Módulo 4.

FUNDAMENTOS DE LA CIBERSEGURIDAD.

Oficina Asesora de Informática | Digitalízate Comunidad

Contenido.

1.Herramientas importantes de la ciberseguridad.

1.1 Video: Introducción a la semana 4.

Te damos la bienvenida a la sección final de este curso. Presentaremos herramientas y lenguaje de programación utilizados comúnmente en el campo de la ciberseguridad. Son fundamentales para el monitoreo de la seguridad en una organización porque mejoran la eficiencia con la automatización de tareas. Si bien en este momento solo estamos presentando estos conceptos y herramientas, podrás usarlos más adelante en el programa en actividades prácticas diversas. En los siguientes videos, aprenderás sobre las herramientas de información de seguridad y gestión de eventos, o SIEM. También conocerás otras herramientas como manuales de estrategias y analizadores de protocolos de red. Luego, aprenderás acerca del sistema operativo Linux, y de las tareas relacionadas con la seguridad iniciadas por medio de lenguajes de programación, como SQL y Python. Para mí, SQL es una de las herramientas más útiles. Me permite explorar todas las fuentes de datos que recolectamos, y le permite a mi equipo hacer un análisis de tendencias. Tómate tu tiempo para analizar los videos y vuelve a verlos si lo necesitas. Estas herramientas se analizarán con mucho más detalle, y podrás practicar de primera mano más adelante en el programa. Si bien las organizaciones tienen sus herramientas y materiales que aprenderás a usar en el trabajo, este programa te brindará conocimiento fundamental que te ayudará a tener éxito en la industria de la ciberseguridad. ¡Empecemos!

1.2. Video: Herramientas habituales de la ciberseguridad.

Como ya se mencionó, la seguridad es como prepararse para una tormenta. Si identificas una fuga, el color o la forma del balde que usarás para atrapar el agua no importa. Lo importante es mitigar los riesgos y amenazas a tu hogar mediante el uso de las herramientas a tu disposición. Como analista de seguridad de nivel inicial, tendrás un montón de herramientas en tu kit que puedes usar para mitigar riesgos potenciales. En este video, analizaremos los propósitos principales y las funciones de algunas herramientas comúnmente usadas. Y más adelante, tendrás oportunidad de practicar su uso. Antes de seguir con las herramientas, analicemos brevemente los registros, que son las fuentes de datos que las herramientas que veremos deben organizar. Un registro es un historial de eventos que ocurren dentro de los sistemas de una organización. Algunos ejemplos incluyen registros de inicios de sesión de empleados/as en sus computadoras o accesos a servicios en la red. Los registros ayudan a las/los profesionales de la seguridad a identificar vulnerabilidades y potenciales fugas de información.

Las primeras herramientas que veremos son herramientas de información de seguridad y gestión de eventos, o herramientas SIEM. Una herramienta SIEM es una aplicación que recolecta y analiza datos de registro para monitorear actividades críticas en una organización. El acrónimo S-I-E-M puede pronunciarse "SIM" o "SIEM", pero usaremos "SIEM" a lo largo de este programa. Las herramientas SIEM recopilan información en tiempo real, o instantánea, y permite que las/los analistas de seguridad identifiquen fugas potenciales mientras ocurren. Imagina tener que leer páginas y páginas de registros para determinar si hay amenazas de seguridad. Según la cantidad de datos, puede tomar horas o días. Las SIEM reducen la cantidad de datos que un/a analista debe revisar al brindar alertas para tipos específicos de riesgos y amenazas. Ahora repasemos ejemplos de herramientas SIEM de uso común: Splunk y Chronicle. Splunk es una plataforma de análisis de datos, y Splunk Enterprise proporciona soluciones SIEM. Splunk Enterprise es una herramienta autoalojada que se usa para retener, analizar y buscar datos de registro de una organización. Otra herramienta SIEM es Chronicle, de Google. Chronicle es una SIEM nativa de la nube, que almacena datos de seguridad para búsqueda y análisis. El ser nativa de la nube significa que Chronicle permite una entrega rápida de nuevas características. Ambas herramientas SIEM, y las SIEM en general, recopilan datos de distintos lugares, luego los analizan y filtran para permitir a los equipos de seguridad prevenir y reaccionar rápidamente ante posibles amenazas a la seguridad. Como analista de seguridad, puede que te encuentres usando las SIEM para analizar eventos y patrones filtrados, realizar análisis de incidentes o buscar amenazas de forma proactiva. Según la configuración de las SIEM y el enfoque de riesgo de tu organización, las herramientas y la manera en que estas funcionan puede diferir. Pero en última instancia, todas se usan para mitigar el riesgo. Otras herramientas clave que usarás como analista de seguridad, y cuyo uso podrás practicar más adelante en el programa, son los manuales de estrategias, y analizadores de protocolo de red. Un manual de estrategias proporciona detalles acerca de cualquier acción operativa, como la forma de responder a un incidente. Estos manuales, que varían de acuerdo a la organización, orientan a las/los analistas sobre cómo manejar un incidente de seguridad antes, durante y después de que ocurrió.

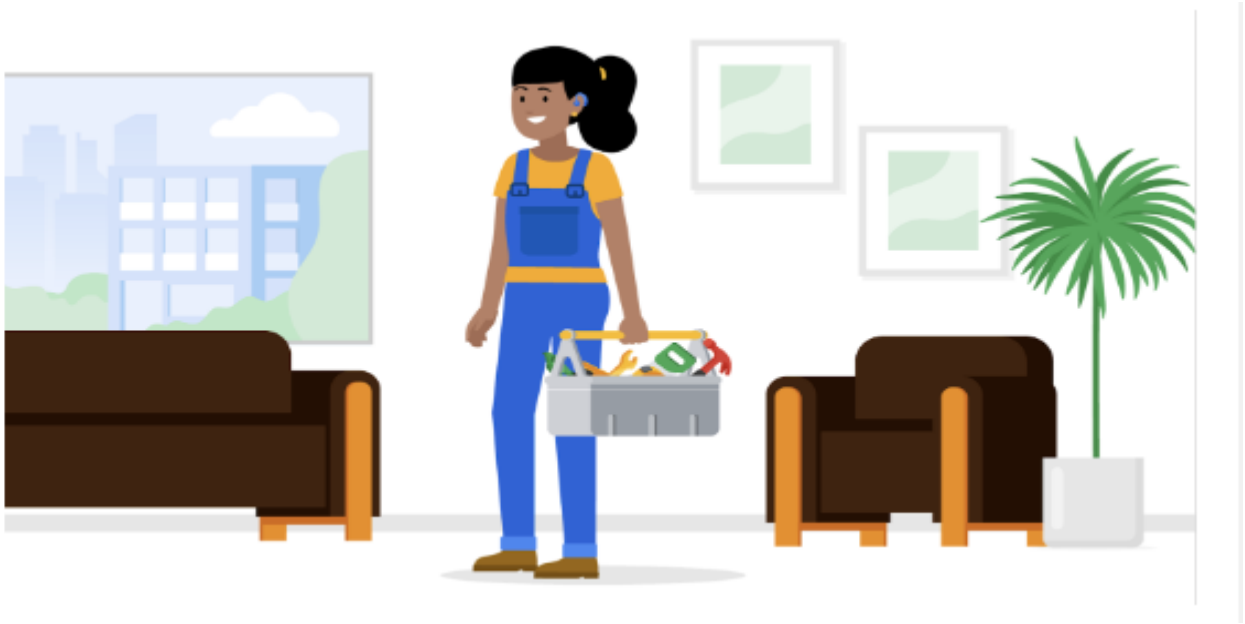
Pueden corresponder a revisiones de conformidad o seguridad, gestión del acceso y muchas otras tareas

organizacionales que requieren un proceso documentado de inicio a fin. Otra herramienta que puedes usar como analista de seguridad es un analizador de protocolos de red, o Sniffer de paquetes. Un Sniffer de paquetes es una herramienta diseñada para capturar y analizar el tráfico de datos dentro de una red. Los analizadores de protocolos de red comunes incluyen TCPdump y Wireshark. Como analista de nivel inicial, no tienes que ser un/a experto/a en estas herramientas. A medida que avances en este programa y obtengas más práctica, entenderás más y más acerca de cómo usar estas herramientas para identificar, evaluar y mitigar los riesgos.

1.3. Lectura: herramientas para proteger las operaciones comerciales.

Anteriormente, te presentamos distintas habilidades técnicas que las/los analistas de seguridad necesitan desarrollar, además de algunas herramientas que las/los analistas de nivel inicial pueden tener en su caja de herramientas. En esta lectura, profundizarás sobre cómo las habilidades y herramientas técnicas ayudan a mitigar los riesgos.

La caja de herramientas de un/a analista de nivel inicial: Cada organización puede proporcionar una caja de herramientas diferente, dependiendo de sus necesidades de seguridad. Como futuro analista, es importante que te familiarices con las herramientas estándar de la industria y que puedas demostrar tu capacidad para aprender a usar otras similares, en un lugar de trabajo diferente.

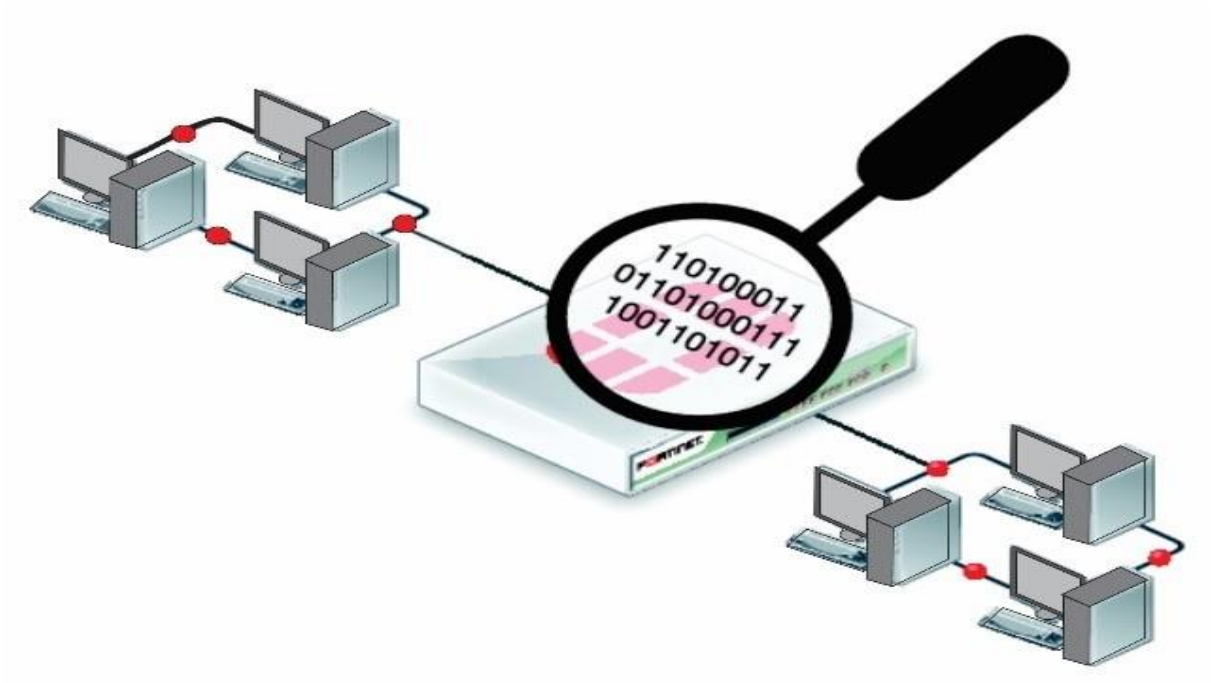


Herramientas de información de seguridad y gestión de eventos (SIEM) Una herramienta SIEM es una aplicación que recopila y analiza datos de registro para monitorear actividades críticas en una organización. Un registro recopila eventos que ocurren dentro de los sistemas de una organización. Dependiendo de la cantidad de datos con los que estés trabajando, podría tomarte horas o días filtrar los datos del registro. Las herramientas SIEM proporcionan alertas para tipos específicos de amenazas, riesgos y vulnerabilidades, lo que reduce la cantidad de datos que un/a analista debe revisar.

Además, las herramientas SIEM ofrecen una serie de paneles con indicadores (dashboards) que organizan visualmente los datos en categorías, lo cual permite a los/las usuarios/as seleccionar aquellos que desean analizar. Las diferentes herramientas SIEM tienen distintos tipos de paneles de control, que muestran la información a la cual tienes acceso.

Las herramientas SIEM también cuentan con diferentes opciones de alojamiento: on-premise (local) y en la nube. Las organizaciones pueden elegir la opción de alojamiento que prefieran, en función de la experiencia de los miembros del equipo de seguridad. Por ejemplo, dado que una versión alojada en la nube suele ser más fácil de configurar, usar y mantener que una versión local, un equipo de seguridad con menos experiencia puede elegir esta opción.

Analizadores de protocolo de red (programas detectores de paquetes): Un analizador de protocolo de red, también conocido como un programa detector de paquetes, es una herramienta diseñada para capturar y analizar el tráfico de datos en una red. Esto significa que la herramienta mantiene un registro de todos los datos que encuentra una computadora dentro de la red de una organización. Más adelante en el programa, tendrás la oportunidad de practicar el uso de algunas de las herramientas más comunes de un analizador de protocolos de red.



Manual de estrategias

Un manual de estrategias (o playbook) brinda detalles sobre cualquier acción operativa, como la forma de responder a un incidente de seguridad. En general, las organizaciones tienen varios manuales de estrategias, que documentan los procesos y procedimientos para que sus equipos los sigan. Los manuales de estrategias varían de una organización a otra, pero todos tienen un propósito similar: guiar a las/los analistas mediante una serie de pasos, para completar tareas específicas relacionadas con la seguridad.

Por ejemplo, considera que estás trabajando como analista de seguridad para una empresa de respuesta a incidentes y se te presenta un caso que involucra una clínica médica pequeña que fue víctima de una fuga de información. Tu trabajo es ayudar con la investigación forense y proporcionar evidencia a una compañía de seguros de ciberseguridad. De acuerdo a los hallazgos obtenidos, se determinará si la clínica recibirá o no el pago del seguro.

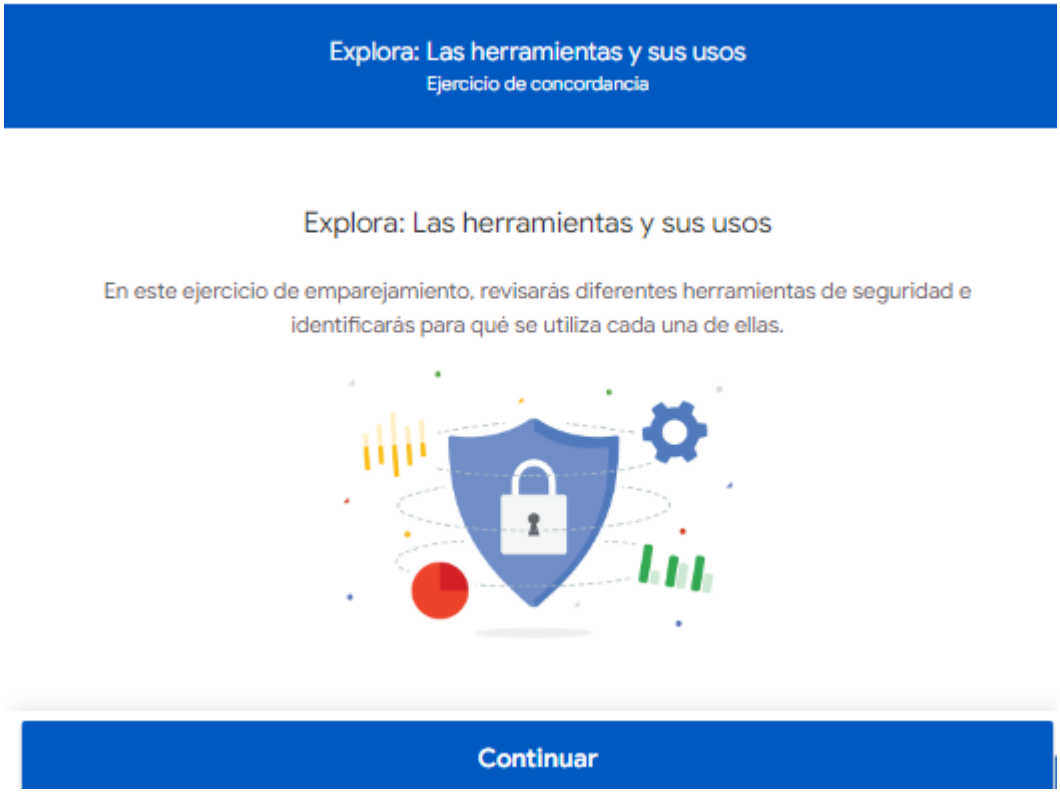
En este ejemplo, los manuales describirán las acciones específicas que debes tomar para llevar a cabo la investigación. También ayudan a que te asegures de que estás siguiendo los protocolos y procedimientos adecuados. Cuando trabajas en un caso forense, hay dos manuales que puedes seguir:

El primero que puedes consultar es el manual de la cadena de custodia. La cadena de custodia es el proceso de documentar la posesión y el control de la evidencia durante el ciclo de vida del incidente. Como analista de seguridad involucrado/a en un análisis forense, trabajarás con los datos que fueron vulnerados. Junto con el equipo forense, también deberás documentar quién, qué, dónde y por qué tienen la evidencia recopilada. Mientras estén en tu poder, las pruebas son tu responsabilidad, y deben rastrearse y

mantenerse seguras. Cada vez que la evidencia se mueve, debe reportarse. Esto permite a todas las partes involucradas saber exactamente dónde está en todo momento.

El segundo manual de estrategias que tu equipo podría usar se llama manual de protección y preservación de la evidencia. La protección y preservación de la evidencia es el proceso de trabajar adecuadamente con evidencia digital frágil y volátil. Como analista de seguridad, es fundamental comprender qué es la evidencia digital frágil y volátil, y por qué existe un procedimiento. Al seguir este manual, consultarás el orden de volatilidad, que es una secuencia que describe el orden de los datos que deben conservarse, del primero al último. Prioriza los datos volátiles, que son datos que pueden perderse si el dispositivo en cuestión se apaga, independientemente de la razón. Durante una investigación, la gestión inadecuada de la evidencia digital puede comprometerla y alterarla. Cuando esta se maneja incorrectamente durante una investigación, ya no se puede usar. Por esta razón, la prioridad en cualquier investigación es preservar adecuadamente los datos. Para conservar los datos, puedes hacer copias y utilizarlas al llevar a cabo la investigación.

1.4. Complemento no calificado: Explora: Herramientas y sus propósitos.



1.5 Cuestionario practico: Pon a prueba tus conocimientos: Herramientas importantes de ciberseguridad.

1. ¿Qué herramienta está diseñada para capturar y analizar el tráfico de datos dentro de una red? 1 punto

- ◯ Splunk Enterprise
- ◯ analizador de protocolo de red (programa rastreador de paquetes)
- ◯ Google Chronicle
- ◯ Lenguaje de consulta estructurado (SQL)

2. ¿Cuáles de las siguientes son ejemplos de herramientas SIEM? Selecciona dos respuestas. 1 punto

- ☐ Splunk Enterprise
- ☐ Google Chronicle
- ☐ Python
- ☐ Linux

3. ¿Para qué utilizan los registros principalmente las/los profesionales de seguridad? 1 punto

- ◯ Para seleccionar qué miembros del equipo de seguridad responderán a un incidente.
- ◯ Para recopilar y analizar datos y así monitorear actividades críticas en una organización.
- ◯ Para identificar vulnerabilidades y posibles fugas de información.
- ◯ Para investigar y optimizar las capacidades de procesamiento dentro de una red.

4. Completa el espacio en blanco: _____ brinda detalles sobre las acciones operativas. 1 punto

- ◯ Un manual de estrategias
- ◯ Una lista de verificación
- ◯ Un historial de caso
- ◯ Un directorio

2. Conocimientos y habilidades básicas de la ciberseguridad.

2.1 Video: Introducción a Linux, SQL y Python

En esta guía entendemos que las organizaciones usan una variedad de herramientas, como **SIEM, manuales de estrategias** y **detectores de paquetes para gestionar**, monitorear y analizar mejor las amenazas a la seguridad. Pero esas no son las únicas herramientas en el kit de un/a analista. También usan lenguajes de programación y sistemas operativos para lograr tareas esenciales. En este video, te presentaremos la programación **SQL** y **Python,** y el sistema operativo **Linux.** Tendrás la oportunidad de practicar y usarlas más adelante en el programa. Las organizaciones pueden usar la programación para crear instrucciones específicas que una computadora ejecute. La programación permite a las/los analistas completar tareas y procesos repetitivos con un alto grado de precisión y eficiencia. También ayuda a reducir el riesgo de error humano, y puede ahorrar horas o días en comparación con el trabajo manual. Ahora que sabes para qué se usan los lenguajes de programación, analicemos un sistema operativo específico y relacionado llamado **Linux** y dos lenguajes de programación**: SQL** y **Python**. **Linux** es un sistema operativo de código abierto o públicamente disponible. A diferencia de otros SO con los que puedas estar familiarizado/a, como MacOS o Windows, Linux depende de una línea de comandos como la interfaz de usuario principal. **Linux** en sí no es un lenguaje de programación, pero sí permite el uso de comandos de texto entre el usuario y el sistema operativo. Aprenderás más sobre Linux más adelante. Un uso común de Linux para las/los analistas de seguridad de nivel inicial es la examinación de registros para entender mejor lo que ocurre en un sistema. Por ejemplo, quizá uses comandos para revisar un registro de errores mientras investigas un tráfico de red inusualmente alto. A continuación, veamos **el SQL**.

SQL significa lenguaje de consulta estructurado. **SQ**L es un lenguaje de programación usado para crear, interactuar y solicitar información de una base de datos. Una base de datos es una colección organizada de información o datos. Puede haber millones de datos en estas bases. Entonces, un/a analista de seguridad de nivel inicial usaría **SQL** para filtrar los datos y recuperar información específica. El último lenguaje de programación que presentaremos es **Python**. Las/los profesionales de la seguridad pueden usar **Python** para realizar tareas repetitivas y desgastantes, y que requieren un alto nivel de detalle y precisión. Como futuro/a analista, es importante entender que el kit de herramientas de cada organización puede ser diferente según sus necesidades de seguridad. Lo importante es que te familiarices con algunas herramientas estándar, ya que es les mostrará a los/las empleadores/as que tienes la habilidad de aprender a usar sus herramientas para proteger la organización y sus clientes.

¡Muy buen trabajo! Más adelante, aprenderás más sobre Linux y lenguajes de programación. También practicarás mediante el uso de estas herramientas en escenarios relacionados con la seguridad.

2.2. Lectura: Usa herramientas para proteger las operaciones comerciales.

Anteriormente, te presentamos la programación, los sistemas operativos y las herramientas que usan comúnmente las/los profesionales de la ciberseguridad. En esta lectura, aprenderás más sobre la programación y los sistemas operativos, así como otras herramientas que las/los analistas de nivel inicial utilizan para ayudar a proteger a las organizaciones y las personas a las que sirven.

Herramientas y sus propósitos.

Programación: La programación es un proceso que se puede usar para crear un conjunto específico de instrucciones para que una computadora ejecute tareas. Las/los analistas de seguridad utilizan lenguajes de programación, como Python, para ejecutar la automatización. La automatización es el uso de la tecnología para reducir el esfuerzo humano y manual en la realización de tareas comunes y repetitivas. También ayuda a reducir el riesgo de errores humanos.

Otro lenguaje de programación que utilizan las/los analistas se llama Structured Query Language (SQL). SQL se utiliza para crear, interactuar y solicitar información de una base de datos. Una base de datos es una colección organizada de información o datos. Puede haber millones de datos en una base. Un dato es una pieza específica de información.

Sistemas operativos: Un sistema operativo es la interfaz entre el hardware de la computadora y el usuario. Linux®, macOS® y Windows son sistemas operativos. Cada uno ofrece diferentes funcionalidades y experiencias de usuario.

Ya mencionamos a Linux como un sistema operativo de código abierto. El código abierto significa que el código está disponible para el público y permite a las personas hacer contribuciones para mejorar el software. Linux no es un lenguaje de programación; sin embargo, sí implica el uso de una línea de comandos dentro del sistema operativo. Un comando es una instrucción que indica a la computadora que haga algo. Una interfaz de línea de comandos es una interfaz de usuario basada en texto que utiliza comandos para interactuar con la computadora.

Vulnerabilidad de la web: Una vulnerabilidad de la web es un código o comportamiento malicioso que se utiliza para aprovechar las fallas de codificación en una aplicación web. Agentes de amenaza pueden explotar las aplicaciones web vulnerables, lo que permite el acceso no autorizado, el robo de datos y la implementación de software malicioso.

Software antivirus: El software antivirus (o anti-malware) es un programa utilizado para prevenir, detectar, y eliminar malware y virus. Dependiendo del tipo de software antivirus, puede escanear la memoria de un dispositivo para encontrar patrones que indiquen la presencia de software malicioso.

Sistema de detección de intrusiones: Un sistema de detección de intrusiones (IDS) es una aplicación que monitorea la actividad del sistema y alerta sobre posibles intrusiones. El sistema escanea y analiza paquetes de red, que transportan pequeñas cantidades de datos a través de una red. La pequeña cantidad de datos hace que el proceso de detección sea más fácil para que un IDS identifique posibles amenazas a los datos confidenciales. Otras ocurrencias que un IDS es capaz de detectar pueden incluir el robo y el acceso no autorizado.

Cifrado: El cifrado es el proceso de convertir datos de un formato legible a un formato codificado. La codificación criptográfica significa convertir texto plano en texto cifrado seguro. El texto plano es información sin cifrar y el texto cifrado seguro es el resultado del cifrado. Una forma criptográfica de código se utiliza para comunicarse en secreto y evitar el acceso no autorizado y no aprobado a datos, programas o dispositivos.

Nota: la codificación y el cifrado sirven para diferentes propósitos. La codificación utiliza un algoritmo de conversión pública para permitir que los sistemas que utilizan diferentes representaciones de datos compartan información. El cifrado hace que los datos sean ilegibles y difíciles de decodificar para usuarios/as no autorizados/as; su objetivo principal es garantizar la confidencialidad de los datos privados.

Pruebas de penetración: Las pruebas de penetración, también llamadas pen testing, son testeos que simulan un ataque, con el objetivo de ayudar a identificar vulnerabilidades en sistemas, redes, sitios web, aplicaciones y procesos. Mediante este cálculo de riesgos exhaustivo se pueden evaluar e identificar amenazas externas e internas, así como debilidades.

2.3 Cuestionario practico: Pon a prueba tus conocimientos: Conocimientos y habilidades básicos de ciberseguridad.

1. ¿Qué utilizan las/los profesionales de seguridad para interactuar y solicitar información de una base de datos? 1 punto

- ◯ Lenguaje de consulta estructurado (SQL)
- ◯ Linux
- ◯ Tríada de confidencialidad, integridad y disponibilidad (CID)
- ◯ Python

2. ¿Para qué suele utilizarse la programación? Selecciona dos respuestas. 1 punto

- ☐ Para crear un conjunto específico de instrucciones para que una computadora ejecute tareas.
- ☐ Para habilitar operaciones de código abierto.
- ☐ Para registrar eventos que tienen lugar dentro de los sistemas de una organización.
- ☐ Para completar tareas y procesos repetitivos.

3. Completa el espacio en blanco: Linux es _____ de código abierto que se puede utilizar para examinar los registros. 1 punto

- ◯ un sistema operativo
- ◯ un algoritmo
- ◯ un lenguaje de programación
- ◯ una base de datos

4. Un manual de estrategias brinda detalles sobre cómo responder a un incidente solo después de que haya ocurrido. 1 punto

- ◯ Verdadero
- ◯ Falso

2.4. Lectura: Crea una carrera de ciberseguridad.

A lo largo de este programa de certificación, tendrás múltiples oportunidades para desarrollar una cartera profesional de ciberseguridad para mostrar tus habilidades y conocimientos de seguridad.

En esta lectura, aprenderás qué es una cartera y por qué es importante desarrollar una cartera profesional de ciberseguridad. También aprenderás sobre las opciones para crear una cartera en línea o autoalojada que puedes compartir con posibles empleadores/as cuando empieces a buscar trabajo en temas de ciberseguridad.

¿Qué es una cartera profesional y por qué es necesaria?
Las/las profesionales de ciberseguridad utilizan carteras para demostrar su educación, habilidades y conocimientos en seguridad cuando solicitan puestos de trabajo. Así, pueden mostrar a los/las potenciales empleadores/as que les apasiona su trabajo y que pueden desempeñar el puesto que solicitan. Las carteras profesionales son más completas que un currículum, que por lo general es un resumen de una a dos páginas que brinda información sobre educación relevante, experiencia laboral y logros. En el último curso de este programa, tendrás la oportunidad de desarrollar un currículum y finalizar tu cartera.

¿Qué es una cartera profesional y por qué es necesaria?
Las/las profesionales de ciberseguridad utilizan carteras para demostrar su educación, habilidades y conocimientos en seguridad cuando solicitan puestos de trabajo. Así, pueden mostrar a los/las potenciales empleadores/as que les apasiona su trabajo y que pueden desempeñar el puesto que solicitan. Las carteras profesionales son más completas que un currículum, que por lo general es un resumen de una a dos páginas que brinda información sobre educación relevante, experiencia laboral y logros. En el último curso de este programa, tendrás la oportunidad de desarrollar un currículum y finalizar tu cartera.

Opciones para crear tu cartera.

Hay muchas maneras de presentar una cartera, incluidas las opciones autoalojadas y en línea, como:

- Carpeta de documentos
- Google Drive o Dropbox™
- Google Sites
- Repositorios Git

Opción 1: Carpeta de documentos.

Descripción: Una carpeta de documentos es una carpeta creada y guardada en el disco duro de tu computadora. Tú administras la carpeta, las subcarpetas, los documentos y las imágenes dentro de ella.

Las carpetas de documentos te permiten tener un acceso directo a tu documentación. El tener tus documentos profesionales, imágenes y otra información bien organizados puede ahorrarte mucho tiempo cuando vayas a solicitar un trabajo. Por ejemplo, es posible que quieras crear una carpeta principal titulada "Documentos profesionales". Luego, dentro de tu carpeta principal, puedes crear subcarpetas con títulos como:

- Currículum
- Educación
- Documentos de la cartera
- Herramientas de ciberseguridad
- Programación

Configuración: las carpetas de documentos se pueden crear de varias maneras, dependiendo del tipo de computadora que utilices. Si no tienes claro cómo crear una carpeta en tu dispositivo, puedes buscar en Internet videos o documentos instructivos, de acuerdo al tipo de computadora que usas.

Opción 2: Google Drive o Dropbox

Descripción: Google Drive y Dropbox ofrecen funcionalidades similares que te permiten almacenar tu documentación profesional en una plataforma en la nube. Ambas opciones también tienen funciones para compartir archivos, por lo que puedes compartir fácilmente los documentos de tu cartera con posibles empleadores/as. Cualquier adición o cambio que hagas en un documento de esa carpeta se verá reflejado automáticamente y así lo verá cualquier persona que tenga acceso a tu cartera.

Al igual que una carpeta de documentos, mantener bien organizada tu cartera basada en Google Drive o Dropbox será útil a medida que comiences o avances en tu trayectoria profesional.

Configuración: para saber cómo cargar y compartir archivos en estas aplicaciones, visita los sitios web de Google Drive y Dropbox.

Opción 3: Google Sites

Descripción: Google Sites y las opciones de alojamiento de sitios web similares tienen una variedad de funcionalidades fáciles de usar para ayudarte a presentar los elementos de tu cartera, que incluyen diseños personalizables, páginas web responsivas, capacidades de contenido incrustado y publicación web.

Las páginas web responsivas ajustan automáticamente su contenido para adaptarse a una variedad de dispositivos y tamaños de pantalla. Esto es útil porque los/las empleadores/as potenciales pueden revisar tu contenido utilizando cualquier dispositivo y tus medios se mostrarán como tú quieras. Cuando tengas todo listo, puedes publicar tu sitio web y recibir una URL única. Puedes agregar este enlace a tu currículum para que las personas a cargo de las contrataciones accedan fácilmente a tu trabajo.

Configuración: para saber cómo crear un sitio web en Google Sites, visita el sitio web de Google Sites.

Opción 4: Repositorio Git

Descripción: un repositorio Git es una carpeta dentro de un proyecto. En este caso, el proyecto es tu cartera, y puedes usar tu repositorio para almacenar los documentos, laboratorios y capturas de pantalla que completes durante cada curso del programa de certificado. Hay varios sitios de repositorios Git que puedes usar, entre ellos:

- GitLab
- Bitbucket™
- GitHub

Cada repositorio Git te permite mostrar tus habilidades y conocimientos en un espacio personalizable. Para crear una cartera de proyectos en línea en cualquiera de los repositorios mencionados, debes usar una versión de Markdown.

Configuración: para obtener información sobre cómo crear una cuenta de GitHub y usar Markdown, sigue los pasos descritos en el documento.

Cartera de proyectos.
Como mencionamos anteriormente, tendrás múltiples oportunidades a lo largo del programa de certificación para desarrollar elementos para incluir en tu cartera. Estas oportunidades incluyen:

- Redacción de una declaración profesional
- Realización de una auditoría de seguridad
- Análisis de la estructura y seguridad de la red
- Uso de comandos de Linux para administrar permisos de archivos
- Aplicación de filtros a consultas SQL
- Identificación de vulnerabilidades para una pequeña empresa
- Documentación de incidentes con el diario de un gestor de incidentes
- Importación y análisis de un archivo de texto en un escenario relacionado con la seguridad
- Creación o revisión de un currículum

Nota: no incluyas en tu carpeta documentos privados, protegidos por derechos de autor o de propiedad intelectual. Además, si utilizas uno de los sitios descritos en esta lectura, mantén tu sitio configurado en "privado" hasta que termines.

3.Revision: Herramientas de ciberseguridad y lenguaje de programación.

3.1. Video: Resumen.

Así completamos la introducción a herramientas de seguridad y lenguajes de programación. En esta sección, analizamos herramientas SIEM como Splunk y Chronicle. También vimos cómo las usan las/los analistas de seguridad para completar diferentes tareas. Luego, analizamos otras herramientas como los manuales de estrategias y los analizadores de protocolo de red, también llamados detectores de paquetes. Por último, presentamos el sistema Linux y los lenguajes de programación SQL y Python. Recuerda que lleva tiempo entender estas herramientas por completo, pero tener un entendimiento básico pueden ayudarte a conseguir trabajo en el área de la ciberseguridad.

3.2. Lectura: Términos del glosario semana 4.

Términos y definiciones del curso 1, semana 4.

- Analizador de protocolo de red (rastreador de paquetes): Herramienta diseñada para capturar y analizar el tráfico de datos dentro de una red.
- Base de datos: Colección organizada de información o datos estructurados.
- Información de seguridad y gestión de eventos (SIEM): Solución de seguridad que recopila y analiza los datos de registro para monitorear actividades críticas en una organización.
- Linux: Sistema operativo de código abierto.
- Orden de volatilidad: Secuencia que establece el orden en que deben conservarse los datos, del primero al último, en relación al tiempo en que estarán disponibles.
- Programación: Proceso que permite crear un conjunto específico de instrucciones para que una computadora ejecute tareas.
- Protección y preservación de la evidencia: Proceso de trabajar adecuadamente con evidencia digital frágil y volátil.
- Punto de dato: Elemento de información específico.
- Registro: Inventario de eventos que tienen lugar dentro de los sistemas de una organización.
- Sistema de detección de intrusiones (IDS): Aplicación que monitorea la actividad del sistema en busca de actividades intrusivas y toma medidas para detenerlas.
- Software de antivirus: Programa utilizado para prevenir, detectar, y eliminar software malicioso y virus.
- SQL (Structured Query Language): Lenguaje de programación utilizado para crear, interactuar y solicitar información de una base de datos.