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 II
Código y Número	:	INSE 5202
Créditos	:	Tres (3)
Término Académico	:	
Profesor(a)	:	
Horas de Oficina	:	
Teléfono de la Oficina	:	787-250-1912 Ext 2230
Correo Electrónico	:	

II. DESCRIPCIÓN

Examen de evidencias de ataques a la Web. Análisis de correos electrónicos, de dispositivos móviles y de las estrategias para el manejo y presentación de evidencia. Evaluación de los aspectos legales y las tendencias futuras de la Informática Forense. Requiere horas adicionales en un laboratorio abierto virtual. Requisito: INSE 5201

III. OBJETIVOS

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

1. Describir la naturaleza de los ataques de los "hackers"
2. Realizar un análisis forense.
3. Mencionar y describir algunos aspectos legales en el área forense.

Revisado por Dr. José R. Vallés diciembre/2016

IV. CONTENIDO TEMÁTICO

A. Evidencia de ataques Web

4. Los tipos de ataques Web
5. Cross Site Scripting (XSS)
6. Cross site Request Forgery (CSRF)
7. Análisis de un ataque CSRF
8. Rastreo de IP
9. Analizando vulnerabilidades de un servicio web

B. Análisis de Correos Electrónicos

1. Funcionamiento de un cliente y servidor de correo
2. Rastreo de un email
3. Recuperación de emails borrados o Almacenes corruptos

C. Análisis Forense de

1. Móviles y PDA
2. Introducción
3. Pasos de PDA Forense
4. Métodos de Investigación
5. Herramientas utilizadas

D. Presentación de la Evidencias

1. Normas para la presentación de Evidencias
2. Armado de Líneas de Sucesos

E. Consideraciones Legales

1. Leyes internacionales sobre los cibercrimenes
2. El discurso probatorio en informática
3. Aplicaciones en distintos Países

F. Direcciones Futuras

1. "Digital Evidence Response Team"(Equipo de Respuesta a Evidencias Digitales)
2. Preparación Forense de Redes
3. Análisis Forense en sistemas inalámbricos
4. Anonimato y seguimiento

Revisado por Dr. José R. Vallés diciembre/2016

5. Retos y problemáticas legales

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

Carvey, H.(2012). Windows Forensic Analysis Toolkitby, Elsevier Science.

Taroni, F., et.al (2010).Data Analysis in Forensic Science, John Wiley and Sons.

Morrissey, S.(2010). iOS Forensic Analysis for iPhone, iPad, and iPod Touch, Springer.

McCarthy, N.K.(2012). The Computer Incident Response Planning Handbook, McGraw-Hill Companies,Inc.

Mandia, K.and Prosise, C. (2013). Incident Response and Computer

Forensics 3/E (EBOOK), McGraw Hill.

Liu, D.(2009). Cisco Router and Switch Forensics, Elsevier Science.

Maras, M.H.(2011). Computer Forensics: Cybercriminals, Laws, and Evidence, Jones and Bartlett Learn.

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.