Módulo 2.

FUNDAMENTOS DE LA CIBERSEGURIDAD •

Contenido

1.La historia de la ciberseguridad.

1.1. Video: bienvenida a la semana 2.

Este es un gran momento para aprender sobre seguridad. El haber aprendido acerca de los hackeos internacionales que afectan tanto a empresas privadas como a organizaciones gubernamentales me inspiró a trabajar en seguridad, porque me di cuenta de lo dinámico e importante que es esta área. Una razón por la que hay tantos puestos en el área de seguridad hoy en día tiene que ver con ataques que sucedieron en los años 80 y 90. Décadas después, las/los profesionales de seguridad continúan trabajando activamente para proteger las organizaciones y personas de variaciones de estos ataques informáticos. En esta sección del curso, analizaremos virus y software malicioso y presentaremos el concepto de ingeniería social. Luego, discutiremos acerca de cómo la era digital marcó el comienzo de una nueva era de agentes de amenaza. Conocer la evolución de cada ataque es clave para protegerse contra futuros ataques. Por último, daremos una visión general de ocho dominios de seguridad. A continuación, vamos a viajar en el tiempo, para explorar algunos de los virus, filtraciones de datos y ataques de software malicioso que ayudaron a dar forma a la industria tal como la conocemos hoy en día.

1.2 Video: ataques de seguridad pasados.

La industria de la seguridad está en constante evolución, pero muchos ataques actuales no son del todo nuevos. A menudo, las/los atacantes alteran o mejoran métodos anteriores. Comprender los ataques pasados puede orientarnos acerca de cómo manejar o investigar incidentes en tu trabajo como analista de seguridad. Primero, repasemos un par de términos clave que te ayudarán a entender los ataques que analizaremos. Un virus informático es un código malicioso escrito para interferir con operaciones informáticas y causar daños a los datos y el software. El virus se adhiere a programas o documentos en una computadora. Luego se propaga e infecta una o más computadoras en una red. Un gusano es un tipo de virus informático que puede duplicarse y propagarse por su cuenta, sin participación humana. Hoy en día, los virus son más conocidos como software malicioso, que es software diseñado para dañar dispositivos o redes. Hablaremos de dos ataques tempranos de software malicioso: el virus Brain y el gusano Morris. Fueron creados por desarrolladores de software malicioso para cumplir tareas específicas. Sin embargo, los desarrolladores subestimaron el impacto que su malware tendría y la cantidad de computadoras que este iba a infectar. Profundicemos un poco más en estos ataques y analicemos cómo ayudaron a dar forma a la ciberseguridad como la conocemos

hoy en día. En 1986, los hermanos Alvi crearon el virus Brain, si bien la intención del virus era rastrear copias ilegales de software médico y evitar las licencias piratas, lo que el virus terminó haciendo fue inesperado. Una vez que una persona usaba una copia pirata del software, el virus infectaba esa computadora. Luego, cualquier disco que se insertara en la computadora también se infectaba. El virus se propagaba a una computadora nueva cada vez que alguien usaba uno de los discos infectados. Desapercibido, el virus se propagó por todo el mundo en un par de meses. Aunque la intención no era destruir datos o hardware, el virus ralentizó la productividad e impactó significativamente en las operaciones comerciales. El virus Brain alteró radicalmente la industria informática. Destacó la necesidad de un plan para mantener la seguridad y productividad.

Como analista de seguridad, seguirás y mantendrás estrategias implementadas para asegurar que tu organización tenga un plan para mantener la seguridad de sus datos y personas. Otro ataque a computadoras influyente fue el gusano Morris. En 1988, Robert Morris desarrolló un programa para calcular el tamaño de Internet. El programa rastreó la web y se instaló en otras computadoras para calcular el número de equipos conectados a Internet. Parece sencillo, ¿verdad? Sin embargo, el programa no logró hacer un seguimiento de las computadoras que ya había puesto en riesgo, y seguía reinstalándose hasta que las computadoras se quedaron sin memoria y colapsaron. Cerca de 6000 computadoras se vieron afectadas, lo cual representaba el 10% de Internet en ese momento. Este ataque costó millones de dólares en daños debido a alteraciones en las empresas y a los esfuerzos necesarios para eliminar el gusano. Después del gusano Morris, se establecieron equipos de respuesta ante emergencias informáticas, conocidos como CERT, para responder a incidentes de seguridad informática. Los CERT aún existen, pero su lugar en la industria de la seguridad se amplió, e incluye más responsabilidades. Más adelante en este programa, aprenderás más acerca de las funciones básicas de estos equipos de ciberseguridad, y podrás practicar con herramientas de detección y respuesta. Los primeros ataques jugaron un papel clave a la hora de dar forma a la industria de ciberseguridad actual. Y a continuación, analizaremos cómo los ataques evolucionaron en la era digital.

1.3. Video: ataques en la era digital.

Con la expansión de una Internet confiable y de alta velocidad, el número de computadoras conectadas a ella aumentó muchísimo. Como el software malicioso puede propagarse por Internet, los agentes de amenaza ya no necesitaban de discos físicos para propagar virus. Para comprender mejor los ataques en la era digital, analizaremos dos ataques notables que dependieron de Internet: el ataque LoveLetter y la fuga de información de Equifax.

En el año 2000, Onel De Guzmán creó el malware LoveLetter para robar credenciales de inicio de sesión en Internet. Este ataque se extendió rápidamente y se aprovechó de personas que no habían aprendido a sospechar de los correos electrónicos no deseados. Los/las usuarios/as recibieron un correo con un "Te amo" en el asunto. Cada correo contenía un archivo adjunto titulado "Carta de amor para ti". Al abrir el archivo adjunto, el software malicioso escaneaba la libreta de direcciones de un/a usuario/a. Luego, se enviaba automáticamente a cada persona en la lista e instalaba un programa para recopilar información de usuario y contraseñas. Las personas pensaban que recibían un correo de un amigo, pero en realidad era software malicioso. LoveLetter terminó infectando a 45 millones de computadoras en todo el mundo, y se cree que causó daños por más de 10 mil millones de dólares. El ataque de LoveLetter es el primer ejemplo de ingeniería social. La ingeniería social es una manipulación técnica que explota el error humano para obtener información privada, acceso u objetos de valor. Luego de LoveLetter, los atacantes entendieron el poder de la ingeniería social. El número de ataques de ingeniería social aumenta con cada nueva aplicación de redes sociales que permite acceso público a los datos de personas. Hoy se prioriza muchísimo la conveniencia sobre la privacidad. El resultado de este cambio evolutivo es que estas herramientas pueden derivar en una vulnerabilidad mayor si no se usan apropiadamente. Como profesional de la seguridad, tu rol es identificar y gestionar un uso inapropiado de la tecnología que pueda poner a tu organización y todas las personas asociadas a ella en riesgo. Una forma de proteger a tu organización son las capacitaciones internas regulares. Como futuro analista de seguridad, puede que se te pida que las dirijas o que participes de ellas. Hoy en día, es común que se capacite a los/las empleados/as acerca de cómo identificar ataques de ingeniería social. Específicamente el phishing a través de correos que reciben. El phishing es el uso de comunicaciones digitales para engañar personas y provocar que revelen datos confidenciales o para propagar software malicioso. Ahora, hablemos de la fuga de información de Equifax. En 2017, atacantes se infiltraron con éxito en la agencia de informes de crédito Equifax. Esto dio lugar a una de las fugas de información más grandes de las que se tenga registro. Se robaron más de 143 millones de registros de clientes, y la fuga afectó a casi el 40% de todos/as los/las estadounidenses. Los registros contenían información personal identificable como números de seguridad social, fechas de nacimiento, licencias de conducir, domicilios y números de tarjetas de crédito. Desde el punto de vista de la seguridad, la fuga se produjo debido a múltiples fallas por parte de Equifax. No fue una única vulnerabilidad que los atacantes aprovecharon, sino varias. La empresa no tomó las medidas necesarias para reparar múltiples vulnerabilidades conocidas en los meses previos a la fuga. Al final, Equifax llegó a un acuerdo con el gobierno de los EE.UU. y pagó más de 575 millones de dólares para resolver reclamos de los clientes y cubrir las multas requeridas. Si bien hubo otras fugas de información antes y después de Equifax, el importante acuerdo con el gobierno

de EE.UU. alertó a las empresas del impacto financiero de una fuga y de la necesidad de implementar medidas preventivas. Estos son solo un par incidentes conocidos que moldearon la industria de la seguridad. Saber de ellos te ayudará en tu carrera de ciberseguridad. Comprender los diferentes tipos de malware y los ataques de ingeniería social te permitirá comunicar acerca de los riesgos de seguridad en futuras entrevistas de trabajo. Como futuro profesional de seguridad, adaptarte y formarte constantemente acerca de las tácticas y técnicas de agentes de amenaza será parte de tu trabajo. Al observar tendencias, patrones y metodologías similares, tal vez puedas identificar una posible fuga y limitar daños futuros. Por último, comprender cómo la seguridad afecta la vida de las personas es un buen recordatorio de por qué el trabajo que harás es tan importante.

1.4. Lectura: ataques comunes y su eficacia.

Anteriormente, aprendiste acerca de los ataques pasados y actuales que ayudaron a moldear el campo de la ciberseguridad. Estos incluyeron el ataque LoveLetter, también conocido como virus ILOVEYOU, y el gusano Morris. Uno de sus resultados fue el desarrollo de equipos de respuesta, que ahora se denominan más comúnmente equipos de respuesta ante incidentes de seguridad informática (CSIRT, por sus siglas en inglés). En esta lectura conocerás más detalles sobre los métodos de ataque más comunes. Si te familiarizas con los distintos métodos de ataque y las tácticas y técnicas cambiantes que utilizan los agentes de amenaza, podrás proteger mejor a las organizaciones y a las personas.

Phishing

Phishing es el uso de comunicaciones digitales en las que se suplanta la identidad de una persona o empresa con el objetivo de engañar a otras personas para que revelen datos confidenciales o implementen un software malicioso.

Algunos de los tipos más comunes de ataques de phishing actuales son:

- **Compromiso del correo electrónico empresarial (BEC):** el agente de amenaza envía un mensaje de correo electrónico que parece provenir de una fuente conocida, para efectuar una solicitud aparentemente legítima de información o intentar que realice una acción, con el fin de obtener un beneficio financiero.

- **Phishing localizado (Spear phishing):** un tipo de phishing focalizado en el que se envía un correo electrónico malicioso a un/a usuario/a o a un grupo de usuarios/as específicos/as, que parece provenir de una fuente confiable.

- **Ataque "caza de ballenas" (Whaling):** un tipo de phishing localizado mediante el cual los agentes de amenaza buscan acceder a los datos confidenciales de ejecutivos/as de una empresa.

- **Vishing:** un tipo de estafa por suplantación de identidad en la que se busca obtener información sensible a través de una llamada telefónica.

- **Smishing:** ataque de phishing por SMS que implica el uso de mensajes de texto para engañar a los/las usuarios/as, con el fin de obtener información confidencial o hacerse pasar por una fuente conocida.

Software malicioso

El software malicioso es un software diseñado para dañar dispositivos o redes. El propósito principal de quienes realizan el ataque es obtener dinero o, en algunos casos, información que pueda utilizarse en contra de una persona, una organización o un territorio.

Algunos de los tipos más comunes de ataques de software malicioso actuales son:

- **Virus informático:** un código malicioso creado para interferir con las operaciones de la computadora y dañar datos, software y hardware. El virus se instala en programas o documentos de una computadora y luego, se propaga e infecta una o más computadoras en una red.

- Gusano: un software malicioso que puede duplicarse y propagarse por sí mismo en los sistemas.

- **Ransomware (secuestro de datos):** un ataque malicioso en el que los agentes de amenaza cifran los datos de una organización y exigen un pago (rescate) para restablecer el acceso a ellos.

- **Spyware:** un tipo de software malicioso que se usa para recabar y vender información sin consentimiento. El spyware se puede usar para acceder a dispositivos, lo cual permite a los agentes de amenaza recopilar datos personales, como correos electrónicos, mensajes de texto, grabaciones de voz e imagen y ubicaciones de índole privada.

Ingeniería social

La ingeniería social es una técnica de manipulación que aprovecha errores humanos para obtener información privada, acceso a sistemas o bienes de valor. A menudo, los errores humanos se deben al exceso de confianza en alguien. La misión de un agente de amenaza que actúa como ingeniero social es crear un entorno de confianza falso y mentir para aprovecharse del mayor número posible de gente.

Algunos de los tipos más comunes de ataques de ingeniería social actuales son:

- **Ataque de suplantación de identidad en redes sociales (Phishing en redes sociales):** un tipo de ataque en el que el agente de amenaza contacta a la víctima en alguna red social, con el fin de robar información personal o tomar el control de la cuenta.

- **Ataque de "agujero de agua":** un agente de amenaza ataca un sitio web visitado con frecuencia por un grupo específico de usuarios/as.

- **Cebo USB:** un agente de amenaza deja estratégicamente una unidad USB que contiene software malicioso para que un/a empleado/a la encuentre y la instale, con el fin de causar la infección involuntaria de una red.

- **Ingeniería social física:** un agente de amenaza se hace pasar por una persona ligada a la empresa para obtener acceso no autorizado a una ubicación física.

Principios de la ingeniería social

La ingeniería social es asombrosamente eficaz porque las personas suelen ser confiadas y tienen muy arraigado el respeto a la autoridad. La cantidad de ataques de ingeniería social aumenta a medida que crece la cantidad de aplicaciones de redes sociales que permiten el acceso público a los datos de las personas. Aunque compartir datos personales (como tu ubicación o fotos) puede ser conveniente, también plantea un riesgo.

Los motivos por los cuales los ataques de ingeniería social son eficaces son:

Autoridad: los agentes de amenaza se hacen pasar por personas con autoridad porque los individuos suelen respetarlas.

Intimidación: los agentes de amenaza utilizan tácticas de hostigamiento, como asustar a las víctimas para que sigan sus órdenes.

Consenso/prueba social: como las personas a veces hacen cosas convencidas de que otras también las hacen, los agentes de amenaza utilizan esta confianza en los demás para dar una impresión de legitimidad. Por ejemplo, para obtener acceso a datos privados, un agente de amenaza puede decir a un/a empleado/a que otros miembros de la empresa ya le han otorgado el acceso en otras ocasiones.

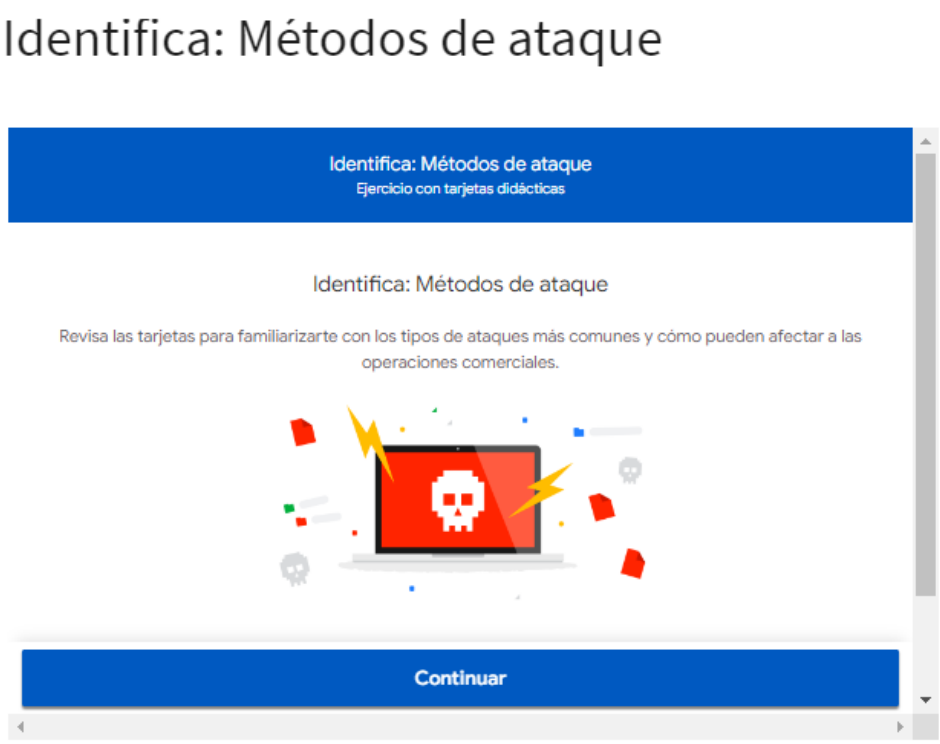
Escasez: el agente de amenaza le da a entender a la persona que existe disponibilidad limitada de ciertos bienes o servicios, para convencerla de hacer algo.

Familiaridad: los agentes de amenaza establecen falsos lazos emocionales con los/las usuarios/as de quienes desean aprovecharse,para lograr su objetivo.

Confianza: los agentes de amenaza establecen una relación afectiva con los/las usuarios/as, que les permite aprovecharse de ellos con el paso del tiempo. Hacen uso de esta relación para ganarse la confianza de la víctima y acceder a su información personal.

Urgencia: un agente de amenaza persuade a las personas para que respondan con rapidez sin hacer preguntas.

1.5. Complemento no calificado: Identifica: Métodos de ataque.



1.6. Cuestionario Practico.

Verifica tus conocimientos: La historia de la ciberseguridad

Revisar los objetivos de aprendizaje

Envía tu tarea

Comenzar tarea

1. Llena el espacio en blanco: Un virus informático es un(a) _____ malicioso(a) que interfiere con las operaciones de la computadora y causa daños. 1 punto

   - ○ código
   - ○ secuencia
   - ○ hardware
   - ○ formateo

2. ¿En qué forma ayudó el gusano Morris a moldear la industria de la seguridad? 1 punto

   - ○ Llevó al desarrollo de equipos de respuesta ante emergencias informáticas.
   - ○ Llevó a las organizaciones a tomar más conciencia sobre el gran impacto financiero que tienen los incidentes de seguridad.
   - ○ Inspiró a los autores de las amenazas a formular nuevos tipos de ataques de ingeniería social.
   - ○ Impidió el desarrollo de copias de software ilegales.

3. ¿Cuáles fueron los impactos clave de la filtración de datos de Equifax? Selecciona dos respuestas. 1 punto

- ☐ Debido a la indignación del público, el phishing se convirtió en una práctica ilegal.
- ☐ El robo de información de identificación personal de millones de clientes.
- ☐ Los/las desarrolladores/as pudieron rastrear copias de software ilegales y evitar la piratería de licencias.
- ☐ Una mayor conciencia de las graves consecuencias financieras de una vulneración de este tipo.

4. La ingeniería social, como el phishing, es una técnica de manipulación que aprovecha errores informáticos para obtener información privada, acceso a sistemas o bienes de valor. 1 punto

- ○ Verdadero
- ○ Falso

2. Los ocho dominios de seguridad del CISSP.

2.1. Video: Introducción a los ocho dominios de seguridad del CISSP parte 1.

Así como evolucionan las tácticas de amenaza, también lo hacen los roles de las/los profesionales de ciberseguridad. Comprender bien los conceptos de seguridad básicos te ayudarán a crecer en esta área. Una forma de entender mejor estos conceptos básicos es organizarlos en categorías, llamadas dominios de seguridad. A partir de 2022, el CISSP definió ocho dominios para organizar el trabajo de las/los profesionales de ciberseguridad. Es importante entender que están relacionados, y que las fallas en un dominio pueden tener consecuencias negativas en toda una organización. También es importante entenderlos porque eso puede ayudarte a comprender mejor tus objetivos profesionales y tu rol dentro de una organización. A medida que aprendas más sobre los elementos de cada dominio, puede atraerte más el trabajo que involucra uno de ellos, que los demás. Este dominio puede convertirse en un camino para explorar aún más. El CISSP define ocho dominios en total, y analizaremos todos ellos entre este video y el siguiente. En este video, cubriremos los cuatro primeros: gestión de riesgos y seguridad, seguridad de los activos, arquitectura e ingeniería de seguridad, y seguridad de la comunicación y la red.

Empecemos por el primer dominio**: gestión de riesgos y seguridad.** Este se centra en definir metas y objetivos de seguridad, mitigación de riesgos, cumplimiento, continuidad del negocio y la ley. Por ejemplo, las/los analistas de seguridad pueden tener que actualizar las políticas de una empresa relacionadas con la información de salud privada si se hace un cambio a una regulación de cumplimiento federal como la Ley de Transferencia y Responsabilidad de Seguros Médicos, o HIPAA.

El segundo dominio es la **seguridad de los activos**. Este se centra en la seguridad de activos digitales y físicos. También se relaciona con el almacenamiento, mantenimiento, retención y destrucción de datos. Al trabajar con este dominio, las/los analistas de seguridad podrían tener la tarea de asegurarse de que los equipos viejos se eliminen y destruyan adecuadamente, incluido todo tipo de información confidencial. El tercer dominio es la **ingeniería y arquitectura de seguridad.** Este se centra en optimizar la seguridad de los datos al asegurarse de que las herramientas, sistemas y procesos efectivos estén en su lugar. Como analista de seguridad, quizá se te pida configurar un firewall. Un cortafuegos es un dispositivo que monitorea y filtra el tráfico que entra y sale de la red informática. Configurar un cortafuegos correctamente ayuda a prevenir ataques que podrían afectar la productividad. El cuarto dominio de seguridad es **comunicación y seguridad de la red.** Este se centra en la gestión y seguridad de las redes físicas y las comunicaciones inalámbricas. Como analista de seguridad, tal vez se te pida que analices el comportamiento de los/las usuarios/as dentro de tu organización. Imagina que descubres que los/las usuarios/as se conectan a puntos de acceso inalámbricos no seguros. Esto podría exponer a la organización y sus empleados/as a ataques. Para garantizar que las comunicaciones sean seguras, crearías una política de red para prevenir y mitigar la exposición. Mantener la seguridad de una organización es un esfuerzo de equipo, y tiene muchas partes móviles. Como analista de nivel inicial, seguirás desarrollando tus habilidades aprendiendo a mitigar los riesgos y así mantener seguras a personas y datos. No tienes que ser un/a experto/a en todos los dominios, pero tener un entendimiento básico de ellos te ayudará en tu trayectoria como profesional de la ciberseguridad.

2.2. Video: Introducción a los ocho dominios de seguridad del CISSP parte 2.

En el último video, te presentamos los cuatro primeros dominios de seguridad. En este video, te presentaremos los siguientes cuatro dominios de seguridad: gestión de accesos e identidad, evaluación de seguridad y pruebas, operaciones de seguridad y seguridad de desarrollo de software. Familiarizarte con estos dominios te permitirá navegar por el complejo mundo de la ciberseguridad. Los dominios describen y organizan cómo las/los profesionales de ciberseguridad trabajan en equipo. Dependiendo de la organización, los roles de analista pueden ubicarse en la intersección de múltiples dominios o enfocarse en un dominio en específico. Saber dónde encaja un rol en particular dentro del panorama de seguridad te ayudará en entrevistas laborales y a la hora de trabajar en un equipo de seguridad. Pasemos al quinto dominio: gestión de acceso e identidad. La gestión de acceso e identidad se enfoca en mantener seguros los datos al garantizar que se sigan políticas establecidas para controlar y administrar activos físicos, como espacios de oficina, y activos lógicos, como redes y aplicaciones. Validar las identidades de empleados/as y documentar roles de acceso es fundamental para resguardar la seguridad digital y física de la organización. Por ejemplo, como analista de seguridad, quizá se te asigne la configuración de la tarjeta de acceso a edificios de los/las

empleados/as. El sexto dominio es la evaluación de seguridad y pruebas. Este dominio se centra en realizar pruebas de control de seguridad, recolectar y analizar datos y realizar auditorías de seguridad para monitorear riesgos, amenazas y vulnerabilidades. Las/los analistas de seguridad pueden realizar auditorías periódicas de permisos de usuario para asegurarse de que tengan el nivel de acceso correcto. Por ejemplo, el acceso a la información de la nómina suele limitarse a ciertos/as empleados/as, así que se les puede pedir a las/los analistas que auditen permisos regularmente para asegurarse de que ninguna persona no autorizada pueda ver los salarios de los/las empleados/as. El séptimo dominio es el de operaciones de seguridad. Este se dedica a realización de investigaciones y la implementación de medidas preventivas. Imagina que tú, como analista de seguridad, recibes una alerta de que un dispositivo desconocido se conectó a tu red interna. Deberás seguir las políticas y procedimientos de la organización para detener rápidamente la potencial amenaza. El octavo y último dominio es seguridad de desarrollo de software. Este se centra en el uso de prácticas seguras de codificación, que son una serie recomendaciones que se utilizan para crear aplicaciones y servicios seguros. Un/a analista de seguridad puede trabajar con equipos desarrolladores de software para garantizar que las prácticas de seguridad se incorporen en el ciclo de vida del desarrollo de software. Si, por ejemplo, uno de tus equipos asociados está creando una nueva aplicación móvil, se te puede pedir que brindes asesoramiento acerca de las políticas de contraseñas o que te asegures de que los datos de usuario se protegen y gestionan adecuadamente. Esto pone fin a nuestra introducción a los ocho dominios de seguridad del CISSP. Ponte el reto de comprender mejor cada uno de estos dominios y cómo afectan la seguridad general de una organización. Aunque quizá todavía tengas dudas en esta parte inicial del programa, analizaremos estos dominios en mayor detalle en el próximo curso.

2.3. Lectura: Como determinar el tipo de ataque.

Anteriormente, conociste cuáles son los ocho dominios de seguridad del profesional certificado en seguridad de sistemas de información (CISSP), que te permiten entender cómo organizar en categorías las responsabilidades de un analista de seguridad. Además, pueden ayudarte a comprender cómo gestionar el riesgo. En esta lectura, conocerás otros métodos de ataque. También podrás reconocer los tipos de riesgo que estos ataques presentan.

Tipos de ataques.

Ataque de contraseña: Un ataque de contraseña tiene el propósito de acceder a dispositivos, sistemas, redes o datos protegidos por contraseña. Algunos tipos de ataques de contraseña que conocerás más adelante en el programa de certificación son:

- Fuerza bruta

- Tabla arcoíris o Rainbow

Los ataques de contraseña pertenecen al dominio de seguridad de las comunicaciones y las redes.

Ataque de ingeniería social: La ingeniería social es una técnica de manipulación que aprovecha errores humanos para obtener información privada, acceso a sistemas o bienes de valor. Algunos de los tipos de ataque de ingeniería social que seguirás conociendo en el transcurso del programa son:

- Phishing (Suplantación de identidad)
- Smishing
- Vishing
- Phishing localizado (Spear phishing)
- Ataque de caza de ballena (Whaling)
- Ataque en redes sociales (Phishing en redes sociales)
- Compromiso del correo electrónico empresarial (BEC)
- Ataque de “agujero de agua”
- Cebo USB (Baiting)
- Ingeniería social física

Los ataques de ingeniería social están relacionados con el dominio de seguridad y gestión de riesgos.

Ataque físico: Un ataque físico es un incidente de seguridad que afecta no solo a los entornos digitales, sino también a los físicos en los que se produce el incidente. Algunos tipos de ataques físicos son:

- Cable USB malicioso
- Unidad flash maliciosa
- Clonación y skimming de tarjetas

Los ataques físicos pertenecen al dominio de seguridad de los activos.

Inteligencia artificial antagónica: La inteligencia artificial antagónica es una técnica que manipula la tecnología de inteligencia artificial y el aprendizaje automático para perpetrar ataques de manera más eficiente. Pertenece a los dominios de seguridad de comunicaciones y redes y al de gestión de identidad y acceso.

Ataque a la cadena de suministro: Un ataque a la cadena de suministro se dirige a los sistemas, las aplicaciones, el hardware y el software con el fin de identificar una vulnerabilidad en la que instalar software malicioso. Como cada artículo que se vende pasa por un proceso que involucra a terceros, esto significa que la vulneración de seguridad puede producirse en cualquier punto de la cadena de suministro. Estos ataques resultan costosos porque pueden afectar a varias organizaciones y a las personas que trabajan para ellas. Los ataques a la cadena de suministro pertenecen a los dominios de seguridad y gestión de riesgos, arquitectura e ingeniería de seguridad y operaciones de seguridad.

Ataque criptográfico: Un ataque criptográfico afecta a las formas seguras de comunicación protegidas por un sistema criptográfico. Algunos tipos de ataques criptográficos son:

- Cumpleaños
- Colisión
- Degradación

Los ataques criptográficos pertenecen al dominio de seguridad de las comunicaciones y las redes.

Conclusiones clave.

Los ocho dominios de seguridad del CISSP pueden ayudar a una organización y a su equipo de seguridad a reforzar sus defensas y prepararse para una filtración de datos. Las filtraciones de datos pueden ser simples o complejas y pertenecer a uno o más dominios. Considera que los métodos de ataque que hemos analizado son solo unos pocos de los muchos que existen. Durante el programa de certificación, aprenderemos sobre estos y otros tipos de ataques.

Conoce a los atacantes

Anteriormente, te presentamos el concepto de agente de amenaza. A modo de recordatorio, un agente de amenaza es cualquier persona o grupo que presenta un riesgo de seguridad. En este artículo, aprenderás acerca de los diferentes tipos de agentes de amenaza. Además, conocerás sus motivaciones, sus intenciones y su influencia en la industria de la ciberseguridad.

2.4 Lectura: Conoce a los atacantes.

Tipos de agentes de amenaza.

Amenazas avanzadas persistentes: Una amenaza persistente avanzada (APT) es un conjunto de procesos informáticos sigilosos orquestados por un tercero con la intención y la capacidad de atacar de forma avanzada y continuada en el tiempo, un objetivo determinado. Las APT suelen investigar a sus objetivos (p. ej., grandes corporaciones u organismos de gobierno) con antelación y pueden permanecer indetectables por un período prolongado. Sus intenciones y motivaciones pueden incluir:

- Dañar infraestructura crítica, como la red eléctrica y recursos naturales
- Acceder a propiedad intelectual, como secretos comerciales o patentes

Amenazas internas: Las amenazas internas abusan de su acceso autorizado para obtener datos que pueden perjudicar a una organización. Sus intenciones y motivaciones pueden incluir:

- Sabotaje
- Corrupción
- Espionaje
- Acceso no autorizado a datos o filtraciones de datos

Hacktivistas: Las/los hacktivistas son agentes de amenaza que actúan por motivaciones políticas. Abusan de la tecnología digital para alcanzar sus metas, las cuales pueden incluir:

- Manifestaciones
- Propaganda
- Campañas de cambio social
- Fama

Tipos de hackers.

Un/a hacker es cualquier persona o grupo que utiliza computadoras para acceder a datos sin autorización. Puede tratarse de una persona sin experiencia o profesional, experta en tecnología, que usa sus habilidades para diversos fines. Estas son las tres categorías principales de hackers**:**

- Los/las hackers autorizados/as también se denominan hackers éticos. Respetan un código de ética y cumplen la ley para realizar evaluaciones de riesgos de una organización. Su motivación es proteger a las personas y a las organizaciones de los agentes de amenaza maliciosos.

- Los/las hackers semiautorizados/as se consideran investigadores/as. Buscan vulnerabilidades, pero no aprovechan las que identifican.

- Los/las hackers no autorizados/as también se denominan hackers no éticos. Son agentes de amenaza maliciosos/as que no cumplen ni respetan la ley. Su objetivo es recopilar y vender información confidencial para obtener un beneficio financiero.

Nota: existen varios tipos de hackers que pertenecen a una o más de estas tres categorías.

Los agentes de amenazas sin experiencia y poco hábiles tienen diversos objetivos, como por ejemplo:

- Aprender y desarrollar sus habilidades de hackeo

- Llevar a cabo una venganza

- Aprovechar las vulnerabilidades de seguridad utilizando software malicioso, secuencias de comandos de programación y otras tácticas existentes

Otros tipos de hackers no tienen otra motivación que no sea realizar el trabajo para el que fueron contratados.

También existen hackers que se consideran a sí mismos/as como vigilantes, y su propósito principal es proteger al mundo de las/los hackers no éticos.

Conclusiones clave

Los/las agentes de amenaza y los/las hackers son hábiles en el campo técnico. Comprender sus motivaciones e intenciones te ayudará a prepararte mejor para proteger a tu organización y a las personas a las que esta sirve contra los ataques maliciosos ejecutados por algunos de estos grupos o personas.

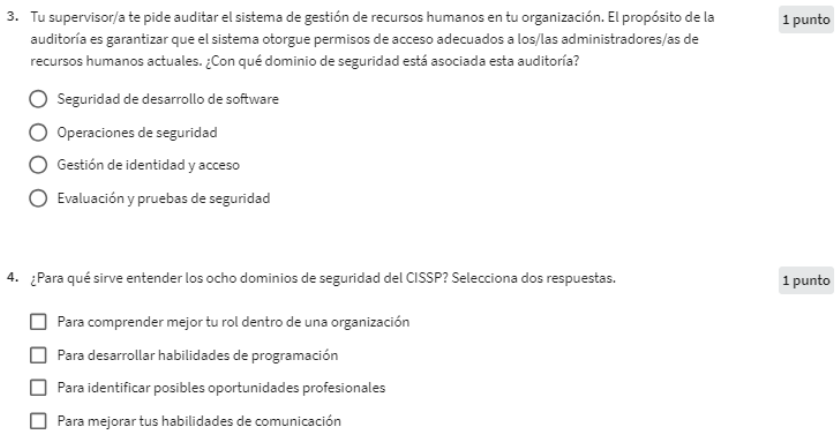
2.5. Cuestionario practico: Verifica tus conocimientos: Los ocho dominios de seguridad del CISSP.

1. Llena el espacio en blanco. Algunos ejemplos de _____ de seguridad incluyen seguridad y gestión de riesgos, así como arquitectura e ingeniería de seguridad. — 1 punto

   - ◯ redes
   - ◯ activos
   - ◯ datos
   - ◯ dominios

2. Un/a profesional de la seguridad es responsable de garantizar que los servidores de la empresa estén configurados para almacenar, mantener y retener información delicada de identificación personal (SPII) de manera segura. ¿A qué dominio de seguridad atañen estas responsabilidades? — 1 punto

   - ◯ Seguridad de los activos
   - ◯ Arquitectura e ingeniería de seguridad
   - ◯ Seguridad de las comunicaciones y las redes
   - ◯ Seguridad y gestión de riesgos



3. Tu supervisor/a te pide auditar el sistema de gestión de recursos humanos en tu organización. El propósito de la auditoría es garantizar que el sistema otorgue permisos de acceso adecuados a los/las administradores/as de recursos humanos actuales. ¿Con qué dominio de seguridad está asociada esta auditoría? 1 punto

- ○ Seguridad de desarrollo de software
- ○ Operaciones de seguridad
- ○ Gestión de identidad y acceso
- ○ Evaluación y pruebas de seguridad

4. ¿Para qué sirve entender los ocho dominios de seguridad del CISSP? Selecciona dos respuestas. 1 punto

- ☐ Para comprender mejor tu rol dentro de una organización
- ☐ Para desarrollar habilidades de programación
- ☐ Para identificar posibles oportunidades profesionales
- ☐ Para mejorar tus habilidades de comunicación

3. Repaso: La evolución de la ciberseguridad.

Con esto concluimos nuestra breve presentación de algunos de los ataques de seguridad más influyentes de la historia y los ocho dominios de seguridad del CISSP. Repasemos lo que analizamos. Primero, hablamos de virus, como el Brain y el gusano Morris, y vimos cómo estos primeros tipos de software malicioso delinearon la industria de la seguridad. También vimos cuántos ataques hoy en día son variantes de estos ejemplos tempranos. Comprender los ataques anteriores es fundamental para las/los profesionales que trabajan para proteger a organizaciones y personas de variantes futuras posibles. También hablamos de ingeniería social y de los móviles de los agentes de amenaza con el ataque LoveLetter y la fuga de datos de Equifax. Estos incidentes mostraron los impactos masivos y los costos asociados de fugas de información más recientes en la era digital. Por último, presentamos los ocho dominios de seguridad del CISSP y señalamos cómo pueden usarse para categorizar diferentes áreas de enfoque dentro de la profesión de la ciberseguridad. Espero que confíes en tus conocimientos básicos acerca de ciberseguridad. Aprender la historia de la ciberseguridad permite comprender mejor la industria actual. Los ocho dominios de seguridad del CISSP ofrecen una manera de organizar el trabajo de los profesionales de la seguridad. Recuerda: cada profesional de la seguridad es fundamental. Tu punto de vista único, tu experiencia profesional y tu conocimiento son valiosos, por lo que la diversidad que traigas al área mejorará aun más la industria de la seguridad y ayudará a mantener seguras a las organizaciones y las personas.