Universidad Tecnológica de la Mixteca

Clave DGP: 200089

Maestría en Sistemas Distribuidos

PROGRAMA DE ESTUDIOS

Con formato: Color de fuente: Texto 1

NOMBRE DE LA ASIGNATURA
Seguridad en Sistemas Distribuidos

SEMESTRE	CLAVE DE LA ASIGNATURA	TOTAL DE HORAS
Tercer Semestre	**100303V**	**80**

OBJETIVO(S) GENERAL(ES)DE LA ASIGNATURA
Que el alumno obtenga conocimientos actualizados y de frontera para el análisis y estudio de temas de seguridad en sistemas distribuidos implementados sobre redes de computadoras, redes que por su actualidad e importancia requieren de adecuados fundamentos teóricos y un alto nivel de síntesis empírica.

TEMAS Y SUBTEMAS

1. Introducción a la seguridad en redes
   - 1.1. Vulnerabilidades, riesgos y ataques.
   - 1.2. Elementos de seguridad.
     - 1.2.1. Identificación y autenticación.
     - 1.2.2. Control de acceso, no repudio y responsabilidad.
   - 1.3. Organizaciones, estándares y certificaciones.

2. Mecanismos de seguridad basados en criptografía
   - 2.1. Áreas de la criptología.
   - 2.2. Máquinas criptográficas.
   - 2.3. Clasificación de los algoritmos criptográficos
     - 2.3.1. Algoritmos criptográficos simétricos.
     - 2.3.2. Algoritmos criptográficos asimétricos.
   - 2.4. Certificados digitales.

3. Protocolos de seguridad
   - 3.1. Protocolos de la capa de red.
   - 3.2. Protocolos de la capa de transporte.
   - 3.3. Protocolos de la capa de aplicación.
   - 3.4. Protocolos en tiempo real.

4. Mecanismos de protección
   - 4.1. Seguridad física: Protección de hardware, acceso físico y personal.
   - 4.2. Seguridad lógica.
     - 4.2.1. Identificación y autenticación.
     - 4.2.2. Control de acceso interno.
     - 4.2.3. Control de acceso externo.
   - 4.3. Herramientas de seguridad.
     - 4.3.1. Escaneo de puertos y analizador de vulnerabilidades.
     - 4.3.2. Tablas de direccionamiento y cortafuegos (firewalls).
     - 4.3.3. Detector de intrusos (snort techniques) y vigías (sniffers y warkshare)
   - 4.4. Políticas de seguridad: Relación entre herramientas, servicios y políticas de seguridad.

5. Seguridad en redes inalámbricas
   5.1. Estándares internacionales.
   5.2. Protocolos de la IEEE.
   5.3. Sistemas de cifrado (wired equivalent privacy y wi-fi protected access).

6. Seguridad en dispositivos móviles
   6.1. Vulnerabilidades de hardware y software en dispositivos móviles.
   6.2. Ataques y contramedidas a la telefonía fija.
   6.3. Ataques y contramedidas a la telefonía celular.

7. Tendencias en seguridad
   7.1. Sistemas y herramientas para la detección de intrusos.
   7.2. Cómputo y análisis forense.
   7.3. Metodologías de la seguridad en las organizaciones y en los sistemas.
   7.4. Auditorias y evaluación de la seguridad.
   7.5. Diseño de sistemas seguros.
      7.5.1. Caso de estudio: Sistemas comerciales seguros (on-line).
      7.5.2. Caso de estudio: Vulnerabilidad en base de datos, inyección de consultas (code inyection)

ACTIVIDADES DE APRENDIZAJE

Listas de ejercicios, lecturas, y programas básicos en algún lenguaje de programación de computadoras con facilidades de interconexión. Simulación de ataques y técnicas de defensa.

CRITERIOS Y PROCEDIMIENTOS DE EVALUACIÓN Y ACREDITACIÓN

Exámenes parciales y final. Evaluación general de conocimientos por medio de realización de proyectos. Esto tendrá una equivalencia del 100% en la calificación final del curso.

BIBLIOGRAFÍA (TIPO, TITULO, AUTOR, EDITORIAL Y AÑO)

Básica:

1. Computer Communications Security: Principles, Standard Protocols and Techniques. Warwick Ford. Prentice Hall; 1 edition. 1993. ISBN-10: 0137994532. ISBN-13: 978-0137994533.
2. Técnicas criptográficas de protección de datos. Amparo Fúster. Publisher: Ra-Ma. 2003. ISBN-10: 8478975942. ISBN-13: 978-8478975945.
3. Network and Internetwork Security: Principles and Practice. William Stallings. Prentice Hall; 2 edition. 1995. ISBN-10: 0024154857. ISBN-13: 978-0024154835.
4. Cryptography and Network Security: Principles and Practice. William Stallings. Prentice Hall; 6 edition. 2013. ISBN-10: 0133354695. ISBN-13: 978-0133354690.

Consulta:

1. Applied Cryptography: Protocols, Algorithms, and Source Code in C. Bruce Schneier. Wiley; 2 edition. 1996. ISBN-10: 0471117099. ISBN-13: 978-0471117094.
2. Handbook of Applied Cryptography. Alfred J. Menezes, Paul C. van Oorschot. CRC Press; 1 edition. 1996. ISBN-10: 0849385237. ISBN-13: 978-0849385230.
3. Digital Evidence and Computer Crime. Eoghan Casey BS MA. Academic Press; 3 edition. 2011. ISBN-10: 0123742684. ISBN-13: 978-0123742681.
4. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. Richard Bejtlich. No Starch Press; 1 edition. 2013. ISBN-10: 1593275099. ISBN-13: 978-1593275099.

PERFIL PROFESIONAL DEL DOCENTE
Maestría o doctorado en áreas de ingeniería o ciencias de la computación o afín. Con experiencia en esta modalidad educativa.