CNS - Cisco Network Security

Duración: 70 hrs

Descripción general

El curso oficial Cisco Network Security proporciona los conocimientos necesarios para especializarse en ámbito del diseño y la implementación de la seguridad en infraestructuras de redes Cisco, con una orientación práctica y enfocado a implementar soluciones en escenarios reales.

El curso abarca tecnologías de protección de dispositivos y de las comunicaciones, de gestión y tráfico de usuario, de controles de acceso basados en AAA, de cortafuegos por políticas de zona. También se tratan los algoritmos de cifrado, resumen y firmas digitales como elementos básicos para la conformación de una infraestructura de clave pública (PKI), así como la implementación de comunicaciones seguras mediante estándares como IPSec.

Los participantes aprenderán las habilidades necesarias para diseñar, instalar, resolver problemas y monitorizar dispositivos de redes para mantener la integridad, confidencialidad y disponibilidad de los datos y dispositivos.

Este curso se enmarca en el programa Cisco Networking Academy, proyecto diseñado por la multinacional Cisco Systems, con el objetivo de acercar a la comunidad IT una formación y certificación oficial en el ámbito tecnológico, especializándose en redes e Internet.

Objetivos

- Describir la necesidad de la automatización de infraestructuras en la prestación ágil de servicios y operaciones
- Describir los distintos tipos de amenazas y ataques.
- Explicar las herramientas y procedimientos para mitigar los efectos del malware y los ataques comunes a la red.
- Configurar autorización de órdenes con niveles de privilegios y CLI basada en roles.
- Implementar la gestión y monitorización segura de los dispositivos de red.
- Configurar AAA para asegurar una red.
- Implementar ACL para filtrar el tráfico y mitigar los ataques de red.
- Implementar un firewall basado en políticas de zona mediante la CLI.

- Explicar el uso de los sistemas de prevención de intrusiones basados en la red.
- Explicar las vulnerabilidades de los equipos terminales y los métodos de protección.
- Implementar medidas de seguridad para mitigar los ataques de Capa 2.
- Explicar cómo los tipos de cifrado, hashes y firmas digitales funcionan juntos para proporcionar: confidencialidad, integridad y autenticación.
- Explicar cómo se utiliza una infraestructura de clave pública (PKI) para garantizar la confidencialidad de los datos y proporcionar autenticación.
- Configurar VPNs IPsec de sitio a sitio, con autenticación PSK mediante CLI.
- Explicar la operación del firewall ASA como firewall avanzado con estado.
- Implementar configuraciones de firewall ASA.
- Comprobar el estado de la seguridad de la red.

Prerrequisitos del curso

Así mismo, para un mayor aprovechamiento del curso, es recomendable que se disponga de conocimientos básicos de sistemas operativos - Windows y/o Linux -, y de redes equivalentes al nivel de los dos primeros módulos del curso Cisco CCNA v7

Dirigido a:

El curso está dirigido a profesionales IT (ingenieros de Networking, administradores de redes, etc.) que quieran conocer y desarrollar en profundidad los principios en los que se asienta la seguridad en redes, así como conocer las herramientas de configuración e implementación disponibles. Los contenidos del curso preparan en las habilidades requeridas en perfiles con una orientación profesional dirigida a la protección frente a amenazas y al diseño e implementación de infraestructuras de red seguras.

Esquema del curso

Módulo 1. Protegiendo las Redes.

Módulo 2. Amenazas de red.

Módulo 3. Mitigación de amenazas.

Módulo 4. Acceso seguro a dispositivos.

Módulo 5. Asignar Roles Administrativos.

Módulo 6. Monitorización y Gestión de Dispositivos.

Módulo 7. Autenticación, Autorización y Contabilidad (AAA).

Módulo 8. Listas de Control de Acceso.

Módulo 9. Tecnologías de cortafuegos.

Módulo 10. Firewalls Basados en Políticas de Zona.

Módulo 11. Tecnologías IPS.

Módulo 12. Operación e Implementación de IPS.

Módulo 13. Seguridad de equipos terminales.

Módulo 14. Consideraciones de seguridad de Layer 2.

Módulo 15. Servicios criptográficos.

Módulo 16. Fundamentos de Integridad y Autenticidad.

Módulo 17. Criptografía de clave pública.

Módulo 18. VPNs.

Módulo 19. Implementar VPN site-to-site IPsec con CLI.

Módulo 20. Introducción al ASA.

Módulo 21. Configuración del Firewall ASA.

Módulo 22. Pruebas de Seguridad de redes.