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

PRONTUARIO

I. INFORMACIÓN GENERAL

Título del Curso	:	**Prácticas para la Detección y Prevención de Intrusos**
Código y Número	:	INSE 6100
Créditos	:	3
Término Académico	:	
Profesor/a	:	
Horas de Oficina	:	
Teléfono de la Oficina	:	787-250-1912 Ext 2230
Correo Electrónico	:	

II. DESCRIPCIÓN

Detección y análisis de intrusiones a un sistema informático, desde el punto de vista del intruso. Establecimiento de un plan de respuesta a incidentes tomando en cuenta medidas preventivas para evitar futuras intrusiones. Configuración de un IDS ("Intrusion Detection System"). Recuperación y documentación de un sistema afectado por intrusiones. Requiere horas adicionales en un laboratorio abierto.

III. OBJETIVOS

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

1. Establecer el nivel de conocimiento de un intruso.
2. Aplicar procedimientos de detección y rastreo de intrusiones
3. Identificar intentos de intrusión y anomalías en una red informática.
4. Implementar Sistemas de Detección de Intrusiones (IDS).
5. Evaluar un sistema afectado por intrusiones.
6. Aplicar técnicas de recuperación en un sistema afectado por intrusiones.

Revisado por Dr. José R. Vallés diciembre/2016

7. Redactar un informe sobre un Análisis Forense Informático y sus implicaciones legales.

IV. CONTENIDO TEMÁTICO

A. Intrusiones e intentos de intrusión
   1. Nivel de conocimiento de un intruso
      a. ¿Qué es una intrusión?
   2. Tipos de intrusiones
   3. Estadísticas de intrusiones

B. Procedimientos de detección y rastreo de intrusiones.
   1. Metodologías de ataque e investigación
   2. Políticas para las intrusiones
      a. Políticas de detección
      b. Políticas de rastreo
      c. Responsabilidades
      d. Sistemas efectivos para la detección de intrusos
         i. Computer Emergency Readiness Team **(**CERT)
         ii. Argentina- CERT (ArCERT)

C. Descubrimiento de intrusiones
   1. Intento y existencia de intrusiones
   2. Anomalías en la red
      a. Intrusión bajo UNIX
      b. Intrusión bajo Windows NT
      c. Intrusión en estaciones de trabajo
   3. Manejo de incidentes de seguridad y de intrusiones

D. Sistemas de Detección de Intrusiones (IDS).
   1. Tecnología de IDS
      a. ¿Qué es un IDS?
      b. ¿Por qué usar los IDS?
      c. ¿Cómo funcionan los IDS?
   2. Modelos de detección
   3. Sistemas IDS actuales
   4. Sistemas NFR, RealSecure y Snort
      a. Consultas simples y con condiciones
      b. Consultas que requieren varias tablas (Join)
      c. Consultas con subconsultas
      d. Consultas que requieren uso de funciones

E. Implementación de Sistemas de Detección de Intrusiones
   1. Selección del sistema de detección de intrusiones adecuado.
      a. Ubicación del IDS.

b. Administración del IDS.

2. Configuración y tuning del IDS.
    a. Integración entre los componentes (Firewalls, IDS, Routers, etc)
    b. Configuración de las alarmas y respuestas

F. Rastreo de intrusos

1. Lectura de LOGS
    a. Windows NT/2000
    b. Sistemas UNIX.
2. Contactos para el rastreo y tracing de intruso
    a. Rastreo de intrusos a través de Internet.
    b. Rastreo de intrusos a través de líneas telefónicas.
    c. Rastreo de intrusos a través de redes públicas y privadas.

G. Anatomía de una intrusión

1. ¿Cómo es una intrusión?
    a. ¿Qué hacen los intrusos?
    b. ¿Cómo intentan ingresar a los sistemas?
2. Origen de la Intrusión.
    a. Contactos en empresas.
    b. Estudio de los intrusos.

H. Recuperación de sistemas afectados

1. Análisis de sistemas afectados por la intrusión
2. Evaluación y detección de Backdoors, rootkits y programas troyanos
3. Limpieza de los sistemas afectados por la intrusión
4. Recuperación de un sistema ante un ataque

I. Análisis Forense Informático

1. Análisis forense informático.
    a. Recolección de evidencia en estaciones de trabajo.
    b. Recolección de evidencia en Servers
        i. UNIX
        ii. Windows,
        iii. AS/400
2. Métodos de copia de imágenes de discos.
3. Análisis de evidencia
4. Evaluación de un Web Server comprometido.
5. Evaluación de un DNS Server comprometido.
6. Evaluación de un Mail Server comprometido.
7. Generación de pruebas judiciales.

G. Medidas Legales y Futuro

1. Medidas legales actuales.
2. La legislación en la Argentina.

Revisado por Dr. José R. Vallés diciembre/2016

3. La legislación en el resto de los países.
4. Futuro de los intrusos.
5. Futuro de la detección de intrusos.

V. ACTIVIDADES

A. Enseñanzas

1. Estudio de módulos
2. Presentaciones electrónicas (on-line)
3. Discusiones electrónicas (Foros)
4. Conversaciones electrónicas (Chats)
5. Ejercicios de práctica
6. Ejercicios de aplicación
7. Lecturas y ejercicios suplementarios
8. Búsqueda bibliográfica

VI. 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

A. Servicios auxiliares o asistencia especial

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.

B. Advertencia de honradez, fraude y plagio según se dispone en el Capitulo V, Articulo 1 del Reglamento general del estudiante:

http://www.inter.edu/files/REGESTU071.pdf

Revisado por Dr. José R. Vallés diciembre/2016

El plagio, la falta de honradez, el fraude, la manipulación o falsificación de datos y cualquier otro comportamiento inapropiado relacionado con la labor académica o cualquier acción encaminada a tal fin, son contrarios a los principios y normas institucionales y están sujetos a sanciones disciplinarias, según establece el Capitulo V, Articulo 1, Sección B.2, P. 44-47 del RGE.

C. REQUISITOS DE LOS MATERIALES DEL CURSO

Todo estudiante deberá de comprar el libro de texto ya que este lo necesitará para desarrollar e interactuar en los foros. Este curso requiere que el estudiante tenga accesible una computadora con Internet.

D. 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).

D. REQUISITOS DEL CURSO

Es responsabilidad del estudiante:

- Tener los programas requeridos para la realización de las tareas.
- Cumplir con las fechas estipuladas
- Cumplir con el reglamento general del estudiante

Revisado por Dr. José R. Vallés diciembre/2016

- Leer: el Manual del Estudiante, los enlaces de Netetiquette, tutorial de Blackboard
- Si confronta algún problema con Blackboard comunicarse con el Sr. Jairo Pulido, Director Centro de Aprendizaje a Distancia y Desarrollos Tecnológicos al teléfono (787) 250-1912 extensión 2387, 3387, correo electrónico: jpulido@metro.inter.edu o webmaster@metro.inter.edu.

Portal de apoyo a estudiantes y facultad de la Universidad Interamericana de Puerto Rico: http://adistancia.inter.edu/webct/

VIII. RECURSOS EDUCATIVOS

Libro de texto

Ethical Hacking & Countermeasures. EC-Council

Recursos y Materiales Necesarios

A. Profesor del curso
B. Conferencias Online
C. Blackboard
D. Enlaces del Web
E. Libro de texto
F. Presentaciones

IX. BIBLIOGRAFÍA

A. Libros y artículos de revistas

Di Pietro, R., and Mancini, L.V.(2008).Intrusion Detection Systems,Springer.

Tsai, J.J.P.(2011). Intrusion Detection, World Scientific.

Cox, K.J. and Gerg, C.(2009). Managing Security with Snort & IDS Tools, O'Reilly Media

Bray, R., Cid, D. and Hay, A.(2008). OSSEC Host-Based Intrusion Detection Guide, Elsevier Science.

Vacca, J.R. (2010). Managing Information Security, Elsevier Science,

Oriyano, S. and Shimonski, R.(2012). Client Side Attacks and Defense, Elsevier Science.

Revisado por Dr. José R. Vallés diciembre/2016

B. Referencias electrónicas:

ARCERT- Argentina-Computer Emergency Readiness Team
http://www.utn.edu.ar/comiteseguridad/arcert.utn
http://www.cert.uy/Usuario/pdf/presentaci%C3%B3n-workshop-uruguay-20081017-v5.pdf

BAXWARE.COM - Herramientas gratuitas de seguridad informática
http://www.baxware.com/deteccion-intrusos-ids.htm

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

Social engineering
http://www.us-cert.gov/cas/tips/ST04-014.html

Security Focus
http://www.securityfocus.com/

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.

Revisado por Dr. José R. Vallés diciembre/2016

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.

Detección de Intrusos en Tiempo Real
http://www.segu-info.com.ar/proteccion/deteccion.htm

NFR- Network Flight Recorder
http://www.nfr.net

Revisado por Dr. José R. Vallés diciembre/2016