Aprobado por resolución Nº113 del CFI de fecha 04.07.2017

FACULTAD DE INGENIERIA

UNIVERSIDAD DE LA REPÚBLICA URUGUAY

Programa de Taller de Seguridad Informática

1. NOMBRE DE LA UNIDAD CURRICULAR

Taller de Seguridad Informática

2. CRÉDITOS

10 créditos

3. OBJETIVOS DE LA UNIDAD CURRICULAR

Profundizar en los conceptos de seguridad informática. Introducir al estudiante en la implementación de servicios y funcionalidades orientadas al ámbito de seguridad, por ejemplo, desarrollando funciones de autenticación, plugins para herramientas de seguridad, modificando y configurando funcionalidades complejas de los sistemas operativos, etc.

Adquirir conocimientos de desarrollo de aplicaciones seguras mediante el estudio de las estructuras y funcionalidades provistas por diferentes frameworks de seguridad disponibles.

Objetivos específicos:

- Que el estudiante comprenda las principales decisiones de diseño que deben ser tomadas para la implementación de diversas herramientas de seguridad.
- Que el estudiante adquiera conocimiento de estructuras y algoritmos desde un punto de vista de seguridad que son utilizados para el desarrollo.
- Que el estudiante implemente nuevos servicios.
- Realizar trabajos prácticos que apliquen los conceptos y técnicas vistas a lo largo de este curso y del curso Fundamentos de Seguridad Informática.

4. METODOLOGÍA DE ENSEÑANZA

El curso posee una duración de 12 semanas con 3 horas semanales de teórico-práctico y reuniones periódicas con los docentes supervisores de los laboratorios. El trabajo en esta asignatura será esencialmente práctico. El equipo docente presentará trabajos de laboratorio que deberán ser resueltos por los estudiantes que se organizarán en grupos de a lo máximo 2 (dos) personas. Los grupos de trabajo serán asistidos y supervisados por el equipo docente a lo largo de la realización de cada laboratorio. Se realizarán clases teóricas según lo requieran las tareas a ser desarrolladas.

La realización de trabajos prácticos tiene como objetivo principal formar al estudiante en el desarrollo y utilización de herramientas de seguridad.

CARGA TOTAL DE TRABAJO: 156 horas

- Horas clase (teórico/práctico): 43
- Horas evaluación: 20

Subtotal horas presenciales/virtuales: 63

- Horas estudio: 30
- Horas resolución ejercicios/prácticos: 63

Total de horas de dedicación del estudiante:156

5. TEMARIO

El temario de base para este curso lo constituye los conceptos fundamentales de criptografía aplicada, seguridad de sistemas operativos, de redes, y desarrollo de aplicaciones seguras. Los trabajos prácticos o laboratorios podrán variar en diferentes ediciones del curso, pero el objetivo es cubrir aspectos ingenieriles de cada unas de las mencionadas áreas, que son resumidas a continuación:

Criptografía Aplicada

Algoritmos de clave pública/privada. Tipos de ataques a los que debe ser inmune un algoritmo. Cifrado perfecto. "One time pads". Clasificaciones: Cifrados de clave simétrica, de clave pública, en bloque, en flujo. Encadenamiento de algoritmos en bloques. Otras funciones criptográficas. Hashes. Diffie-Hellman. Gestión de claves. Firma electrónica. Infraestructura de clave pública (PKI). Certificados digitales. Protocolos criptográficos.

Seguridad de Sistemas

Identificación, Autenticación: mecanismos tradicionalmente utilizados en los sistemas operativos comunes. Métodos de Autenticación. Algoritmos y protocolos de autenticación. Políticas de seguridad. Mecanismos de control de acceso: ACL, Single Sign-On. Seguridad en Windows. Seguridad en Unix.

Seguridad en Redes TCP/IP

Introducción a la seguridad en redes TCP/IP. Problemas en las distintas capas del modelo OSI simplificado. Seguridad por debajo de la capa 3. Seguridad física. Seguridad en los protocolos de capa 2 y capa MAC. Ataques a estos protocolos. Redes inalámbricas. (IN)Seguridad en capa 3 y 4. Ataques a

los protocolos IP, TCP, UDP, ICMP. Qué nos dá IPSec y qué no. Seguridad en los protocolos de aplicación. Servicios de infraestructura críticos: DNS. Ataques a las aplicaciones. Seguridad de la infraestructura. Ataques a la infraestructura. (IN)Seguridad en los protocolos de ruteo. Herramientas para la seguridad en redes TCP/IP: Firewalls, VPNs, IDS, Honeypots. El estado de la seguridad en Internet: DDoS, Ataques "Man in the middle", Ataques a las aplicaciones. Botnets, Canales encubiertos, Ataques "sociales". El factor humano. Phishing, etc.

Seguridad en las Aplicaciones

Errores en los programas y defensas: Ataques al Stack, Bugs en el formato de los strings, Ataques de Timing, Defensas contra estos ataques. Diseño de código seguro: Diseño modular, Herramientas para hacer código seguro, Verificadores de modelos. Manejando código inseguro: Sandboxing, Máquinas virtuales. Seguridad en los browsers: Cookies, Privacidad y multitudes, Java Script, Java Applets y ActiveX. Secure Coding.

6. BIBLIOGRAFÍA

Aunque la bibliografía será especificada en cada laboratorio para guiar al estudiante en la temática objetivo cubierta y en el uso de las herramientas necesarias para el desarrollo de los mismos, a continuación se lista la bibliografía básica común a todos los laboratorios:

- Gollman, Dieter (2011), Computer Security, Wiley Computng Publishing, 3rd. Editon.
- Anderson, Ross (2020), Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd. Editon, Wiley.
- Stallings, W. (2016), Cryptography and Network Security, 7Th Edition, Perason.
- Garinkel,S.k Spaford; G. & Schuartz, A., Practical Unix & Internet Security, Ed. O'Reilly, 3rd Editon.

7. CONOCIMIENTOS PREVIOS EXIGIDOS Y RECOMENDADOS

7.1 Conocimientos Previos Exigidos: Sólidos conocimientos de redes de computadoras, sistemas operativos y programación.

7.2 Conocimientos Previos Recomendados: Esta asignatura asume como ya adquiridos por el estudiante conceptos básicos de Seguridad Informática. En caso de no contar con los mismos, la incorporación de esos conceptos será responsabilidad única del estudiante , lo que redundará en una mayor dedicación horaria.

ANEXO A
Para todas las Carreras

Esta primera parte del anexo incluye aspectos complementarios que son generales de la unidad curricular.

A1) INSTITUTO

Instituto de Computación

A2) CRONOGRAMA TENTATIVO

Consiste en un cronograma de avance semanal con detalle de las horas de clase asignadas a cada tema.

	Presentación del curso	150 minutos
Semana 1	**Presentación Laboratorio 1**	**150 minutos**
	Clases prácticas	150 minutos
Semana 2	**Clases prácticas**	150 minutos
	Clases prácticas	150 minutos
Semana 3	**Entrega y prueba**	**150 minutos**
	Defensa	150 minutos
Semana 4	**Presentación Laboratorio 2**	**150 minutos**
	Clases prácticas	150 minutos
Semana 5	**Clases prácticas**	150 minutos
	Clases prácticas	150 minutos
Semana 6	**Entrega y prueba**	**150 minutos**
	Defensa	150 minutos
Semana 7	**Presentación Laboratorio 3**	**150 minutos**
	Clases prácticas	150 minutos
Semana 8	**Clases prácticas**	150 minutos
	Clases prácticas	150 minutos
Semana 9	**Entrega y prueba**	**150 minutos**
	Defensa	150 minutos
Semana 10	**Presentación Laboratorio 4**	**150 minutos**
	Clases prácticas	150 minutos
Semana 11	**Clases prácticas**	150 minutos
	Clases prácticas	150 minutos
Semana 12	**Entrega y prueba**	**150 minutos**
	Defensa	150 minutos

A3) MODALIDAD DEL CURSO Y PROCEDIMIENTO DE EVALUACIÓN

El curso será dictado en modalidad híbrida (Presencial/Virtual).

La asignatura se evaluará por medio de una prueba al finalizar cada laboratorio y por la suficiencia de los trabajos de laboratorio. El nivel mínimo de suficiencia en los trabajos de laboratorio es eliminatorio. El puntaje obtenido en cada laboratorio se integrará al puntaje total del curso, prorrateándose con el puntaje obtenido en cada prueba.

La asistencia a las clases prácticas y teóricas será obligatoria, requiriendo una asistencia mínima al 80% de las actividades.

En todos los casos de los resultados obtenidos surgen dos posibilidades:

- Exoneración del curso
- Insuficiencia en el curso; el estudiante reprueba el curso

Se presenta a continuación el esquema de evaluación del curso

Exoneración. El estudiante debe cumplir los siguientes requisitos:

- llegar al nivel mínimo en cada uno de los trabajos de laboratorio, y
- reunir al menos el 60% del puntaje de cada prueba.

Insuficiencia. El estudiante no cumple los requisitos especificados para exonerar el curso.

A4) CALIDAD DE LIBRE

No acepta Calidad de Libre.

A5) CUPOS DE LA UNIDAD CURRICULAR

No tiene cupo

FACULTAD DE INGENIERIA

UNIVERSIDAD DE LA REPÚBLICA URUGUAY

ANEXO B para la carrera Ingeniería en Computación (plan 87)

B1) ÁREA DE FORMACIÓN

No corresponde.

B2) UNIDADES CURRICULARES PREVIAS

Para el curso: Tener aprobado tercer año completo y el examen de Comunicación de Datos

Para el examen: No aplica

Observación: Esta unidad curricular se corresponde con una electiva

FACULTAD DE INGENIERIA

UNIVERSIDAD DE LA REPÚBLICA URUGUAY

ANEXO B para la carrera Ingeniería en Computación (plan 97) y Licenciatura en Computación

B1) ÁREA DE FORMACIÓN

Arquitectura, Sistemas Operativos y Redes de Computadores.

B2) UNIDADES CURRICULARES PREVIAS

Para el Curso:

- Examen aprobado de Programación 3
- Examen aprobado de Fundamentos de Bases de Datos
- Curso aprobado de Redes de Computadoras

Para el Examen: No aplica

Esta unidad curricular no acumula créditos con la unidad curricular Taller de Seguridad Informática (1437).

RES CONSEJO DE FAC. 01/08/23 Exp. 060120-000127-23