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

PRONTUARIO

I. INFORMACIÓN GENERAL

Título del Curso	:	Fundamentos de Seguridad en Redes I
Código y Número	:	INSE 5101
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 las prácticas para la detección y prevención de intrusiones desde el exterior-interior de un sistema informático. Descripción de las técnicas y herramientas de última generación que utilizan los “hackers” para disminuir la vulnerabilidad de los sistemas de información. Requiere horas adicionales en un laboratorio abierto virtual.

III. OBJETIVOS

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

1. Definir la terminología relacionada al *hacking* de sistemas informáticos
2. Diferenciar las técnicas no autorizadas de obtención de información
3. Identificar la vulnerabilidad de los sistemas informáticos

IV. CONTENIDO DEL CURSO

A. Seguridad en sistemas informáticos
   1. Terminología

a. Ethical Hacking
    i. Qué es *ethical hacking*?
    ii. Tipos de *Hacker*s
    iii. Diferencias entre EH, VA y *Pentest*
2. Impacto en las empresas

B. Footprinting
1. Definición de *Footprinting*
2. Metodologías para obtener información
3. Footprinting Countermeasures

C. Scanning
1. Definición de *Scanning*
2. Tipos de *Scanning*
3. Técnicas de *Scanning*
4. Scanning Countermeasures

D. Enumeration
1. Definición de *Enumeration*
2. Técnicas de *Enumeration*
3. Enumeration Countermeasures

E. Buffer Overflow
1. Qué es un *Buffer Overflow*
2. Tipos de *Buffer Overflow*
3. ShellCode
4. Buffer Overflow Countermeasures

F. Hackeando Sistemas
1. Explotando vulnerabilidades
2. Escalando privilegios
3. Password Cracking
4. Countermeasures

G. Vulnerabilidades en Aplicaciones y Servidores Web
1. Vulnerabilidades en aplicaciones Web
2. Vulnerabilidades en IIS y Apache
3. Countermeasures

H. Anonimato, evasión y borrado de huellas
1. Navegando anónimamente
2. Evadiendo IDS, IPS y *Honeypot*
3. Borrando rastros
4. Countermeasures

Revisado por Dr. José R. Vallés diciembre/2016

V. ACTIVIDADES

1. Lecturas
2. Estudio de módulos …..
3. Discusiones electrónicas (Foros)
4. Búsqueda bibliográfica
5. Ejercicios prácticos
6. Conversaciones electrónicas (Chats)

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 Network Defense Professional, Global Learning and Consulting

Recursos

- Computadora
- Servicio de Internet

IX. BIBLIOGRAFÍA

A. Libros y artículos de revistas

CERT-Computer Emergency Readiness Team
http://www.cert.org/
http://www.us-cert.gov/

http://en.wikipedia.org/wiki/Network_security

Introduction to Network Security,
http://www.interhack.net/pubs/network-security/

Revisado por Dr. José R. Vallés diciembre/2016

http://www.bitpipe.com

http://netsecurity.about.com/

Revisado por Dr. José R. Vallés diciembre/2016