TIC 2: REDES Y SEGURIDAD

CARACTERÍSTICAS

Especialidad 1

REDES CISCO

1.1. CCNA Routing & Switching
1.2. Ethical Hacking & CCNA Security

Especialidad 2

SEGURIDAD CISCO

2.1. CCNP Secure Access: Infraestructuras de Seguridad
2.2. CCNP Security: Mobilidad y control de amenazas

Especialidad 1: **REDES CISCO**
MÓDULO 1.1. CCNA ROUTING & SWITCHING

CARACTERÍSTICAS

PEARSON VUE AUTHORIZED TEST CENTER

MODALIDAD

Tele-formación

DURACIÓN

TOTAL: 200 horas

- Formación técnica: 50 horas de contenidos y tutorías (mixta: asíncrona y en directo).
- Formación específica: 100 horas de contenidos (clases en directo).
- Proyecto + Certificación: 50 horas de formación (mixta: asíncrona y en directo).

OBJETIVO

Siguiendo el programa de Cisco Certified Network Associate (CCNA) Routing and Switching, aprender los conocimientos necesarios para instalar, configurar, operar y solucionar problemas de infraestructuras de red. Adquirir los conocimientos fundamentales para el acceso y control de trafico de internet, seguridad en comunicaciones e infraestructuras.

REQUISITOS PREVIOS

Conocimientos básicos de informática e internet.

REQUERIMIENTOS

Conexión a internet ADSL o Fibra (descarga de contenido multimedia) / Sistemas Windows o Mac.

CERTIFICACIONES

Cisco CCNA Routing and Switching

FORMACIÓN TÉCNICA

FUNDAMENTOS DE REDES

- MAC
- Redes Ethernet
- VLAN
- Puertos de acceso
- Conectividad interswitch
- Protocolos de la capa 2
- Protocolo Cisco Discovery. 802.1Q
- Native VLAN
- LLDP
- Gestión de paquetes a través de la red
- Fuentes de información
- Inter-VLAN Routing

- Routing estático, routing dinámico
- RIPv2 para IPv4

INTERCONEXIÓN DE DISPOSITIVOS DE RED CISCO 1. EXAMEN 200-105 ICND2

FORMACIÓN ESPECÍFICA

FUNDAMENTOS DE SWITCHING LAN y FUNDAMENTOS DE ROUTING

- MACRedes Ethernet
- VLAN
- Puertos de acceso
- Conectividad interswitch
- Protocolos de la capa 2
- Protocolo Cisco Discovery
- 802.1Q
- Native VLAN. LLDP
- Gestión de paquetes a través de la red
- Fuentes de información
- Inter-VLAN Routing
- Routing estático, routing dinámico
- RIPv2 para IPv4

SERVICIOS DE INFRAESTRUCTURA y MANTENIMIENTO DE LA INFRAESTRUCTURA

- Búsqueda de DNS
- Operación NTP en modo cliente / servidor
- Configuración, verificación y resolución de problemas IPv4 y NAT
- Monitorización de dispositivos con syslog
- Configuración de copias de seguridad y restauración
- Cisco Discovery Protocol
- LLDP
- Autenticación local
- Contraseñas seguras
- Actualizaciones Cisco IOS
- Gestión del sistema de archivos
- Monitor de terminal
- Log de eventos

INTERCONEXIÓN DE DISPOSITIVOS DE RED CISCO 1. EXAMEN 200-105 ICND2

TECNOLOGÍAS SWITCHING LAN y TECNOLOGÍAS ROUTING

- Configuración de VLANs
- Conectividad interswitch
- DTP, VTP
- Protocolos STP
- Configuración, verificación y resolución de problemas de las capas 2 y 3
- EtherChannel
- PAGP
- LACP
- Configuración de routing inter-VLAN
- SVI
- Protocolos de routing interior y exterior
- OSPFv2 de área única y multitarea para IPv4
- OSPFv3 de área única y multitarea para IPv6
- Configuración, verificación y resolución de problemas EIGPR para IPv4 / IPv6

TECNOLOGÍAS WAN y SERVICIOS Y MANTENIMIENTO DE LA INFRAESTRUCTURA

- Configuración de PPP y MLPPP en interfaces WAN mediante autenticación local
- Interfaces PPPoE cliente
- Conectividad de túnel GRE
- MetroEthernet
- Internet VPN
- Configuración, verificación y resolución de problemas HSRP
- Recursos cloud para la arquitectura de red empresarial
- Configuración, verificación y resolución de problemas de acceso IPv4 / IPv6 para filtro de tráfico
- Verificación de ACL mediante APIC-EM Path Trace ACL
- SPAN local
- Gestión de dispositivos mediante AAA con TACACS+ y RADIUS.

PROYECTO + CERTIFICACIÓN

Proyecto de implantación sobre los conocimientos adquiridos y simulación de exámenes “tipo” para preparar, en caso de presentarse, las certificaciones oficiales.

Especialidad 1: **REDES CISCO**

MÓDULO 1.2. CCNA SECURITY & ETHICAL HACKING

CARACTERÍSTICAS

MODALIDAD

Tele-formación

DURACIÓN

TOTAL: 200 horas

- Formación técnica: 50 horas de contenidos y tutorías (mixta: asíncrona y en directo).
- Formación específica: 100 horas de contenidos (clases en directo).
- Proyecto + Certificación: 50 horas de formación (mixta: asíncrona y en directo).

OBJETIVO

Aprender las habilidades necesarias para evitar ataques e intrusiones informáticas y también técnicas de investigación forense de ataques de seguridad.

REQUISITOS PREVIOS

Conocimientos básicos de informática e Internet. Es recomendable acceder a este curso tras haber finalizado el curso de CCNA Routing & Switching, o estar realizando dicho curso.

REQUERIMIENTOS

Conexión a internet ADSL o Fibra (descarga de contenido multimedia) / Sistemas Windows o Mac.

CERTIFICACIONES

CCNA Security
CEH EC Council

FORMACIÓN TÉCNICA

CCNA SECURITY. EXAMEN 210-260 IINS. IMPLEMENTING CISCO NETWORK SECURITY I

- Principios de seguridad
- Tecnología SIEM
- Amenazas comunes
- Criptografía
- Topologías de red
- Accesos seguros
- AAA
- Autenticación 802.1X
- BYOD
- RADIUS
- TACACS+

FORMACIÓN ESPECÍFICA

CCNA SECURITY. EXAMEN 210-260 IINS. IMPLEMENTING CISCO NETWORK SECURITY II

- VPN
- Protocolos IPsec
- Acceso remoto
- Seguridad en routers Cisco
- Ataques comunes a la capa 2
- Procedimientos de mitigación
- Seguridad VLAN
- Tecnologías Cisco Firewall
- Implementación de NAT en Cisco ASA 9.x
- Tecnologías IPS
- Mitigación de amenazas de e-mail, web y usuario final

COMPUTER HACKING FORENSIC INVESTIGATOR I

- Informática forense
- Planificación forense
- Crímenes cibernéticos
- Investigación cibernética
- Acceso a recursos
- Evidencia digital en la investigación forense
- Teoría Empresarial de Investigación (ETI)
- Proceso y metodología de investigación del crimen informático
- Preparación del ordenador para la investigación forense
- Laboratorio forense: requisitos de hardware y software

COMPUTER HACKING FORENSIC INVESTIGATOR II

- Proceso de investigación de Informática forense
- Búsqueda e incautación de equipos
- Evidencia digital
- Procedimientos de primera respuesta
- Laboratorio de informática forense
- Windows forense
- Adquisición y duplicación de datos
- Recuperación de archivos borrados y particiones eliminadas
- Herramientas de investigación forense: Access Data Forensic Toolkit (FTKR), FTK Case Manager, desencriptar carpetas y archivos EFS.

PROYECTO + CERTIFICACIÓN

CERTIFIED ETHICAL HACKER TRAINING PROGRAM (Impartido con laboratorios EC-Council)

- Emphasis on cloud computing technology
- CEHv9 hacking attacks to the emerging cloud computing technology
- Covers wide-ranging countermeasures to combat cloud computing attacks
- Methodology for cloud systems to identify threats in advance
- Emphasis on mobile platforms and tablet computers
- CEHv9 latest hacking attacks targeted to mobile platform tablet computers
- Coverage of latest development in mobile and web technologies
- New vulnerabilities are addressed
- Heartbleed CVE-2014-0160
- Detailed coverage and labs in module 18: Cryptography
- Shellshock CVE-2014-6271
- Shellshock exposes vulnerability in bash, the widely -used shell for Unix-based operating systems such as Linux and OS X
- Hacking webservers
- Poodle CVE-2014-3566
- POODLE lets attackers decrypt SSLv3 connections and hijack the cookie session that identifies you to a service, allowing them to control your account without needing your password
- Cryptography
- Hacking using mobile phones
- CEHv9 focuses on performing hacking using mobile phones
- Coverage of latest trojan, virus, backdoors. Courseware covers information security controls and information
- Security laws and standards
- Labs on hacking mobile platforms and cloud computing
- Addressing security issues to the latest operating systems
- Addressing the existing threats to operating environments dominated by diferent operating systems (backward compatibility).

Especialidad 2: **SEGURIDAD CISCO**

MÓDULO 2.1. CCNP SECURE ACCESS: Infraestructuras de Seguridad

CARACTERÍSTICAS

MODALIDAD

Tele-formación

DURACIÓN

TOTAL: 200 horas

- Formación técnica: 50 horas de contenidos y tutorías (mixta: asíncrona y en directo).
- Formación específica: 100 horas de contenidos (clases en directo).
- Proyecto + Certificación: 50 horas de formación (mixta: asíncrona y en directo).

OBJETIVO

Aprender las habilidades necesarias para desarrollar e implantar una infraestructura de seguridad, para reconocer y mitigar amenazas y vulnerabilidades en la red .

REQUISITOS PREVIOS

Haber realizado con anterioridad el curso CCENT Routing and Switching. La certificación CCENT es imprescindible para poder presentarse a la certificación CCNA Security.

REQUERIMIENTOS

Conexión a internet ADSL o Fibra (descarga de contenido multimedia) / Sistemas Windows o Mac.

CERTIFICACIONES

Cisco CCNP Security

FORMACIÓN TÉCNICA

CompTIA SECURITY +

- Principios de administración de la seguridad de la red
- Seguridad operacional
- Vulnerabilidades
- Tecnologías de control
- Volatilidad
- Respuesta a incidentes de seguridad
- Control de daños y pérdidas
- Seguridad física, bloqueo de hardware, barricadas, alarmas, detección de señales
- Controles disuasorios, preventivos, de detección, técnicos, administrativos

FORMACIÓN ESPECÍFICA

CCNP SECURITY. EXAMEN 300-208 SISAS. IMPLEMENTING CISCO SECURE ACCESS SOLUTIONS

- Administración de dispositivos
- Opciones AAA
- TACACS+
- RADIUS
- Native AD
- LDAP
- Gestión de identidades
- Autenticación y autorización
- Implementación de cuentas
- Implementación 802.1X
- MAB
- ISE
- Autorización de red
- Dacl
- SGA
- CoA
- Implementación CWA
- Perfiles
- IOS Device Sensor
- Servicios cliente
- Agentes
- Cuarentena
- Acceso BYOD
- Arquitectura TrustSec
- Resolución de problemas
- Monitorización
- Arquitecturas de defensa ante amenazas
- Arquitecturas de gestión de identidades

CCNP SECURITY. EXAMEN 300-206 SENSS. IMPLEMENTING CISCO EDGE NETWORK SECURITY SOLUTIONS (I)

- Implementación firewall ASA / IOS
- ACLs
- NAT/PAT
- Detección de amenazas
- Detección y mitigación de amenazas a la capa 2
- DHCP
- Seguridad de puertos
- MACSec
- Verificación de fuente IP
- Configuración de hardware
- Accesos SSHv2, HTTPS, SNMPv3
- Implementación de RBAC en ASA/IOS usando CLI y ASDM
- Cisco Prime Infrastructure
- Cisco Security Manager

PROYECTO + CERTIFICACIÓN

Proyecto de implantación sobre los conocimientos adquiridos y simulación de exámenes “tipo” para preparar, en caso de presentarse, las certificaciones oficiales.

Especialidad 2: **SEGURIDAD CISCO**

MÓDULO 2.2. CCNP SECURITY: Mobilidad y control de amenazas

CARACTERÍSTICAS

MODALIDAD

Tele-formación

DURACIÓN

TOTAL: 200 horas

- Formación técnica: 50 horas de contenidos y tutorías (mixta: asíncrona y en directo).
- Formación específica: 100 horas de contenidos (clases en directo).
- Proyecto + Certificación: 50 horas de formación (mixta: asíncrona y en directo).

OBJETIVO

Aprender las habilidades necesarias para desarrollar e implantar una infraestructura de seguridad, para reconocer y mitigar amenazas y vulnerabilidades en la red.

REQUISITOS PREVIOS

Haber realizado con anterioridad el curso CCNP 1 Security (Secure access) . La certificación CCNA Security es imprescindible para poder presentarse a la certificación CCNP Security.

REQUERIMIENTOS

Conexión a internet ADSL o Fibra (descarga de contenido multimedia) / Sistemas Windows o Mac.

CERTIFICACIONES

Cisco CCNP Security

FORMACIÓN TÉCNICA

CompTIA SECURITY +

- Tolerancia a fallos
- Recuperación de desastres
- Confidencialidad, integridad, disponibilidad, seguridad
- Amenazas y vulnerabilidades
- Tipos de ataques
- Herramientas y técnicas para descubrir amenazas y ataques de seguridad
- Seguridad de aplicaciones, datos y host. Cloud
- Control de acceso y gestión de identidades
- Criptografía.

CCNP SECURITY. EXAMEN 300-206 SENSS. IMPLEMENTING CISCO EDGE NETWORK SECURITY SOLUTIONS (II)

- Gestión de servicios en dispositivos Cisco
- Exportador NetFlow
- SNMPv3. Logging
- NTP con autenticación
- CDP
- DNS
- SCP
- SFTP
- DHCP
- Resolución de problemas
- Herramientas de monitorización e informes
- CLI/ASDM
- Arquitecturas de defensa
- Solución firewall
- Soluciones de seguridad de la capa 2
- Seguridad de componentes

FORMACIÓN ESPECÍFICA

CCNP SECURITY. EXAMEN 300-209. IMPLEMENTING CISCO SECURE MOBILITY SOLUTIONS

- Comunicaciones seguras
- GETVPN
- mplementar IPsec
- DMVPN
- FlexVPN
- Acceso remoto
- Implementar AnyConnect IKEv2 VPNs en ASA y routers
- AnyConnect SSLVPN en ASA y routers
- Implementar FLEX VPN en routers
- Resolución de problemas VPN con ASDM & CLI
- Arquitecturas de comunicaciones seguras
- Soluciones VPN site-to-site
- Soluciones VPN de acceso remoto
- Encriptación
- Hashing
- Next Generation Encryption.

CCNP SECURITY. EXAMEN 300-210 SITCS V1.5. IMPLEMENTING CISCO THREAT CONTROL SOLUTIONS

- Cisco Cloud Web Security
- Implementar conectores IOS y ASA
- Implementar módulo Cisco AnyConnect Web Security
- AVC
- Cisco Web Security Appliance
- Seguridad de datos
- Cisco Email Security Appliance
- Encriptación de email
- Políticas antispam
- Políticas DLP
- ESA GUI
- Amenazas de red
- Cisco Next-Generation Firewall Security Services. Cisco Advanced Malware Protection
- Cisco FirePOWER Next-Generation IPS
- Redirección de tráfico
- Métodos de captura
- SNORT. Despliegues
- Arquitecturas de seguridad
- Cisco FirePOWER NGFW, WSA, CWS
- Seguridad email
- Diseño de soluciones Cisco FirePOWER
- Resolución de problemas
- Herramientas de monitorización e informes

PROYECTO + CERTIFICACIÓN

Proyecto de implantación sobre los conocimientos adquiridos y simulación de exámenes “tipo” para preparar, en caso de presentarse, las certificaciones oficiales.