UNIVERSIDAD INTERAMERICANA DE PUERTO RICO
RECINTO METROPOLITANO
FACULTAD DE CIENCIAS Y TECNOLOGÍA
DEPARTAMENTO DE CIENCIAS DE COMPUTADORAS Y MATEMÁTICAS
PROGRAMA GRADUADO DE CIENCIAS EN
SEGURIDAD DE LA INFORMACIÓN

PRONTUARIO

I. INFORMACIÓN GENERAL

Título del Curso	:	Informática Forense I
Código y Número	:	INSE 5201
Créditos	:	Tres (3)
Término Académico	:	
Profesor(a)	:	
Horas de Oficina	:	
Teléfono de la Oficina	:	787-250-1912 Ext 2230
Correo Electrónico	:	

II. DESCRIPCIÓN

Revisión y aplicación general de las herramientas y los fundamentos necesarios en el mundo de la Informática Forense. Discusión e investigación de crímenes cibernéticos. Identificación de las posibles fallas de seguridad, su origen y evidencia de vulnerabilidad en los niveles de seguridad. Requiere horas adicionales en un laboratorio abierto virtual.

III. OBJETIVOS

Se espera que al finalizar el curso, el estudiante pueda:

1. Identificar brechas en el área de seguridad
2. Analizar la naturaleza de los crímenes cibernéticos
3. Definir conceptos aplicados a los incidentes que violen la seguridad en las redes

IV. CONTENIDO TEMÁTICO

A. Módulo 1: El Lenguaje del crimen cibernético
   1. Crecimiento del crimen cibernético
   2. Abusos y usos indebidos de redes

B. Modulo 2: Los Hackers
   1. Modus operandi, motivos y tecnología
   2. Caracterización de los penetradores de crímenes cibernéticos
   3. (SKRAM)
   4. Herramientas y métodos aplicados

C. Modulo 3: Investigando un crimen cibernético
   1. Definición de lo que es un crimen cibernético
   2. Modelo de Investigación
   3. Proceso de Investigación Forense
   4. Herramientas Forenses
   5. Análisis de cada elemento en un escenario Forense

D. Modulo 4: Adquisición Y Duplicación de datos
   1. Técnicas de adquisición de datos
   2. Duplicación de discos bit a bit
   3. Creación de imágenes de disco
   4. Recuperación de datos y particiones eliminados

E. Modulo 5: Introducción a la Criptografía
   1. Conceptos generales de criptografía
   2. Algoritmos de encriptación
   3. Cracking de claves de archivos protegidos a nivel sistema operativo y aplicaciones
   4. Esteganografía

F. Modulo 6: Análisis de Logs
   1. Huellas de hackeo
   2. Registros de intento de intrusión
   3. Firewall Analyzer: Analizando los registros

G. Modulo 7: Evidencia Digital en Redes

1. Análisis del Tráfico de red
2. Análisis de Logs
3. Network Intrusion Detection
4. Registros y datos a través del modelo OSI
5. Análisis de Incidentes en Seguridad en Redes

V. ACTIVIDADES

1. Lecturas
2. Discusiones electrónicas (Foros)
3. Búsqueda bibliográfica
4. Ejercicios prácticos
5. Correo electrónico

VI. MEDIOS DE EVALUACIÓN

		Puntuación	% Nota Final
1.	Foros y Asignaciones	100	25
2.	Prueba Cortas	100	25
3.	Laboratorios	100	25
4.	Examen Final	100	25
	Total	400	100

VII. NOTAS ESPECIALES

1. Recuerde que cualquier tarea del curso debe cumplir con el Reglamento General de Estudiantes de Estudiante, Capítulo V, Artículo 1, Sección B.2 que establece "El plagio, la falta de honradez, el fraude, la manipulación o falsificación de datos y cualquier otro comportamiento inapropiado relacionado con la labor académica son contrarios a los principios y normas institucionales y están sujetos a sanciones disciplinarias."

2. Todo estudiante que requiera servicios auxiliares o asistencia especial deberá solicitar los mismos al inicio del curso o tan pronto como adquiera conocimiento de que los necesita, mediante el registro correspondiente en la oficina del Consejero Profesional José Rodríguez, Coordinador de Servicios a los estudiantes con Impedimentos, ubicada en el Programa de Orientación Universitaria.

3. Uso de dispositivos electrónicos
   Se desactivaran los teléfonos celulares y cualquier otro dispositivo electrónico que pudiese interrumpir los procesos de enseñanza y

aprendizaje o alterar el ambiente conducente a la excelencia académica. Las situaciones apremiantes serán atendidas, según corresponda. Se prohíbe el manejo de dispositivos electrónicos que permitan acceder, almacenar o enviar datos durante evaluaciones o exámenes.

4. Cumplimiento con las disposiciones del Título IX

La Ley de Educación Superior Federal, según enmendada, prohíbe el discrimen por razón de sexo en cualquier actividad académica, educativa, extracurricular, atlética o en cualquier otro programa o empleo, auspiciado o controlado por una institución de educación superior independientemente de que esta se realice dentro o fuera de los predios de la institución, si la institución recibe fondos federales.

Conforme dispone la reglamentación federal vigente, en nuestra unidad académica se ha designado un(a) Coordinador(a) Auxiliar de Titulo IX que brindará asistencia y orientación con relación a cualquier alegado incidente constitutivo de discrimen por sexo o género, acoso sexual o agresión sexual. Se puede comunicar con el Coordinador(a) Auxiliar, George Rivera, Director de Seguridad, al teléfono 787-250-1912, extensión 2147, o al correo electrónico grivera@metro.inter.edu .

El Documento Normativo titulado Normas y Procedimientos para Atender Alegadas Violaciones a las Disposiciones del Título IX es el documento que contiene las reglas institucionales para canalizar cualquier querella que se presente basada en este tipo de alegación. Este documento está disponible en el portal de la Universidad Interamericana de Puerto Rico (www.inter.edu).

VIII. RECURSOS EDUCATIVOS

Libro de texto

Certified Cybercrime Forensic Investigator

Recursos electrónicos:

Materiales Necesarios

- Computadora
- Servicio de Internet

IX. BIBLIOGRAFÍA

A. Libros y artículos de revistas

Pfleeger, C.P. y Pfleeger, S. L.. (2003). **Security in Computing Third Edition.** Upper Saddle River, NJ: Prentice Hall.

Code, E., Krutz, R. L., Conley, J. W. Reisman, B. Ruebush, M., y Gollman, D.. (2008). **Network Security Fundamentals**. NJ: Wiley.

Stallings, W. (2005). **Cryptography and Network Security: Principles and Practice 4rd Edition**. Upper Saddle River, NJ: Prentice Hall.

Stallings, W. (2006). **Network Security Essentials: Applications and Standards (3rd Edition)**. Upper Saddle River, NJ: Prentice Hall.

Bishop, M. (2002) **Computer Security: Art and Science**. Addison-Wesley Professional.

Brenton, C y Hunt, C. (2002). **Mastering Network Security**. Sybex

Gollmann, D. (2006) **Computer Security**. Wiley

Goldreich, O. (2004) **Foundations of Cryptography: Volume 2, Basic Applications**. Cambridge University Press

B. Referencias electrónicas:

http://www.linuxsecurity.com/ - página de Linux Security que contiene información de seguridad bajo el sistema operativo Linux.

http://www.microsoft.com/security/default.mspx - página de Microsoft que contiene información sobre seguridad (Ingles)

http://webdia.cem.itesm.mx/ac/rogomez/seguridad/index.html - página del Grupo de Interés de Seguridad Computacional del ITESM-CEM

http://www.microsoft.com/spain/technet/seguridad/recursos/glosario/default.mspx - página de Microsoft que contiene un Glosario de seguridad.

http://www.criptored.upm.es/paginas/software.htm : esta página provee acceso a programas de prácticas en criptografía y el Programa chinchon para análisis de riesgo.

http://www.mundotutoriales.com/tutoriales_seguridad_informatica-mdpal14063.htm - página de Mundo de Tutoriales que provee acceso a tutoriales de informática y seguridad.

http://www.sans.org/ - página que provee información sobre cursos y certificaciones en seguridad para diferentes sistemas operativos.

http://www.securityfocus.com - página que provee información sobre seguridad para diferentes sistemas operativos.

http://www.microsoft.com/spanish/msdn/latam/estudiantes/ - página de Microsoft para Estudiantes que proveen las últimas noticias sobre Microsoft Student Live y otros.