FICHA DE LA ASIGNATURA: MONITORIZACIÓN Y SEGURIDAD INALÁMBRICA			
CARÁCTER:	**Obligatorio**	**LENGUA/S EN LA/S QUE SE IMPARTE:**	**Español**
ECTS:	**4**	**CUATRIMESTRE**	**2**
Asignatura de la MATERIA SEGURIDAD EN SISTEMAS			
PROFESORES QUE IMPARTEN LA ASIGNATURA			
Antonio Molina Cabrera **Mercedes Rodríguez García (coordinadora)**			
COMPETENCIAS QUE SE ADQUIEREN: *(indicar código)*			
Comp. Básicas	**Comp. Generales**	**Comp. Específicas**	**Comp. Transversales**
CB6, CB7, CB8, CB9, CB10	**CG1, CG2, CG3, CG4, CG5**	**CE6, CE19, CE20**	**CT1**

RESULTADOS DE APRENDIZAJE:

Comprender los aspectos básicos de la monitorización de la seguridad de redes y diseñar una estrategia adecuada de monitorización.
Identificar los datos adquiridos en el proceso de monitorización.
Distinguir y comprender los sistemas de detección y prevención de intrusiones.
Usar aplicaciones de monitorización de seguridad.
Identificar las amenazas y riesgos de seguridad que afectan a las redes inalámbricas.
Conocer los mecanismos de autenticación y cifrado de las redes inalámbricas.
Diseñar e implementar servicios de acceso inalámbricos seguros.
Conocer los principales métodos utilizados para proteger el anonimato en redes ad-hoc.

CONTENIDOS:

<u>Bloque 1: Monitorización de la seguridad en redes</u>

TEMA 1. Introducción a la monitorización de la seguridad en redes
- 1.1 Breve evolución histórica de los sistemas de monitorización de seguridad
- 1.2 ¿Qué es la monitorización en seguridad en redes (NSM)?
  - 1.2.1 Monitorización continua frente a NSM
  - 1.2.2 Aspectos legales de la monitorización
- 1.3 Estrategias de monitorización
- 1.4 Consideraciones del despliegue de monitorización
  - 1.4.1 Modelos de amenaza y zonas de monitorización
  - 1.4.2 Conoce tu red

TEMA 2. Análisis de datos en la monitorización de redes
- 2.1 Datos de contenido completo de paquetes
- 2.2 Datos de alto nivel
- 2.3 Datos estadísticos
- 2.4 Datos referentes a alertas

TEMA 3. Sistemas de detección y prevención de intrusiones (IPS & IDS)
- 3.1 Arquitecturas de detección de intrusiones
  - 3.1.1 Modelo de intrusiones
- 3.2 Componentes de los IDS
- 3.3 Tipos de IDS

3.4 Sistema de detección de intrusiones de red (NIDS)
3.4.1 Detección de intrusiones mediante herramientas software: *Snort*, *Suricata, Bro, etc.*
3.5 Sistema de detección de intrusiones en el host (HIDS)
3.6 Sistemas de detección de intrusiones para redes inalámbricas (WIDS)
3.7 Limitaciones y soluciones de los sistemas de detección de intrusiones
3.8 Sistemas de prevención de intrusos (IPS)
3.9 Caso práctico: monitorización de la seguridad de red

TEMA 4. Herramientas de monitorización
4.1 Security information and event management (SIEM) software
4.1.1 Open Source Security Information Management (OSSIM)
4.1.2 Security onion
4.2 Visualización avanzada de eventos

Bloque 2: Seguridad en redes inalámbricas

TEMA 5. Topologías de redes inalámbricas
5.1 Redes de infraestructura
5.2 Redes Ad-Hoc
TEMA 6. Amenazas y riesgos de seguridad
6.1 Puntos de acceso no autorizados (*Rogue* AP)
6.2 Ataque ARP *poisoning*
6.3 Otros ataques
TEMA 7. Métodos de cifrado utilizados en las comunicaciones inalámbricas
7.1 WEP
7.2 TKIP
7.3 CCMP
7.4 WPA
TEMA 8. Métodos de autenticación
8.1 Autenticación de sistema abierto
8.2 Autenticación de claves compartidas (PSK)
8.3 Autenticación 802.1X/ EAP
TEMA 9. Infraestructuras de seguridad
9.1 Controladores WLAN
9.2 Portales cautivos
TEMA 10. Seguridad en redes Ad-Hoc
10.1 Comunicaciones anónimas

OBSERVACIONES / REQUISITOS PREVIOS:

Algunas de las actividades podrán realizarse en inglés.

Haber adquirido las competencias de la asignatura criptografía aplicada a la protección de datos del Máster Universitario en Seguridad Informática (Ciberseguridad) y poseer conocimientos básicos de redes de ordenadores

ACTIVIDADES FORMATIVAS CON SUS CRÉDITOS ECTS:	**Id de la Actividad Formativa**	**Nº de horas**	**Presencialidad (%)**
	Clases teórico-prácticas	32	100

	Actividades académicas no presenciales	65	0
	Evaluación	3	100

METODOLOGÍAS DOCENTES:
Lección magistral expositiva
Resolución de problemas y casos prácticos
Prácticas de laboratorio
Realización de trabajos

SISTEMAS DE EVALUACIÓN DE ADQUISIÓN DE COMPETENCIAS:

Denominación Sistema Evaluación	Ponderación Mínima	Ponderación Máxima
Exposiciones de ejercicios, temas o trabajos	30%	70%
Pruebas escritas u orales	30%	70%
Prácticas de laboratorio	15%	25%

BIBLIOGRAFÍA RECOMENDADA:

Bejtlich, Richard. *The practice of network security monitoring: understanding incident detection and response*. No Starch Press, 2013.

Sanders, Chris, and Jason Smith. *Applied network security monitoring: collection, detection, and analysis*. Elsevier, 2013.

Fry, Chris, and Martin Nystrom. *Security monitoring*. "O'Reilly Media, Inc.", 2009.

Bejtlich, Richard. *Extrusion detection: security monitoring for internal intrusions*. Addison-Wesley Professional, 2005.

Bejtlich, Richard. *The Tao of network security monitoring: beyond intrusion detection*. Pearson Education, 2004.

Sanders, Chris. *Practical packet analysis: Using Wireshark to solve real-world network problems*. No Starch Press, 2017.

David D. Coleman, David A. Westcott, Bryan E. Harkins. CWSP: Certified Wireless Security Professional Study Guide, 2nd Edition. Wiley, 2016.