Instituto Tecnológico y de Estudios Superiores de Monterrey

Campus Monterrey

Análisis de criptografía y seguridad

Nombre del profesor:

Oscar Eduardo Labrada Gómez

Alejandro Parra Briones

Evidencia 1. Auditoría de Seguridad: Reporte Técnico

Equipo #1 | Integrantes:

Diego Olalde Tristán	IDM	A01612555
Ana Camila Saavedra Casillas	IDM	A01252957
Carlos Alberto Gómez San Pedro	IDM	A01658377
Arath Mendivil Mora	IDM	A01660670
Facundo Bautista Barbera	IDM	A01066843

14 de marzo de 2024

Índice

Introducción

El presente documento aborda diversas facetas relacionadas con la seguridad informática y la gestión de vulnerabilidades en redes privadas. Se inicia exponiendo los resultados obtenidos de un escaneo de vulnerabilidades del inventario realizado en una red privada utilizando la herramienta Nessus. Este escaneo fue llevado a cabo bajo la licencia “Essentials”, la cual permitió el análisis de hasta 16 hosts, revelando un total de 41 vulnerabilidades, que van desde categorías de baja hasta crítica, siendo estas últimas de especial preocupación en cuanto a su impacto potencial en la seguridad de la red.

Siguiendo esta línea, se propone una metodología detallada para la implementación de un análisis de vulnerabilidades en la infraestructura de la red, basándose en las lecciones aprendidas durante el escaneo inicial. Este análisis busca identificar y evaluar las debilidades y exposiciones potenciales en la arquitectura de la red, con el objetivo de fortalecer las defensas contra posibles ataques cibernéticos y garantizar la integridad, confidencialidad y disponibilidad de los datos.

Se hace hincapié en la selección de metodologías y herramientas adecuadas para llevar a cabo este análisis de manera efectiva, tomando en consideración diferentes escenarios de amenazas y maximizando la precisión y fiabilidad de los resultados obtenidos.

Por último, se describe en detalle la implementación de la herramienta Nessus para realizar un levantamiento de inventario de los activos tecnológicos y detectar vulnerabilidades potenciales en los mismos. Este ejercicio proporcionó información crucial para la identificación de puntos críticos de riesgo dentro de la infraestructura tecnológica, sirviendo como base sólida para la toma de decisiones estratégicas en materia de gestión de riesgos y seguridad de la información. En conjunto, estos tres enfoques ofrecen una visión integral y pragmática para abordar los desafíos de seguridad en redes privadas en la era digital.

Etapa 1: Inventario de la empresa

Resultados

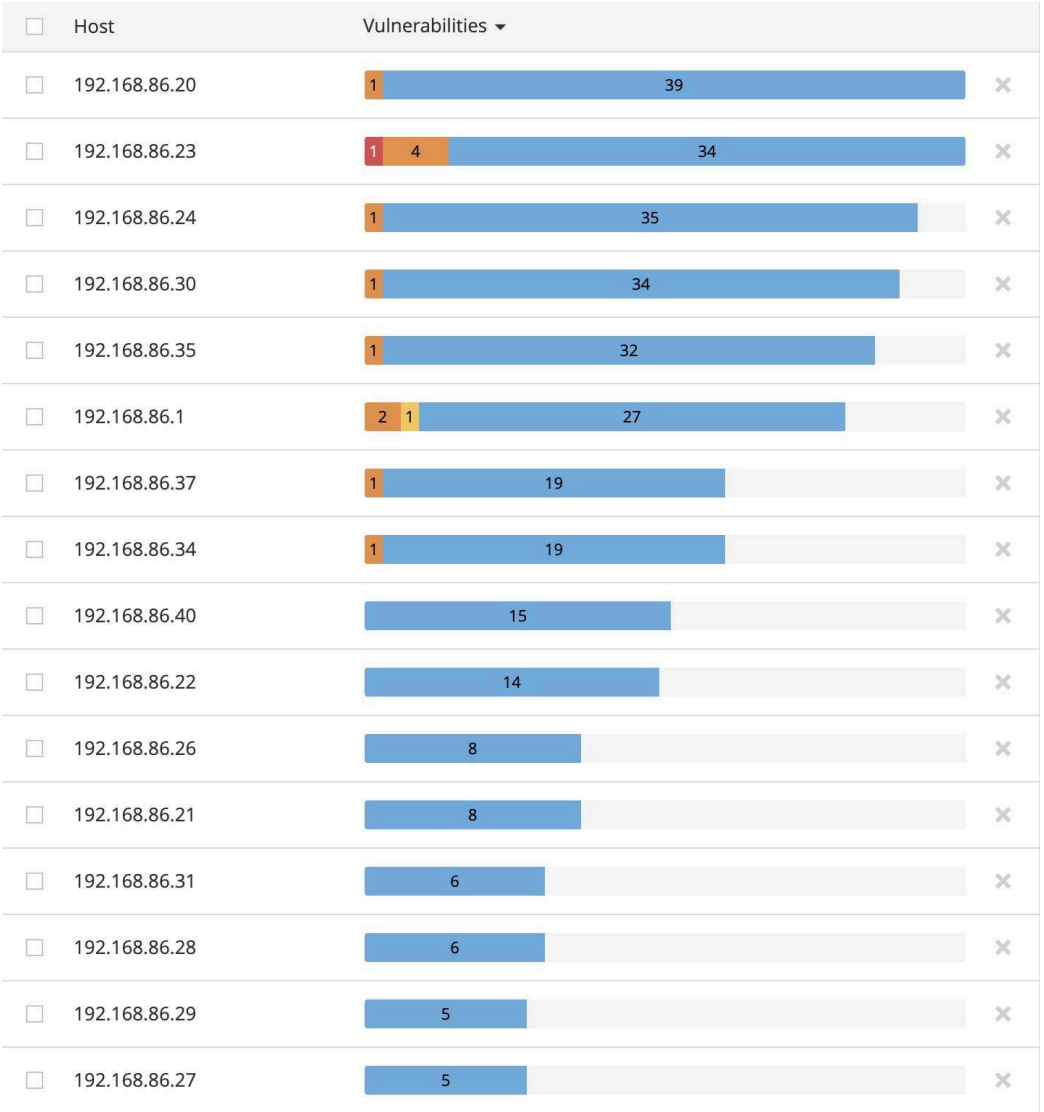

Figura 1: Hosts resultantes del escaneo utilizando Nessus

Sev	CVSS	VPR	Nam...	Family	Count
HIGH	7.5	4.4	N...	Misc.	1
MEDIUM	6.5	4.9	IP...	Firewalls	3
MEDIUM	6.1	5.7	J...	CGI abuses : XSS	1
MEDIUM	5.8		N...	Misc.	1
MIXED	...	...	5	SSGeneral	20
MIXED	...	...	2	DIDNS	3
MIXED	...	...	2	N¡Web Servers	2
MIXED	...	...	2	O¡Misc.	2
LOW	3.3 *		D...	Service detection	1

Figura 2: Lista de resultados de las vulnerabilidades encontradas

Etapa 2: Diseño e implementación de un plan de evaluación de la empresa

Plan de análisis de vulnerabilidades

Preparación

A continuación se mencionan múltiples herramientas y técnicas que deberán llevarse a cabo para el análisis de vulnerabilidades.

Configuración de Nessus

Nessus es una herramienta de escaneo de vulnerabilidades ampliamente utilizada en el ámbito de la ciberseguridad. Es desarrollado por Tenable Network Security. Es un programa diseñado para detectar múltiples tipos de vulnerabilidades en los sistemas de red, incluyendo dispositivos y aplicaciones. El software realiza escaneos automáticos de la red, analizando dispositivos conectados, sistemas operativos, aplicaciones, configuraciones, etc. Buscando fallos de seguridad conocidos. Nessus utiliza una base de datos de vulnerabilidades conocidas, la cual es actualizada regularmente para comprobar y detectar puntos débiles.
Se recomienda la utilización de esta herramienta para detectar vulnerabilidades de manera continua.

Actualización y Configuración

Asegurar que Nessus esté actualizado a la última versión para incluir las últimas definiciones de vulnerabilidad es un punto clave para aprovechar esta herramienta al máximo.
Deberá configurarse un perfil de escaneo que se ajuste a los activos de la red doméstica, priorizando aquellos críticos identificados durante la fase de preparación.

Ejecución de Nessus

Realizar un escaneo completo utilizando Nessus para identificar vulnerabilidades en dispositivos y software. Debe incluir escaneos de puertos, servicios y análisis de la configuración para obtener una visión completa de la seguridad de la red.

Revisión de reportes de Nessus

Analizar los reportes generados por Nessus para identificar y priorizar las vulnerabilidades encontradas, prestando especial atención a aquellas que representan un riesgo mayor para la red.

Implementación de un sistema Honeypot

Un sistema “Honeypot” es aquel que utiliza una pequeña trampa para permitir conexiones entrantes con el fin de descubrir vulnerabilidades. Este sistema permite la entrada de dichas conexiones a pesar de poder ser fraudulentas o críticas para el sistema, con el fin de encontrar las fuentes de dichas conexiones, o el punto de exposición que está ocasionando esta vulnerabilidad.

Selección y Configuración

Elegir un software de “honey-potting” adecuado para entornos domésticos, como Honeyd o Kippo, y configurarlo para simular sistemas vulnerables atractivos para los atacantes. Esto puede ayudar a identificar patrones de ataque y potenciales amenazas sin exponer los verdaderos activos a la red. Este proceso puede permanecer activo indefinidamente, ya que puede estar constantemente pendiente de posibles ataques.

Monitoreo del sistema Honeypot

Monitorear la actividad en el sistema Honeypot para identificar intentos de ataque o patrones sospechosos. Esta información puede revelar nuevas vulnerabilidades o tácticas de ataque que no son detectadas por el escaneo de vulnerabilidades tradicionales.

Evaluación de la actividad

Evaluar los datos recopilados por el honeypot para entender mejor las amenazas específicas a las que la red está expuesta. Utilizar esta información para ajustar las estrategias de defensa y mitigación de vulnerabilidades.

Configuración del Firewall

Un firewall es un dispositivo de seguridad de red que controla el tráfico de red entrante y saliente y decide si permite o bloquea cierto tráfico de acuerdo con un conjunto de reglas de seguridad.

Los firewalls pueden ser hardware, software o ambos. El software o los dispositivos de hardware y software especializados funcionan bloqueando o permitiendo paquetes de datos de manera específica. Generalmente, el objetivo es ayudar a prevenir actividades maliciosas y evitar que cualquier persona, dentro o fuera de la red privada, participe en actividades no autorizadas en la misma. Los firewalls están diseñados para proteger las redes privadas y los dispositivos finales que se encuentran en ellas, llamados hosts de red. Un host de red es un dispositivo que se comunica con otros hosts de red. Además de enviar y recibir tráfico desde redes externas, también envían y reciben tráfico entre redes internas.

Revisión y fortalecimiento

Evaluar la configuración actual del firewall para identificar posibles debilidades. Fortalecer las reglas del firewall para bloquear tráfico no deseado, permitiendo solo las conexiones necesarias para la operación normal de la red.

Desarrollo de un plan de remediación

Acciones a partir de Nessus

Para cada vulnerabilidad identificada, desarrollar un plan de acción que incluya la aplicación de parches, cambios de configuración y otras medidas de mitigación.

Fortalecimiento a partir del sistema Honeypot

Utilizar la información recopilada a través del sistema Honeypot para desarrollar estrategias de defensa contra ataques específicos o patrones de ataque observados.

Mejoras de la configuración del firewall

Con base en los resultados del análisis de vulnerabilidades y la actividad del honeypot, realizar ajustes continuos en la configuración del firewall para mejorar la defensa contra ataques conocidos y emergentes.

Implementación y seguimiento

Ejecución del Plan de Remediación

Implementar las acciones correctivas planificadas, comenzando por las vulnerabilidades de mayor prioridad.

Monitoreo continuo

Mantener un monitoreo continuo de la red utilizando Nessus, el honeypot y el firewall ajustado, para detectar y responder rápidamente a nuevas vulnerabilidades o intentos de ataque.

Este plan detallado no solo se enfoca en la identificación y mitigación de vulnerabilidades utilizando Nessus, sino que también incorpora la inteligencia de amenazas proporcionada por el honeypot y fortalece la defensa perimetral a través de una configuración de firewall más robusta. Al integrar estos elementos, se logra una comprensión más profunda y una protección más efectiva contra las amenazas a la seguridad de la red doméstica.

Etapa 3: Plan de mitigación de vulnerabilidades de la empresa

Resultados obtenidos a partir del escaneo

El escaneo de a través de Nessus mostró un resultado de 16 hosts (dispositivos con IP conectados) para la red 192.168.86.0/24. Este resultado ha sido limitado ya que Nessus Essentials tiene un límite de Escaneo de 16 hosts, es decir la cantidad que se obtuvo. Dentro de ese resultado, se detectaron 11 dispositivos que mostraron algún nivel de vulnerabilidad, a continuación la lista:

- **192.168.86.1, Puerto 67** (Riesgo Bajo) - **DHCP Server Detection**
    - Problema: Este script contacta al servidor DHCP remoto para intentar obtener información de configuración.
      Solución: Aplicar filtrado para evitar que esta información sea accesible desde redes no autorizadas.
- **192.168.86.1, Puerto 53** (Riesgo Medio) - **Multiple Vendor DNS Response Flooding Denial Of Service**
    - Problema: El servidor DNS remoto es vulnerable a un ataque de denegación de servicio por inundación de respuestas DNS.
    - Solución: Actualizar el software de tu servidor DNS a la última versión disponible que aborde esta vulnerabilidad.
- **192.168.86.20** (Riesgo Medio) - **SSL Certificate Cannot Be Trusted**
    - Problema: El certificado X.509 del servidor no puede ser confiado por una o varias de las siguientes razones: es auto-firmado, está caducado, o el emisor del certificado no es confiable.
    - Solución: Adquirir e instalar un certificado SSL válido de una Autoridad Certificadora (CA) de confianza.

- **192.168.86.23** (Riesgo Alto) - **Network Time Protocol Daemon (ntpd) read_mru_list Crafted Mode 7 Packet Denial of Service**
    - Problema: El servidor NTP remoto se ve afectado por un ataque de denegación de servicio.
    - Solución: Actualizar la implementación de NTP a la última versión que corrige esta vulnerabilidad.

- **192.168.86.23** (Riesgo Medio) - **Network Time Protocol (NTP) Mode 6 Scanner**
    - Problema: El servidor NTP remoto responde a consultas del modo 6, lo cual podría ser explotado de manera malintencionada.
    - Solución: Actualizar la implementación de NTP a la última versión que corrige esta vulnerabilidad.
- **192.168.86.23** (Riesgo Medio) - **nginx < 1.17.7 Information Disclosure**
    - Problema: La versión del servidor nginx es susceptible a la divulgación de información.
    - Solución: Actualizar nginx a la versión 1.17.7 o superior para solucionar esta vulnerabilidad.
- **192.168.86.23** (Riesgo Medio) - **JQuery 1.2 < 3.5.0 Multiple XSS**
    - Problema: La versión auto-reportada de JQuery es vulnerable a múltiples vulnerabilidades de tipo cross-site scripting (XSS).
    - Solución: Actualizar JQuery a la versión 3.5.0 o superior para corregir estas vulnerabilidades.
- **192.168.86.23** (Riesgo Medio) - **SSH Terrapin Prefix Truncation Weakness (CVE-2001-0144)**
    - Problema: El servidor SSH remoto es vulnerable a ataques de intermediario debido a una debilidad en la truncación de prefijos.
    - Solución: Asegúrarse de que el servidor SSH esté actualizado a la última versión disponible que corrija este problema.
- **192.168.86.24**, **192.168.86.30**, **192.168.86.35** (Riesgo Medio) - **SSL Certificate Cannot Be Trusted**
    - Problema: El certificado X.509 del servidor no puede ser confiado por una o varias de las siguientes razones: es auto-firmado, está caducado, o el emisor del certificado no es confiable.
    - Solución: Adquirir e instalar un certificado SSL válido de una Autoridad Certificadora (CA) de confianza.
- **192.168.86.1, 192.168.86.34**, **192.168.86.37** (Riesgo Medio) - **IP Forwarding Enabled**
    - Problema: El host remoto tiene habilitado el reenvío IP, lo que podría permitir que atacantes redirijan el tráfico a través de él.

- Solución: Para deshabilitar el reenvío IP en Linux de forma temporal, se puede usar sudo sysctl -w net.ipv4.ip_forward=0 para IPv4 y sudo sysctl -w net.ipv6.conf.all.forwarding=0 para IPv6, pero estos cambios no persistirán después de reiniciar. Para hacerlos permanentes, se debe modificar /etc/sysctl.conf agregando net.ipv4.ip_forward = 0 y net.ipv6.conf.all.forwarding = 0, aplicando los cambios con sudo sysctl -p. En Windows, la desactivación requiere editar el registro en HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters, cambiando IPEnableRouter a 0 y reiniciando el sistema. En macOS, la desactivación temporal se logra con sudo sysctl -w net.inet.ip.forwarding=0 para IPv4 y la versión IPv6 equivalente, mientras que para hacerlo permanente, se debe editar o crear /etc/sysctl.conf con las líneas adecuadas para IP forwarding y no es necesario reiniciar. Cada administrador debe aplicar la configuración adecuada a su sistema operativo y verificar que el reenvío IP esté correctamente deshabilitado.

Imagenes de resultados

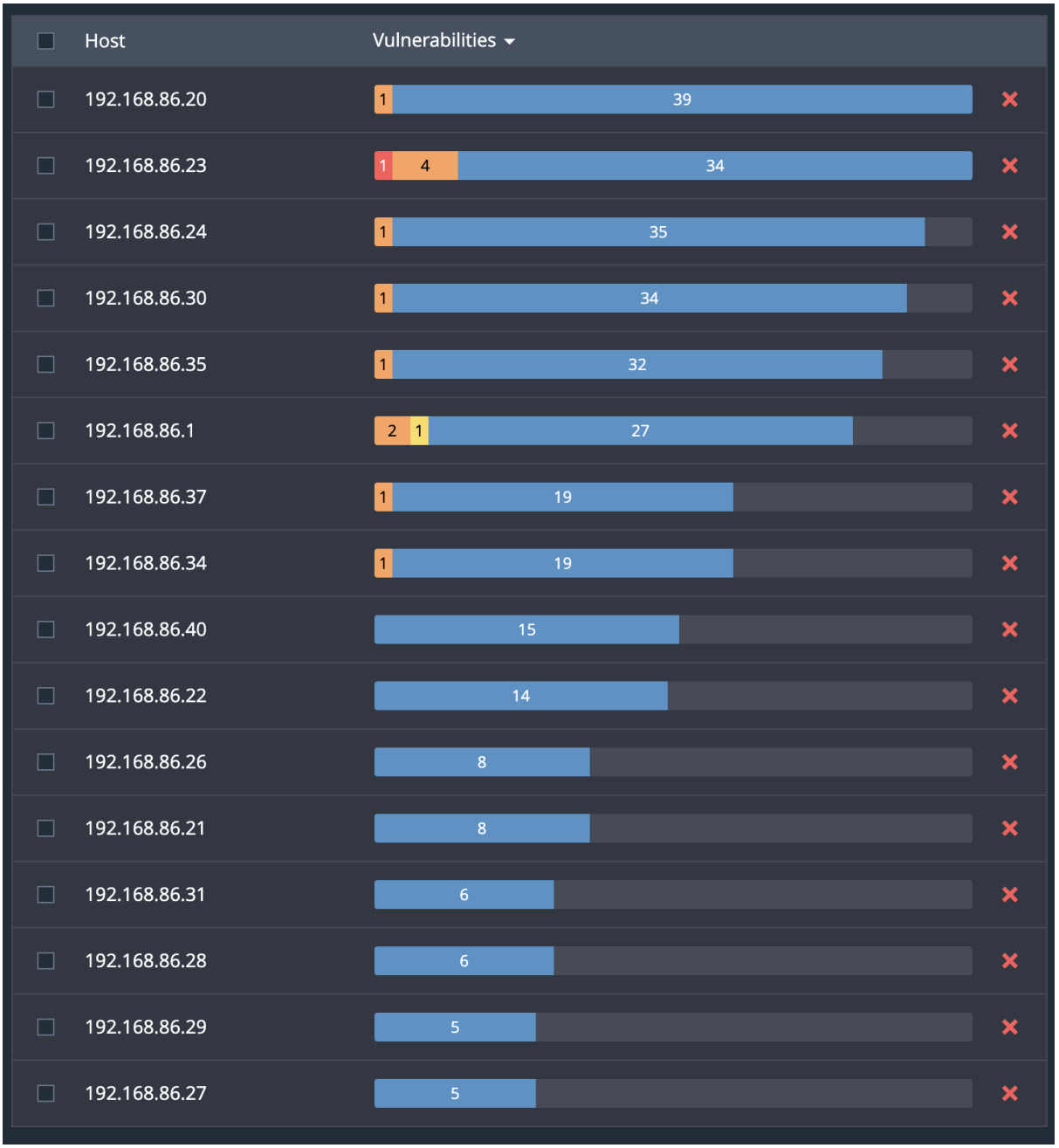

Figura 1: Lista de Hosts en Nessus

Sev	CVSS	VPR	Nam...	Family	Count
HIGH	7.5	4.4	N...	Misc.	1
MEDIUM	6.5	4.9	IP...	Firewalls	3
MEDIUM	6.1	5.7	J...	CGI abuses : XSS	1
MEDIUM	5.8		N...	Misc.	1
MIXED	...	...	5	SSGeneral	20
MIXED	...	...	2	DIDNS	3
MIXED	...	...	2	N¦Web Servers	2
MIXED	...	...	2	O¦Misc.	2
LOW	3.3 *		D...	Service detection	1

Figura 2: Lista de vulnerabilidades en Nessus (sólo Low a Critical incluido)

Conclusión

En resumen, la propuesta planteada presenta un plan detallado para abordar la seguridad de la infraestructura de la red, destacando la importancia de herramientas como Nessus y la estratégica implementación de un sistema HoneyPot. De igual manera, es de vital importancia mantener Nessus constantemente actualizado y configurado de manera precisa, priorizando los activos críticos de la red para una evaluación exhaustiva. Además, se enfatiza la evaluación minuciosa y el fortalecimiento proactivo del firewall para gestionar y controlar el tráfico, permitiendo únicamente las conexiones autorizadas.

En este trabajo no solo se realizó una identificación de vulnerabilidades, sino que también se desarrolló un plan de reparación completo y detallado. Este plan aborda acciones específicas basadas en las vulnerabilidades identificadas, así como también integra la información recopilada del sistema para desarrollar estrategias de defensa contra patrones de ataque observados. Se destaca la importancia de un seguimiento continuo y monitoreo activo para la detección y pronta respuesta a amenazas emergentes.

En conclusión, la propuesta ofrece una estrategia sólida y exhaustiva para garantizar la seguridad de la infraestructura de la red, combinando herramientas avanzadas, técnicas proactivas y un enfoque continuo en la mejora constante de la ciberseguridad. El escaneo realizado con Nessus reveló información importante sobre la infraestructura tecnológica, identificando vulnerabilidades que abarcan desde riesgos bajos hasta potenciales ataques. Las soluciones propuestas contribuirán significativamente a fortalecer la postura de ciberseguridad, mitigando las amenazas identificadas y mejorando la resistencia de la infraestructura ante los posibles ataques.

Referencias

Introducing Tenable.io. (s.f.). Tenable®. https://www.tenable.com/products/nessus

KeepCoding, R. (2023). Escaneo básico con Nessus | KeepCoding Bootcamps. *KeepCoding Bootcamps*. https://keepcoding.io/blog/escaneo-basico-con-nessus/

¿Qué es un análisis de vulnerabilidades? – SAYNET. (s.f.). https://saynet.com.mx/que-es-un-analisis-de-vulnerabilidades/

¿Qué es un firewall? (2023). Cisco. https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

¿Qué es un honeypot? (2023). latam.kaspersky.com. https://latam.kaspersky.com/resource-center/threats/what-is-a-honeypot

Security, P. (2023). *Evaluación de vulnerabilidad: qué es y cómo realizarla*. Panda Security Mediacenter. https://www.pandasecurity.com/es/mediacenter/evaluacion-vulnerabilidad/