Guía docente
230993 - TMA - Monitorización y Análisis del Tráfico de Red

Última modificación: 08/06/2023

Unidad responsable: Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona
Unidad que imparte: 701 - DAC - Departamento de Arquitectura de Computadores.

Titulación: MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD (Plan 2020). (Asignatura obligatoria).

Curso: 2023 **Créditos ECTS:** 5.0 **Idiomas:** Inglés

PROFESORADO

Profesorado responsable: Consultar aquí / See here: https://telecos.upc.edu/ca/estudis/curs-actual/professorat-responsables-coordinadors/responsables-assignatura

Otros: Consultar aquí / See here: https://telecos.upc.edu/ca/estudis/curs-actual/professorat-responsables-coordinadors/professorat-assignat-idioma

CAPACIDADES PREVIAS

Conocimientos básicos de redes de computadores

METODOLOGÍAS DOCENTES

- Clases magistrales
- Clases de laboratorio practicas / Proyecto
- Trabajo en grupo (remoto)
- Trabajo individual (remoto)
- Presentaciones orales
- Control
- Examen final

OBJETIVOS DE APRENDIZAJE DE LA ASIGNATURA

Objetivos de aprendizaje de la asignatura:

El objetivo de esta asignatura es estudiar las principales técnicas, tecnologías y herramientas de monitorización y análisis del tráfico de red, y sus aplicaciones en el campo de la ciberseguridad. El curso revisará las principales estrategias para medir Internet (monitorización activa y pasiva), las técnicas utilizadas para la identificación del tráfico de aplicaciones y servicios (clasificación de tráfico), y los métodos de monitorización de la seguridad de red, como la detección y mitigación de ataques de denegación de servicio distribuidos (DDoS) utilizando técnicas de aprendizaje automático. La asignatura también abordará los principales retos técnicos relacionados con la monitorización de redes a consecuencia del incremento continuo de la velocidad de los enlaces y el volumen de tráfico. Finalmente, se discutirá sobre las implicaciones éticas y de privacidad de la monitorización del tráfico de red, y las regulaciones actuales sobre la materia, como el Reglamento General de Protección de Datos (RGPD) de la UE.

Resultados de aprendizaje de la asignatura:

- Entender los retos tecnológicos asociados a la monitorización y el análisis de tráfico de red, y los métodos necesarios para abordarlos.
- Entender y ser capaces de aplicar las herramientas y métodos existentes de monitorización de tráfico, clasificación de tráfico, y detección de ataques y anomalías.
- Entender las implicaciones éticas. sociales y legales relacionadas con la monitorización y el análisis de tráfico de red, y los mecanismos y regulaciones sobre protección de datos.

HORAS TOTALES DE DEDICACIÓN DEL ESTUDIANTADO

Tipo	Horas	Porcentaje
Horas grupo grande	26,0	20.80
Horas grupo pequeño	13,0	10.40
Horas aprendizaje autónomo	86,0	68.80

Dedicación total: 125 h

CONTENIDOS

Introducción

Descripción:
- Por qué medir Internet
- Retos de medir Internet
- Clasificación de las técnicas de monitorización
- Monitorización activa vs pasiva
- Comunidad TMA: Congresos, fórums, etc.
- Revisión de la arquitectura de Internet

Dedicación: 12h
Grupo grande/Teoría: 4h
Aprendizaje autónomo: 8h

Monitorización de red: Métodos y retos

Descripción:
- Monitorización a nivel de paquete: Libpcap
- Monitorización a nivel de flujo: NetFlow
- Algoritmos y estructuras de datos: Muestreo de tráfico, Bloom filters, Sketches
- Herramientas, repositorios e infraestructuras

Dedicación: 35h
Grupo grande/Teoría: 7h
Grupo pequeño/Laboratorio: 4h
Aprendizaje autónomo: 24h

Clasificación de tráfico de red

Descripción:
- Métodos basados en los números de puerto
- Métodos de inspección profunda de paquetes (DPI)
- Métodos de clasificación basados en Aprendizaje Automático

Dedicación: 26h
Grupo grande/Teoría: 5h
Grupo pequeño/Laboratorio: 3h
Aprendizaje autónomo: 18h

Monitorización de la seguridad de red

Descripción:
- Detección de anomalías
- Detección de intrusiones y ataques
- Métodos de detección basados en Aprendizaje Automático

Dedicación: 26h
Grupo grande/Teoría: 5h
Grupo pequeño/Laboratorio: 3h
Aprendizaje autónomo: 18h

Privacidad online e implicaciones éticas

Descripción:
- Implicaciones éticas i de privacidad de la monitorización de red
- Reglamento General de Protección de Datos (RGPD)
- Tracking online: Mecanismos, implicaciones y defensas

Dedicación: 26h
Grupo grande/Teoría: 5h
Grupo pequeño/Laboratorio: 3h
Aprendizaje autónomo: 18h

SISTEMA DE CALIFICACIÓN

Examen parcial: 20%
Examen final: 30%
Laboratorio / Proyecto: 40%
Participación: 10%

NORMAS PARA LA REALIZACIÓN DE LAS PRUEBAS.

Las clases de laboratorio (proyecto) se realizaran en grupos de 4 o 5 estudiantes.
Es necesario disponer como mínimo de un portátil por grupo.

BIBLIOGRAFÍA

Básica:
- Sanders, C.; Smith, J. Applied network security monitoring: collection, detection, and analysis [en línea]. Waltham, MA: Syngress, 2014 [Consulta: 15/07/2020]. Disponible a: https://www.sciencedirect.com/science/book/9780124172081. ISBN 9780124172081.
- Bejtlich, Richard. The Practice of network security monitoring: understanding incident detection and response [en línea]. San Francisco: No Starch Press, 2013 [Consulta: 02/07/2020]. Disponible a: https://ebookcentral.proquest.com/lib/upcatalunya-ebooks/detail.action?docID=1572876. ISBN 9781593275341.
- Crovella, M.; Krishnamurthy, B. Internet measurement: infrastructure, traffic, and applications. Chichester: John Wiley & Sons, 2006. ISBN 047001461X.

Complementaria:
- Kurose, James F; Ross, Keith W. Computer networking : a top-down approach [en línea]. 7th ed. Boston (Mass.) ; London ; Paris [etc.]: Pearson, cop. 2017 [Consulta: 08/02/2023]. Disponible a: https://ebookcentral.proquest.com/lib/upcatalunya-ebooks/detail.action?docID=5187270. ISBN 9781292153599.
- Bejtlich, Richard. The Tao of network security monitoring : beyond intrusion detection. Boston [etc.]: Addison-Wesley, cop. 2005. ISBN 9780321246776.