

Seguridad en Sistemas Informáticos (4º grado)

Curso 2018/19

Seguridad en Sistemas Informáticos
4º Grado en Ingeniería Informática
ESEI

Septiembre-2018

Profesores

Francisco José Ribadas Pena

- Despacho 303, ribadas@uvigo.es
- Tutorías: Lunes: 16:00-17:00; Martes: 9:00-10:30, 15:30-17:00; Jueves 16:00-17:00

Víctor M. Darriba Bilbao

- Despacho 304, darriba@uvigo.es
- Tutorías: Lunes: 10:00-12:30, 16:00-19:30

Contenidos de teoría I

Tema 1. Introducción

1. Conceptos y terminología
 - Confidencialidad, integridad, disponibilidad
 - Activos, amenazas, vulnerabilidades, riesgos, contramedidas
2. Niveles de la seguridad (tipos de controles)
 - seguridad física
 - seguridad lógica
 - seguridad organizativa
3. Normas, recomendaciones y estándares
 - Familia de normas ISO 27000
 - Metodología de gestión de riesgos: MARGERIT

Tema 2. Criptografía

1. Fundamentos y evolución
 - Conceptos básicos
 - Tipología
 - Criptografía clásica
2. Cifrado simétrico
 - Fundamentos del cifrado simétrico
 - Algoritmo DES
 - Fundamentos: Redes Feistel
 - Componentes y arquitectura DES
 - Variantes y mejoras
 - Otros algoritmos simétricos: AES

Contenidos de teoría II

3. Cifrado asimétrico
 - Fundamentos del cifrado asimétrico
 - Algoritmo RSA
 - Fundamentos matemáticos
 - Usos, debilidades y ataques
 - Usos: firma digital
 - Funciones HASH criptográficas
 - Usos: distribución de claves. Algoritmo de Diffie-Hellman
4. Infraestructuras criptográficas
 - Certificados digitales. Formato de Certificados X.509
 - Autoridades de certificación
 - Infraestructura de clave pública(PKI)

Tema 3. Seguridad en el desarrollo de aplicaciones

1. Tipos de vulnerabilidades y amenazas del software
 - Desbordamiento de buffer
 - Vulnerabilidades WEB: OWASP top ten
 - Inyección de código
 - SQL injection
 - Cross Site Scripting (XSS)
2. Explotación de vulnerabilidades
 - Tareas y fases típicas
3. Programación segura
 - Recomendaciones generales
 - Guías OWASP para desarrollo web

Contenidos de teoría III

Tema 4. Administración segura de SS.OO.

1. Mecanismos de autenticación
 - Autenticación en Unix, GNU/Linux
 - Módulos PAM y LDAP
 - Autenticación en MS Windows
 - Active Directory
2. Herramientas de monitorización
 - Logs en Unix, GNU/Linux
 - Logs en Windows
3. Vulnerabilidades típicas
 - Vulnerabilidades y problemas de configuración en Unix, GNU/Linux
 - Vulnerabilidades y problemas de configuración en MS Windows
4. Respuesta ante incidentes

Tema 5. Seguridad en redes 1: protocolos seguros

1. Vulnerabilidades en redes TCP/IP
2. Seguridad en nivel de red: IPsec
 - Protocolos AH yESP
 - Modo tunel vs. modo transporte
 - VPNs IPsec
3. Seguridad en nivel de transporte:SSL/TLS
 - Servicios de seguridad
 - Arquitectura
 - Protocolo de negociación

Contenidos de teoría IV

4. Seguridad en nivel de aplicación: SSH
 - Arquitectura y funcionamiento
 - Redirección de puertos (túneles SSH)

Tema 6. Seguridad en Redes 2: protección perimetral

1. Firewalls/cortafuegos
 - Tipos de cortafuegos
 - Filtros de paquetes
 - Inspección de estados
 - Proxies de aplicación
 - Topologías típicas
 - Zonas desmilitarizadas (DMZ)
 - iptables/NETFILTER
2. Redes privadas virtuales
 - Ejemplos: OpenVPN
3. Detección de intrusos
 - Funcionamiento de los sistemas IDS
 - Tipos y ejemplos: SNORT
4. Análisis de seguridad en redes
 - Auditorias y test de intrusión

Prácticas de laboratorio

Proyecto de Programación con algoritmos criptográficos

- Uso del API de cifrado de Java (JCE/JCA)
- Individual o en parejas
- Entrega: <pendiente>

Seguridad en redes

- Ejercicios guiados sobre seguridad en redes y GNU/Linux
- Lista provisional de temas)
 1. Tests de intrusión (pentest)
 - Ejemplo con Metasploit framework
 2. Vulnerabilidades en aplicaciones web: prevención y detección
 - Ataque a aplicaciones web vulnerables (WebGOAT, Damm Vulnerable Web App, ...)
 3. Uso de sniffers(Wireshark) y escáneres de puertos (nmap)
 4. Firewall "complejo" con iptables (DMZ) + redes privadas virtuales (OpenVPN)
 5. Detección de intrusiones (SNORT) y análisis de logs
- Individuales o en parejas
- Entrega: <pendiente>

Trabajos de investigación

Trabajos de investigación

- Idealmente en parejas
- Lista de temas cerrada (alumnos pueden proponer otros)
- Presentación en clase
 - A partir de noviembre
 - 15-20 minutos
 - Cada trabajo tiene una fecha de presentación asignada
- Entrega: <pendiente>

Evaluación (ver detalles en **guía docente**)

Asistentes

- Examen: 40 % (hasta 4 puntos)
- Prácticas: 45 %
 - Práctica "Cifrado en Java": hasta 1 punto
 - Prácticas "Seguridad en Redes": hasta 3,5 puntos
- Trabajo: 15 %
 - Memoria: hasta 1 punto
 - Presentación: hasta 0,5 puntos
- Requisitos
 - Se exige un mínimo del 40 % de la nota máxima prevista en "Prácticas"
 - Se exige un mínimo del 40 % de la nota máxima prevista en "Examen"
 - Se exige un mínimo de 5 puntos para aprobar la materia

No asistentes

- Examen: 50 % (hasta 5 puntos)
- Prácticas redes: 35 % (hasta 3,5 puntos)
- Práctica cifrado: 15 % (hasta 1,5 puntos)
- Se exige un mínimo del 50 % de la nota máxima de cada uno de los 3 apartados y sumar al menos 5 puntos para aprobar

En caso de constatar un comportamiento no ético (copia, plagio) en alguna de las entregas realizadas (total o parcial), se anulará la totalidad de la contribución del correspondiente elemento de evaluación ("Examen", "Trabajo" ó "Prácticas")

Bibliografía

Web de la materia

- <http://faitic.uvigo.es/>
- <http://ccia.esei.uvigo.es/docencia/SSI>

Libros

- W. Stallings, *Cryptography and Network Security: Principles and Practice, 5th edition*, Prentice Hall, 2011
- W. Stallings, L. Brown, *Computer Security: Principles and Practice, 2nd edition*, Prentice Hall, 2012,
- J. L. García Rambla, *Ataques en redes de datos IPv4 e IPv6, 2da edición*, 0xWORD, 2014,
- Libros electrónicos en la web de la materia