TALLER APLICADO DE SEGURIDAD DE LA INFORMACIÓN

Ataques de red, hardware y software

Unidad 1

ESCUELA DE CONSTRUCCIÓN E INGENIERÍA

Director: Marcelo Lucero Yañez

ELABORACIÓN

Experto disciplinar: Eder Moran Heredia

Diseñador instruccional: Antonio Colmenares Prieto

Editora instruccional: María José Fonseca Palacios

VALIDACIÓN

Experto disciplinar: Alex Flores Fuentealba

Jefa de Diseño Instruccional: Alejandra San Juan Reyes

EQUIPO DE DESARROLLO

Didactic

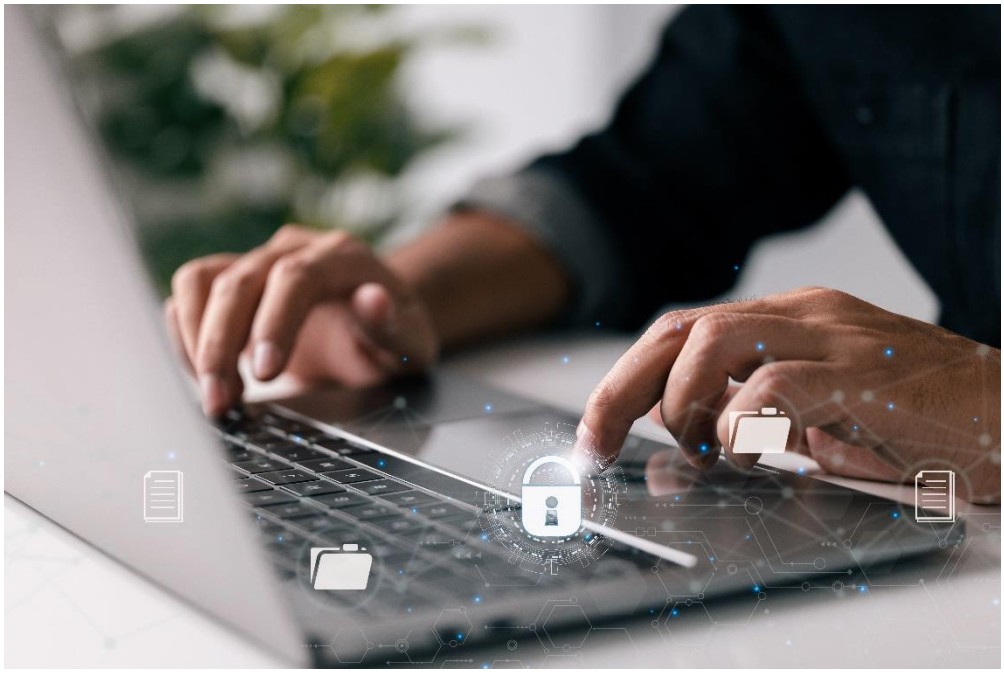
AÑO

2022

Tabla de contenidos

Aprendizaje esperado

Utilizan herramientas de análisis de vulnerabilidades en el marco de Ethical Hacking, de acuerdo con los estándares de la industria.



Introducción

En la seguridad informática, es crucial ocuparnos en tener mayor prevención cuando utilizamos sistemas informáticos y también cuidar la privacidad cuando navegamos por internet. Podemos encontrar una serie de conceptos asociados al momento buscar las vulnerabilidades que advierten a los sistemas informáticos, por ejemplo: *amenazas, riesgos, vulnerabilidades*, que conocerás en este módulo.

Existen muchas noticias relacionadas con seguridad informática, con hackeos, vulnerabilidades de seguridad en diferentes aplicaciones y software, además día a día surgen nuevos manuales y tutoriales para configurar de manera segura nuestra red local y equipos que utilizamos, ya sea para trabajar en nuestra compañía o de uso privado.

A continuación, aprenderás las principales herramientas que se utilizan al momento de ejecutar un hacking ético, teniendo presente las más utilizadas en el mercado y en la industria de seguridad de la información.

Conocerás las vulnerabilidades que afectan a un sistema informático y por qué es tan importante el cuidar y controlar los datos que trabajamos día a día, para ello profundizarás contenidos sobre las herramientas de la gestión del riesgo, de tal manera de calcular los riesgos que afectan a la empresa en términos de seguridad de la información. Además, conocerás algunos controles técnicos o tecnológicos que pueden ser aplicados para cubrir los objetivos de ciberseguridad, vectores de ataques y herramientas a utilizar para la búsqueda de vulnerabilidades.

1. Conceptos de evaluación de vulnerabilidades

1.1 Vulnerability Research o investigación de vulnerabilidades

En la actualidad la interconexión de servicios por intermedio de una red y por supuesto las hiperconectividad, que nos entrega internet, supone un tremendo desafío, en lo relacionado con el control de explotación de las vulnerabilidades que pueda tener un sistema informático o de networking.

El desafío es poder diseñar controles eficientes y efectivos, para poder detectar estas vulnerabilidades, considerando, además, que nos enfrentamos a diversas plataformas, sistemas operativos, aplicaciones de escritorio, APPs, etc., que dificultan aún más este trabajo. En la actualidad, se han diseñado, estrategias diversas en el mercado, pero no todas poseen, un sistema de puntuación de vulnerabilidades, limitando así la información que un administrador de sistemas computacionales pueda obtener sobre el riesgo al que está expuesto.

Recordemos que una vulnerabilidad, en términos informáticos, es una debilidad o fallo en un sistema de información, pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad. La procedencia de estas vulnerabilidades se

produce por errores de diseño, falta de procedimientos, errores de configuración, etc.

Otro concepto que recordar es amenaza, la que vamos a definir como toda acción que explota estas vulnerabilidades. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado).

También es conveniente considerar y clasificar la información. Para este propósito vamos a clasificar la información así:

Confidencial: Información que solo puede ser accedida por los altos ejecutivos de la compañía.

Secreta: Información que solo puede ser accedida por los gerentes estratégicos de la compañía.

Restringida: Información que puede ser leída por muchos usuarios, pero que solo puede ser modificada por altos ejecutivos.

Pública: Información que puede ser accedida por cualquier usuario, incluso fuera de la compañía.

Teniendo presente los conceptos anteriores, vulnerabilidades y amenazas, entonces, vamos a introducir un tercer concepto denominado riesgo, el cual es la probabilidad de que se produzca un incidente de seguridad, materializándose una amenaza y causando pérdidas o daños a la empresa u organización. Dado lo anterior, podemos resumir lo anterior en la siguiente imagen:

Figura 1. Riesgo.

Fuente: Civittas.com (2020)

1.2 Clasificación de vulnerabilidades o Vulnerability Classification

Para asegurar nuestras empresas, contaremos con diferentes mecanismos y herramientas para asegurar la continuidad de la operación. Para ello es necesario la gestión de riesgo.

El principal objetivo de la gestión de riesgos es alcanzar el equilibrio optimo entre la minimización de vulnerabilidades y perdidas y las ganancias y oportunidades de la organización. En otras palabras, llevar el riesgo a niveles que sean aceptables por la organización. La gestión de riesgos debe vigilar que éste no tenga impacto significativo en los procesos críticos de negocio.

Como es sabido, el riesgo es inherente a toda actividad, por lo tanto, se debe realizar una gestión para garantizar la preservación de la compañía.

La principal herramienta con la que opera la gestión de Riesgos son los controles de seguridad, dado que, cada vez que se aplica un control, ya sea una política, un procedimiento o un control tecnológico, se disminuye el riesgo. Además, la evaluación de riesgos puede ser cualitativa o cuantitativa.

Gestión de Riesgos Cuantitativa: Es aquella que se puede medir en forma numérica, que a su vez indica la magnitud del impacto asociado. Generalmente se traduce en la perdida financiera asociada si el riesgo se materializa.

Gestión de Riesgos Cualitativa: Es aquella que no se puede medir en forma numérica, solo conceptualmente, es decir basado en la experiencia o sensibilidad de los activos de información. Generalmente se utiliza una escala de: *Alto, Medio y Bajo*.

Antes de implementar medidas de mitigación, es necesario reconocer los activos de información, definamos entonces estos conceptos:

Activo de información: Son todos recursos considerados valiosos por la compañía y debe ser protegidos. Un activo puede ser un archivo, un servidor, una base de datos, documentos, etc.

Amenaza: Es una acción posible que pudiese causar daño y puede ocurrir con una determinada probabilidad. Un ejemplo de amenaza son los huracanes, terremotos y en el mundo informático, virus o ataques.

Vulnerabilidad: Es una falla de un sistema informático que, al ser explotada, puede causar daño a la información. Otra definición es, la debilidad de un activo que puede ser explotado por una amenaza para materializar una agresión sobre dichos activos, se clasifica en alta, media y baja.

Medición del Riesgo: Para realizar la medición del riesgo debemos considerar ciertos factores, como lo son:

- Amenaza: es una acción posible que pudiese causar daño y puede ocurrir con una determinada probabilidad. Un ejemplo de amenaza son los huracanes, terremotos y en el mundo informático, virus o ataques.
- Probabilidad: Posibilidad de que un evento ocurra. La probabilidad es un factor fundamental asociado al riesgo, es condicional y se presenta por evento. La probabilidad de ocurrencia.
- Impacto: Nos da una idea del valor del daño que se podría causar.

Para poder visualizar de una mejor manera los riesgos, utilizaremos una matriz que denominaremos matriz de riesgo:

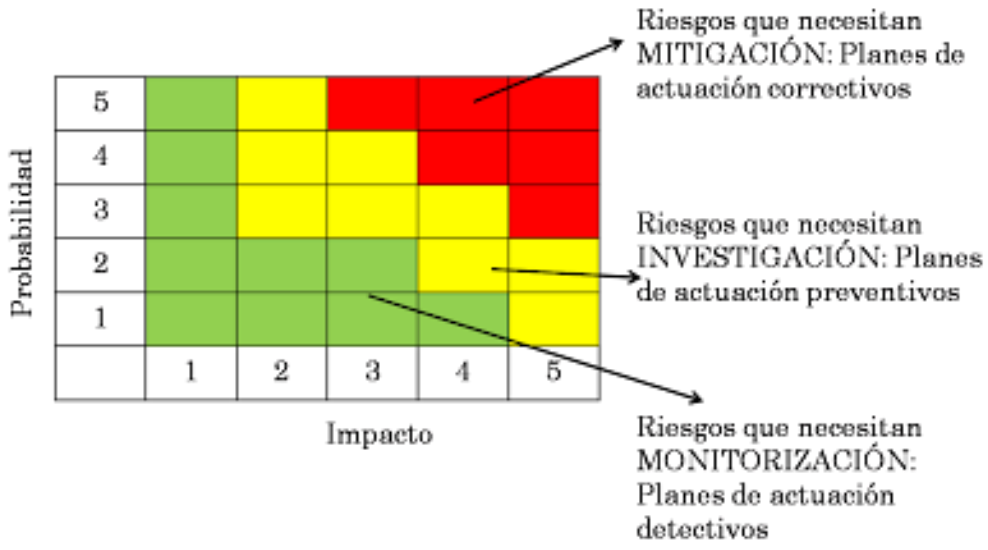


Figura 2. Matriz de riesgo.

Fuente: Sitegoogle.com (s.f)

Su principal aporte es que presenta en una sola vista, todos los riesgos que han sido detectados, su magnitud respectiva y permite realizar un plan de "mitigación" de riesgos, partiendo por aquellos que son de mayor valor.

1.3 Evaluación de vulnerabilidades

Cálculo del riesgo:

Formula: ALE= ARO x SLE

ARO (Annual Rate of Occurrence): es el número de veces que ocurre un incidente en el plazo de un año.

SLE (Single Loss Expentancy): es el costo en el que incurre la organización cuando se materializa el incidente.

SLE = Valor del Activo * Factor de Exposición

ALE (Annual Loss Expentancy): es el costo anual del riesgo y se obtiene de la anterior formula.

Factor de exposición

Corresponde al porcentaje de tiempo que está expuesto el activo a ser víctima de un incidente. Un ejemplo de esto es el caso de notebooks, que no tienen exposición de ser robados, mientras están en las dependencias de la organización, pero si, una vez que los usuarios los sacan y los llevan a sus casas.

En este caso, si el notebook estas 9 horas dentro de las dependencias y 15 horas fuera, el factor de exposición será 15/24, es decir:

FE = 62,5%

1.4 Tipos de evaluaciones de vulnerabilidades

Hardening de servidores

El proceso de hardening mínimo para cumplir los requerimientos del negocio de cada sistema operativo se denomina “baseline”.

Actividades típicas de un proceso de hardening:

- Cerrar los puertos no utilizados
- Deshabilitar protocolos no utilizados
- Cambiar parámetros por defecto
- Eliminar usuarios no utilizados
- Utilizar comunicaciones cifradas
- Eliminar los directorios y archivos temporales
- Grabar los registros de log en un servidor independiente y monitoreo de servidores y servicios.

Monitoreo de servidores y servicios:

Según icinga.com "Uno de los aspectos más importantes para la seguridad de un servidor es poder monitorear permanente sus servicios, para ello existen varias herramientas basadas en los protocolos ICMP y SNMP. Una de las más utilizadas es ICINGA, de licencia GNU y que permite monitorear las variables más importantes de un servidor."

Principios de seguridad en hardening de servidores:

- Mínimo privilegio: para mayor seguridad es altamente recomendable que los usuarios trabajen en los servidores con el usuario de más bajo privilegio, al igual que las aplicaciones que se ejecutan en el servidor, en ningún caso con las cuentas de root o Administrador.

- Mínimo punto de exposición: el acceso a los servidores solo debe ser posible desde aquellos puntos o redes que requiere para su función, esto reduce considerablemente la posibilidad de que una vulnerabilidad no parchada, pueda ser explotada.

Protección contra DHCP Spoofing:

Este ataque consiste en el envío de una dirección IP a un requerimiento DHCP desde un servidor falso. Una de las formas de protegerse es recibir estos requerimientos solo desde una dirección IP autorizada, la del verdadero DHCP server de la red.

Listas de control de acceso (ACL):

Permiten definir los atributos de usuarios en los archivos y directorios del sistema operativo, sus comandos básicos son:

- setfacl: se utiliza para establecer ACL en los archivos o directorios.
- getfacl: se utiliza para determinar las ACL que tiene configurado un archivo o directorio.

Almacenamiento de logs

En seguridad es fundamental mantener registros en línea de los eventos más importantes en forma centralizada y con un acceso ágil y robusto. Los eventos más importantes que se deben registrar son:

- Inicios de sesión.
- Accesos a recursos.
- Intentos de ataque.

Es importante considerar también, que las estrategias o actividades que apoyen el control de las vulnerabilidades no solo pasen por aspectos técnicos, lo ideal es que se consideren también aspectos administrativos. Por lo anterior, definamos los tipos de controles:

Administrativos: Están involucrados con procedimientos, políticas o entrenamiento, no involucran tecnología. *Ejemplo: política de seguridad.*

Técnicos: Son aquellos que involucran tecnología para cumplir su función, ya sea de control de acceso o protección de la información.

Ejemplo: autenticación, cifrado.

Físicos: Son aquellos que controlan el acceso físico de usuarios a la información. *Ejemplo: cámaras de vigilancia, bóvedas de seguridad.*

Ciclo de vida de la gestión de vulnerabilidades

Las soluciones para la gestión de vulnerabilidades generalmente se basan en el siguiente ciclo:

Figura 3. Gestión de vulnerabilidades

Fuente: antimalware.es (s.f)

1.5 Fases de la evaluación de vulnerabilidades

Identificación de la Vulnerabilidad: Es donde se detecta la vulnerabilidad.

Análisis: Una vez identificada la Vulnerabilidad es analizada para poder clasificarla.

Asignación de Riesgo: Una vez analizada la vulnerabilidad se le asignará el factor de riesgo para ver su nivel de prioridad.

Remediación: En esta etapa se aplican las remediales para eliminar la vulnerabilidad detectada.

Figura 4. Fases

Fuente: kapa7.com (s.f)

2. Soluciones de evaluación de vulnerabilidades

Las soluciones para la gestión de vulnerabilidades toman los actuales desafíos de seguridad cibernética al insistir en un proceso completo y continuo que identifica, clasifica, remedia y mitiga las vulnerabilidades antes de que los atacantes puedan explotarlas. Por lo general estos programas de gestión de vulnerabilidades suelen escanear vulnerabilidades para así evaluar y comprender automáticamente el riesgo al que está expuesto la infraestructura, la información la entrega mediante fáciles de analizar que recomiendan a las empresas que priorizar de forma más adecuada y así rápidamente remediar o mitigar las vulnerabilidades.

2.1 Productos y Servicios basados en soluciones

BaaS (Backup as a Service)

La copia de seguridad como servicio conocida por sus siglas en inglés (BaaS) consiste en una solución para la copia de seguridad que consiste en la recuperación que implica comprar estos servicios que son administrados por un proveedor de servicios cloud.

IaaS (Infrastructure as a Service)

"La Infraestructura como servicio (IaaS) es una solución de cloud computing, mediante la cual un proveedor proporciona a los usuarios acceso a recursos informáticos como servidores, almacenamiento y redes. Las empresas utilizan sus propias plataformas y aplicaciones en una infraestructura del proveedor de servicios." *(fuente: edapi.cl)*

PaaS (Platform as a Service)

La Plataforma como servicio (PaaS) es una solución de cloud computing en que un proveedor de servicios se encarga de gestionar y proporcionar una plataforma de software de aplicaciones y el hardware donde usuario es el que maneja los datos y la aplicación. Esta solución es útil para los para programadores y desarrolladores, ya que tienen plataformas que permiten ejecutar, desarrollar y gestionar sus propias aplicaciones, sin la necesidad de tener que diseñar ni mantener la infraestructura asociada. Algunas plataformas de nube son que son un tipo de PaaS son: *Alibaba Cloud, Microsoft Azure, Google Cloud, Amazon Web Services (AWS) e IBM Cloud.*

SaaS (Software as a Service)

El SaaS es un servicio proporciona a los usuarios una aplicación web ejecutable en el navegador, que es gestionado por el proveedor de servicios. Lo referente a gestión de software, errores y otros procesos generales de mantenimiento corren por cargo del usuario gestionándolas a través de un panel o una API. El SaaS no se instala como aplicación en los terminales de cada usuario, lo que garantiza una mejora en los métodos de acceso en equipo al sistema de software.

2.2 Solución basada en análisis de vulnerabilidades

Las soluciones en la nube que están enfocadas en análisis de vulnerabilidades son rápidas, escalables y de fácil uso, lo que plantea un dilema. Si no existe un control, se pueden implementar rápidamente activos complejos en la producción y aumentar la exposición a estas en el proceso. Un aspecto positivo es que estas soluciones permiten tener una visibilidad completa de los activos efímeros en casi tiempo real.

2.3 Tipos de soluciones de evaluación de vulnerabilidades

Existe una enorme variedad de soluciones de evaluación de vulnerabilidades entre ellas, muchas empresas ofrecen una amplia gama de soluciones para Amazon Web Services (AWS), Google Cloud Platform y Microsoft Azure que permiten habilitar la detección casi en tiempo real de nuevas implementaciones de activos informáticos en sus entornos multinube.

Una de las soluciones más conocidas es Nessus, que es un programa de escaneo de vulnerabilidades para diversos sistemas operativos que basa su escaneo de puertos en NMAP, y que intenta varios exploits para descubrir vulnerabilidades, arrojando un informe después de este escaneo.

3. Herramientas para el análisis de vulnerabilidades

3.1 Qualys Vulnerabity Management

Qualys VMDR 2.0 es una solución integral de gestión de vulnerabilidades que está basada en riesgos y así prioriza vulnerabilidades de los activos en función del riesgo y la criticidad del negocio. VMDR se integra fácilmente con las bases de datos de administración de configuración (CMDB) junto con las soluciones de administración de parches y así logra descubrir, priorizar y remediar automáticamente las vulnerabilidades para reducir el riesgo. Además, se puede integrar con soluciones de ITSM como ServiceNow para poder automatizar y lograr que la gestión de vulnerabilidades esté operativa de principio a fin.

Figura 5. Logo Qualys.

Fuente: Qualys.com (s.f)

3.2 Nessus and GFI Languard

Anteriormente en el presente documento nos referimos a la solución Nessus y mencionamos sus características, cabe destacar que existen dos versiones, una gratuita y una de pago.

Figura 6. Logo Nessus.

Fuente: tenable.com s.f

GFI LanGuard permite administrar y mantener la protección de todos los endpoints presentes en una red. A través de informes brinda visibilidad de todos los elementos de la red, ya que evalúa dónde puede haber vulnerabilidades

potenciales para así repararlas. Es una solución de gestión de parches y auditoría de red que es muy fácil de usar y de implementar. Solo existe en versión de pago.

Figura 7. Logo GFI Languard.

Fuente: gfi.com (s.f)

3.3 OpenVAS

OpenVAS es un scanner de vulnerabilidades bastante completo que detecta problemas de diferente relevancia, tanto de bajo riesgo para usuarios, como vulnerabilidades de mayor importancia en endpoints en dispositivos en red. Según cifras oficiales tiene más de 50.000 datos y test de vulnerabilidades que a diario son aumentadas por la empresa y por parte de la comunidad y sus expertos. Cuenta con una interfaz gráfica para que el proceso de análisis se más útil visualmente y sencillo para el usuario.

3.4 ADVS: automated vulnerabity detection system

Cuando hablamos de ADVS nos referimos a todos los escáneres de vulnerabilidades de aplicaciones web que detectan vulnerabilidades técnicas, entre ellas, por ejemplo, vulnerabilidades SQLi (inyección SQL), secuencias de comandos

en sitios cruzados (XSS) o CSRF (Falsificación de solicitudes en sitios cruzados). Esto es porque, al presentarse vulnerabilidades técnicas, las respuestas que recibe la aplicación web durante el análisis de vulnerabilidades generalmente entregan una buena evidencia para determinar la presencia o no de una vulnerabilidad en particular.

3.5 Burp Suite

Burp Suite es una solución digital que contiene herramientas especializadas para realizar pentesting en aplicaciones web. Burp Suite tiene dos versiones: una gratuita (Burp Free) y una versión de pago (Burp Professional). Las diferenciaremos para establecer cómo se usan para realizar hacking ético de páginas web.

Burp Suite Community Edition es la versión gratuita de esta plataforma, viene instalada en Kali Linux por defecto. Su función principal es la de actuar como proxy HTTP de la aplicación para hacer el pentesting.

Burp Proffessional es un software de pago que fue desarrollado por PortSwigger. Además del proxy HTTP incluye algunas herramientas para pentesting web.

Cierre

Después de revisar lo estudiado en la semana, se puede graficar lo siguiente.

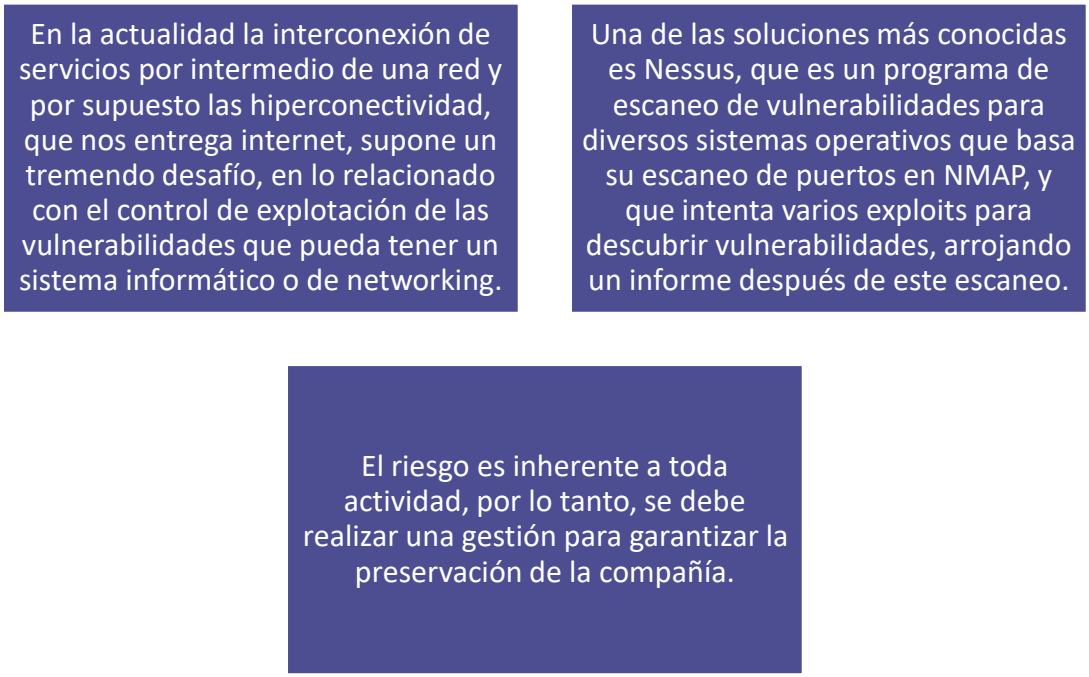


Figura 8. Ideas claves semana 5.

Fuente: Moran, E. (2022)

Referencias Bibliográficas

Pasos de la gestión de vulnerabilidades. Recuperado de https://antimalwares.es/pasos-de-un-programa-de-gestion-de-vulenrabilidades

¿Qué es OpenVAS?. Recuperado de https://openwebinars.net/blog/que-es-openvas/

Proceso de evaluación de vulnerabilidad. Recuperado de https://manageengine.com.mx/vmp/proceso-de-evaluacion-de-la-vulnerabilidad

Tenable y Nessus. Recuperado de https://es-la.tenable.com/solutions/vulnerability-management

Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios. David A. Franco, Jorge L. Perea y Luis C. Tovar. Universidad de Cartagena, Facultad de Ingeniería, Grupo de Investigación en Tecnologías de las Comunicaciones e Informática.

Qualys. Recuperado de https://www.qualys.com/apps/vulnerability-management-detection-response/

Soluciones según servicio. Recuperado de https://www.edapi.cl/soluciones-ti/soluciones-as-a-service/

GFI Landguard. Recuperado de https://www.gfi.com/products-and-solutions/network-security-solutions/languard

Automatización de la detección de vulnerabilidades de control de acceso en aplicaciones web. Recuperado de https://link.springer.com/article/10.1007/s42979-022-01271-1

Burp Suite. Recuperado de https://keepcoding.io/blog/que-es-burp-suite/