Network Security

Descripción general del curso

Las organizaciones de hoy tienen el desafío de responder rápidamente a las amenazas emergentes a la seguridad de la red. El personal de seguridad configura y monitorea diversas medidas de mitigación de amenazas a la seguridad de la red, como el refuerzo de dispositivos, los sistemas de prevención de intrusiones y los firewalls, para proteger los activos de datos y los sistemas de red contra ataques. El propósito de este curso es proporcionar habilidades y conocimientos en el campo de la seguridad de redes.

Objetivos:

- Proporcionar una comprensión teórica profunda de la seguridad de la red.
- Proporcionar el conocimiento y las habilidades necesarias para diseñar y respaldar la seguridad de la red.
- Proporcionar un curso orientado a la experiencia que emplea enfoques de instrucción relevantes para preparar a los estudiantes para trabajos en la industria.
- Permitir que los estudiantes tengan una interacción práctica significativa con los equipos de TI para prepararlos para los exámenes y las oportunidades profesionales.

A quién va dirigido:

El curso Network Security está diseñado para estudiantes de Cisco Networking Academy que buscan habilidades de seguridad de red de nivel de entrada orientadas a una carrera. Los estudiantes incluyen personas inscritas en programas de tecnología o ingeniería en instituciones de educación superior y profesionales de TI que desean seguir una carrera en el campo de la seguridad de redes. Los alumnos de este curso están expuestos a los conocimientos básicos necesarios para responder a las amenazas a la seguridad de la red a través de diversas medidas de mitigación de amenazas.

Requisitos previos:

- Habilidades de navegación por Internet y PC
- Familiaridad con Cisco Packet Tracer
- Conocimientos básicos de redes informáticas (nivel CCNA ITN y SRWE)

Contenido general (22 capítulos):

1. Asegurando redes
2. Amenazas de red

3. Mitigando las amenazas
4. Acceso seguro a dispositivos
5. Asignando roles administrativos
6. Administración y monitoreo de dispositivos
7. Autenticación, Autorización y Registro
8. Listas de control de acceso
9. Tecnologías de firewall
10. Políticas de firewall basados en zonas
11. Tecnologías de IPS
12. Operación e implementación de IPS
13. Seguridad de dispositivos de usuario final
14. Consideraciones de seguridad de capa 2
15. Servicios de criptografía
16. Integridad y autenticación
17. Criptografía de clave pública
18. VPNs
19. Implementando VPN site-to-site
20. Introducción al ASA
21. Configurando el firewall ASA
22. Pruebas de Seguridad de red

Duración:
60 horas