Security+

Guía de estudio para la Certificación

(Examen SY0-601)

Por Seolito Rodríguez, MBA
CISSP, CRISC, CISM, CISA, Security+, MCSE, MCT, VCP, ITIL, CCNA, Network, & A+

¿Qué es el Security+?

CompTIA Security+ es la primera certificación de seguridad que los profesionales de TI deben obtener. Establece el conocimiento básico requerido de cualquier rol de ciberseguridad y proporciona una plataforma esencial para trabajos de ciberseguridad de nivel intermedio. CompTIA Security+ es una certificación de confianza global y neutral para el proveedor que valida las habilidades básicas necesarias para realizar funciones básicas de seguridad y seguir una carrera de seguridad de TI.

¿Qué aprenderá en este curso?

El examen Security+ certificará que tiene los conocimientos y habilidades necesarios para evaluar la postura de seguridad de un entorno empresarial, recomendar e implementar soluciones de seguridad adecuadas, supervisar y proteger entornos híbridos, operar con conocimiento de las leyes y políticas aplicables e identificar, analizar y responder a eventos e incidentes de seguridad.

Esquema del curso

9. Virtualización, seguridad en la nube y protección de dispositivos móviles

10. Protección de datos y aplicaciones

11. Evaluaciones de seguridad

12. Respuesta a incidentes, análisis forense y recuperación

13. Gestión de riesgos

14. Gobernanza y cumplimiento

Tabla de contenido

Tabla de Contenidos

1. Introducción

1.1 Descripción general de la seguridad

1.1.1 El panorama de la seguridad

Este curso está diseñado para ayudarle a comprender el panorama de la seguridad de la información y le preparará para convertirse en un profesional de la seguridad.

Pero antes de que podamos sumergirnos en las aguas turbias siempre cambiantes que es la seguridad de la información, primero tenemos que hablar sobre el panorama de la seguridad que todos los profesionales de la seguridad deben enfrentar.

Una carrera armamentista interminable

En el mundo de hoy, los ciberdelincuentes son una amenaza muy real y peligrosa. Una forma de pensar en la seguridad de la información es la de una carrera armamentista interminable, en la que la sofisticación de las armas que se utilizan avanza exponencialmente. Cada día los ciberdelincuentes están encontrando formas nuevas e innovadoras de explotar e infiltrarse incluso en los sistemas más seguros y el mundo de la seguridad apenas es capaz de mantenerse al día.

Atrás han quedado los días simples de proteger un sistema del hacker individual al azar. En cambio, ahora estamos combatiendo una fuerza muy organizada, avanzada y poderosa que viene en muchas formas diferentes, desde los aspirantes a hackers hasta los hackers de naciones, el crimen organizado, los hacktivistas y todo lo demás.

Nuestro trabajo como profesional de la seguridad es defendernos de estas organizaciones y de las diversas técnicas que utilizan. Muchas veces esto significa que tenemos que pensar como lo hacen ellos y mirar nuestros sistemas y red desde el punto de vista de un atacante. También significa que tenemos que intentar ir un paso por delante de ellos en todo momento. Sin embargo, esto se está volviendo cada vez más difícil a medida que aumenta el número de dispositivos conectados a Internet y la velocidad a la que las personas esperan que surjan nuevas tecnologías.

La minimización es el objetivo

Mientras más rápido se desarrolla y se crean nuevas tecnologías, menos tiempo tenemos para probar a fondo las vulnerabilidades, agujeros, exploits, etcétera. Además, cada nuevo dispositivo que se conecta a una red presenta un nuevo punto de entrada para un atacante que no existía antes. Aún más inquietantes son las hazañas que ni siquiera se han descubierto todavía que los atacantes podrían utilizar.

Debido a todas estas variables, el objetivo para los profesionales de la seguridad nunca puede ser el de eliminar ataques o brechas completamente, eso es imposible. Nuestro objetivo principal es minimizar esos riesgos.

No estoy diciendo que esto signifique que debamos rendirnos. Tenemos que proteger nuestros sistemas y tomar todas las precauciones necesarias para reducir la superficie de la amenaza. Sin embargo, sepa que si su sistema está conectado a Internet, entonces es esencialmente imposible proteger su red de todos y cada uno de los ataques.

Entendienda esto, el objetivo de un profesional de la seguridad debe ser minimizar la ocurrencia de ataques y reducir el daño causado por una violación. En otras palabras, es necesario asegurar y proteger adecuadamente los sistemas, mientras que al mismo tiempo la comprensión de que una violación va a ocurrir. Y cuando lo hace, debe ser capaz de identificar el momento en que se produjo la violación y detenerla lo más rápido posible.

Ser proactivo

Para ello es necesario adoptar un enfoque proactivo de la seguridad. Pero ¿cómo se hace eso?

Algunos aspectos obvios de este enfoque incluyen mantener los sistemas actualizados, implementar políticas y procedimientos adecuados, reforzar los sistemas y las redes, etc. Pero otro aspecto, muchas veces descuidado, de este enfoque incluye estar informado.

Debido a que el panorama de la seguridad está en constante cambio, debe ser muy diligente en mantenerse al día sobre las vulnerabilidades y exploits más recientes utilizados por los ciber criminales, así como las últimas técnicas y tecnologías de seguridad utilizadas por los profesionales de la seguridad. Internet es un suministro interminable de información, así que asegúrese de usarlo. Blogs, medios de comunicación, foros, podcasts, la lista continúa, todos estos son excelentes recursos que le ayudarán a mantenerse al día sobre las últimas tendencias de seguridad.

Resumen

Recuerde, como profesional de la seguridad, es su trabajo tratar de mantenerse un paso por delante de un atacante. Puede hacerlo adoptando un enfoque proactivo de la seguridad. Manténgase informado, lea el panorama, conozca sus sistemas y la red, y comprenda que solo puede proteger una red hasta cierto punto. Más allá de eso, es su trabajo saber cómo se ve un ataque y detenerlo antes de que pueda ocurrir cualquier daño sustancial.

1.1.2 Conceptos de seguridad

Para ser un profesional de la seguridad eficaz, debe estar familiarizado con los conceptos y los roles que rodean la seguridad de la información. Esto le ayudará a entender los términos y la jerga de la industria, y también proporcionará una gran cantidad de contexto a medida que avanza a través de este curso.

Activo

El primer concepto de seguridad de la información con el que debe estar familiarizado es el de un activo.

Un activo es simplemente algo que tiene valor para un individuo o una organización. Puede ser un dispositivo físico, como un portátil o un iPad, o puede ser información electrónica, como un documento pdf en un servidor. Sin embargo, la mayoría de las veces que hablamos de un activo nos referimos a este último.

Por ejemplo, supongamos que tenemos un servidor en nuestra organización, y en este servidor hay una base de datos que contiene información del cliente, incluidos los números de tarjetas de crédito y el

historial de pedidos. Esta base de datos tiene mucho valor para la organización y, por lo tanto, se considera un activo.

Amenazas

El siguiente concepto de seguridad que debe tener en cuenta son las amenazas. Las amenazas representan cualquier cosa que tenga el potencial de causar la pérdida de un activo.

Una amenaza puede venir en muchas formas diferentes. Puede ser un virus, un troyano, un hacker externo, un empleado interno. Debido a que las amenazas vienen en todas las formas y tamaños, a veces nos referimos a ellas como amenazas combinadas.

Para continuar con nuestro ejemplo, algunas amenazas a nuestra base de datos de clientes incluyen ransomware, exfiltración de datos, "que es una forma elegante de decir robo de datos", troyanos y piratas informáticos.

Agentes de amenazas

Un agente de amenaza es la persona o entidad real que lleva a cabo una amenaza.

Cuando se trata de agentes de amenazas, hay algunas características, o atributos, que pueden categorizarlos. Por ejemplo, los agentes de amenazas pueden ser internos o externos; pueden tener poco o ningún recurso o financiación, o pueden estar fuertemente financiados con una gran cantidad de recursos; también pueden ser oportunistas, es decir, simplemente están atacando un sistema porque tiene una vulnerabilidad, o pueden tener una intención o motivo específico.

Ahora, dentro de estas categorías de agentes de amenaza, hay diferentes tipos de actores: el tipo de entidad que lleva a cabo el ataque. Por ejemplo, un actor podría ser un sindicato del crimen organizado que intenta robar información de tarjetas de crédito. Un actor también podría ser un Estado o Nación que intenta robar información clasificada. Incluso los competidores de negocios pueden ser un tipo de actor que tratan de robar secretos de la empresa con el fin de obtener una ventaja económica.

Un ejemplo de un actor de estado nación con el que podría estar familiarizado es Corea del Norte. El 24 de noviembre de 2014, los hackers norcoreanos obtuvieron acceso a las redes de Sony Pictures y robaron información confidencial, incluidos registros de empleados, correos electrónicos personales y copias de películas inéditas. La información fue luego divulgada al público en internet.

Vulnerabilidad

Para que los agentes de amenazas lleven a cabo una amenaza, necesitan una apertura, "una debilidad en el sistema". Esto se conoce como una vulnerabilidad.

Por ejemplo, una vulnerabilidad podría ser un empleado interno descontento que resulta ser un profesional de la seguridad de la información y tiene un nivel elevado de acceso a un sistema de servidor. Otra vulnerabilidad es un puerto USB habilitado.

Explotar

Y el último concepto del que hablaremos es un exploit. Un exploit es un procedimiento, una pieza de software o una secuencia de comandos que se aprovecha de una vulnerabilidad para llevar a cabo un ataque.

Por ejemplo, supongamos que tenemos un puerto USB habilitado en nuestra base de datos de clientes,"primera vulnerabilidad—" y también tenemos un empleado descontento—"segunda vulnerabilidad.

Digamos que el empleado decide usar una unidad USB para robar la base de datos del cliente. Esto es un exploit. El empleado utilizó la vulnerabilidad del puerto USB habilitado y sus permisos elevados para robar la base de datos del cliente.

Resumen

Debido a que la seguridad es un acto de equilibrio constante entre la comodidad y la protección, buscará constantemente formas de mitigar el riesgo y las amenazas al tiempo que mantiene un nivel aceptable de facilidad de uso.

Sin embargo, al comprender los conceptos básicos de la seguridad de la información, tendrá mucho más fácil evaluar los riesgos para sus sistemas e identificar las formas en que puede protegerlos.

1.1.3 Introducción a la seguridad

La seguridad es el grado de protección contra el peligro, el daño, la pérdida y la actividad delictiva.

En esta lección se tratan los siguientes temas:

- Desafíos de seguridad
- Términos de seguridad
- Componentes de seguridad
- gestión de riesgos
- Agentes de amenazas

Desafíos de seguridad

Con respecto a la seguridad de la información, los equipos y las redes de TI, los desafíos de seguridad actuales incluyen los siguientes:

Desafíos	Descripción
Ataques sofisticados	Los ataques sofisticados son complejos, lo que los hace difíciles de detectar y frustrar. Ataques sofisticados: • Utiliza herramientas y protocolos comunes de Internet, lo que dificulta distinguir un ataque del tráfico legítimo. • Varía su comportamiento, haciendo que el mismo ataque aparezca de manera diferente cada vez.

Proliferación de software de ataque	Una amplia variedad de herramientas de ataque está disponibles en Internet, lo que permite a cualquier persona con un nivel moderado de conocimientos técnicos para descargar las herramientas y ejecutar un ataque.
Escala y velocidad de ataque	La escala y la velocidad de un ataque pueden crecer a millones de computadoras en cuestión de minutos o días debido a su capacidad de proliferar en Internet. Dado que los ataques modernos no se limitan a las interacciones del usuario, como el uso de un disquete, para propagar un ataque de un equipo a otro, los ataques a menudo afectan a un gran número de equipos en un período de tiempo relativamente corto.

Términos de seguridad

Entre los términos de seguridad comunes se incluyen los siguientes:

Término	Descripción
Confidencialidad	La confidencialidad garantiza que los datos no se divulguen a personas no deseadas. Esto se proporciona a través del *cifrado,* que convierte los datos en un formato que hace que sea menos probable que sean utilizables por un destinatario no deseado.
Integridad	La integridad garantiza que los datos no se modifiquen ni manipulen. Esto se proporciona a través *de hashing.*
Disponibilidad	La disponibilidad garantiza el tiempo de actividad del sistema para que los datos estén disponibles cuando sea necesario.
No repudio	El no repudio proporciona validación del origen de un mensaje. Por ejemplo, si un usuario envía un correo electrónico firmado digitalmente, no puede afirmar más adelante que no se envió el correo electrónico. El no repudio se aplica mediante *firmas digitales.*

La CIA de Seguridad se refiere a la confidencialidad, integridad y disponibilidad. Estos son a menudo identificados como los tres objetivos principales de la seguridad. A esto se le conoce como la triada de la CIA.

Componentes de seguridad

Entre los componentes de seguridad clave se incluyen los siguientes:

Componentes	Descripción
Seguridad física	La seguridad física incluye todo el hardware y software necesario para proteger los datos, como firewalls y software antivirus.

Usuarios y administradores	Los usuarios y administradores son las personas que utilizan el software y las personas que administran el software, respectivamente.
Políticas	Las directivas son las reglas que una organización implementa para proteger la información.

Gestión de riesgos

La gestión de riesgos es el proceso de identificar problemas de seguridad y decidir qué contramedidas tomar para reducir el riesgo a un nivel aceptable. El objetivo principal es reducir el riesgo para una organización a un nivel que sea considerado aceptable por la alta dirección. La gestión de riesgos generalmente tiene en cuenta los siguientes elementos:

Elementos	Descripción
Activo	Un *activo* es algo que tiene valor para la persona u organización, como la información confidencial de una base de datos.
Amenaza	Una *amenaza* es una entidad que puede causar la pérdida de un activo o cualquier peligro potencial para la confidencialidad, integridad o disponibilidad de información o sistemas, como una violación de datos que resulta en el robo de una base de datos.
Agente de amenaza	Un *agente de amenazas* (a veces conocido como atacante*)* es una entidad que puede llevar a cabo una amenaza, como un empleado descontento que copia una base de datos en una unidad usb y la vende a un competidor.
Vulnerabilidad	Una *vulnerabilidad* es una debilidad que permite llevar a cabo una amenaza, como un puerto USB que está habilitado en el servidor que aloja la base de datos o una puerta de la sala de servidores que con frecuencia se deja entreabierta. Los dispositivos USB representan la mayor amenaza para la confidencialidad de los datos en la mayoría de las organizaciones seguras. Hay tantos dispositivos que pueden admitir el almacenamiento de archivos que robar datos se ha vuelto fácil, y prevenirlo es difícil.
Exploit	Un *exploit* es un procedimiento o producto que se aprovecha de una vulnerabilidad para llevar a cabo una amenaza, como cuando un empleado descontento espera a que la puerta de la sala de servidores se deje entreabierta, copia la base de datos en una unidad usb y luego la vende.

Agentes de amenazas

Entre los tipos de agentes de amenazas se incluyen los siguientes:

Tipo	Descripción
Empleado	Los empleados pueden ser el agente de amenazas más pasado por alto pero más peligroso porque tienen mayor acceso a los activos de información que cualquier persona en el exterior tratando de entrar. Los empleados también se conocen como amenazas *internas.* Los empleados pueden: • Disgustarse con su empleador • Ser sobornado por un competidor • Ser un participante involuntario en un ataque • Eliminar accidentalmente o causar daños en los datos
Espía	Los espías pueden ser empleados en el espionaje corporativo para obtener información sobre los competidores con fines comerciales. Los espías se implementan normalmente en los siguientes escenarios: • Un espía solicita un trabajo con un competidor comercial y luego explota vulnerabilidades internas para robar información y devolverla a su cliente. • Un espía ataca a una organización desde el exterior explotando vulnerabilidades externas y luego devuelve la información a su cliente.
Hacker	En general, un *hacker* es cualquier agente de amenaza que utiliza sus conocimientos técnicos para eludir los mecanismos de seguridad para explotar una vulnerabilidad para acceder a la información. Entre las subcategorías de hackers se incluyen las siguientes: • *Script kiddies*, que descargan y ejecutan ataques disponibles en Internet, pero generalmente no son lo suficientemente inteligentes técnicamente como para crear su propio código o script de ataque. • *Los ciberdelincuentes*, que por lo general buscan explotar las vulnerabilidades de seguridad para algún tipo de recompensa financiera o venganza. • *Ciber terroristas*, que generalmente utilizan Internet para llevar a cabo actividades terroristas, como la interrupción de instituciones dependientes de la red.

2. Amenazas, ataques y vulnerabilidades

3. Físico

4. Redes y diseño y diagnóstico de hosts

5. Dispositivos e infraestructura

6. Identidad, acceso y administración de cuentas

7. Criptografía y PKI

8. Amenazas inalámbricas

9. Virtualización, seguridad en la nube y protección de dispositivos móviles

10. Protección de datos y aplicaciones

11. Evaluaciones de seguridad

12. Respuesta a incidentes, análisis forense y recuperación

13. Gestión de riesgos

14. Gobernanza y cumplimiento

Laboratorios y prácticas

Examen Final

Referencias

https://www.comptia.org/certifications/security