Curso taller
Certificación CompTIA Security+

INTRODUCCIÓN

La Certificación CompTIA Security+: es una credencial neutral para proveedores. El examen Security+ es una validación reconocida internacionalmente de habilidades y conocimientos básicos sobre seguridad y es usada por organizaciones y profesionales de seguridad alrededor del mundo. Las habilidades y conocimientos medidos por este examen provienen de un Análisis de Tareas de Trabajo (JTA) en toda la industria y fueron validados mediante una encuesta mundial de toda la industria en el cuarto trimestre de 2007. Los resultados de esta encuesta fueron usados para validar el contenido de los dominios y objetivos y las ponderaciones en general de los dominios, garantizando la importancia relativa del contenido.

La Certificación CompTIA Security+ está dirigida a un profesional de TI que tenga:

- Un mínimo de 2 años de experiencia en administración de red con enfoque en seguridad
- Experiencia diaria en seguridad de información técnica
- Amplios conocimientos de asuntos e implementación de seguridad incluyendo los temas

que se encuentran en la lista de dominio a continuación

Contenidos

1.0 Sistemas de Seguridad
1.1 Diferenciar entre las diversas amenazas a la seguridad de los sistemas.
1.2 Explicar los riesgos a la seguridad relativos al hardware y los periféricos del sistema.
1.3 Implementar prácticas y procedimientos de fortalecimiento del sistema operativo para lograr seguridad en las estaciones de trabajo y el servidor.
1.4 Realizar los procedimientos apropiados para establecer seguridad de aplicaciones.
1.5 Implementar aplicaciones de seguridad.
1.6 Explicar el propósito y la aplicación de la tecnología de virtualización.

2.0 Infraestructura de Red
2.1 Diferenciar entre los diferentes puertos y protocolos, sus respectivas amenazas y técnicas de mitigación.
2.2 Distinguir entre elementos y componentes de diseño de red.
2.3 Determinar el uso apropiado de herramientas de seguridad de red para facilitar la seguridad de la red.
2.4 Aplicar las herramientas de red apropiadas para facilitar la seguridad de la red.
2.5 Explicar las vulnerabilidades y mitigaciones asociadas con dispositivos de red.
2.6 Explicar las vulnerabilidades y mitigaciones asociadas con diversos medios de transmisión.

2.7 Explicar las vulnerabilidades e implementar mitigaciones asociadas con conexión inalámbrica en red.

3.0 Control de Acceso

3.1 Identificar y aplicar las mejores prácticas de la industria para métodos de control de acceso.
3.2 Explicar modelos comunes de control de acceso y las diferencias entre cada uno de ellos.
3.3 Organizar usuarios y computadoras en grupos y roles de seguridad apropiados al distinguir entre derechos y privilegios apropiados.
3.4 Aplicar controles de seguridad apropiados para recursos de archivo e impresión.
3.5 Comparar e implementar métodos lógicos de control de acceso.
3.6 Resumir los diversos modelos de autenticación e identificar los componentes de cada uno.
3.7 Desplegar diversos modelos de autenticación e identificar los componentes de cada uno.
3.8 Explicar la diferencia entre identificación y autenticación (comprobación de identidad).
3.9 Explicar y aplicar métodos de seguridad de acceso físico.

4.0 Evaluaciones y Auditorias

4.1 Realizar análisis de riesgos e implementar mitigación de riesgos.
4.2 Realizar evaluaciones de vulnerabilidad usando herramientas comunes.
4.3 Dentro de la esfera de las evaluaciones de vulnerabilidad, explicar el uso apropiado de pruebas de penetración versus escaneo de vulnerabilidad.
4.4 Usar herramientas de monitoreo en sistemas y redes y detectar anomalías relacionadas con seguridad.
4.5 Comparar y contrastar diversos tipos de metodologías de monitoreo.
4.6 Ejecutar procedimientos apropiados de ingreso al sistema y evaluar los resultados.
4.7 Realizar auditorias periódicas de los parámetros de seguridad del sistema.

5.0 Criptografía

5.1 Explicar conceptos generales de criptografía.
5.2 Explicar conceptos básicos de hashing y mapear diversos algoritmos a aplicaciones apropiadas.
5.3 Explicar conceptos básicos de cifrado y mapear diversos algoritmos a aplicaciones apropiadas.
5.4 Explicar e implementar protocolos.
5.5 Explicar conceptos centrales de criptografía de clave pública.
5.6 Implementar administración de PKI y certificados.

6.0 Seguridad de la Organización

6.1 Explicar planificación de redundancia y sus componentes.
6.2 Implementar procedimientos de recuperación de desastres.
6.3 Diferenciar entre y ejecutar procedimientos apropiados de respuesta a incidentes.
6.4 Identificar y explicar la legislación aplicable y las políticas de la organización.
6.5 Explicar la importancia de los controles ambientales.
6.6 Explicar el concepto de y cómo reducir los riesgos de la ingeniería social.

Tiempo: 40 hora

Instructor Certificado.