ESPE - Innovativa

EMPRESA PÚBLICA

Presentación del Curso

CCNA Bridging

Tabla de contenido

CCNA Bridging

Descripción general

El presente curso se desarrollará en la modalidad presencial, el cual le permitirá conocer los nuevos temas a los participantes que han completado todos los cursos de CCNA R&S versión 6.0 y planean tomar el examen de certificación Cisco Certified Network Associate v2.0 (CCNA 200-301).

Este curso se encuentra organizado en siete capítulos, el cual ofrece una cobertura integral y completa de los temas de redes, en el que aprenderá:

- Detectar varias amenazas a la seguridad de la red.
- Implementar protocolos para administrar la red.
- Explicar cómo las tecnologías de automatización afectan las redes en evolución.

El curso es apropiado para el público en general de muchos niveles de educación y tipos de instituciones, como escuelas secundarias, institutos de enseñanza superior, universidades, escuelas técnicas y de formación profesional, y centros comunitarios, que brindará numerosas oportunidades de experiencia práctica y desarrollo de destrezas profesionales.

También usted podrá desarrollar un pensamiento crítico y habilidades para resolver problemas mediante equipamientos reales y utilizar el simulador de Cisco llamado Packet Tracer.

Con esta capacitación le permitirá ser uno de las pocas personas que conocerá los **temas nuevos de los cursos CCNA Switching, Routing, and Wireless Essentials y del curso CCNA Enterprise Networking, Security and Automation**.

Público Objetivo

El curso de CCNA BRIDGING está dirigido a todas las personas que estén interesadas en fortalecer sus conocimientos, habilidades y destrezas relacionadas con Tecnologías de la Información, Ingeniería Electrónica, Ingeniería en Sistemas o afines.

Objetivos de aprendizaje

Objetivo general:

- Fomentar la actualización de conocimientos en los estudiantes que han completado los cursos CCNA R&S versión 6.0 y desean prepararse para el nuevo examen de certificación CCNA (200-301), a través del estudio teórico práctico de Redes Informáticas.

Objetivos específicos:

Los participantes que finalicen el curso CCNA BRIDGING serán capaces de:

- Configurar las WLAN utilizando las mejores prácticas de seguridad WLC y L2.
- Explicar cómo se pueden mitigar las vulnerabilidades, amenazas y exploits para mejorar la seguridad de la red.
- Explicar cómo las VPN e IPsec aseguran la conectividad de site-to-site y de acceso remoto.
- Explicar cómo se habilita la automatización de red a través de API RESTful y herramientas de administración de configuración.

Duración

El curso tiene una duración de 70 horas.

Contenidos

CAPITULO 1: CONCEPTOS DE SEGURIDAD LAN

1.1. Seguridad de punto final
1.2. Control de acceso
1.3. Amenazas de seguridad de capa 2
1.4. Ataque a la tabla de direcciones MAC
1.5. Ataques LAN

CAPITULO 2: CONFIGURACIÓN DE SEGURIDAD DEL SWITCH

2.1. Implementar seguridad de puertos
2.2. Mitigar los ataques de VLAN
2.3. Mitigar los ataques DHCP
2.4. Mitigar los ataques ARP
2.5. Mitigar ataques STP

CAPITULO 3: CONCEPTOS DE WLAN

3.1. Introducción a la tecnología inalámbrica
3.2. Componentes WLAN
3.3. Operación WLAN
3.4. Operación CAPWAP
3.5. Gestión de canales
3.6. Amenazas WLAN
3.7. WLAN seguras

CAPITULO 4: CONFIGURACIÓN DE WLAN

4.1. Configuración de WLAN de sitio remoto
4.2. Configure una WLAN básica en el WLC
4.3. Configure un WPA2 Enterprise WLAN en el WLC
4.4. Solucionar problemas de WLAN

CAPITULO 5: CONCEPTOS DE SEGURIDAD DE RED

5.1. Estado actual de ciberseguridad
5.2. Actores de amenaza
5.3. Herramientas para actores de amenazas
5.4. Malware
5.5. Ataques de red comunes
5.6. Vulnerabilidades y amenazas de IP
5.7. Vulnerabilidades de TCP y UDP
5.8. Servicios de IP
5.9. Mejores prácticas de seguridad de red
5.10. Criptografía

CAPITULO 6: CONCEPTOS DE VPN e IPsec

6.1. Tecnología VPN
6.2. Tipos de VPN
6.3. IPsec

CAPITULO 7: AUTOMATIZACIÓN DE RED

7.1. Resumen de automatización
7.2. Formatos de datos
7.3. APIs
7.4. REST
7.5. Herramientas de administración y configuración
7.6. IBN y Cisco DNA Center

Competencias previas

Conocimientos: Es recomendable que los participantes de este curso, hayan aprobado los 4 módulos de CCNA R&S v6.0 o tener conocimientos de competencias previas en los temas antes de realizar el examen.

Habilidades o destrezas: Los participantes deben tener uno o más años de experiencia implementando y administrando soluciones de Cisco, conocimiento de direccionamiento IP básico y una buena comprensión de los fundamentos de la red.

Valores: Los participantes deben establecer criterios éticos respecto al manejo y evaluación de los comportamientos observables de las personas.

Recursos

- Habilidades de navegación de PC y de Internet
- Tiempo para el desarrollo de las actividades de aprendizaje planificadas, así como para las actividades que realice de manera autónoma
- Disponer de una computadora con conexión a internet.
- Tener una cuenta de correo electrónico.

Aspectos metodológicos

- La capacitación se desarrollará en la modalidad presencial, para lo cual, se realizará un control de asistencia de los participantes en el horario establecido.
- Los contenidos del curso están a su disposición las 24 horas del día y los 7 días de la semana dentro del tiempo establecido para la duración del curso, por lo que, todos los participantes pueden organizar su propio horario de estudio.
- El curso es teórico – práctico, por cuanto el estudiante se apoyará en la plataforma de NetAcad, para lo cual se creará un nombre de usuario y contraseña para el acceso.
- Cada día se presentan contenidos que son estructurados con actividades individuales y colaborativas, recursos complementarios y herramientas que estarán disponibles en formatos para navegar.
- El seguimiento tutorial efectuado es constante y proactivo, lo que garantiza el éxito del proceso de aprendizaje.

Criterios de aprobación

El Programa de Capacitación CISCO que administra ESPE INNOVATIVA EP es de aprobación, para lo cual se aplican las siguientes evaluaciones académicas por cada uno de los módulos:

Exámenes electrónicos por capítulo, estos exámenes pueden presentarlos en base a la planificación académica del instructor en el horario de las clases presenciales o fuera de ellas.

Prácticas de laboratorio por cada capítulo y práctica final (skills).

- Examen Final Teórico
- Examen Final Práctico
- Examen Feedback (Satisfacción del Cliente)

Todas las evaluaciones son calificadas sobre 100 puntos, por lo que para aprobar cada uno de los módulos el participante debe obtener una nota promedio de todas las evaluaciones descritas de 80/100 puntos y registrar una asistencia mínima del 80% a las sesiones presenciales.

Certificado

El participante que cumpla con los criterios de aprobación, recibirá dos certificados:

- Certificado con el aval de la Universidad de las Fuerzas Armadas – ESPE, ESPE INNOVATIVA EP.
- Certificado avalado por Academy Networking CISCO.

Perfil del Facilitador

Formación académica

Pregrado:

Título de grado de tercer nivel en carreras como Ingeniería Electrónica, Sistemas, Tecnologías de la Información o afines.

Posgrado (De preferencia):

- Redes y Telecomunicaciones
- Gerencia de Sistemas y Tecnología Empresarial
- Gestión de la Seguridad de la Información
- Seguridad Informática y Hacking Ético

Otros:

- Certificación activa de Cisco Certified Network Associate v2.0 (CCNA 200 – 301) o superior

Experiencia relacionada:

- Desempeño profesional en el área de su especialidad
- Docencia en áreas relacionadas a su especialidad
- Instructor de cursos CCNA en la Academy Networking Cisco