CCNA SECURITY 2.0

Objetivo: El programa de estudios Cisco CCNA Security ofrece el siguiente paso para los estudiantes que quieran mejorar sus conocimientos de nivel CCNA y ayuda a satisfacer la creciente demanda de profesionales de seguridad de la red. El programa de estudios proporciona una introducción a los conceptos básicos de seguridad y los conocimientos necesarios para la instalación, resolución de problemas y supervisión de los dispositivos de red para mantener la integridad, confidencialidad y disponibilidad de los datos y los dispositivos. CCNA Security ayuda a preparar a los alumnos para las oportunidades profesionales de nivel básico relacionadas con la seguridad y para la certificación Cisco CCNA Security, reconocida internacionalmente.

Se trata de una solución de aprendizaje práctica y orientada hacia el ámbito profesional que hace hincapié en la experiencia práctica para ayudar a los alumnos a desarrollar habilidades especializadas de seguridad, así como el pensamiento crítico y las habilidades de resolución de problemas complejos. CCNA Security es un programa de estudios que combina el aprendizaje online con las clases presenciales. Los alumnos que se matriculan en el curso CCNA Security deben tener un conocimiento de los conceptos de redes y unas habilidades de nivel CCNA, además de conocimientos informáticos y de navegación en Internet básicos.

TEMARIO

CAPÍTULO 1:

AMENAZAS MODERNAS DE SEGURIDAD DE RED

1.1 Introducción.
1.2 Principios fundamentales de una Red Segura
- 1.2.1 La evolución de Seguridad de la Red
- 1.2.2. Controladores para Seguridad de Redes
- 1.2.3 Organizaciones de Seguridad de Red
- 1.2.4 Dominios de la Red de Seguridad
- 1.2.5 Dominios de la Red de Seguridad
- 1.2.6 Políticas de Seguridad de Red

1.3 Virus, gusanos, tecnologías de ataque
- 1.3.1 Virus
- 1.3.2 Gusanos
- 1.3.3 Caballo de Troya
- 1.3.4 Mitigando Virus, gusanos y Troyanos

1.4 Metodologías de ataque.
- 1.4.1 Ataques de reconocimiento
- 1.4.2 Ataque de Acceso
- 1.4.3 Ataques de denegación de servicio

1.5 Cisco Network Foundation Protection Framework
1.6 Resumen

CAPÍTULO 2:

SEGURIDAD DE DISPOSITIVO DE ACCESO

2.1 Introducción.
2.2 Seguridad de Dispositivos de Red
2.3 Asignación de Roles Administrativos.
    2.3.1 Configurando Privilegios
    2.3.2 Configurando Roles de Acceso
2.4 Monitorizando y gestionando dispositivos.
    2.4.1 Asegurando IOS Cisco y Ficheros de Configuración
    2.4.2 Una gestión segura y reportando
    2.4.3 Utilizando syslog en la Seguridad de la Red
    2.4.4 Utilizando NTP
2.5 Automatizando las funciones de seguridad
    2.5.1 Haciendo una auditoría de seguridad
    2.5.2 Bloqueo de un router con Autosecure
    2.5.3 Bloqueo de un router con Cisco SDM
2.6 Resumen.

CAPÍTULO 3:

AUTENTICACIÓN, AUTORIZACIÓN Y CONTABILIDAD

3.1 Reglas de la comunicación
3.2 Propósito de AAA.
    3.2.1 Descripción de AAA
    3.2.2 Características de AAA
3.3 Autenticación Local de AAA
    3.3.1 Configuración de autenticación local AAA con CLI
    3.3.2 Configuración de autenticación local AAA con SDM
    3.3.3 Solución de problemas de autenticación local AAA
3.4 Server-based AAA.
    3.4.1 Características Server-Based AAA
    3.4.2 Protocolos de comunicación Server-Based AAA
    3.4.3 Cisco Secure ACS
    3.4.4 Configuración de Seguridad de Cisco ACS
    3.4.5 Configuración de Seguridad de Cisco ACS Usuarios y grupos
3.5 Autenticación Server Based AAA
    3.5.1 Configuración del servidor de autenticación Server-Based AAA con CLI
    3.5.2 Configuración de autenticación Server-Based AAA con SDM
    3.5.3 Solución de problemas del servidor de autenticación basado en la AAA
3.6 Server-Based AAA, Autorización y Contabilidad
    3.6.1 Configuración del servidor basado en AAA Autorización
    3.6.2 Configuración de Contabilidad Server-Based AAA
3.7 Resumen

CAPÍTULO 4:

IMPLEMENTACIÓN DE TECNOLOGÍAS FIREWALL

4.1 Introducción
4.2 Listas de control de acceso
- 4.2.1 Configuración de ACLs Estándar y Extendidas de la CLI
- 4.2.2 Utilización de ACLs estándar y extendidas
- 4.2.3 Tipología y flujo para las ACL
- 4.2.4 Configuración de ACLs estándar y extendidas son SDM
- 4.2.5 Configuración de ACLs reflexivas y TCP Established
- 4.2.6 Configuración de ACLs Dinámicas
- 4.2.7 Configuración de ACLs basadas en tiempo
- 4.2.8 Resolución de problemas de implementaciones con ACL complejas
- 4.2.9 Mitigación de ataques con ACLs

4.3 Tecnologías Firewall
4.4 Zone-Based Policy Firewall
4.5 Resumen

CAPÍTULO 5:

IMPLEMENTACIÓN DE PREVENCIÓN DE INTRUSIONES

5.1 Introducción
5.2 IPS Tecnologías
- 5.2.1 IDS y IPS Características
- 5.2.2 Implementación e IPS basados en Host
- 5.2.3 Implementado IPS basado en Red.

5.3 IPS Firmas
- 5.3.1 IPS Características de las Firmas
- 5.3.2 Alarmas de la Firma
- 5.3.3 Tuning IPS signature Alarms
- 5.3.4 Acciones de las firmas IPS
- 5.3.5 Gestión y Monitoreo del IPS

5.4 Implementación IPS
5.5 Verificación y supervisión IPS
5.6 Resumen

CAPÍTULO 6:

ASEGURANDO LA RED DE ÁREA LOCAL

6.0 Introducción
6.1 Seguridad Endpoint
- 6.1.1 Introducción a la Seguridad de los Dispositivos finales
- 6.1.2 Asegurando los Dispositivos finales con IronPort
- 6.1.3 Asegurando los Dispositivos finales con NAC

6.1.4 Asegurando la red con el Agente de Seguridad Cisco

6.2 Consideraciones de Seguridad de Capa 2

6.2.1 Introducción a la Seguridad de Capa 2

6.2.2 Ataques de Suplantación de Direcciones MAC

6.2.3 Ataques de desbordamiento a la Tabla de direcciones MAC

6.2.4 Ataques de Manipulación de STP

6.2.5 Ataques de Tormentas LAN

6.2.6 Ataques de VLANs

6.3 Configurando Seguridad de Capa 2

6.3.1 Configurando Port Security

6.3.2 Verificando Seguridad de Puerto (Port Security)

6.3.3 Configurando BPDU Guard y Root Guard

6.3.4 Configurando Control de Tormentas

6.3.5 Configurando Troncales Seguras para las VLANs

6.3.6 Configurando CISCO SPAN (Switched Port Analyzer)

6.3.7 Configurando CISCO RSPAN (Remote Switched Port Analyzer)

6.4 Wireless, VoIP, y Seguridad SAN

6.4.1 Consideraciones de Seguridad de la Tecnología Avanzada Empresarial

6.4.2 Consideraciones de Seguridad para Redes Inalámbricas

6.4.3 Consideraciones de Seguridad en Redes Inalámbricas

6.4.4 Consideraciones de Seguridad para VoIP

6.4.5 Soluciones de Seguridad para VoIP

6.4.6 Consideraciones de Seguridad para la SANs

6.4.7 Soluciones de Seguridad para las SANs

6.5 Resumen

CAPÍTULO 7:

SISTEMAS CRIPTOGRÁFICOS

7.0 Introducción

7.1 Servicios Criptográficos

7.1.1 Comunicaciones Seguras

7.1.2 Criptografía

7.1.3 Criptoanálisis

7.1.4 Criptología

7.2 Integridad y autenticidad básica

7.2.1 Critographic Hashes

7.2.2 Integridad con MD5 y SHA-1

7.2.3 Autenticación con HMAC

7.2.4 Administración de claves

7.3 Confidencialidad

7.4 Criptografía de clave pública
- 7.4.1 Simétrica versus encriptación asimétrica
- 7.4.2 Firmas Digitales
- 7.4.3 Rivest, Sahdir y Alderman
- 7.4.4 Infraestructura de llave pública
- 7.4.5 Estándares PKI
- 7.4.6 Autoridades de certificación
- 7.4.7 Los certificados digitales y Cas

CAPÍTULO 8:

IMPLEMENTACIÓN DE REDES PRIVADAS VIRTUALES

8.0 Introducción
8.1 VPNs
- 8.1.1 Descripción general de una VPN
- 8.1.2 Topologías VPNs
- 8.1.3 Soluciones VPNs

8.2 GREE VPNs
- 8.2.1 Configurando un túnel GRE sitio a sitio

8.3 Componentes y Operación de VPN IPsec
- 8.3.1 Introducción a IPsec
- 8.3.2 Protocolos de seguridad IPsec
- 8.3.3 Intercambio de claves en Internet

8.4 Implementando VPNs Sitio-a-Sitio con CLI
8.5 Implementando VPNs Sitio-a-Sitio con CCP
8.6 Implementando VPNs de Acceso-Remoto
- 8.6.1 El entorno empresarial cambiante
- 8.6.2 Introduciendo a las VPN de acceso remoto
- 8.6.3 VPNs SSL
- 8.6.4 Cisco Easy VPN
- 8.6.5 Configurando un VPN Server con SDM
- 8.6.6 Conectándose con un VPN Cliente

8.7 Resumen

CAPÍTULO 9:

IMPLEMENTACIÓN DE CISCO ADAPTIVE SECURITY APPLIANCE (ASA)

9.0 Introducción
9.1 Introducción al ASA
9.2 Configuración de firewall ASA

9.3 Configuración VPN ASA
9.4 Resumen

CAPÍTULO 10:

LA GESTIÓN DE UNA RED SEGURA

10.0 Introducción
10.1 Principios de diseño de redes seguras
- 10.1.1 Garantizando una red segura
- 10.1.2 Identificación de amenazas y análisis de riesgos
- 10.1.3 Gestión de riesgos y prevención de riesgos

10.2 Arquitectura de seguridad
- 10.2.1 Introduciendo a la auto defensa en profundidad de la red Cisco
- 10.2.2 Soluciones para SDN de Cisco
- 10.2.3 Cisco Carpeta de Seguridad Integrada

10.3 Operaciones de seguridad
- 10.3.1 Presentación de las operaciones de seguridad
- 10.3.2 Separación de funciones o cargos

10.4 Testeando la seguridad de la red
- 10.4.1 Introducción de las pruebas de seguridad en la red

10.5 Planificación y recuperación de desastres
- 10.5.1 Planificación constante
- 10.5.2 Interrupciones y backups

10.6 Ciclo de vida del desarrollo de un sistema de seguridad
- 10.6.1 Ciclo de vida de desarrollo de sistemas
- 10.6.2 Inicialización

10.7 Desarrollando Exhaustivas Políticas de seguridad
- 10.7.1 Definiciones
- 10.7.2 Estructura de una política de seguridad
- 10.7.3 Estándares, guías y procedimientos
- 10.7.4 Roles y responsabilidades
- 10.7.5 Conciencia de seguridad y entrenamiento
- 10.7.6 Leyes y éticas

10.8 Resumen