Máster CCNA Seguridad de CISCO

CARACTERÍSTICAS

DURACIÓN
130 horas

MODALIDADES
Presencial

OBJETIVOS
Los alumnos que realicen esta formación Cisco se introducirán en las tecnologías claves de seguridad y aprenderán cómo desarrollar políticas de seguridad. Este curso proporcionará a los estudiantes los conocimientos y habilidades necesarias para especializarse en el mundo de la seguridad de redes Cisco. Es un curso práctico, orientado a soluciones con casos prácticos reales.

Es un curso en el que el alumno aprenderá a instalar, resolver conflictos y monitorizar dispositivos de red, manteniendo la integridad, la confidencialidad y la disponibilidad de datos y dispositivos. En definitiva, permitirá al alumno desarrollar políticas de seguridad y mitigar los riesgos, adquirir las habilidades necesarias para desarrollar una infraestructura de seguridad, reconocer las vulnerabilidades de las redes y mitigar las amenazas potenciales de la seguridad.

Como centro examinador autorizado Pearson Vue, damos a nuestros alumnos la posibilidad de realizar las evaluaciones de acreditación oficiales de CISCO en nuestras instalaciones.

A QUIÉN VA DIRIGIDO
El curso de CISCO CCNA Security, está diseñado para especializar a los estudiantes de Cisco Networking Academy en el mundo de la seguridad de redes.

REQUISITOS
El plan de estudios asume que los estudiantes tengan conocimientos previos de informática a nivel de usuario medio -avanzado. Se espera de ellos una buena capacidad de lectura y expresión escrita, un buen nivel en matemáticas, así como un deseo de aprender el programa de estudios .

Imprescindibles:
- Disponer de horas adicionales (entre 5 y 10) a la semana para realizar ejercicios
- Tener hecho el CISCO CCENT

Recomendables
- Ser capaz de leer textos en inglés y comprender la idea principal del mismo

PROGRAMA
1. Amenazas de seguridad en las redes modernas

1.1. Principios fundamentales de las redes seguras

1.2. Gusanos, virus y troyanos
1.3. Metodologías de ataque

2. Securizando dispositivos de red

2.1. Securizando el acceso y los ficheros de los dispositivos
2.2. CLI basada en roles
2.3. Dispositivos de monitorización
2.4. Utilización de características automatizadas

3. Autenticación, autorización y contabilidad

3.1. Propósito de AAA
3.2. Configuración local de AAA
3.3. Configuración de AAA basada en servidor

4. Implementación de tecnologías de cortafuegos

4.1. Listas de control de acceso
4.2. Tecnologías de cortafuegos
4.3. Control de acceso basado en contexto
4.4. Políticas de cortafuegos

5. Implementación de la prevención de la intrusión

5.1. Tecnologías IPS
5.2. Implementación de IPS

6. Securizando la red de área local

6.1. Consideraciones finales de seguridad
6.2. Consideraciones de seguridad de capa 2
6.3. Wireless, VoIP y consideraciones de seguridad SAN
6.4. Configuración de la seguridad del switch
6.5. SPAN y RSPAN

7. Criptografía

7.1. Servicios criptográficos
7.2. Resúmenes, firmas digitales y autentificación
7.3. Encriptación simétrica y asimétrica

8. Implementación de las redes privadas virtuales

8.1. VPNs
8.2. Componentes y operaciones de las VPNs IPSEC
8.3. Implementación de VPNs site-to-site.
8.4. Implementación de VPNs de acceso remoto
8.5. Implementación de SSLVPNs

9. Gestionar una red segura

9.1. Ciclo de vida de una red segura
9.2. Red de autodefensa
9.3. Construcción de una política integral de seguridad