y prevenir ataques tanto al sistema como a la red. En la auditoría de vulnerabilidades en la red se requiere realizar las siguientes actividades:

- ✓ Instalar y analizar el equipo
- ✓ Analizar un equipo en búsqueda de posibles ataques como son virus, accesos o percances en red.
- ✓ Adjuntar el reporte generado desde la herramienta o capturar el resultado del análisis

Al finalizar redactaremos una conclusión sobre la importancia de lo realizado en la actividad dentro del campo laboral o vida cotidiana.

## Justificación

La detección de amenazas es tan necesaria como cualquier otro protocolo o medida de seguridad. El papel de estos procesos es fundamental para detener los ataques antes de que causen daños irreparables. Al identificar y neutralizar amenazas a tiempo, las empresas pueden evitar que el impacto se extienda a otras áreas críticas de la organización

Implementar y mantener un sistema efectivo de detección de amenazas es una de las mejores prácticas para reducir riesgos y vulnerabilidades. Además, ofrece diferentes beneficios, como el ahorro de tiempo y recursos, la generación y preservación de la confianza del cliente, el cumplimiento normativo y la protección de información sensible. Cada uno de estos aspectos es esencial para asegurar el éxito a largo plazo de cualquier organización. Como podemos ver, la detección y prevención de amenazas no solo protege a una empresa de posibles consecuencias imprevistas, sino que también puede ser clave para evitar situaciones críticas, desde la pérdida de confianza hasta la quiebra,

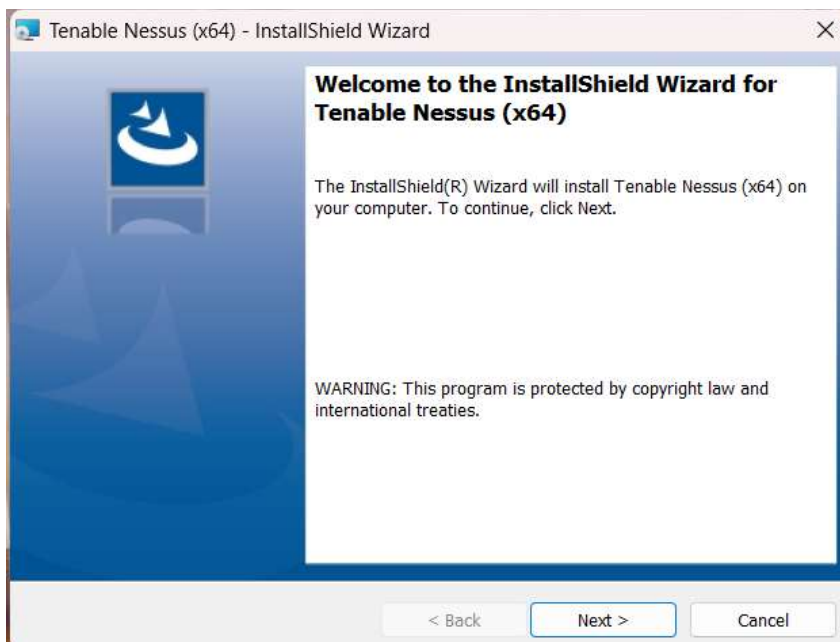
## Desarrollo

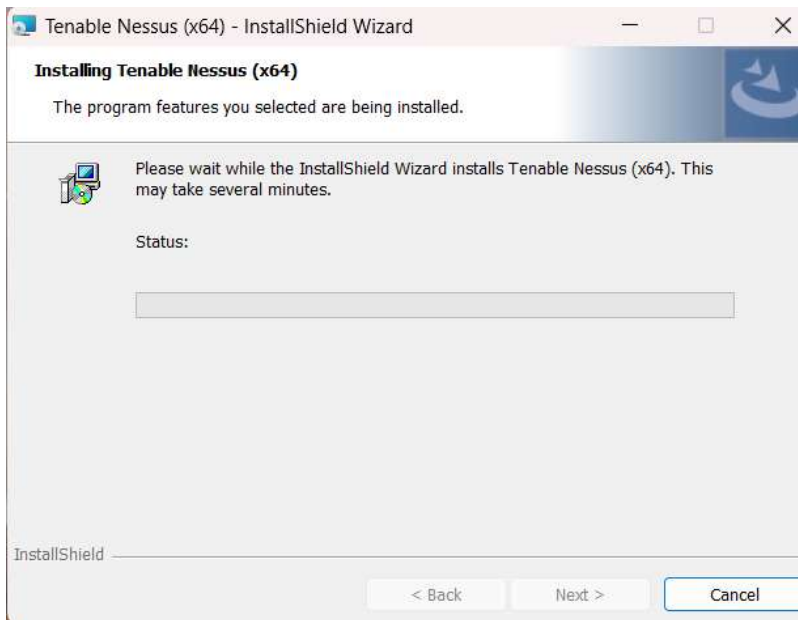
### Incidencias encontradas

Para esta actividad vamos a dar inicio con la descarga de Nessus, un programa de ciberseguridad con versiones tanto de código abierto como de pago, cuya función es escanear las vulnerabilidades de distintos sistemas operativos.

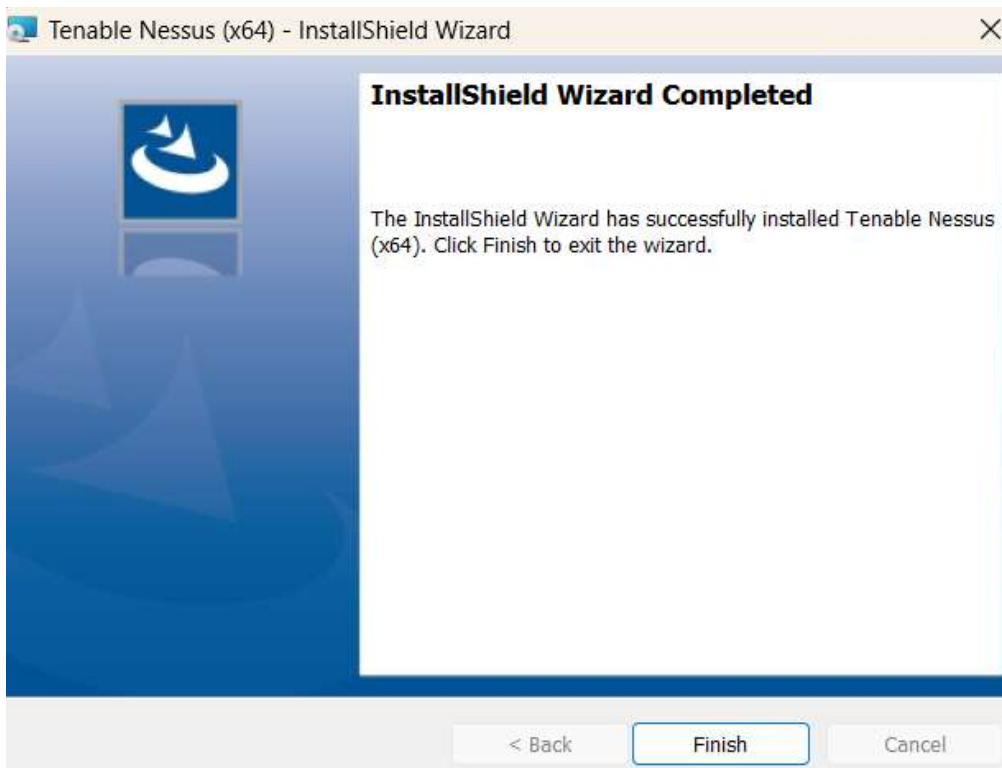


Como podemos observar, descargar e instalar Nessus es un proceso muy sencillo, ya que este programa está disponible para distintas versiones y sistemas operativos.





Una vez que hemos instalado el programa podremos ver el aviso del sistema, es importante darle en la opción de “finalizar” para continuar con el proceso.



Una vez que ha sido descargado podremos ver la página de Nessus en donde nos permite conectarnos via SSL, el cual significa establecer una conexión segura y cifrada entre el cliente y el servidor de Nessus utilizando el protocolo SSL/TLS.

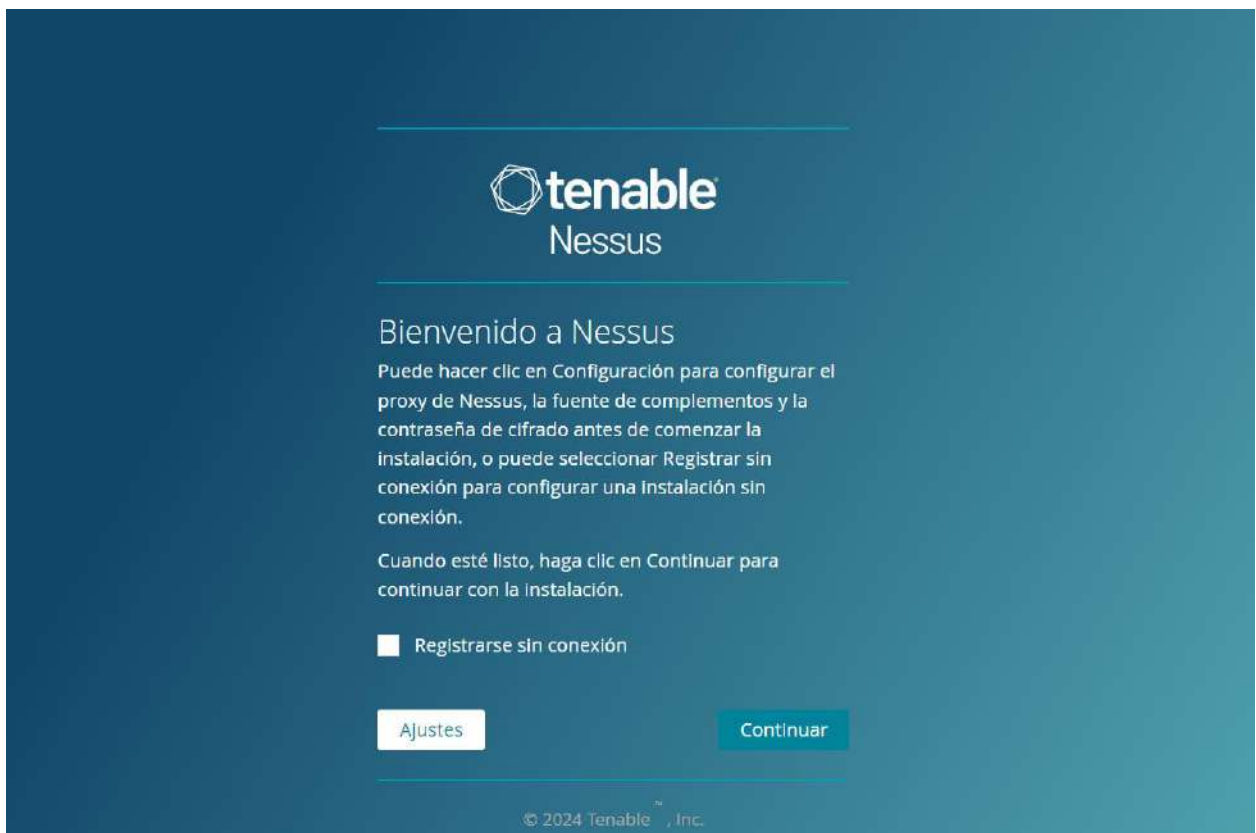


Una vez seleccionada la opción de Conectar vía SSL, podremos observar una pantalla de advertencia en donde nos indica que esta conexión no es privada, por lo que debemos ingresar a “Opciones avanzadas” y “Permitir conexión por localhost” para poder avanzar de manera correcta.





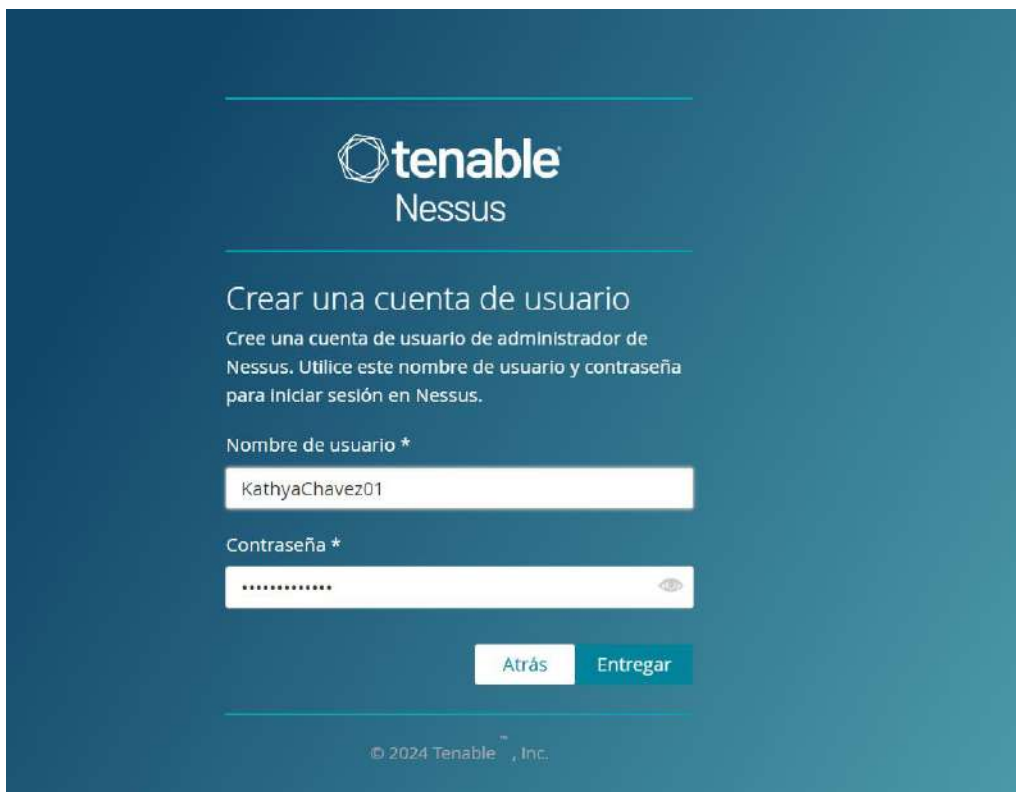
Ya realizados estos pasos, podremos observar como Nessus comienza a iniciarse para comenzar con la configuración y delimitación de nuestra cuenta.



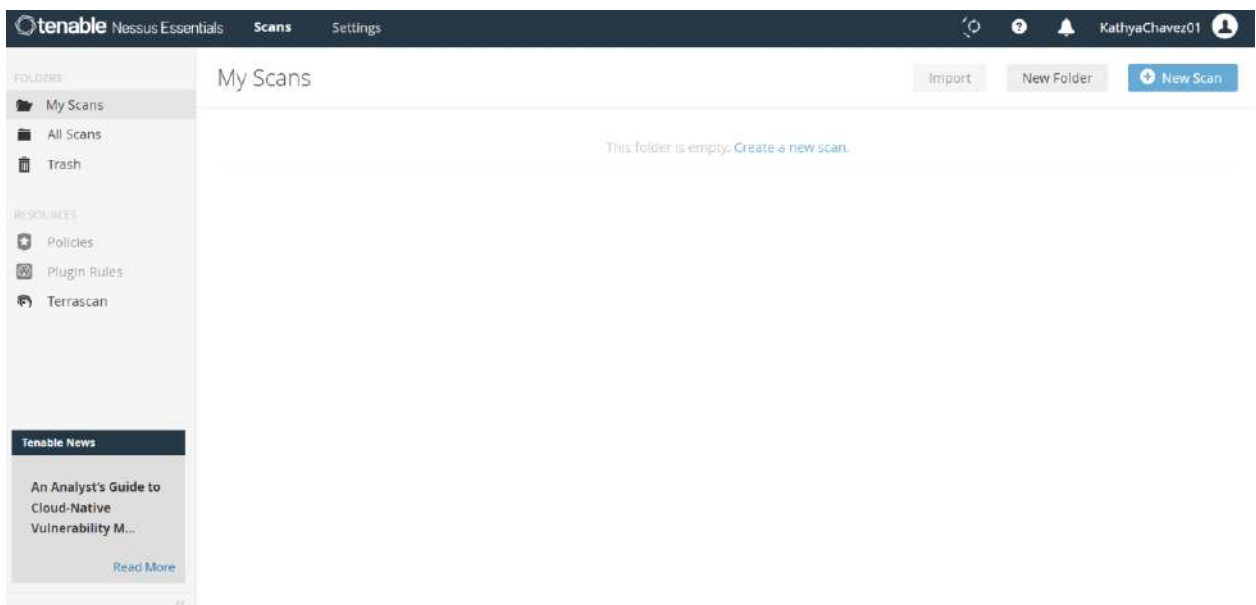
Como podemos observar, Nessus ofrece diferentes opciones o paquetes de los cuales debemos de elegir dependiendo de la necesidad que tengamos como usuarios, en nuestro caso seleccionaremos “Nessus Essentials” el cual es una versión gratuita de la plataforma.



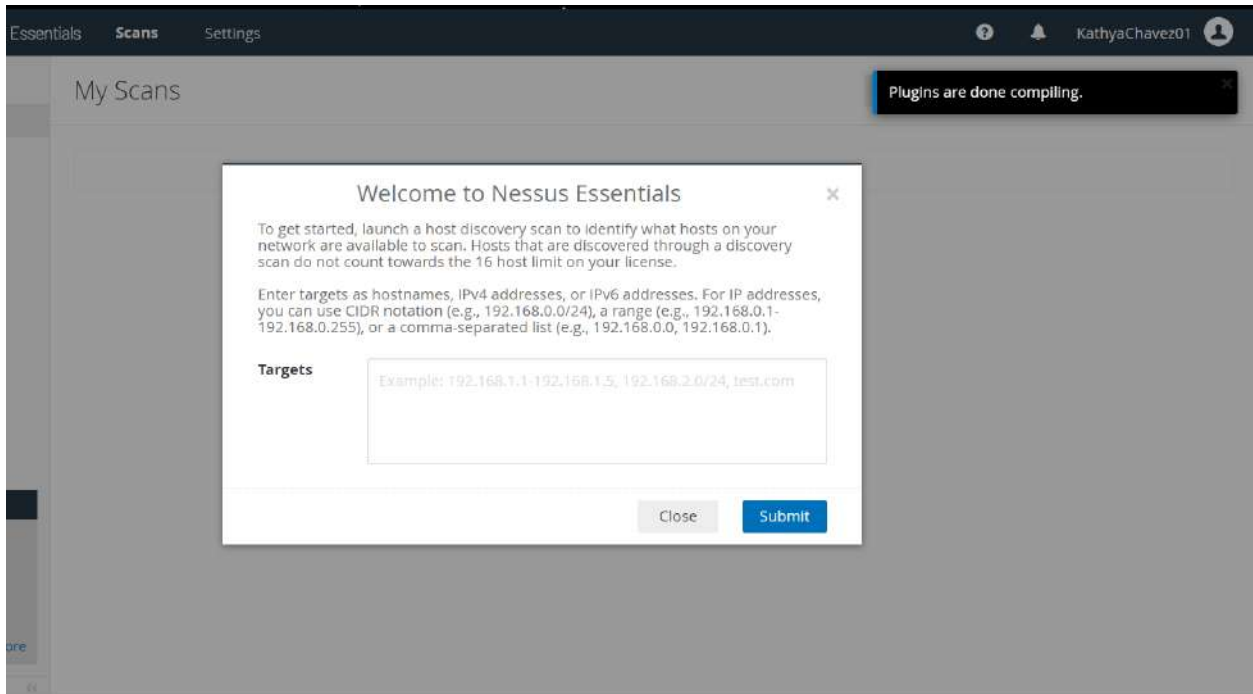
Una vez elegido el plan o programa que estaremos utilizando, Nessus nos indicara la información de licencia y nos permitirá crear una cuenta de usuario que nos permita administrar los escaneos y las vulnerabilidades encontradas en nuestro equipo de cómputo.



De esta manera, tendremos la información necesaria para que Nessus pueda iniciar con los complementos que le hemos definido en los pasos anteriores. Así mismo es importante esperar a que se descarguen los “plugins” para que Nessus pueda iniciar de manera correcta, ya que sin estos plugins nos faltan los fragmentos de código que se utilizan para realizar los escaneos correspondientes.



Una vez finalizada la descarga de los plugins, Nessus nos solicitará ingresar los datos o dispositivos en la red que serán analizados en busca de vulnerabilidades. Los dispositivos o host pueden ingresarse de diferentes formas, como direcciones o rangos de IP, nombres de dominio o CIDR. Para esta práctica utilizamos la dirección IP de nuestro equipo para realizar el escaneo de vulnerabilidades.



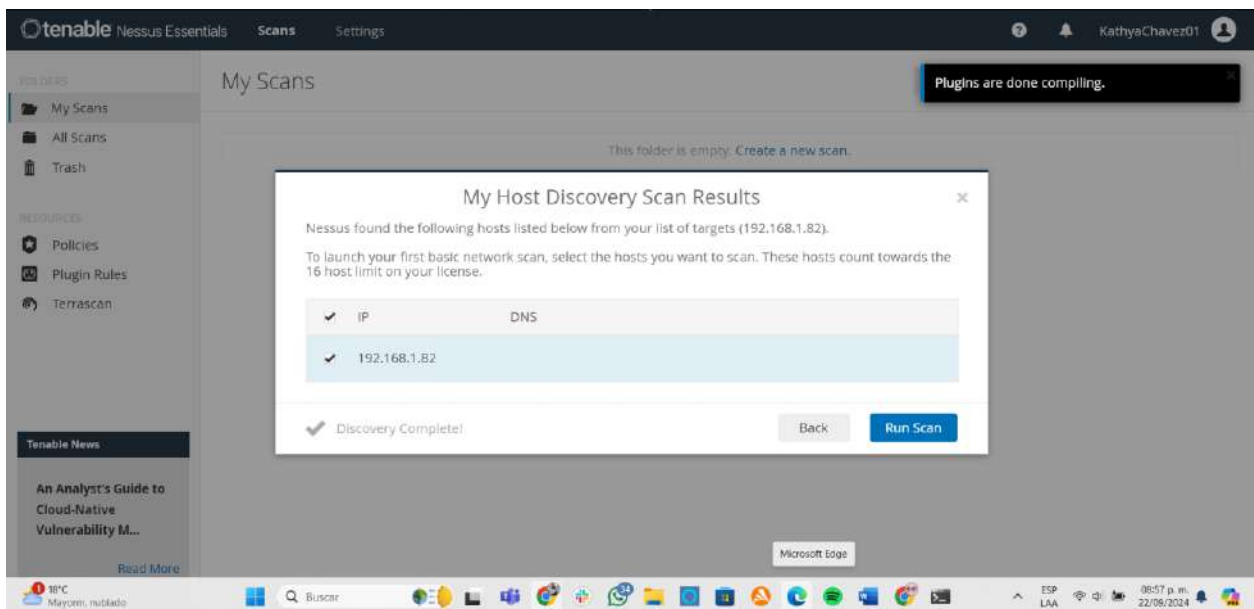
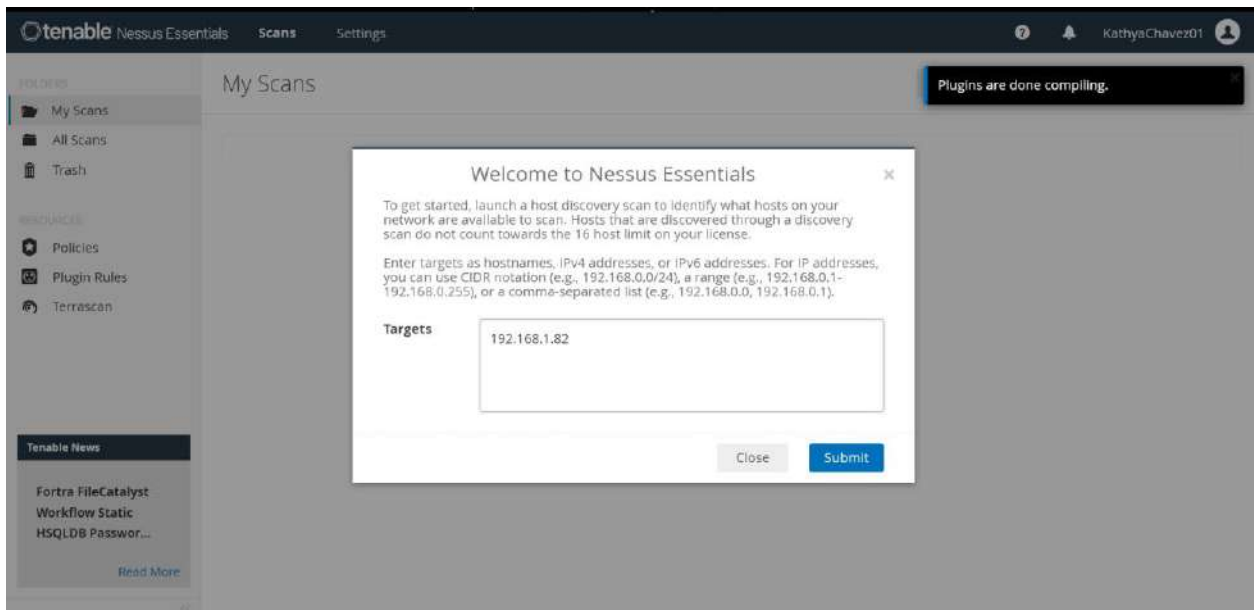
```
Simbolo del sistema
Adaptador de Ethernet Ethernet 2:
  Sufijo DNS específico para la conexión. . . :
  Vínculo: dirección IPv6 local. . . : fe80::3eb6:9765:629a:485c%17
  Dirección IPv4. . . . . : 192.168.56.1
  Máscara de subred . . . . . : 255.255.255.0
  Puerta de enlace predeterminada . . . . . :

Adaptador de LAN inalámbrica Local Area Connection* 3:
  Estado de los medios. . . . . : medios desconectados
  Sufijo DNS específico para la conexión. . . :

Adaptador de LAN inalámbrica Local Area Connection* 4:
  Estado de los medios. . . . . : medios desconectados
  Sufijo DNS específico para la conexión. . . :

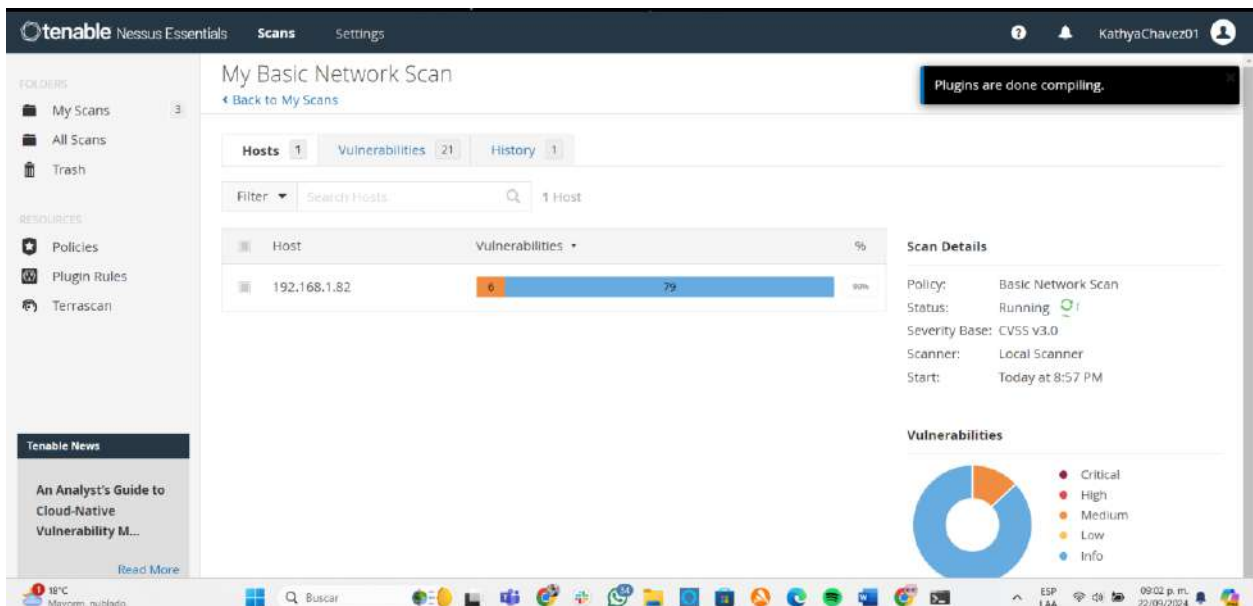
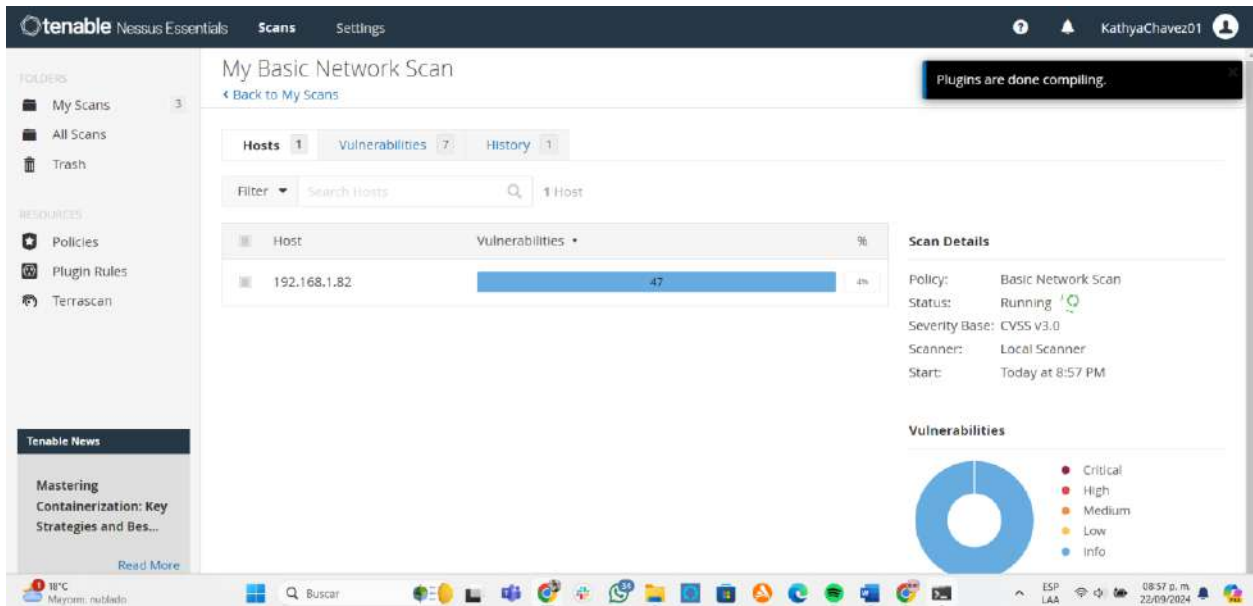
Adaptador de LAN inalámbrica Wi-Fi:
  Sufijo DNS específico para la conexión. . . :
  Dirección IPv6 . . . . . : 2806:105e:1:e895:a240:a728:5d0:cf64
  Dirección IPv6 temporal. . . . . : 2806:105e:1:e895:381f:49d1:3207:4e2b
  Vínculo: dirección IPv6 local. . . : fe80::a79f:68d0:1223:dfea%6
  Dirección IPv4. . . . . : 192.168.1.82
  Máscara de subred . . . . . : 255.255.255.0
  Puerta de enlace predeterminada . . . . . : fe80::1%6
                                           192.168.1.254
C:\Users\kathy>
```

Al ingresar la IP correctamente, el dispositivo aparecerá en la lista, permitiendo seleccionarlo y acceder al reporte de vulnerabilidades detectadas.



## Reporte


Como podemos observar, el reporte generado por Nessus incluye información sobre el “Host”, que corresponde a los dispositivos conectados para el escaneo, un listado de vulnerabilidades y el historial de escaneos.



Un aspecto clave del reporte de vulnerabilidades es la categorización de los riesgos, que indica al usuario el nivel de riesgo; informativo, bajo, medio, alto y crítico. Esta clasificación facilita la identificación de vulnerabilidades y permite establecer un plan que priorice aquellas que representan un mayor riesgo.

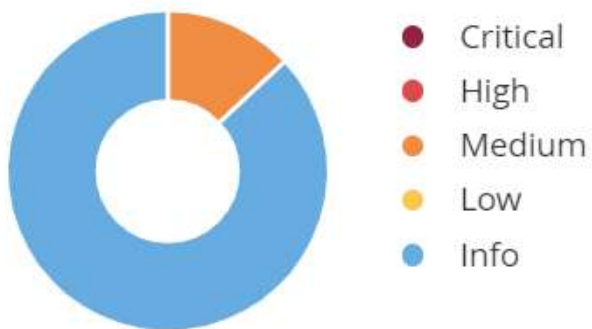
### Scan Details

---

Policy: Basic Network Scan  
Status: Running   
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 8:57 PM

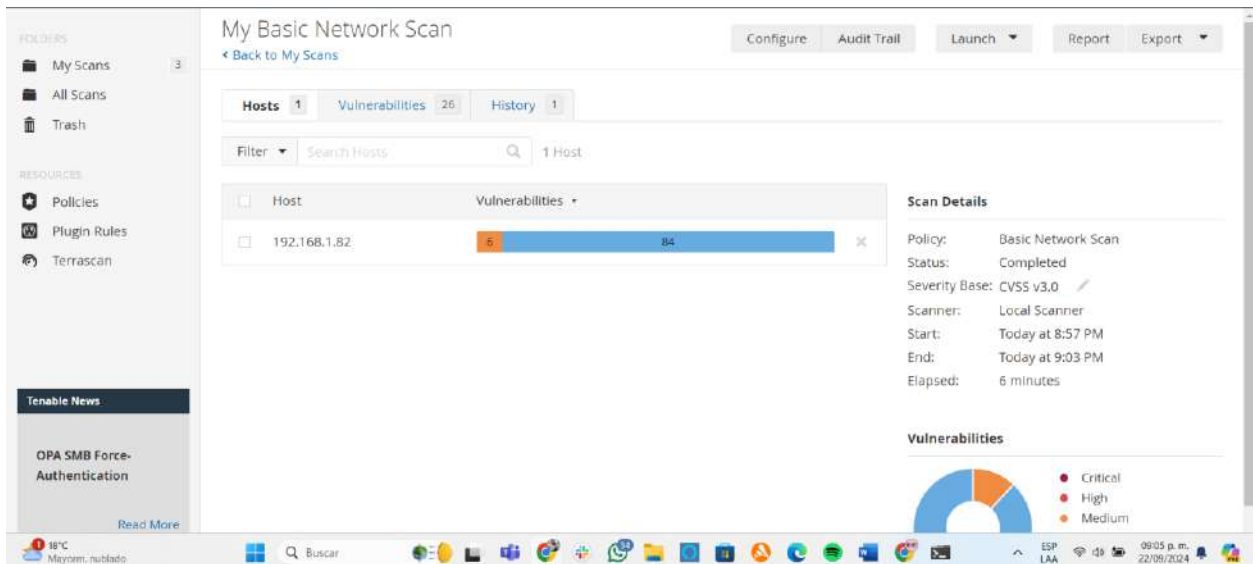
### Vulnerabilities

---





Como podemos observar, el reporte indica un total de 26 vulnerabilidades, de las cuales 20 son informativas y seis representan un riesgo medio.



En la lista de vulnerabilidades, se puede observar el nivel de severidad de cada una, Por ejemplo, la primera vulnerabilidad tiene un riesgo medio, lo que significa que podría permitir acceso no autorizado o generar impacto, aunque no tan grave como una vulnerabilidad crítica. Además, contamos con el campo “CVSS” (Common Vulnerability Scoring System), un sistema de puntuación que evalúa la severidad de las vulnerabilidades. En nuestro ejemplo, la vulnerabilidad presenta una puntuación de 5.3, lo que indica un riesgo moderado.

The screenshot shows the Tenable Vulnerability Scanner interface. The main section displays a table of vulnerabilities from a 'My Basic Network Scan'. The table has columns for severity, CVSS score, VPR, EPSS, family, and count. The first vulnerability is 'MEDIUM' with a CVSS score of 5.3. The right sidebar shows scan details: 'Basic Network Scan Completed', 'CVSS v3.0 Local Scanner', and the scan time 'Today at 8:57 PM' to 'Today at 9:03 PM' (6 minutes). A severity distribution chart is also visible.

Sev	CVSS	VPR	EPSS	Family	Count
MEDIUM	5.3			Misc.	1
MIXED	...	...	...	General	11
MIXED	...	...	...	Service detection	6
INFO	...	...	...	Windows	6
INFO	...	...	...	Web Servers	4
INFO	...	...	...	General	3
INFO	...	...	...	Windows	2

The screenshot shows a list of vulnerabilities, all with an 'INFO' severity level. The table has columns for severity, CVSS score, VPR, EPSS, family, and count. The right sidebar shows scan details: 'Basic Network Scan Completed', 'CVSS v3.0 Local Scanner', and the scan time 'Today at 8:57 PM' to 'Today at 9:03 PM' (6 minutes). A severity distribution chart is also visible.

Sev	CVSS	VPR	EPSS	Family	Count
INFO	...	...	...	Misc.	1
INFO	...	...	...	Service detection	1
INFO	...	...	...	Misc.	1
INFO	...	...	...	Settings	1
INFO	...	...	...	Service detection	1
INFO	...	...	...	General	1
INFO	...	...	...	General	1
INFO	...	...	...	Misc.	1
INFO	...	...	...	Settings	1
INFO	...	...	...	Service detection	1
INFO	...	...	...	Settings	1

Cuando accedemos a cada vulnerabilidad, podremos ver una descripción detallada junto con su solución. Además, se proporcionan enlaces a páginas o sitios web donde es posible obtener información adicional para corregir la vulnerabilidad.

The screenshot displays the Nessus web interface. On the left sidebar, there are sections for 'CARPETAS' (Folders) with 'Mis escaneos' (3), 'Todos los escaneos', and 'Basura'; 'RECURSOS' (Resources) with 'Políticas', 'Reglas del complement...', and 'Terrascan'; and 'Noticias sostenibles' (Sustainable news) with 'Secuencias de comandos entre sitios almacenadas de Flowise' and a 'Leer más' link. The main content area is titled 'Mi escaneo de red básico / Plugin n.º 57608' and includes a 'Volver a Vulnerabilidades' link. Below the title, there are tabs for 'Anfitriones: 1', 'Vulnerabilidades: 26', and 'Historia: 1'. On the right, there are buttons for 'Lanzamiento', 'Informe', 'Exportar', 'Configurar', and 'Pista de auditoría'. The vulnerability entry is titled 'MEDIO No se requiere firma SMB'. It includes a 'Descripción' (Description) stating that no signature is required on the remote SMB server, a 'Solución' (Solution) section with instructions on how to configure Windows and Samba, and a 'Ver también' (See also) section with several links. To the right of the description, there is a 'Detalles del complemento' (Plugin details) section with fields for 'Gravedad: Medio', 'IDENTIFICACIÓN: 57608', 'Versión: 1.20', 'Tipo: remoto', 'Familia: Misceláneo', 'Publicado: 19 de enero de 2012', and 'Modificado: 5 de octubre de 2022'. Below this is an 'Información de riesgo' (Risk information) section showing 'Factor de riesgo: medio', 'Puntuación base del CVSS v3.0: 5,3', 'CVSS v3.0 Vectorial: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N', and 'Vector temporal: CVSS v3.0:'. The bottom of the image shows a Windows taskbar with the date '26/09/2024' and time '09:35 p. m.'.

Carpetas

- Mis escaneos 3
- Todos los escaneos
- Basura

Recursos

- Políticas
- Reglas del complement...
- Terrascan

Noticias sostenibles

- Secuencias de comandos entre sitios almacenadas de Flowise
- Leer más

Mi escaneo de red básico / Plugin n.º 57608

Volver a Vulnerabilidades

Anfitriones: 1 Vulnerabilidades: 26 Historia: 1

Lanzamiento Informe Exportar

Configurar Pista de auditoría

**MEDIO** No se requiere firma SMB

**Descripción**

No es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede aprovechar esto para realizar ataques de Intermediario contra el servidor SMB.

**Solución**

Imponer la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de política 'Servidor de red de Microsoft: Firmar digitalmente las comunicaciones (siempre)'. En Samba, la configuración se denomina 'Firma de servidor'. Consulta los vínculos 'Ver también' para obtener más detalles.

**Ver también**

- <http://www.nessus.org/u?df39b8b3>
- <http://technet.microsoft.com/en-us/library/cc731957.aspx>
- <http://www.nessus.org/u?74b80723>
- <https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>

**Detalles del complemento**

Gravedad: Medio

IDENTIFICACIÓN: 57608

Versión: 1.20

Tipo: remoto

Familia: Misceláneo

Publicado: 19 de enero de 2012

Modificado: 5 de octubre de 2022

**Información de riesgo**

Factor de riesgo: medio

**Puntuación base del CVSS v3.0: 5,3**

CVSS v3.0 Vectorial: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Vector temporal: CVSS v3.0:

### Análisis e identificación de mejoras

Con base en el análisis y la lista de vulnerabilidades, se recomienda priorizar los siguientes puntos identificados, con el objetivo de optimizarlos y garantizar un mayor nivel de seguridad.

- **No se puede confiar en el certificado SSL:** Mantener el certificado SSL en condiciones óptimas es crucial para garantizar la seguridad de las comunicaciones en línea. Corregir esta vulnerabilidad es esencial para proteger la privacidad, autenticidad e integridad de los datos transmitidos y provenir ciberataques. Para solucionarlo debemos comprar un certificado SSL válido de una autoridad confiable, instalarlo de manera correcta verificando que este vinculado a la cadena de certificación y mantener el software actualizado con los últimos parches de seguridad.
- **Detección del protocolo TLS versión 1.0:** Corregir esta vulnerabilidad es esencial para cumplir con las normas de seguridad actuales y garantizar la protección de las comunicaciones en línea. Además, es necesario para asegurar el correcto funcionamiento de los equipos y sistemas. Para resolver este problema, es imprescindible habilitar el soporte para TLS 1.2 y 1.3 y deshabilitar el soporte para TLS 1.0, ya que, a partir del 31 de marzo de 2020, los puntos finales que no sean compatibles con TLS 1.2 o versiones posteriores dejaron de funcionar correctamente en los principales navegadores web.
- **Certificado auto firmado SSL:** La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida, lo que la hace insegura para entornos de producción, ya que los navegadores no la consideran confiable, lo que genera advertencias para los usuarios y aumenta el riesgo de ciberataques. Debido

a esto es necesario adquirir un certificado de una autoridad certificadora confiable e instalarlo correctamente, así como asegurarse que se mantenga actualizado.


## Conclusión

A través de esta actividad, tuvimos la oportunidad de trabajar en la plataforma Nessus, una herramienta clave en la gestión de vulnerabilidades. Esta herramienta nos permitió realizar un escaneo y generar un reporte de vulnerabilidades encontradas en nuestro equipo, para así, con la información completa proponer las mejoras para mantener la seguridad. Gracias a esta práctica, exploramos las diferentes funcionalidades que Nessus ofrece para auditorías de seguridad, además aprendimos a interpretar los elementos clave que componen los reportes de vulnerabilidades, lo cual es crucial para una correcta gestión de riesgos.

Otro aspecto por destacar es la importancia de utilizar herramientas como Nessus el cual es útil no solo para auditorías o revisiones, sino también de manera preventiva y periódica, con el fin de reducir el riesgo de ciberataques. Finalmente, es esencial que, una vez identificadas las vulnerabilidades, se establezcan planes de acción para corregirlas y así mitigar las posibles amenazas de seguridad.

**Link GitHub:** <https://github.com/KathyaCh/DPAASI.git>

## Referencias

- I. *An overview of HTTP - HTTP / MDN*. (2024, 2 septiembre). MDN Web Docs.  
<https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview>
- II. *Ataques contra la ciberseguridad e infracciones de la ciberseguridad*. (2022, 7 noviembre). /. [https://latam.kaspersky.com/resource-center/preemptive-safety/how-to-prevent-cyberattacks?srsltid=AfmBOorX-eTr61MLnX49f7pZih1Yyc6JdaT0JLk3JoACWB\\_DZbxMsjQO](https://latam.kaspersky.com/resource-center/preemptive-safety/how-to-prevent-cyberattacks?srsltid=AfmBOorX-eTr61MLnX49f7pZih1Yyc6JdaT0JLk3JoACWB_DZbxMsjQO)
- III. Cilleruelo, C. (2024, 27 mayo). ¿Qué es Nessus? [2024] | KeepCoding Bootcamps.  
*KeepCoding Bootcamps*. <https://keepcoding.io/blog/que-es-nessus/>
- IV. Contando Bits. (2024, 9 enero). *Como Instalar y Usar NESSUS en Windows 10*  [Tutorial Escaneo de Vulnerabilidades] [Vídeo]. YouTube.  
<https://www.youtube.com/watch?v=-8l2Hqp-eRo>
- V. *CVSS v4.0 Specification Document*. (s. f.). FIRST — Forum Of Incident Response And Security Teams. <https://www.first.org/cvss/specification-document>
- VI. *Detección y prevención de amenazas informáticas*. (s. f.).  
<https://preyproject.com/es/blog/deteccion-y-prevencion-de-amenazas-su-guia-para-mantenerse-a-salvo#:~:text=C%C3%B3mo%20Prevenir%20Estas%20Amenazas&text=Aseg%C3%BArese%20de%20que%20su%20personal,el%20software%20parcheado%20y%20actualizado.>
- VII. Gómez, J. A. (2024, 14 mayo). *Certificado SSL/TLS: qué es, cómo funciona y tipos*.  
<https://www.deltaprotect.com/blog/certificado-ssl-tls>

VIII. *Prevención y detección de intrusiones.* (s. f.).

<https://www.fortra.com/es/soluciones/ciberseguridad/infraestructura/deteccion-prevencion-intrusiones>

IX. *¿Qué es la detección y respuesta ante amenazas (TDR)?* / *Seguridad de Microsoft.*

(s. f.). <https://www.microsoft.com/es-es/security/business/security-101/what-is-threat-detection-response-tdr>

X. *What is an SSL Certificate?* / *DigiCert.* (s. f.). <https://www.digicert.com/what-is-an-ssl-certificate>