UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA
PROGRAMA DE CURSO

1.Nombre del Curso: Fundamentos de Seguridad en Redes

2.Clave: ACP-158	**3.**	**H.T.S.**	**H.P.S.**	**T.H.S.**	**Créditos**
		2	2	4	6

4. Cursos Previos Recomendados: ACP134 Diseño de Ruteo y Administración (Redes IV)

5. Cursos inmediatos posteriores con que se vincula:

6. Total de Horas de Curso: 64

7. Descripción mínima: Identificar las amenazas y vulnerabilidades de las redes, el acceso seguro a dispositivos de enrutamiento, configuración de protocolos de seguridad, implementación de políticas mediante listas de acceso, manejo de sistemas de detección y prevención de intrusos, configuraciones de seguridad de capa 2, comprensión de tecnologías que permiten la integridad, confidencialidad y autenticidad de la información así como la creación de redes privadas virtuales y la administración de la seguridad en una red.

8. Justificación o vínculos de la asignatura con los objetivos generales de la carrera: Los aspectos de seguridad son fundamentales en cualquier red que se deba diseñar, implementar y administrar para garantizar que los recursos de la misma estén siempre disponibles y puedan ser utilizados en forma responsable y eficiente.

9. Objetivo General:

Identificar y comprender las amenazas y vulnerabilidades de las redes así como desarrollar las competencias específicas para planear e implementar un esquema de seguridad eficiente que proteja los recursos informáticos.

Objetivos Particulares:

- Describir los dominios de la seguridad informática.
- Identificar los tipos de ataques a la seguridad informática.
- Configurar listas de control de acceso IP.

- Configurar la inspección de paquetes IP en modo *stateful.*
- Configurar en el firewall políticas basadas en zona.
- Comprender el funcionamiento de sistemas para la detección y/o prevención de intrusiones.
- Describir los ataque más comunes a la red local como: *spoofing* de dirección, manipulación STP, desbordamiento de dirección MAC, etcétera así como, la forma de mitigar los efectos de estos ataques.
- Comprender los fundamentos del cifrado y del criptoanálisis.
- Describir los conceptos y tecnologías fundamentales de las VPN's.
- Describir los principios del diseño de una red segura, hacer análisis de riesgo e identificar de amenazas.

10. Contenido de la Asignatura:

Horas por Unidad: 4

Unidad 1 Amenazas a la seguridad en las redes modernas
Objetivo: Describir los dominios de la seguridad informática así como identificar los diferentes tipos de ataques a la seguridad informática
Requisitos Conocimientos generales de informática y redes
Subtemas:

1.1. Principios básicos de la seguridad en las redes
  1.1.1. Evolución de la seguridad en las redes
  1.1.2. La seguridad de red en las organizaciones
  1.1.3. Los dominios de la seguridad en redes
  1.1.4. Políticas de seguridad en redes
1.2. Virus, gusanos y caballos de troya
  1.2.1. Virus
  1.2.2. Gusanos
  1.2.3. Caballos de Troya
  1.2.4. Mitigación de los efectos de los virus, gusanos y troyanos
1.3. Metodologías de ataque
  1.3.1. Ataque de reconocimiento
  1.3.2. Ataques de acceso
  1.3.3. Ataques de denegación de servicio
  1.3.4. Mitigación de los efectos de los ataques

Horas por Unidad: 8

Unidad 2 Aseguramiento de dispositivos de red
Objetivo: Incrementar la fiabilidad en el proceso de instalación física del enrutador y del acceso administrativo desde la línea de comandos, CLI
Requisitos Configuración de enrutadores
Subtemas:

2.1. Aseguramiento de dispositivos de acceso
  2.1.1. Aseguramiento de la frontera del enrutador
  2.1.2. Configuración segura del acceso administrativo
  2.1.3. Configuración de la seguridad mejorada con cuentas de acceso virtuales, *logins*
  2.1.4. Configuración del protocolo SSH
2.2. Definición de roles administrativos
  2.2.1. Configuración de niveles de privilegios
  2.2.2. Configuración de acceso basado en roles
2.3. Administración y monitoreo de dispositivos
  2.3.1. Configuración de archivos y administración del sistema operativo

2.3.2. Administración y reportes de seguridad
2.3.3. Utilización de registros de sistema para la seguridad de la red, *logs*
2.3.4. Protocolo SNMP
2.3.5. Protocolo NTP
2.4. Utilización de características de seguridad automáticas
2.4.1. Auditoría de seguridad

Horas por Unidad: 8

Unidad 3 Autenticación, Autorización y Cuentas , AAA -*Authentication, Authorization and Accounting*
Objetivo: Comprender la función y operación del AAA
Requisitos Conocimientos generales de informática y redes
Subtemas:
3.1. Autenticación, Autorización y Cuentas, AAA
3.1.1. Propósito de AAA
3.1.2. Panorama de AAA
3.1.3. Características de AAA
3.1.4. Autenticación Local AAA
3.1.5. AAA Basada en servidor
3.1.6. Autenticación AAA basada en servidor
3.1.7. Registro de cuentas y Autorización basada en servidor

Horas por Unidad: 8

Unidad 4 Corta Fuegos -*Firewall*
Objetivo: Configurar los diversos tipos de listas de control de acceso IP (reflexivo, dinámico y basado en tiempo), configurar la inspección de paquetes IP en modo *stateful* y configurar políticas basadas en zona en el *firewall*.
Requisitos Configuración de enrutadores y conocimientos generales de redes e informática
Subtemas:
4.1. Listas de control de acceso, ACL´s
4.1.1. Configuración estándar y mejorada
4.1.2. Usos de las configuraciones estándar y mejorada
4.1.3. Topología y flujo para las listas de control de acceso
4.1.4. Configuración de ACL's
4.1.4.1. Estándar y Mejorada
4.1.4.2. Reflexiva
4.1.4.3. Dinámica
4.1.4.4. Basada en tiempo
4.1.5. Tecnología de *firewall*
4.1.5.1. Tipos de *firewall*
4.1.5.2. Los *firewall* en el diseño de redes
4.1.6. Control de acceso basado en contexto
4.1.7. Política de *firewall* basada en zona

Horas por Unidad: 8

Unidad 5 Sistemas de Prevención de Intrusos, IPS
Objetivo: Comprender el funcionamiento de sistemas para la detección y/o prevención de intrusiones.
Requisitos Configuración de enrutadores y conocimientos generales de redes e informática
Subtemas:

5.1. Tecnologías de Sistemas de Prevención de Intrusiones IPS
  5.1.1. Características de los IPS e IDS, *Intrusion Detection Systems*
  5.1.2. Implementaciones de IPS basados en *host*
  5.1.3. Implementaciones de IPS basados en red
5.2. Archivos de firmas de IPS
  5.2.1. Configurando los archivos de firmas de IPS
  5.2.2. Actualización de los archivos de firmas
  5.2.3. Administración y monitoreo del IPS
5.3. Implementación de IPS
5.4. Verificación y Monitoreo del IPS

Horas por Unidad: 8

Unidad 6 Aseguramiento de la red local
Objetivo: Describir los ataques más comunes a la red local como: *spoofing* de dirección, manipulación STP, desbordamiento de dirección MAC, etcétera así como la forma de mitigar los efectos de estos ataques.
Requisitos Configuración de conmutadores y conocimientos de capa dos del modelo OSI
Subtemas:

6.1. Consideraciones de seguridad en la capa 2
  6.1.1. Ataques de suplantación de identidad de la dirección MAC
  6.1.2. Ataque de desbordamiento de la tabla de direcciones MAC
  6.1.3. Ataque de manipulación de STP
  6.1.4. Ataque de *storm* a la red de área local
  6.1.5. Ataque a las VLAN´s
6.2. Configuración de seguridad en la capa 2
  6.2.1. Configuración de seguridad de puerto
  6.2.2. Verificación de seguridad de puerto
  6.2.3. Configuración de control *Storm*
  6.2.4. Configuración de seguridad VLAN *TRunk*
  6.2.5. Configuración de analizador de puertos

Horas por Unidad: 8

Unidad 7 Sistemas Criptográficos
Objetivo: Comprender los fundamentos del cifrado y del criptoanálisis
Requisitos Conocimientos generales de redes e informática
Subtemas:

7.1. Servicios de Criptografía
  7.1.1. Aseguramiento de las comunicaciones
  7.1.2. Criptografía
  7.1.3. Criptoanálisis
7.2. Principios de Autenticidad e Integridad
  7.2.1. Hashes criptográficos
  7.2.2. Integridad con MD5 y SHA-1
  7.2.3. Autenticidad con HMAC
  7.2.4. Administración de claves
7.3. Confidencialidad
  7.3.1. Cifrado
  7.3.2. Sistema de encriptado de datos, DES (*Data Encryption System*)
  7.3.3. 3DES
  7.3.4. Sistema de encriptación avanzado, AES (*Advanced Encryption System*)
  7.3.5. Algoritmos de encriptación alternos

7.3.6. Intercambio de claves Diffie-Hellman
7.4. Criptografía de clave pública
7.4.1. Cifrado simétrico vs cifrado asimétrico
7.4.2. Firmas Digitales
7.4.3. Rivest Shamir y Alderman RSA
7.4.4. Infraestructura de Clave Pública
7.4.5. Estándares de Infraestructura de clave pública, PKI
7.4.6. Autoridades certificadoras
7.4.7. Certificados Digitales

Horas por Unidad: 6

Unidad 8 Redes Privadas Virtuales
Objetivo: Describir los conceptos y tecnologías fundamentales de las redes privadas virtuales
Requisitos Configuración de enrutadores y conocimientos generales de redes e informática
Subtemas:

8.1. Redes Privadas Virtuales
8.1.1. Panorama General de las Redes privadas virtuales, VPN
8.1.2. Topologías de VPN's
8.1.3. Soluciones de VPN's
8.1.4. VPN con el protocolo Encapsulación de ruta genérica, GRE
8.1.5. Configuración de túnel sitio a sitio con GRE
8.2. Componentes y operación de VPN con IPSec
8.2.1. Introducción a IPSec
8.2.2. Protocolos de Seguridad IPSec
8.2.3. Intercambios de claves en Internet, IKE

Horas por Unidad: 6

Unidad 9 Administración de una red segura
Objetivo: Describir los principios del diseño de una red segura, hacer análisis de riesgo e identificación de amenazas
Requisitos Conocimientos generales de redes e informática
Subtemas:

9.1. Principios del diseño de una red segura
9.1.1. Cómo incrementar la seguridad en la red
9.1.2. Identificación de amenazas y análisis de riesgo.
9.1.3. Administración del riesgo
9.2. Operaciones de Seguridad
9.3. Pruebas de Seguridad en la red
9.4. Planificación de la continuidad
9.4.1. Planeación de la continuidad del negocio y recuperación ante desastres
9.4.2. Disrupción y respaldos de seguridad
9.5. Desarrollar una política de seguridad completa
9.5.1. Políticas de seguridad
9.5.2. Estructura de una política de seguridad
9.5.3. Procedimientos, guías y estándares
9.5.4. Responsabilidades y roles

11. Habilidades a Desarrollar:	12: Actitudes a fomentar:
• Identificar las amenazas y vulnerabilidades de las redes, • Configurar acceso seguro a dispositivos de enrutamiento • configurar protocolos de seguridad • Implementar políticas de seguridad mediante listas de acceso • Administrar sistemas de detección y prevención de intrusos • Configurar la seguridad a nivel de capa 2 • Comprender las tecnologías que permiten la integridad, confidencialidad y autenticidad de la información • Crear redes privadas virtuales • Administrar la seguridad de una red	• Superación. • Ética. • Respeto por la confidencialidad, autenticidad e integridad de la información • Entender el valor de la información y los recursos de la red así como el daño ocasionado al violar las medidas de seguridad • Fomentar el buen uso de los recursos de la red • Responsabilidad • Trabajo en equipo

13. Bibliografía

Clave	Título	Básica	Complementaria
BIB01	CCNA Security Study Guide: Exam 640-553, Tim Boyles, ISBN: 978-0-470-52767-2	☒	☐
BIB02	Alonso, Javier Andrés. Redes privadas virtuales / México : Alfaomega Ra-Ma;, 2009.	☒	☐
BIB03	Maiwald, Eric. Fundamentos de seguridad de redes / México: McGraw-Hill Interamericana, 2005.	☒	☐
BIB04	Network security: current status and future directions / Piscataway, NJ: IEEE Press [u.a.], 2007.	☐	☒
BIB05	Mason, Andrew G. Redes privadas virtuales de Cisco Secure / Madrid: Pearson Educación, 2002.	☐	☒
BIB06	Kaeo, Merike. Diseño de seguridad en redes / Madrid: Cisco Press, 2003	☐	☒
BIB07	Book Review: Network Security Assessment	☐	☒

14. Evaluación del curso

Actividad	Porcentaje
Tareas	20%
Prácticas	30%
Evaluaciones Parciales	20%
Evaluación Final	30%

15. Estatus:

Programa de Nueva Creación	☒		
Programa Modificado	☐	En este caso, especificar la fecha de la última actualización:	06/05/2011

16.Programa elaborado o modificado por:	MTI. Vladimir Veniamin Cabañas Victoria, Ing. Rubén E. González Elixavide, MSI. Laura Dávalos Castilla, MTI. Melissa Blanqueto Estrada,

17.Fecha de Elaboración /Modificación:	27/05/2011

18.Fecha de Revisión de Academia:	03/06/2011

19.Sello y Fecha de Registro en Consejo Divisional

UNIVERSIDAD DE QUINTANA ROO
24 AGO 2011
REGISTRADO
DIVISION DE CIENCIA E INGENIERIA
CONSEJO DIVISIONAL