19-20

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

GUÍA DE ESTUDIO PÚBLICA

AUDITORÍA Y MONITORIZACIÓN DE LA SEGURIDAD

CÓDIGO 31109025

19-20

AUDITORÍA Y MONITORIZACIÓN DE LA SEGURIDAD

CÓDIGO 31109025

ÍNDICE

Nombre de la asignatura	AUDITORÍA Y MONITORIZACIÓN DE LA SEGURIDAD
Código	31109025
Curso académico	2019/2020
Título en que se imparte	MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD
Tipo	CONTENIDOS
Nº ETCS	6
Horas	150.0
Periodo	SEMESTRE 1
Idiomas en que se imparte	CASTELLANO

PRESENTACIÓN Y CONTEXTUALIZACIÓN

PRESENTACIÓN

La monitorización de la seguridad representa un reto hoy en día. Es un escenario ideal, sería necesario recopilar los datos de todos los dispositivos y aplicaciones relevantes en una red. Sin embargo, actualmente nos encontramos con el reto de que cada dispositivo es capaz de generar cientos de eventos por minuto. El gran volumen de datos puede abrumar a cualquier programa de monitorización que no haya sido correctamente instalado y configurado. Las decisiones de priorización e inclusión deben basarse en la criticidad del sistema o dispositivo, los requisitos de protección de datos, la vulnerabilidad a la explotación y otros requisitos legales.

Esta asignatura intentará ayudar al estudiante a discernir entre aquellos dispositivos y aplicaciones relevantes para poder construir un centro de operaciones de seguridad eficaz que permita detectar con fiabilidad cualquier intrusión en los sistemas.

CONTEXTUALIZACIÓN

La asignatura de Auditoría y Monitorización de la Seguridad se trata de una asignatura de 6 créditos ECTS, de carácter obligatorio, impartida en el primer semestre del Máster Universitario en Ciberseguridad. Guarda relación con las siguientes asignaturas también disponibles en el mismo Máster:

•Seguridad en Infraestructuras Críticas

•Gestión de Incidentes de Ciberseguridad

•Análisis Forense

•Hacking Ético

.

REQUISITOS Y/O RECOMENDACIONES PARA CURSAR ESTA ASIGNATURA

Se recomienda que los interesados en cursar el Máster tengan un nivel de lectura en inglés suficiente como para entender contenidos técnicos en dicha lengua.

Gran parte de la bibliografía, así como los recursos proporcionados al estudiante en el curso virtual pueden estar únicamente en inglés, debido a la novedad de algunos de los contenidos propuestos para la asignatura.

Son necesarios conocimientos sólidos en sistemas operativos (especialmente Linux) e

infraestructuras/protocolos de red, ya que las herramientas y diseños especificados en la asignatura se apoyan en estas estructuras.
Por otra parte, cada una de las actividades propuestas formativas en la asignatura constarán de una parte de trabajo individual, otra colectiva (si fuera el caso) y la utilización de la plataforma virtual, además de ser eminentemente prácticas. Todo ello de manera conjunta, por lo que la división de horas realizada en el apartado de actividades formativas es orientativa.

EQUIPO DOCENTE

Nombre y Apellidos	RAFAEL PASTOR VARGAS (Coordinador de asignatura)
Correo Electrónico	rpastor@dia.uned.es
Teléfono	91398-8383
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL

Nombre y Apellidos	RAFAEL PASTOR VARGAS (Coordinador de asignatura)
Correo Electrónico	rpastor@scc.uned.es
Teléfono	91398-8383
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL

Nombre y Apellidos	LUIS GRAU FERNANDEZ
Correo Electrónico	lgrau@scc.uned.es
Teléfono	91398-7153
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL

HORARIO DE ATENCIÓN AL ESTUDIANTE

La tutorización de los estudiantes tendrá lugar esencialmente a través de los foros de la plataforma, aunque también podrán utilizarse ocasionalmente otros medios, tales como chats interactivos, servicios de mensajería instantánea y el correo electrónico. Adicionalmente, está también previsto, para temas personales que no afecten al resto de los estudiantes, atender consultas en persona o por teléfono.
El seguimiento del aprendizaje se realizará revisando la participación de los alumnos en los distintos foros de debate y las aportaciones de material nuevo además de la entrega en fecha de los diferentes trabajos prácticos que se han planificado durante la evolución del curso.
En caso de necesitar contactar con el Equipo Docente por medios distintos al curso virtual, se utilizará preferentemente el correo electrónico, pudiéndose también realizar consultas telefónicas y entrevista personal en los horarios establecidos y que se muestran a continuación en la siguiente tabla.

Profesor	Horario de atención	Correo electrónico	Teléfono de contacto
Rafael Pastor Vargas	Lunes de 16 a 18 horas	**rpastor@scc.uned.es**	91 398 8383
Luis Grau fernández	Martes de 15 a 19 horas	**lgrau@scc.uned.es**	91 398 7153

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE

COMPETENCIAS BÁSICAS

CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio

CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios

CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

COMPETENCIAS GENERALES

CG1 - Analizar métodos y técnicas de ciberataques.

CG2 - Diseñar, poner en marcha y mantener un sistema de ciberseguridad.

CG4 - Identificar, gestionar y desarrollar medidas y protocolos de seguridad en la operación y gestión de sistemas informáticos.

COMPETENCIAS TRANSVERSALES

CT1 - Ser capaz de abordar y desarrollar proyectos innovadores en entornos científicos, tecnológicos y multidisciplinares.

CT2 - Ser capar de tomar decisiones y formular juicios basados en criterios objetivos (datos experimentales, científicos o de simulación disponibles).

COMPETENCIAS ESPECÍFICAS

CE2 - Diseñar mecanismos de prevención de amenazas a la seguridad, así como de reconocer y resolver incidentes de seguridad en los sistemas críticos.

CE3 - Utilizar herramientas para monitorizar el tráfico de red y generar, explorar y manipular el tráfico en los sistemas de comunicación.

CE6 - Conocer las tendencias actuales en técnicas de ciberataque, los mecanismos de defensa mediante aprendizaje automático y especialmente dirigido a casos reales.

RESULTADOS DE APRENDIZAJE

Los resultados de aprendizaje que se pretenden alcanzar con el estudio de esta asignatura son los siguientes:

•Describir las principales funciones de un centro de operaciones de seguridad.

•Diseñar un plan de monitorización y auditoria de una organización.

•Evaluar los diversos mecanismos de adquisición de datos y seleccionar los más adecuados al contexto.

•Analizar diversas fuentes de datos y evaluar los resultados en el contexto de la ciberseguridad.

CONTENIDOS

Tema 1: Monitorización y auditoria de sistemas en red

En este tema se analizarán los mecanismos de monitorización de la información que fluye a través de la red (paquetes/protocolos) y como se pueden gestionar y/o almacenar a traves de ficheros de seguimiento (log). A partir de estos datos, que se pueden verificar en tiempo real o en sistemas de procesamiento por lotes, se pueden implementar los mecanismos de detección y proteción de intrusiones. Los apartados de este tema son los siguientes:

1. Introducción a la monitorización y auditoria de sistemas
2. Monitorización de red
3. Gestión de logs y monitorización de la seguridad de red
4. Introducción a los sistemas de detección y protección de intrusiones en la red
5. Seguridad perimetral de la red

Tema 2: Metodologías para la monitorización de sistemas

En este tema se mostrarán las dos metodologías que se pueden implementar en infraestructuras que soporten la monitorización de la red: CM (Continuous Monitoring) y NSM (Network Security Monitoring). Dado que CM es más amplia que NSM y se centra más en las amenzas que en la propia red, la asignatura se centra en esta última metodología. De esta manera se verán las diferentes fases del ciclo de trabajo con NSM. Los apartados de este tema son los siguientes:

1. Monitorización continua (Continuous Monitoring)
2. NSM: Network Security Monitoring
3. Fases del ciclo de trabajo con NSM

Tema 3: Gestión del Centro de Operaciones de Seguridad (SOC)

Un centro de operaciones de seguridad o SOC (Security Operations Center) es el encargado de la gestión de los mecanismos y operaciones de implementación y monitorización de la seguridad de cualquier organización. En este tema veremos cuales son las funciones del SOC y las fases de implantación necesarias para implantar de manera efectiva este centro. Finalmente, se verán los mecanismos/fases específicas que explicitan las operaciones necesarias para la puesta en funcionamiento de NSM. De esta manera se verán las diferentes fases del ciclo de trabajo con NSM. Los apartados de este tema son los siguientes:

1. Introducción a las operaciones de seguridad y SOC
2. Fases de implantación del SOC
3. Fase de diseño y NSM: Generación de los eventos de seguridad y adquisición

Tema 4: Diseño de mecanismos para la adquisición de datos

En este tema nos centraremos en la planificación de la plataforma de monitorización, y su puesta en funcionamiento a través de una definición de la arquitectura de sensores (taps, software, etc.) que sena capaces de capturar la información en diferentes fuentes de datos en la red. Esta información podrá provenir de diferentes fuentes de datos, por lo que es necesario conocer que tipos de datos van a poder ser empleados en las operaciones de monitorización. Los apartados de este tema son los siguientes:

1. Planificación de la adquisión de datos
2. Estructura y topología de la plataforma de sensores
3. Tipos de datos

Tema 5: Análisis e interpretación de la información

Una vez vistos que se dispone del sistema de recolección de información a través de los sensores, es necesario disponer y conocer que herramientas hay disponibles para el análisis de la información (específicamente de tráfico de red) y como se puede emplear esa informacion para implementar mecanismos de deteccion de intrusiones. En este tema se verán que mecanismos existen e incluso como se pueden aplicar técnicas de aprendizaje automático para el reconocimiento de patrones en intrusiones. Los apartados de este tema son los siguientes:

1. Herramientas de consola para el análisis de tráfico de red
2. Herramientas gráficas para el análisis de tráfico de red
3. Mecanismos de detección e indicadores de compromiso

4. Detección de intrusos basada en firmas
5. Detección de intrusos basada en detección de anomalias
6. Aplicaciones del Machine Learning en el análisis de tráfico de red

METODOLOGÍA

Esta asignatura ha sido diseñada para la enseñanza a distancia. Por tanto, el sistema de enseñanza-aprendizaje estará basado en gran parte en el estudio independiente o autónomo del estudiante. Para ello, el estudiante contará con diversos materiales que permitirán su trabajo autónomo y la Guía de Estudio de la asignatura, que incluye orientaciones para la realización de las actividades prácticas. Asimismo, mediante la plataforma virtual de la UNED existirá un contacto continuo entre el equipo docente y los/as estudiantes, así como una interrelación entre los propios estudiantes a través de los foros, importantísimo en la enseñanza no presencial.

Las actividades formativas para el estudio de la asignatura son las siguientes:

•Estudios de contenidos

•Tutorías

•Actividades en la plataforma virtual

•Prácticas Informáticas.

•Trabajos evaluables (cuestionarios)

Los medios necesarios para el aprendizaje son:

1. **Materiales teórico-prácticos** preparados por el Equipo Docente para cubrir los conceptos básicos del temario.
2. **Bibliografía complementaria**. El estudiante puede encontrar en ella información adicional para completar su formación.
3. **Curso Virtual de la asignatura**, donde el estudiante encontrará:

•Una guía de la asignatura en la que se hace una descripción detallada del plan de trabajo propuesto.

•Enunciado de las actividades teórico-prácticas propuestas y zona donde depositar los entregables asociados a dichas actividades.

•Los foros por medio de los cuales el Equipo Docente aclarará las dudas de carácter general y que se usarán también para comunicar todas aquellas novedades que surjan a lo largo del curso. Éste será el principal medio de comunicación entre los distintos participantes en la asignatura.

SISTEMA DE EVALUACIÓN

TIPO DE PRUEBA PRESENCIAL

Tipo de examen	Examen tipo test
Preguntas test	20
Duración del examen	120 (minutos)

Material permitido en el examen

Ninguno

Criterios de evaluación

La prueba presencial consistirá en un test de 20 preguntas a realizar en un tiempo máximo de 2 horas. Para cada pregunta del test se propondrán 3 ó4 respuestas de las que sólo una será correcta. Únicamente puntuarán las respuestas contestadas. Si la respuesta es correcta la puntuación será de 0.5 puntos y si es incorrecta restará 0.2 puntos. Durante la realización de la prueba no se podrá utilizar ningún tipo de material. La prueba presencial se realizará en el Centro Asociado que corresponda a cada estudiante, en las fechas y horarios establecidos por la UNED.

% del examen sobre la nota final	50
Nota del examen para aprobar sin PEC	
Nota máxima que aporta el examen a la calificación final sin PEC	
Nota mínima en el examen para sumar la PEC	

Comentarios y observaciones

El examen se debe aprobar (un cinco) con independencia de la parte préctica (PECs y evaluaciones con video)

CARACTERÍSTICAS DE LA PRUEBA PRESENCIAL Y/O LOS TRABAJOS

Requiere Presencialidad	Si

Descripción

La prueba presencial consistirá en un test de 20 preguntas a realizar en un tiempo máximo de 2 horas. Para cada pregunta del test se propondrán 3 ó4 respuestas de las que sólo una será correcta. Únicamente puntuarán las respuestas contestadas. Si la respuesta es correcta la puntuación será de 0.5 puntos y si es incorrecta restará 0.2 puntos. Durante la realización de la prueba no se podrá utilizar ningún tipo de material. La prueba presencial se realizará en el Centro Asociado que corresponda a cada estudiante, en las fechas y horarios establecidos por la UNED.

Criterios de evaluación

Ponderación de la prueba presencial y/o los trabajos en la nota final	
Fecha aproximada de entrega	

Comentarios y observaciones

PRUEBAS DE EVALUACIÓN CONTINUA (PEC)

¿Hay PEC? Si,PEC no presencial

Descripción

Hay dos PECs, asociadas a los temas 1 y 5.

Criterios de evaluación

Ponderación de la PEC en la nota final: La PEC1 (Tema 1) tiene una ponderación del 15 % en la nota final, mientras que la PEC2 (Tema 5) tiene una ponderación del 30%. En total suman el 45% de la nota

Fecha aproximada de entrega

Comentarios y observaciones

Las PECs se calificarán de 1 a 10 puntos, siendo el 10 la máxima puntuación. Se deben superar por separado cada una de las PECs para que se contabilicen en la nota final para poder aprobar la asignatura (esto es, hay que sacar en cada una al menos un 5)

OTRAS ACTIVIDADES EVALUABLES

¿Hay otra/s actividad/es evaluable/s? Si,no presencial

Descripción

Por cada tema, el estudiante deberá realizar una grabación de 5 minutos como máximo (2 minutos mínimo) de una temática que se explicitará en el curso virtual sobre un apartado/herramienta del tema. Habra cinco pruebas de este tipo, una por cada tema del contenido de la asignatura

Criterios de evaluación

Cada grabación se evaluará con un 1% de peso y en este caso, la evaluación de la grabación será APTO o no APTO (es decir, no habrá puntuación asignada). Se valorarán las siguientes características:

Conocimiento de la temática

Claridad de la exposición

Sintesis del contenido

Calidad de la presentación

Se deberán superar (es decir, ser calificadas como APTAS) al menos tres grabaciones para que se puedan ponderar en la nota final todas las calificaciones de las grabaciones.

Ponderación en la nota final: Las grabaciones realizadas por los estudiantes concentran el 5% de la nota

Fecha aproximada de entrega

Comentarios y observaciones

¿CÓMO SE OBTIENE LA NOTA FINAL?

La nota final se calcula con la siguiente fórmula:
Nota Final = 50% NE + 45% NPECS + 5% NGRABS
donde NE es Nota del examen (de 0 a 10), NPECS es nota de las dos PECS (de 0 a 10 cada una) y NGRABS es la nota total de las cinco grabaciones.
Se deben aprobar por separado el examen y las dos PECs. Adicionalmente, se aplica el criterio especificado para aprobar la parte de las grabaciones. Esto es, al menos se deben haber aprobado (APTO) tres de ellas.

BIBLIOGRAFÍA BÁSICA

ISBN(13):9780124172166
Título:APPLIED NETWORK SECURITY MONITORING
Autor/es:Jason Smith ; Chris Sanders ;
Editorial:SYNGRESS

ISBN(13):9781491962848
Título:NETWORK SECURITY THROUGH DATA ANALYSIS (2nd Edition)
Autor/es:Michael Collins ;
Editorial:O'Reilly Media

ISBN(13):9781593278021
Título:PRACTICAL PACKET ANALYSIS, 3RD EDITION
Autor/es:Chris Sanders ;
Editorial:No starch Press

La bibliografía básica está compuesta por material proporcionado al estudiante dentro del curso virtual, junto a apartados específicos de la bibliografía recomendada (básica y complementaria). Dada la variedad de temas que se incluyen en la asignatura, es necesario usar los libros especificados. En cualquier caso, estos libros están disponibles en línea desde los recursos de libros electrónicos de la biblioteca de la UNED en Learning O'Really (https://learning.oreilly.com/), por lo que están disponibles de manera gratuita para loos estudiantes de la asignatura.
Gran parte de la bibliografía, así como los recursos proporcionados al estudiante en el curso virtual pueden estar únicamente en inglés, debido a la novedad de algunos de los contenidos propuestos para la asignatura.

BIBLIOGRAFÍA COMPLEMENTARIA

ISBN(13):9780128038437
Título:COMPUTER AND INFORMATION SECURITY HANDBOOK (3rd Edition)
Autor/es:John R. Vacca ;
Editorial:MORGAN KAUFMANN

ISBN(13):9781491979907
Título:MACHINE LEARNING AND SECURITY
Autor/es:Clarence Chio ; David Freeman ;
Editorial:O'Reilly Media, Inc.

ISBN(13):9781789138399
Título:PRACTICAL LINUX SECURITY COOKBOOK (Second Edition)
Autor/es:Tajinder Kalsi ;
Editorial:Packt Publishing

RECURSOS DE APOYO Y WEBGRAFÍA

Los/as estudiantes dispondrán de los siguientes recursos de apoyo al estudio:

- **Guía de la asignatura.** Incluye el plan de trabajo y orientaciones para su desarrollo. Esta guía será accesible desde el curso virtual.
- **Curso virtual.** A través de esta plataforma los/as estudiantes tienen la posibilidad de consultar información de la asignatura, realizar consultas al Equipo Docente a través de los foros correspondientes, consultar e intercambiar información con el resto de los compañeros/as.
- **Biblioteca.** El estudiante tendrá acceso tanto a las bibliotecas de los Centros Asociados como a la biblioteca de la Sede Central, en ellas podrá encontrar un entorno adecuado para el estudio, así como de distinta bibliografía que podrá serle de utilidad durante el proceso de aprendizaje. Además, desde la biblioteca digital de la UNED, el estudiante tendrá acceso a Safari Books Online, una biblioteca digital con más de 30.000 libros técnicos en constante actualización.

ADENDA AL SISTEMA DE EVALUACIÓN CON MOTIVO DE LA PANDEMIA COVID 19

https://app.uned.es/evacaldos/asignatura/adendasig/31109025

IGUALDAD DE GÉNERO

En coherencia con el valor asumido de la igualdad de género, todas las denominaciones que en esta Guía hacen referencia a órganos de gobierno unipersonales, de representación, o miembros de la comunidad universitaria y se efectúan en género masculino, cuando no se hayan sustituido por términos genéricos, se entenderán hechas indistintamente en género femenino o masculino, según el sexo del titular que los desempeñe.