Curso: *Seguridad en Ambientes de Redes y Principios de Análisis Forense*

Docente: Wílmer Efrén Pereira González

e-mail: wilmer.pereira@itam.mx
wpereira@ucab.edu.ve

I. Objetivo general del curso

Los sistemas abiertos extienden el uso de los sistemas de información a un amplio espectro de posibilidades lo que redunda en la versatilidad de dichas aplicaciones. Sin embargo, esto los expone a problemas de intrusión, suplantación de identidad, expansión de *malware*, … Es por ello que resulta de vital importancia prevenir las intrusiones antes que exponerse a las consecuencias de daños de los sistemas, robo de información o pérdidas económicas. En consecuencia, en un primer momento, este curso se centra en las estrategias de prevención para atenuar y/o disminuir los ataques a servidores y usuarios.

Sin embargo, si efectivamente, la institución o usuario sufren de ataques que causan daños y pérdidas entonces, en la segunda parte del curso, se estudiaran las técnicas para el levantamiento de la evidencia, análisis de la información recolectada y estructuración de un expediente judicial para que el(los) responsable(s) del ataque sean llevados ante los organismos judiciales competentes.

II. Conocimientos previos necesarios

Aunque se estudiarán los algoritmos y usos de la criptografía que no requieren de un conocimiento previo, el contexto de aplicación de las técnicas de seguridad se sitúa en ambientes interconectados a través de Internet o una red de área local. Por ello es deseable que los participantes tengan buen conocimiento del área de Redes de Computadoras para la primera parte del curso. Para la segunda parte del curso (análisis forense) sería recomendable un nivel de experticia aceptable de los principales sistemas operativos del mercado, a saber, Window, Linux y macOS.

III. Competencias que desarrolla el curso

a) Generales:

- Definir e implantar estrategias de seguridad que mitiguen los daños y pérdidas de una institución y sus usuarios.
- Levantar y analizar las evidencias necesarias para llegar a los responsables y tener las pruebas suficientes para que se presenten las pruebas de ley.

b) Especificas:

- Aplicar los algoritmos criptográficos adaptados a los distintos servicios de seguridad, a saber: confidencialidad, integridad, autentificación, no repudio y disponibilidad.
- Definir políticas de seguridad mediante el estudio del impacto que tienen los riesgos
- Aplicar distintos algoritmos criptográficos para adaptarlos a los servicios de seguridad
- Saber implementar una PKI con certificación digital
- Parametrizar y poner a punto herramientas de protección en ambientes de redes
  Identificar las fases del análisis forense y los instrumentos de documentación para la cadena de custodia
- Utilizar las herramientas para el levantamiento de la evidencia y análisis de la información recolectada

IV. Resultado de aprendizaje del curso

El estudiante estará en capacidad aplicar estrategias de seguridad en ambientes abiertos e interconectados y, en caso de ataques, sabrá como actuar para hacer la adquisición de evidencia y análisis en situaciones sencillas de forénsica.

V. Contenidos detallados

1. Seguridad básica
   - Servicios de seguridad
   - Código abierto y propiedad intelectual
   - Políticas de seguridad y gestión de riesgos
2. Criptografía
   - Algoritmos de clave simétrica y clave pública
   - Criptoanálisis
   - Función de hash y firma digital
   - Mecanismos de autentificación
3. Certificación digital
   - Tipos de autoridades de certificación
   - Tipos de certificados
4. Estrategias de seguridad en redes
   - SSL/TLS para aplicaciones web seguras
   - Mecanismos de pago seguro
   - Cadena de bloque

- Red privada virtual
- Cortafuegos
- Sistemas de detección de intrusos
- Servidor de dominio seguro

5. Amenazas y tipos de ataques
   - Virus y gusanos
   - *Botnet* y troyanos
   - Desbordamiento de buffer
   - DoS y DDoS
6. Principios de análisis forense
   - Cadenas de custodia
   - Leyes internacionales
   - Sistemas operativos especializados en forense
   - Auditabilidad y trazabilidad
7. Sistemas de archivos
   - Discos mecánicos y discos de estado sólido
   - Arreglos de disco
   - Fat32 y NTFS
   - Ext3 y Ext 4
   - HFS+ y APFS
8. Adquisición de evidencia
   - Escena del crimen
   - Datos volátiles y no volátiles
   - Herramientas de captura para Linux y window
9. Análisis de evidencia
   - Fases
   - Herramientas de capturas de archivos borrados
   - Exploración y dragado de información
   - Herramientas para Linux y window

VI. Estrategias Didácticas

Se mostrarán herramientas de seguridad tanto en la primera parte de protección de la información y servidores como para la segunda parte relacionada con la adquisición y análisis de evidencia en presencia de ataques. Los estudiantes deberán instalar algunas herramientas para responder a cuestionarios en los que deben poner a prueba, configurar y parametrizar distintos productos de preferencia código abierto.

Tendrán al menos tres sesiones prácticas en laboratorios respondiendo cuestionarios en grupos de máximo dos personas.

La propuesta inicial para este curso es para 40 horas, intercalando las sesiones de teoría con los laboratorios. Lo ideal es que se realice una sesión inicial para fijar las condiciones de

realización del curso y evaluar los conocimientos previos de los asistentes en redes y sistemas operativos. En ese momento se definira el tipo de nivelación y el estudiante asume el compromiso de realizar un trabajo para adquirir el conocimiento mínimo en las áreas antes mencionadas.

Las 40 horas del curso se cubrirán en al menos tres semanas dada la densidad del contenido teórico y práctico. Para una mejor distribución podría también ser en cuatro semanas para facilitar la asimilación de los conceptos y consolidar la información adquirida.

VII. Evaluación

El curso es teórico-práctico por lo que tendrán exámenes teóricos, sesiones de laboratorio y proyectos de instalación y uso de aplicaciones. Además, se realizará un trabajo inicial en redes y sistemas operativos para ajustar los diferentes niveles de dominio de estas áreas.

Uno de los proyectos será la implementación de un sitio web seguro montando una PKI y el segundo sobre exploración de la imagen de un disco para encontrar evidencia y prueba incriminatorias contra el atacante.

Los porcentajes designados para cada actividad son:

- Tarea de nivelación (10%)
- Tres cuestionarios (10% c/u)
- Proyectos (15% c/u)
- Dos exámenes parciales (15% c/u)

VIII. Bibliografía

- Stalling W. Criptografía y Seguridad de Red: Principios y Práctica, Prentice Hall, 2004
- Huerta A. Seguridad en Unix y redes, NauLibres, 2020
- Parasram S. Digital Forense with Kali Linux, Packt, 2020
- Casey E. Digital Evidence and Computer Crime: Forensic Science, Computer and the Internet, Elsevier, 2011
- Brook Ch. Computer Hacking Forensic Investigator Certification: Exam Guide, McGraw-Hill 2015

IX. Cronograma del desarrollo del curso

El curso debe realizarse en al menos tres semanas aunque se sugiere realizarlo en cuatro semanas (un mes)

La primera semana sería introducción a los servicios de seguridad, criptografía y certificación digital. Durante esa primera parte se harían al menos dos de los laboratorios y se presentaría las bases del primer proyecto.

La segunda semana se cubrirían los temas de: herramientas de seguridad en redes, amenazas y ataques. Al termino de esa semana tendría lugar el primer examen parcial (de preferencia sobre una plataforma como canvas o Moodle) y se realizará el tercer laboratorio.

En la última semana será el estudio de los temas de análisis forense y se presentará el segundo proyecto del curso sobre adquisición y análisis de evidencia.

La entrega de los proyectos será, como máximo, dos semanas después de finalizadas las clases y en ese momento se entregará la calificación definitiva a los alumnos y a servicios escolares.