Universidad Michoacana de San Nicolás de Hidalgo
Facultad de Ingeniería Eléctrica

Nombre de la materia :	**Seguridad de Redes de Computadoras**
Clave:	**IA7605-T**
No. De horas /semana :	**6**
Duración semanas:	**16**
Total de Horas :	**96**
No. De créditos :	**12**
Prerrequisitos :	**IA7601-T Redes de Computadoras II**

Descripción

Este curso presenta la arquitectura, la estructura, las funciones, los componentes y las configuraciones básicas de Seguridad en Redes de Computadoras. Utiliza el modelo de seguridad propuesto por Cisco Systems (Empresa global con sede en San José, California, Estados Unidos, principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones).

Objetivo

El alumno demostrará las habilidades requeridas para desarrollar una infraestructura de seguridad, reconocer amenazas y vulnerabilidades en redes de computadoras, así como mitigar amenazas de seguridad, mediante instalación, resolución de problemas y monitoreo de dispositivos de tecnologías de seguridad Cisco, para mantener integridad, confidencialidad y disponibilidad de datos y equipo.

Contenido sintético

Tema	Duración/Horas
1. Amenazas de Seguridad en Redes Modernas.	8
2. Aseguramiento de Dispositivos de Enrutamiento.	10
3. Autenticación, Autorización y Auditoría (AAA).	6
1ª. Evaluación Parcial	*4*
4. Implementación de Tecnologías de Firewall.	8
5. Implementación Sistemas de Prevención de Intrusiones (IPS).	7
6. Asegurado de Redes LAN.	10
2ª Evaluación Parcial	*4*
7. Sistemas Criptográficos.	7
8. Implementación de Redes Privadas Virtuales.	6
9. Implementación de un ASA.	6
10. Configuración Avanzada de un ASA.	10
11. Administración de una Red Segura.	4
3ª Evaluación Parcial	*4*
Proyecto de Programación de Tecnologías de Cifrado	*2*

Total	96

Bibliografía Básica

- Santos, Omar & Stuppi, John; CCNA Security 210-260 Official Cert Guide; USA; Cisco Press; 2015

Bibliografía complementaria

-

Metodología de enseñanza-aprendizaje

Revisión de conceptos, análisis y solución de problemas en clase:	(X)
Lectura de material fuera de clase:	(X)
Ejercicios fuera de clase (tareas):	(X)
Investigación documental:	(X)
Elaboración de reportes técnicos o proyectos:	(X)
Prácticas de laboratorio en una materia asociada:	( )
Visitas a la industria:	( )

Metodología de evaluación:

Asistencia:	00%
Tareas:	10%
Elaboración de reportes técnicos o proyectos:	40%
Exámenes de Academia o Departamentales	50%

Contenido desarrollado

1.	Amenazas de Seguridad en Redes Modernas.		8
	1.1. Aseguramiento de Redes.	2	
	1.2. Amenazas de Red.	3	
	1.3. Mitigación de Amenazas.	3	
2.	Aseguramiento de Dispositivos de Enrutamiento.		10
	2.1. Aseguramiento de Dispositivos de Acceso.	2	
	2.2. Asignación de Roles Administrativos.	1	
	2.3. Monitoreo y Administración de Dispositivos.	3	
	2.4. Uso de Características de Seguridad Automatizadas.	2	
	2.5. Aseguramiento del Plano de Control.	2	
3.	Autenticación, Autorización y Auditoría (AAA).		6
	3.1. Propósito de AAA.	1	
	3.2. Autenticación AAA Local.	1	
	3.3. AAA Basada en Servidor.	1	
	3.4. Autenticación AAA Basada en Servidor.	2	
	3.5. Autorización y Auditoría AAA Basada en Servidor.	1	
4.	Implementación de Tecnologías de Firewall.		8
	4.1. Listas de Control de Acceso (ACLs).	2	
	4.2. Tecnologías de Firewall.	3	
	4.3. Firewall de Políticas Basadas en Zonas (ZPFs).	3	
5.	Implementación Sistemas de Prevención de Intrusiones (IPS).		7
	5.1. Tecnologías IPS.	1	
	5.2. Firmas de IPSs.	3	
	5.3. Implementación de IPSs.	3	
6.	Asegurado de Redes LAN.		10
	6.1. Seguridad de Puntos Finales.	2	
	6.2. Consideraciones de Seguridad Capa 2.	8	

7.	Sistemas Criptográficos.		7
7.1.	Servicios Criptográficos.	1	
7.2.	Integridad y Autenticidad Básica.	2	
7.3.	Confidencialidad.	2	
7.4.	Criptografía de Llave Pública.	2	
8.	Implementación de Redes Privadas Virtuales.		6
8.1.	VPNs.	2	
8.2.	Componentes y Operación de VPNs IPSec.	2	
8.3.	Implementación de VPNs IPSec Sitio-a-Sitio.	2	
9.	Implementación de un ASA.		6
9.1.	Introducción al ASA.	2	
9.2.	Configuración de un Firewall en ASA.	4	
10.	Configuración Avanzada de un ASA.		10
10.1.	Administrador de Dispositivos de Seguridad ASA.	4	
10.2.	Configuración de VPNs en ASA.	6	
11.	Administración de una Red Segura.		4
11.1.	Pruebas de Seguridad de Red.	1	
11.2.	Desarrollo de Políticas de Seguridad Comprensivas.	3	

Programa propuesto por:

- **M.C. José Francisco Rico Andrade,**

Modificado por:

- **M.C. José Francisco Rico Andrade.**

Aprobación por el H. Consejo Técnico de la FIE: 10 de abril de 2018

Comentarios para la Academia y el H. Consejo Técnico:

- Porcentaje de modificación respecto a la propuesta anterior: 100%
  - Propuesta de Nuevo Tópico Selecto.

- El presente programa, incluye los contenidos del curso “CCNA Security” de Cisco. Lo anterior en cumplimiento del plan de trabajo aprobado para la Licencia con Goce de Salario Integrado (Clausula 61 del Capítulo IV del “Contrato Colectivo de Trabajo del SPUM”), otorgado al M.C. José Francisco Rico Andrade del lunes 22 de Agosto de 2016 al lunes 21 de Agosto de 2017.

Contenido super-desarrollado

1. Amenazas de Seguridad en Redes Modernas. 8
- 1.1. Aseguramiento de Redes. 2
  - 1.1.1. Redes como Objetivos.
  - 1.1.2. Razones para asegurar..
  - 1.1.3. Vectores de Ataques de Red.
  - 1.1.4. Pérdida de Datos.
  - 1.1.5. Modelos de Seguridad para diferentes Redes (CAN, Oficinas Pequeñas, Oficina en Casa, WAN, Centros de Datos, Redes Virtuales y la Nube).
  - 1.1.6. Evolución de la Frontera de Red.
- 1.2. Amenazas de Red. 3
  - 1.2.1. El Hacker.
  - 1.2.2. Evolución de los Hackers.
  - 1.2.3. Cyber Criminales, Hacktivistas, Hackers Patrocinados por el Estado.
  - 1.2.4. Introducción a las Herramientas de Ataque.
  - 1.2.5. Evolución de las Herramientas de Seguridad.
  - 1.2.6. Categorías de las Herramientas de Ataque.
  - 1.2.7. Diferentes tipos de Malware (Virus, Caballos de Troya, Gusanos, Otros Malwares).
  - 1.2.8. Tipos de Ataques de Red (Ataques de Reconocimiento, Acceso, Ingeniería Social y DoS).
- 1.3. Mitigación de Amenazas. 3
  - 1.3.1. Profesionales de la Seguridad de Redes.
  - 1.3.2. Organizaciones de Seguridad de Redes.
  - 1.3.3. Confidencialidad, Integridad y Disponibilidad.
  - 1.3.4. Dominios de la Seguridad de Redes.
  - 1.3.5. Políticas de Seguridad.
  - 1.3.6. La seguridad como una Alcachofa.
  - 1.3.7. Productos y Dispositivos de Seguridad.
  - 1.3.8. Defensa de una Red.
  - 1.3.9. Mitigación de Malware, Gusanos, Ataques de Reconocimiento, Ataques de Acceso, Ataques DoS.
  - 1.3.10. Marco de Protección NFP .
  - 1.3.11. Seguridad en el marco NFP (Plano de Control, Plano Administrativo, Plano de Datos).

2. Aseguramiento de Dispositivos de Enrutamiento. 10
- 2.1. Aseguramiento de Dispositivos de Acceso. 2
  - 2.1.1. El Router de Frontera.
  - 2.1.2. Areas de un Router de Frontera y Esquemas de Seguridad.
  - 2.1.3. Aseguramiento de Acceso Local y Remoto (Contraseñas y Líneas de Acceso).
  - 2.1.4. Mejoras en el Proceso de Acceso Seguro e Inicio de Sesión (Bloqueos tras Cantidad de Intentos Fallidos).
  - 2.1.5. Configuración de SSH.
- 2.2. Asignación de Roles Administrativos. 1
  - 2.2.1. Limitar disponibilidad de Comandos por Nivel de Privilegios.
  - 2.2.2. Configurar Linea de Comandos por Roles.
  - 2.2.3. Configuraciónde Vistas y Supervistas Basadas en Roles.
- 2.3. Monitoreo y Administración de Dispositivos. 3
  - 2.3.1. Configuración Resiliente para IOS y Configuraciones.
  - 2.3.2. Proceso de Recuperación, ante Contraseñas Pardidas.
  - 2.3.3. Tipos de Accesos Administrativos (En Banda vs Fuera de Banda)
  - 2.3.4. Introducción a Syslog, su operación y mensajes.
  - 2.3.5. Uso y Configuración de Syslog para Seguridad de Redes
  - 2.3.6. Introducción a SNMP, y su Base de Información Administrativa.
  - 2.3.7. Versiones SNMP y Vulnerabilidades.
  - 2.3.8. Uso y Configuración de SNMP para Seguridad de Redes

2.3.9. Introducción a NTP.
2.3.10. Uso y Configuración de Servidores y Clientes NTP para Seguridad de Redes
2.4. Uso de Características de Seguridad Automatizadas. 2
2.4.1. Auditoría de Red mediante CDP y LLP.
2.4.2. Configuraciones de Seguridad Aceptables para Protocolos y Servicios.
2.4.3. Uso de AutoSecure en routers Cisco.
2.5. Aseguramiento del Plano de Control. 2
2.5.1. Suplantación de Protocolos de Enrutamiento.
2.5.2. Autenticación de Mensajes de Protocolos de Enrutamiento.
2.5.3. Operaciones de Enrutadores.
2.5.4. Vulnerabilidades y Administración del Plano de Control.
2.5.5. Operación de CoPP.

3. Autenticación, Autorización y Auditoría (AAA). 6
3.1. Propósito de AAA. 1
3.1.1. Autenticación sin AAA
3.1.2. Componentes de AAA
3.1.3. Modos de Autenticación, Autorización y Auditoría
3.2. Autenticación AAA Local. 1
3.2.1. Autenticación de Accesos Administrativos
3.2.2. Métodos de Autenticación.
3.2.3. Configuración Fina de Autenticación.
3.2.4. Debugueo y Resolución de Problemas de Autenticación AAA.
3.3. AAA Basada en Servidor. 1
3.3.1. Comparativa de AAA Local y AAA Basado en Servidor
3.3.2. Introducción a TACACS+ y RADIUS
3.3.3. Integración de AAA con TACACS+, RADIUS, Active Directory, ISE
3.4. Autenticación AAA Basada en Servidor. 2
3.4.1. Configuración de Autentcación AAA Basada en Servidor.
3.4.2. Configuración de Servidores TACAS+ y RADIUS
3.4.3. Integración de Autenticación AAA con los Servidores Configurados.
3.4.4. Monitoreo de Tráfico de Autenticación.
3.4.5. Debugueo y Resolución de Problemas de Autenticación AAA Basada en Servidor.
3.5. Autorización y Auditoría AAA Basada en Servidor. 1
3.5.1. Configuración y Puesta en Marcha de Autorización AAA Basada en Servidor mediante TACACS+ y RADIUS.
3.5.2. Configuración y Puesta en Marcha de Auditoría AAA Basada en Servidor mediante TACACS+ y RADIUS.
3.5.3. Autenticación basada en 802.1X.
3.5.4. Configuración de 802.1X.

4. Implementación de Tecnologías de Firewall. 8
4.1. Listas de Control de Acceso (ACLs). 2
4.1.1. Introducción a las Listas de Control de Acceso.
4.1.2. Tipos de Listas de Control de Acceso.
4.1.3. Configuración y Aplicación de ACLs Numeradas y Nombradas.
4.1.4. Edición de ACLs.
4.1.5. Configuración y Aplicación de ACLs Extendidas.
4.1.6. Mitigación de Ataques con ACLs (Antispoofing, Abuso de ICMPs, Exploits SNMP).
4.1.7. ACLs para IPV6 (Sintaxys y Configuración).
4.2. Tecnologías de Firewall. 3
4.2.1. Definición, Banaficios y Limitaciones de Firewalls.
4.2.2. Tipos de Firewalls (de Filtrado de Paquetes, de Estado-Completo, de Próxima Generación).
4.2.3. El Firewall Clásico y su Operación.
4.2.4. Configuración de un Firewall Clásico.
4.2.5. El Firewall en los diseños de Redes.

4.2.6. Introducción al Firewall Basado en Zonas.
4.3. Firewall de Políticas Basadas en Zonas (ZPFs). 3
4.3.1. Beneficios y Diseños de ZPFs.
4.3.2. Operación de un ZPF (Acciones, Reglas de Tránsito, Reglas de Tráfico).
4.3.3. Configuración de un ZPF (Creación de Zonas, Identificación de Tráfico, Definición de Acciones, Identificar pares de Zonas y Aplicar Políticas).
4.3.4. Verificación de Configuraciones y Consideraciones adicionales.

5. Implementación Sistemas de Prevención de Intrusiones (IPS). 7
5.1. Tecnologías IPS. 1
5.1.1. Monitoreo, Detección y Prevención de Ataques.
5.1.2. Similitudes y Diferencias entre IDSs e IPSs
5.1.3. Tipos de IPSs (HIPS vs Sensores).
5.1.4. Soluciones Cisco de Sensores IPS.
5.1.5. Modos de Implementación de un IPS.
5.1.6. Analizadores de Puerto Switcheado.
5.1.7. Configuración de Puertos Espejo en un Switch.
5.2. Firmas de IPSs. 3
5.2.1. Atributos, Características y Tipos de Firmas.
5.2.2. Archivos de Firmas.
5.2.3. Micro-Motores de Firmas.
5.2.4. Alarmas de Firmas.
5.2.5. Detección Basada en Patrones, Anomalías, Políticas, Tarros de Miel.
5.2.6. Mecanismos Disparadores de Alarmas.
5.2.7. Administración de Alertas.
5.2.8. Acciones de Firmas (Registro de Actividades para Análisis Posterior, Denegación, Reinicio, Bloqueo, y Permisión de Tráfico).
5.2.9. Monitoreo de Actividad y Consideraciones.
5.2.10. Intercambio de Eventos Seguros entre Dispositivos.
5.2.11. Correlación Global de IPSs.
5.2.12. Reputaciones, Listas Negras y Filtros de Tráfico.
5.3. Implementación de IPSs. 3
5.3.1. Implementación de un IPS IOS.
5.3.2. Descarga de Llaves y Firmas.
5.3.3. Habilitación y Carga de Paquetes de Firmas.
5.3.4. Retirado / Des-retirado de Firmas.
5.3.5. Cambios a las Acciones de Firmas.
5.3.6. Verificación y Monitoreo de IPSs.

6. Asegurado de Redes LAN. 10
6.1. Seguridad de Puntos Finales. 2
6.1.1. Aseguramiento de los Elementos de una LAN.
6.1.2. Seguridad Tradicional de Puntos Finales.
6.1.3. La red sin Fronteras.
6.1.4. Aseguramiento de Puntos Finales en la Red sin Fronteras.
6.1.5. Protección Antimalware Avanzada.
6.1.6. AMP y Defensa de Amenazas Administrada.
6.1.7. Aseguramiento de Email y Web.
6.1.8. Control de Admisiones mediante NAC.
6.2. Consideraciones de Seguridad Capa 2. 8
6.2.1. Vulnerabilidades Capa 2.
6.2.2. Ataques a Switches.
6.2.3. Mitigación de Ataques a Tabla CAM (Seguridad de Puerto, Envejecimiento, Notificaciones SNMP).
6.2.4. Ataques en VLANs (VLAN Hopping, Double-Tagging) y su Mitigación (Troncales Manuales y PVLANs).
6.2.5. Ataques a DHCP (Spoofing, Starvation) y su Mitigación (Snooping).

6.2.6. Ataques a ARP (Spoofing, Poisoning) y su Mitigación (Inspección de ARPS Dinámica).
6.2.7. Mitigación de Falseo de Direcciones mediante IP Source Guard.
6.2.8. Ataques a STP y su Mitigación (PortFast, BPDU Guard, Loop Guard).

7. Sistemas Criptográficos. 7
7.1. Servicios Criptográficos. 1
7.1.1. Autenticación, Integridad y Confidencialidad en las Comunicaciones Seguras.
7.1.2. Criptografía (Definición, Historia, Ejemplos Por Transposición y Sustitución).
7.1.3. Criptoanálisis (Definición y Métodos).
7.1.4. Criptología (Definición, Componentes).
7.2. Integridad y Autenticidad Básica. 2
7.2.1. Funciones Hash Criptográficas.
7.2.2. Integridad con MD5, SHA-1 y SHA-2.
7.2.3. Autenticidad con HMAC.
7.2.4. Administración de Llaves (Características, Espacio de Llave, Tipos de Llaves).
7.3. Confidencialidad. 2
7.3.1. Cifrado de Datos.
7.3.2. Tipos de Cifrado (Simétrico, Asimétrico, De Bloque, De Flujo).
7.3.3. Estándares de Cifrado de Datos (DES, 3DES, AES).
7.3.4. Algoritmos de Cifrado Alternativos (SEAL, RC).
7.3.5. Intercambio de llaves seguro mediante Diffie-Hellman (Operación y Algoritmo).
7.4. Criptografía de Llave Pública. 2
7.4.1. Cifrado Simétrico vs Asimétrico.
7.4.2. Tipos de Algoritmos Asimétricos.
7.4.3. Firmas Digitales (Definición, Tipos, Uso, Algoritmos).
7.4.4. Infraestructura de Llave Pública (Marco PKI, Interoperabilidad entre Diferentes Vendedores, Topologías, Autoridades de Registro).

8. Implementación de Redes Privadas Virtuales. 6
8.1. VPNs. 2
8.1.1. Introducción a las VPNs.
8.1.2. Topologías de VPNs (Sitio-a-Sitio, De Acceso Remoto, De Horquilla, De Tunel Dividido).
8.2. Componentes y Operación de VPNs IPSec. 2
8.2.1. Tecnologías IPSec.
8.2.2. Confidencialidad (DES, 3DES, AES, SEAL), Integridad (MD5, SHA) y Autenticación (PSK, RSA) en IPSec.
8.2.3. Intercambio Seguro de Llaves en IPSec (DH1, … , DHn).
8.2.4. Protocolos IPSec (AH, ESP, ESP+AH,).
8.2.5. Intercambio de Llaves en Internet (IKE)
8.2.6. IKE Fase 1 y Fase 2
8.3. Implementación de VPNs IPSec Sitio-a-Sitio. 2
8.3.1. Implementación de VPN Sitio-a-Sitio entre 2 Routers (Configuración de Políticas ISAKMP, IPSec, CryptoMapas, y Verificación)

9. Implementación de un ASA. 6
9.1. Introducción al ASA. 2
9.1.1. Diferentes Tipos de ASA.
9.1.2. Modos de Operación de un ASA (Firewall y Niveles de Seguridad).
9.1.3. Requerimientos de Licencias de un ASA.
9.1.4. Configuración Básica de un ASA.
9.2. Configuración de un Firewall en ASA. 4
9.2.1. Configuraciones Básicas y por Defecto de un Firewall ASA.
9.2.2. Asistentes de Configuración ASA.
9.2.3. Configuraciones de Administración y Servicios de un ASA (Interfaces, VLANs, Enrutamiento Estático, Acceso Remoto, NTP, DHCP).
9.2.4. Grupos de Objetos Tipos y Configuración (Objetos de Red, de Servicios, De Objetos).

9.2.5. Listas de Control de Acceso en ASA (Tipos de ACLs en ASA, Configuraciones, Aplicaciones, uso de Objetos).
9.2.6. NAT en ASA (Tipos y Configuraciones).
9.2.7. AAA en ASA (Local y Basada en Servidor).
9.2.8. Políticas de Servicios en ASA (Mapas de Clases, Políticas y Aplicación).

10. Configuración Avanzada de un ASA. 10
10.1. Administrador de Dispositivos de Seguridad ASA. 4
10.1.1. Introducción a ASDM.
10.1.2. Preparación de ASDM y ASA para Configuración.
10.1.3. Páginas de Elementos en ASDM.
10.1.4. Asistentes de Configuración en ASDM (Startup, VPN, Otros).
10.1.5. Configuración de Administración y Servicios en ASDM (Configuraciones Básicas, Interfaces, Hora, Enrutamiento, Acceso Administrativo, DHCP).
10.1.6. Configuración de Características Avanzadas en ASDM (Objetos, Grupos, ACLs, NAT, AAA).
10.2. Configuración de VPNs en ASA. 6
10.2.1. Configuración de VPNs Sitio-a-Sitio ASA – Router en ASDM (Configuración y Verificación).
10.2.2. VPNs de Acceso Remoto en ASDM (Configuración de Servidor y Cliente SSL y Verificación).
10.2.3. VPNs de Acceso Remoto en ASDM sin Cliente (Configuración de Servidor y Verificación).

11. Administración de una Red Segura. 4
11.1. Pruebas de Seguridad de Red. 1
11.1.1. Operaciones de Seguridad.
11.1.2. Tipos de Pruebas y Evaluación de Seguridad de Redes.
11.1.3. Herramientas para Evaluar la Seguridad de Redes (NMap/ZenMap, SuperScan, SIEM, Otras).
11.2. Desarrollo de Políticas de Seguridad Comprensivas. 3
11.2.1. Estructura de una Política de Seguridad.
11.2.2. Estándares, Guías y Procedimientos.
11.2.3. Roles y Responsabilidades.
11.2.4. Campañas de Conciencia de Seguridad y Capacitaciones.
11.2.5. Respuestas Ante Brechas de Seguridad (Motivo, Oportunidad, Medios).
11.2.6. Recolección de Datos.