Universidad de Alcalá

Estudio Propio: **MÁSTER EN CIBERDEFENSA**

Código Plan de Estudios: **EH70**

Año Académico: **2022-2023**

ESTRUCTURA GENERAL DEL PLAN DE ESTUDIOS:

CURSO	Obligatorios		Optativos		Prácticas Externas	Memoria/ Proyecto	Créditos
	Créditos	Nº Asignaturas	Créditos	Nº Asignaturas	Créditos	Créditos	
1º	54	17				6	60
2º							
3º							
ECTS TOTALES	**54**	**17**				**6**	**60**

PROGRAMA TEMÁTICO:

ASIGNATURAS OBLIGATORIAS

Código Asignatura	Curso	Denominación	Carácter OB/OP	Créditos
702210	1	BASES DE CIBERSEGURIDAD	OB	3
702211	1	INTRODUCCIÓN A LA CIBERDEFENSA	OB	3
702212	1	ASPECTOS LEGALES, POLÍTICOS Y ÉTICOS DEL CIBERESPACIO	OB	3
702213	1	ASPECTOS DOCTRINALES. PLANEAMIENTO DE OPERACIONES	OB	3
702214	1	CIBERAMENAZAS A LA INFRAESTRUCTURAS CRÍTICAS	OB	3
702215	1	EXPERIMENTACIÓN EN CIBERDEFENSA (CD&E)	OB	3
702216	1	ANÁLISIS DE RIESGOS ESTÁTICO Y DINÁMICO	OB	3
702217	1	DETECCIÓN Y DEFENSA FRENTE A AMENAZAS CIBERNÉTICAS	OB	3
702218	1	RESPUESTA A INCIDENTES. ANÁLISIS FORENSE	OB	3
702219	1	ANÁLISIS DE MALWARE	OB	3
702220	1	RECUPERACIÓN Y ANÁLISIS DE DATOS	OB	3
702221	1	CONCIENCIA DE LA SITUACIÓN Y COMPARTICIÓN INFORMACIÓN	OB	3
702222	1	CIBERINTELIGENCIA Y FUENTES ABIERTAS	OB	3
702223	1	AMENAZAS AVANZADAS PERSISTENTES (APT'S)	OB	3
702224	1	HACKING ÉTICO	OB	6
702225	1	ATAQUES DE DENEGACIÓN DE SERVICIO	OB	3
702226	1	INGENIERÍA SOCIAL	OB	3

MEMORIA /PROYECTO

Código Asignatura	Curso	Denominación	Carácter OB/OP	Créditos
702227	1	TRABAJO FIN DE MÁSTER	OB	6

Carácter: OB - Obligatoria; OP – Optativa

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2022-2023	
Estudio	Máster en Ciberdefensa (EH70)	
Nombre de la asignatura	BASES DE CIBERSEGURIDAD	
Carácter (Obligatoria/Optativa)	OB	
Créditos (1 ECTS=25 horas)	3	
Modalidad (elegir una opción)		Presencial
		Semipresencial
	x	On-line
Profesor responsable	Bernardo Alarcos Alcázar	
Idioma en el que se imparte	Español	

DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)	
Número de horas presenciales/on-line asistencia profesor	30
Número de horas de trabajo personal del estudiante	45
Total horas	75

CONTENIDOS (Temario)

UD1. INTRODUCCIÓN A LA CRIPTOGRAFÍA

- Criptografía Clásica.
- Criptografía de Clave Simétrica.
- Criptografía de Clave Asimétrica.
- Criptografía Cuántica.

UD2. MECANISMOS CRIPTOGRÁFICOS

- Introducción a los sistemas criptográficos.
- Funciones Hash.
- Firma digital.
- Infraestructuras de clave pública.
- Funciones HMAC.
- Protocolos de autenticación.

UD3. APLICACIONES CRIPTOGRÁFICAS

- Comercio Electrónico.
- Redes Privadas Virtuales (VPN).
- Correo Electrónico Seguro.
- Seguridad en la Web.
- Establecimiento de sesiones seguras.
- Seguridad WIFI.

EVALUACIÓN

La evaluación de los alumnos se realiza teniendo en cuenta las siguientes valoraciones:

- Unidades Didácticas: 70% de la nota total de la asignatura. Controles de seguimiento conformados por una sala de debate, un test por cada unidad y un caso práctico por cada unidad
- Examen Final: 30% de la nota total de la asignatura.

BIBLIOGRAFÍA

Enlaces

1. Kriptopolis. http://www.kriptopolis.com/
   - Web dedicado a la criptografía en donde podrás mantenerte actualizado de los avances en este campo.
2. Hispasec. http://www.hispasec.com/
   - Web dedicado a la seguridad en general en donde puedes mantenerte actualizado sobre nuevas vulnerabilidades y noticias relacionadas con la seguridad.

Lecturas complementarias

1. Algoritmo AES (Anexo I de la Unidad I)
   - Descripción detallada del algoritmo AES.
2. Métodos de cifrado simétrico. (Anexo II de la Unidad I)
   - Descripción sobre las formas de usar los algoritmos simétricos, es necesario conocerlos para saber cuándo se requiere el uso de vector de inicialización en un algoritmo.
3. Intercambio de clave de Diffie Helmann. (Anexo III de la Unidad I)
   - Descripción detallada del funcionamiento de estos mecanismos para intercambiar un valor secreto.
4. Algoritmo RSA. (Anexo IV de la Unidad I).
   - Descripción detallada del algoritmo de clave simétrica más utilizado, el algoritmo RSA.
5. Criptografía basada en Curvas Elípticas. (Anexo V de la Unidad I).
   - Descripción detallada de los algoritmos basados en curvas elípticas y su uso y ventajas en la criptografía.

Bibliografía recomendada y complementaria

En la Unidad se hace referencias a bibliografía, que permite ampliar los conceptos tratados en el lugar de la referencia.

Laboratorio de criptografía

Se aconseja usar las herramientas didácticas cryptools versión 1 y 2 para hacer prácticas sobre los algoritmos criptográficos clásicos y modernos y poder usar herramientas de criptoanálisis.
https://www.cryptool.org/en/

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2022-2023	
Estudio	Máster en Ciberdefensa (EH70)	
Nombre de la asignatura	INTRODUCCIÓN A LA CIBERDEFENSA	
Carácter (Obligatoria/Optativa)	OB	
Créditos (1 ECTS=25 horas)	3	
Modalidad (elegir una opción)		Presencial
		Semipresencial
	x	On-line
Profesor responsable	Ángel Gómez de Ágreda	
Idioma en el que se imparte	Español	

DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)	
Número de horas presenciales/on-line asistencia profesor	30
Número de horas de trabajo personal del estudiante	45
Total horas	75

CONTENIDOS (Temario)

UD1. EL CIBERESPACIO
- Introducción
- Definición y características
- El ciberespacio como escenario social y geoestratégico

UD2. CIBERSEGURIDAD Y CIBERDEFENSA
- Conceptos y estrategias.
- Amenazas en y desde el ciberespacio.

UD3. CIBERDEFENSA
- Conflicto en el ciberespacio.
- Aproximaciones internacionales a la ciberdefensa.
- Prospectiva sobre una posible evolución del ciberespacio.

EVALUACIÓN

La evaluación de los alumnos se realiza teniendo en cuenta las siguientes valoraciones:
- Unidades Didácticas: 70% de la nota total de la asignatura. Controles de seguimiento conformados por una sala de debate, un test por cada unidad y un caso práctico por cada unidad
- Examen Final: 30% de la nota total de la asignatura.

BIBLIOGRAFÍA

Enlaces
Asociación de Diplomados en Altos Estudios de la Defensa Nacional. Antiguos alumnos del CESEDEN.
http://adalede.org/videoteca/videos-adalede/
"Cybersecurity" and Why Definitions Are Risky
http://isnblog.ethz.ch/intelligence/cybersecurity-and-the-problem-of-definitions

Cyber Security by the Numbers
http://www-935.ibm.com/services/us/en/security/infographic/cybersecurityindex.html?goback=%2Egde_1836487_member_580014770544340173 0#%21
La mano que mueve el ratón
http://revistasic.es/index.php?option=com_content&view=article&id=837&Itemid=820
Documento de opinión: Ciberespacio
http://www.ieee.es/contenido/noticias/2013/06/DIEEEO57-2013.html
La ciberseguridad: un riesgo, pero también una garantía para la libertad
http://abcblogs.abc.es/ley-red/public/post/la-ciberseguridad-un-riesgo-pero-tambien-una-garantia-para-la-libertad-15860.asp/
Cybersecurity: Authoritative Reports and Resources, by Topic
http://www.fas.org/sgp/crs/misc/R42507.pdf

Lecturas complementarias
Monografías del CESEDEN
http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/126_EL_CIBERESPACIO_NUEVO_ESCENARIO_DE_CONFRONTACION.pdf
El ciberespacio como entorno social y de conflicto
http://www.ieee.es/Galerias/fichero/docs_opinion/2012/DIEEEO17_CiberespacioConflicto_Agreda.pdf
Why Cibersecurity must be defined by processs, not tech
http://blogs.wsj.com/cio/2014/12/11/why-cybersecurity-must-be-defined-by-process-not-tech/
Miradas sobre el control de nuestras vidas: Huxley y Orwell
https://www.youtube.com/watch?v=vqTiSXnWD90, http://ssociologos.com/2013/10/18/miradas-sobre-el-control-de-nuestras-vidas-huxley-y-orwell/
IV Jornadas de Estudios de Seguridad
http://iugm.es/publicaciones/colecciones/libros-investigacion/?id=142
Center on Public Diplomacy
http://uscpublicdiplomacy.org/blog/hacking-diplomacy
Geopolíticas en la nube
http://www.blog.rielcano.org/el-espectador-global-geopolitica-en-la-nube/
The Strategic Significance of the Internet Commons
http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?lng=en&id=182692

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2022-2023	
Estudio	Máster en Ciberdefensa (EH70)	
Nombre de la asignatura	ASPECTOS LEGALES, POLÍTICOS Y ÉTICOS DEL CIBERESPACIO	
Carácter (Obligatoria/Optativa)	OB	
Créditos (1 ECTS=25 horas)	3	
Modalidad (elegir una opción)		Presencial
		Semipresencial
	x	On-line
Profesor responsable	Ángel Gómez de Ágreda	
Idioma en el que se imparte	Español	

DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)	
Número de horas presenciales/on-line asistencia profesor	30
Número de horas de trabajo personal del estudiante	45
Total horas	75

CONTENIDOS (Temario)

UD1. ASPECTOS ÉTICOS, POLÍTICOS Y JURÍDICOS DEL CIBERESPACIO

- Introducción.
- Ética y Ciberespacio.
- Política y Ciberespacio.

UD2. ASPECTOS JURÍDICOS DE DERECHO NACIONAL

- La normativa sobre Ciberseguridad.
- El estado de la cooperación sobre ciberseguridad.
- La normativa española sobre ciberseguridad.

UD3. ASPECTOS JURÍDICOS DE DERECHO INTERNACIONAL

- El principio de prohibición del uso y de la amenaza de la fuerza.
- El derecho internacional de los conflictos armados.

EVALUACIÓN

La evaluación de los alumnos se realiza teniendo en cuenta las siguientes valoraciones:

- Unidades Didácticas: 70% de la nota total de la asignatura. Controles de seguimiento conformados por una sala de debate, un test por cada unidad y un caso práctico por cada unidad
- Examen Final: 30% de la nota total de la asignatura.

BIBLIOGRAFÍA

Enlaces

- BARRET JR., Barrington M., “Information Warfare: China’s Response to U.S. Technological Advantages”, International Journal of Intelligence and Counterintelligence 18, número 4 (2005), páginas 682–706.

http://www.tandfonline.com/doi/abs/10.1080/08850600500177135

- BUCKLAND, Benjamin, "Democratic Governance Challenges of Ciber Security", DCAF, 2015.
http://www.dcaf.ch/Publications/Democratic-Governance-Challenges-of-Cyber-Security
- COOK, Tim, "A message to our custormers", 16/02/2016, web de Apple:
http://www.apple.com/customer-letter/
- DEIBERT, Ronald, "The growing dark side of cyberspace", Penn State Journal of Law and International Affairs, volumen 1, tomo 2, noviembre de 2012.
http://elibrary.law.psu.edu/cgi/viewcontent.cgi?article=1012&context=jlia
- FORSYTH, James W. y POPE, B., "Structural Causes and Cyber Effects. Why International Order is Inevitable in Cyberspace", Strategic Studies Quarterly, número de invierno de 2014.
http://www.au.af.mil/au/ssq/digital/pdf/winter_14/forsyth.pdf
- GARCÍA MEXÍA, Pablo, "Internet: el nuevo campo de batalla", Foro de la sociedad civil,
http://www.forosociedadcivil.org/internet-el-nuevo-campo-de-batalla-pablo-garcia-mexia/
- GARCÍA MEXÍA, Pablo, "La Ley en la Red", Blog de ABC.es.
http://abcblogs.abc.es/ley-red/
- International Strategy for Cyberspace,
https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
- JESCHKE, Rebecca, "EFF to Apple Shareholders: Your Company Is Fighting for All of Us", Electronic Frontier Foundation, 26/02/2016:
https://www.eff.org/es/deeplinks/2016/02/eff-apples-shareholders-meeting-statement-support
- KRUGER, L.G., "Internet governance and Developing countries: implications for India". RIS Policy Brief, núm. 63, marzo de 2014.
http://www.ris.org.in/sites/default/files/pdf/RIS%20Policy%20Brief-63.pdf
- KRUGER, L.G., "Internet governance and domain names system. Issues for Congress", Congressional Research Service, 23 de marzo de 2016.
https://www.fas.org/sgp/crs/misc/R42351.pdf
- LERIG, Lawrence, "Code", versión 2.0.
http://codev2.cc/download+remix/Lessig-Codev2.pdf
- LESSIG, Lawrence, "El código y otras leyes del ciberespacio", Taurus Digital, 2001.
http://www.nodo50.org/lecturas/lessig_el_codigo.htm
- LEWIS, J.A., "Internet Governance: Inevitable Transitions", CIGI (Center for International Governance Innovation), paper número 4, octubre de 2013.
https://www.cigionline.org/publications/2013/10/internet-governance-inevitable-transitions
- MAZANEC, B., "Why International Order in Cyberspace Is Not Inevitable", Strategic Studies Quarterly, verano de 2015.
http://www.au.af.mil/au/ssq/digital/pdf/Summer_2015/mazanec.pdf
- PERRY BARLOW, John, "A Declaration of Independence of Cyberspace". 8 de febrero de 1996. Disponible en
https://www.eff.org/es/cyberspace-independence
- SÁNCHEZ DE ROJAS, Emilio, "Cooperación internacional en temas de ciberseguridad", capítulo 5 de la Monografía 137 del CESEDEN "Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa, un reto prioritario", página 262. Publicaciones de Defensa, 2013, ISBN 978-84-9781-862-9Consultado el 22 de marzo de 2016.
http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/137_NECESIDAD_DE_UNA_CONCIENCIA_NACIONAL_DE_CIBERSEGURIDAD_LA_CIBERDEFENSA_UN_RETO_PRIORITARIO.pdf
- Sentencia del TJUE sobre el "Derecho al olvido".
http://www.abogacia.es/wp-content/uploads/2014/05/Sentencia-131-12-TJUE-derecho-al-olvido.pdf
- SINGH, Parminder Jeet, “India’s Proposal Will Help Take the Web out of U.S. Control,” Hindu Online, 17 de mayo de 2012,
http://www.thehindu.com/opinion/op-ed/article3426292.ece
- YANAKOGEORGOS, Panayotis A., "Internet governance and National Security", Strategic Studies Quarterly, volumen 6, número 3, otoño de 2012,

http://www.au.af.mil/au/ssq/2012/fall/yannakogeorgos.pdf

Bibliografía recomendada y complementaria

- LIBICKI, Martin, "Conquest in Cyberspace", New York, Cambridge University Press, 2007
- WU, Tim, "The Master Switch: The Rise and Fall of Information Empires", New York, Alfred A. Knopf, 2010, ISBN 978-0307390998
- ABBATE, Janet, "Inventing the Internet", The MIT Press, 1999, ISBN 9780262011723

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2022-2023	
Estudio	Máster en Ciberdefensa (EH70)	
Nombre de la asignatura	ASPECTOS DOCTRINALES. PLANEAMIENTO DE OPERACIONES	
Carácter (Obligatoria/Optativa)	OB	
Créditos (1 ECTS=25 horas)	3	
Modalidad (elegir una opción)		Presencial
		Semipresencial
	x	On-line
Profesor responsable	Javier Lopez de Turiso y Sánchez	
Idioma en el que se imparte	Español	

DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)	
Número de horas presenciales/on-line asistencia profesor	30
Número de horas de trabajo personal del estudiante	45
Total horas	75

CONTENIDOS (Temario)

UD1. EL CIBERESPACIO COMO ENTORNO OPERATIVO
- Introducción a los instrumentos de poder de los estados.
- El instrumento de poder militar.
- El campo de batalla operativo: el ciberespacio.
- Conceptos del empleo militar en el ciberespacio.
- Doctrinas de empleo del poder militar en el ciberespacio

UD2. CAPACIDADES DE LA CIBERDEFENSA
- Capacidades requeridas para operar en el ciberespacio.
- Fuerzas de ciberdefensa. Estructura y organización.

UD3. OPERACIONES MILITARES EN EL CIBERESPACIO
- Operaciones en el ciberespacio. Carácter estratégico, operacional y táctico.
- Operaciones específicas, conjuntas y combinadas (necesidad de autoridad de control del CS).
- Guerra electrónica y ciberespacio.
- Planeamiento de operaciones en el ciberespacio.

EVALUACIÓN

La evaluación de los alumnos se realiza teniendo en cuenta las siguientes valoraciones:
- Unidades Didácticas: 70% de la nota total de la asignatura. Controles de seguimiento conformados por una sala de debate, un test por cada unidad y un caso práctico por cada unidad
- Examen Final: 30% de la nota total de la asignatura.

BIBLIOGRAFÍA

Cyber Doctrine Towards a coherent evolutionary framework for learning resilience
JP MacIntosh, J Reid and LR Tyler

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2022-2023	
Estudio	Máster en Ciberdefensa (EH70)	
Nombre de la asignatura	CIBERAMENAZAS A LA INFRAESTRUCTURAS CRÍTICAS	
Carácter (Obligatoria/Optativa)	OB	
Créditos (1 ECTS=25 horas)	3	
Modalidad (elegir una opción)		Presencial
		Semipresencial
	x	On-line
Profesor responsable	Manuel Sánchez Rubio	
Idioma en el que se imparte	Español	

DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)	
Número de horas presenciales/on-line asistencia profesor	30
Número de horas de trabajo personal del estudiante	45
Total horas	75

CONTENIDOS (Temario)

UD1. INTRODUCCIÓN A LAS INFRAESTRUCTURAS CRÍTICAS

- Concepto de Infraestructuras críticas y Sistemas de Control Industrial.
- Tipos de Sistemas de Control Industrial (ICS).
- Sistemas SCADA.
- Características de las redes de comunicaciones para el control de infraestructuras críticas.

UD2. AMENAZAS A LAS INFRAESTRUCTURAS CRÍTICAS Y DE CONTROL INDUSTRIAL

- Análisis de vulnerabilidades de las infraestructuras críticas, desde el punto de vista de ciberdefensa.
- Análisis de las amenazas y ciberataques a las infraestructuras críticas.

UD3. CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS Y DE CONTROL INDUSTRIAL

- Organismos que elaboran guías de ciberseguridad para infraestructuras críticas.
- Guías de buenas prácticas para ciberseguridad de infraestructuras críticas.

EVALUACIÓN

La evaluación de los alumnos se realiza teniendo en cuenta las siguientes valoraciones:

- Unidades Didácticas: 70% de la nota total de la asignatura. Controles de seguimiento conformados por una sala de debate, un test por cada unidad y un caso práctico por cada unidad
- Examen Final: 30% de la nota total de la asignatura.

BIBLIOGRAFÍA

Enlaces

1. Blog de Seguridad Informática del sitio Segu-Info. Categoría infraestructuras críticas en Seguridad Informática.

https://seguinfo.wordpress.com/category/infraestructuras-criticas/page/3/

2. Portal CCN- CERT. Portal de Equipo de Respuesta a Incidentes del Centro Criptológico Nacional (CCN) del Gobierno de España, que incluye secciones sobre vulnerabilidades, contiene guías de bastionado de todo tipo de software en idioma español, herramienta de análisis de riesgo Pilar, herramientas, etc. Se incluye otro enlace del sitio web relacionado específicamente con las infraestructuras críticas.

https://www.ccn-cert.cni.es/

3. Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) del Gobierno de España. Es el órgano que se encarga de impulsar, coordinar y supervisar todas las actividades que tiene encomendadas la Secretaría de Estado de Seguridad del Ministerio del Interior en relación con la protección de las infraestructuras críticas españolas. Permite la descarga de guías de protección de sistemas SCADA del CCN en idioma español.

http://www.cnpic.es/Ciberseguridad/4_Guias_Scada/index.html

4. Centre for the Protection of National Infrastructure (CNPI). Organismo del Reino Unido encargado de prestar asesoramiento de seguridad en todo lo relativo a la protección de las IC en materia de seguridad física, personal y lógica. Tiene disponible la descarga de guías de protección de las IC.

http://www.cpni.gov.uk/about/

Lecturas complementarias

1. El Puesto del Operador: Guía básica de protección de Infraestructuras Críticas
    - Destinada a operadores de infraestructuras críticas, la guía tiene como fin fundamental introducir los procedimientos y herramientas esenciales para mejorar la seguridad de los sistemas informáticos que componen las infraestructuras críticas. En la guía se indican normas de buenas prácticas para proteger equipos individuales y el acceso a servicios, como la limitación de los privilegios y servicios a los mínimos necesarios, implantación de políticas de actualización o creación de snapshots con las configuraciones de seguridad. Incluyendo, por supuesto, la necesidad de incorporar medidas antimalware y procedimientos de backup robustos. Además, se hace énfasis en la especial atención requerida en los entornos legacy y en los equipos móviles.
    - https://www.incibe.es/extfrontinteco/img/File/intecocert/ManualesGuias/int_cnpic_proteccion_puesto_operador.pdf
2. Design and Operational Guide to Protect Against "Advanced Persistent Threats", Noviembre 2011.
    - Interesante documento que explica la realidad de las “Advanced Persistent Threats" y cómo diseñar y operar redes y sistemas para contrarrestarlas.
    - http://www.ipa.go.jp/files/000017299.pdf
3. Seguridad de los sistemas de monitorización y control de procesos e infraestructuras (SCADA).
    - Guía que pretende aportar la información necesaria para comprender estos riesgos y concienciar a las empresas que consideren y afronten adecuadamente la seguridad de este tipo de sistemas. En esta Guía se señalan las principales características y beneficios de los SCADA, y los aspectos a tener en cuenta en su implantación y gestión, así como algunas de las soluciones a incorporar para prevenir los riesgos y mitigar los incidentes de seguridad. Del mismo modo, se incluyen una serie de recomendaciones para los distintos actores implicados.
    - http://www.inteco.es/CERT/guias_estudios/guias/Guia_SCADA
4. Centro Criptológico Nacional. Guía 480 SCADA - Seguridad en sistemas SCADA.
    - Presentar la problemática planteada por los sistemas SCADA y sus vulnerabilidades, su impacto y la necesidad imperativa de controlar su seguridad.
    - https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/480-SCADA/480-Seguridad_sistemas_SCADA-mar10.pdf

Vídeos recomendados y complementarios

1. Protección de infraestructuras críticas en España
    - Presentación del Director del Centro de Protección de Infraestructuras críticas y el Jefe de la Sección Internacional sobre la Experiencia en la Protección de recursos informáticos y tecnológicos en el Sector Público en el modelo español de atención e Infraestructura Crítica.

https://www.youtube.com/watch?v=UdmiwC88OJg

2. Critical Infrastructure Protection
    - Robert Stephan es el Subsecretario de Protección de la Infraestructura en el Departamento de Seguridad Nacional realiza una presentación sobre la protección de las IC.

https://www.youtube.com/watch?v=vNozc0cuRJ8

3. Cyber and Physical Threats to Critical Infrastructure" by Tom Finan

    - Tom Finan, analista senior de Cibereguridad y Abogado de DHS NPPD, presenta "Cyber y amenazas físicas a infraestructuras críticas: Un Enfoque Integral sobre Riesgos de las TIC en las IC.

https://www.youtube.com/watch?v=zrED6ObqFzc5

4. Cybersecurity and Critical Infrastructure
    - La ciberseguridad debe abordar amenazas complejas e interconectadas de los ataques cibernéticos en los diversos sectores de las Infraestructuras Críticas: robo datos clasificados, ciberespionaje, ciberguerra y ciberterrorismo. En el video se plantea cuestiones de política y legalidad, incluyendo s propuestas eficaces en los ámbitos de la autoridad reguladora, intercambio de información y responsabilidad de protección, y preservación de la libertad y privacidad en Internet. Este panel se realizó durante el Simposio de Seguridad Nacional de 2012.

https://www.youtube.com/watch?v=14IcYscHomo

5. Los países se preparan para defenderse de una guerra cibernética http://www.rtve.es/alacarta/videos/reporteros-del-telediario/reporteros-del-telediario-paises-se-preparan-para-defenderse-guerra-cibernetica/874432/

Bibliografía recomendada y complementaria

1. Monografía 126 CESDEN “El Ciberespacio. Nuevo Escenario de Confrontación. Año 2012
    - La Monografía se orienta principalmente hacia aspectos relacionados con la ciberdefensa considerada como una cuestión básicamente militar, en el sentido de que se interesa por facetas que involucran a instituciones, organizaciones o profesiones militares, en todo o en parte. No considera sin embargo, al menos explícita y detalladamente, otros aspectos también importantes para el ciudadano, como el robo de datos personales, el ciberdelito económico, etc., y otros, seguramente de interés nacional general, como el ciberespionaje industrial o el uso malicioso de otras herramientas «corrientes» de Internet, como redes sociales, blogs o simples portales web (o medios de comunicación on-line) para hacer apología extremista o sembrar dudas de confianza o reputación de una economía, una nación, una empresa, etc..
    - http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/126_EL_CIBERESPACIO_NUEVO_ESCENARIO_DE_CONFRONTACION.pdf
2. Identificación y reporte de incidentes de seguridad para operadores estratégicos: Guía básica de protección de Infraestructuras Críticas.
    - Esta guía está destinada a servir como manual de actuación a la hora de gestionar y reportar incidentes de seguridad en Infraestructuras Críticas.

- https://www.incibe.es/CERT/guias_estudios/guias/INTECO_publica_guia_reporte_incidentes_IICC

3. Centro Criptológico Nacional. Guía 480A SCADA - Guía de buenas prácticas.
   - Obtener una profunda comprensión de los riesgos a los que se enfrenta el negocio de las amenazas de los sistemas de control de procesos con el fin de identificarlos y conducirlos al nivel adecuado de protección de seguridad que se requiere.
   - http://www.cnpic.es/Ciberseguridad/4_Guias_Scada/index.html
4. Centro Criptológico Nacional. Guía 480B SCADA - Comprender el riesgo de negocio.
   - Basándose en los fundamentos explicados en la guía de CCN-STIC-480A proporciona orientación para estudiar el riesgo del negocio y el estudio continuo de este riesgo.
   - http://www.cnpic-es.es/Ciberseguridad/4_Guias_Scada/index.html
5. Centro Criptológico Nacional. Guía 480C SCADA - Implementar una arquitectura segura.
   - Basándose en los fundamentos explicados en la CCN-STIC-480A proporciona orientación para decidir una arquitectura de seguridad adecuada para los sistemas de control de procesos.
   - http://www.cnpic-es.es/Ciberseguridad/4_Guias_Scada/index.html
   - pic-es.es/Ciberseguridad/4_Guias_Scada/index.html

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2022-2023	
Estudio	Máster en Ciberdefensa (EH70)	
Nombre de la asignatura	EXPERIMENTACIÓN EN CIBERDEFENSA (CD&E)	
Carácter (Obligatoria/Optativa)	OB	
Créditos (1 ECTS=25 horas)	3	
Modalidad (elegir una opción)		Presencial
		Semipresencial
	x	On-line
Profesor responsable	Fernando Llorente Santos	
Idioma en el que se imparte	Español	

DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)	
Número de horas presenciales/on-line asistencia profesor	30
Número de horas de trabajo personal del estudiante	45
Total horas	75

CONTENIDOS (Temario)

UD1. INTRODUCCIÓN AL CD&E
- Concepto desarrollo y experimentación.
- ¿Qué es un experimento?
- Retos para una experimentación eficaz.
- Modelos conceptuales ilustrativos.

UD2. METODOLOGÍA CD&E
- Pasos en un experimento individual.
- Estrategia de experimentación en Ciberdefensa.

UD3. EL CD&E APLICADO
- Métricas de medidas aplicadas a Ciberdefensa.
- Implantación de una unidad CD&E.
- Capture The Flag Contest aplicado a Ciberdefensa.

EVALUACIÓN

La evaluación de los alumnos se realiza teniendo en cuenta las siguientes valoraciones:
- Unidades Didácticas: 70% de la nota total de la asignatura. Controles de seguimiento conformados por una sala de debate, un test por cada unidad y un caso práctico por cada unidad
- Examen Final: 30% de la nota total de la asignatura.

BIBLIOGRAFÍA

1. Título: Developing Systems for Cyber Situational Awareness
   - Es un documento orientado a la concienciación de situación, que quiere concienciar de que el problema cibernético nos afecta a todos ignorarlo no nos va a dejar al margen.

Propone las líneas a seguir para implementar un sistema de concienciación situacional de Cyberdefensa (Cyber SA)
    - http://www.soc.southalabama.edu/~mcdonald/pubs/DevelopingSystemsForCyberSituationalAwareness.pdf
2. Título: Establishing Cyber Warfare Doctrine
    - Tecnología de la información ha alcanzado un nivel de desarrollo e integración en las sociedades modernas que le permite ser usado para dañar el bienestar de una nación. encontrareis ejemplos de ataques que se están produciendo y advierte que los gobiernos deben estar preparados para salvaguardar a la población de las consecuencias, que podrían derivar en un conflicto a gran escala
    - http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1123&context=jss

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2022-2023	
Estudio	Máster en Ciberdefensa (EH70)	
Nombre de la asignatura	ANÁLISIS DE RIESGOS ESTÁTICO Y DINÁMICO	
Carácter (Obligatoria/Optativa)	OB	
Créditos (1 ECTS=25 horas)	3	
Modalidad (elegir una opción)		Presencial
		Semipresencial
	x	On-line
Profesor responsable	Juan Ramón Bermejo Higuera	
Idioma en el que se imparte	Español	

DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)	
Número de horas presenciales/on-line asistencia profesor	30
Número de horas de trabajo personal del estudiante	45
Total horas	75

CONTENIDOS (Temario)

UD1. INTRODUCCIÓN AL ANÁLISIS Y GESTIÓN DEL RIESGO ESTÁTICO Y DINÁMICO

- Introducción al Análisis y gestión de Riesgos.
- Sistemas de Gestión de Seguridad de la Información.
- Metodologías de Análisis y gestión de Riesgos.
- Modelado de amenazas en Aplicaciones.

UD2. PROYECTOS DE ANÁLISIS Y GESTIÓN DE RIESGOS

- Proyectos de Análisis y gestión de Riesgos AARR.
- Herramienta PILAR.

UD3. ANÁLISIS Y GESTIÓN DEL RIESGO DINÁMICO (DRA)

- Introducción al Análisis y Gestión del riesgo dinámico.
- Arquitecturas y tecnologías DRA.
- DRA framework: Sistema CAESARS.

EVALUACIÓN

La evaluación de los alumnos se realiza teniendo en cuenta las siguientes valoraciones:

- Unidades Didácticas: 70% de la nota total de la asignatura. Controles de seguimiento conformados por una sala de debate, un test por cada unidad y un caso práctico por cada unidad
- Examen Final: 30% de la nota total de la asignatura.

BIBLIOGRAFÍA

Enlaces

1. SGSI: NIST RMF:
    - Risk management framework del NIST.

http://csrc.nist.gov/groups/SMA/forum/documents/Forum-121410-Continuous-Monitoring-AJohnson.pdf

2. SGSI: ISO 27001:
    - Portal en español de la ISO 27001

http://www.iso27000.es/sgsi.html

3. SGSI: ENS:
    - Esquema Nacional de Seguridad

http://ametic.es/sites/default/files//media/INTECO%20-%20Implantaci%C3%B3n%20del%20ENS.pdf
https://www.ccn-cert.cni.es/publico/ens/ens/index.html?n=2.html

4. GUÍA STIC 825 sobre el Esquema Nacional de Seguridad:
    - https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/543-ccn-stic-825-ens-iso27001/file.html

5. GUÍA STIC 801 Responsabilidades y funciones en el ENS:
    - https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/501-ccn-stic-801-responsibilidades-y-funciones-en-el-ens/file.html

6. MAGERIT. Ministerio de Administraciones Públicas de España MAP.
    - MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno. Actualizada en 2012 en su versión

http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VDUaiU0cTUA

7. STRIDE de Microsoft. Security Risk Management Guide, de Microsoft.
    - Método de modelado de amenazas de la empresa Microsoft.

http://www.microsoft.com/security/sdl/adopt/threatmodeling.aspx
http://www.microsoft.com/en-us/download/details.aspx?id=14719

8. OWASP thread modeling en aplicaciones web:

https://www.owasp.org/index.php/Application_Threat_Modeling
https://www.owasp.org/index.php/Modelado_de_Amenazas

9. Microsoft thread modeling en aplicaciones web:
    - https://msdn.microsoft.com/en-us/library/ff648644.aspx

10. Diversos métodos de modelado de amenazas en aplicaciones en comparación:
    - http://fortinux.com/wp-content/uploads/2010/12/Analisis-y-Modelado-de-Amenazas.pdf

11. Information Technology Baseline Protection Manual
    - Sitio web donde se puede encontrar catálogos de salvaguardas

http://en.wikipedia.org/wiki/IT_Baseline_Protection_Catalogs

12. ISO/IEC 13335-1:2004
    - Norma ISO donde se puede encontrar catálogos de salvaguardas.

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39066

13. BugTraq.
    - Foros de discusión de seguridad públicos sobre análisis de riesgos.

http://www.securityfocus.com/archive/1
http://catless.ncl.ac.uk/Risks

14. VulnWatch.
    - Listas de direcciones públicas de sistemas atacados

http://www.vulnwatch.org/

Lecturas complementarias

1. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I – Método. Ministerio de Hacienda y Administraciones Públicas.
   - Método de análisis de riesgos de MAGERIT.
   - http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.U2_oe2CKB2E.

2. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos. Método. Ministerio de Hacienda y Administraciones Públicas.
   - Catálogo de elementos de tipos de activos, dimensiones de valoración, criterios de valoración, dimensiones de valoración, amenazas, y salvaguardas.
   - http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.U2_oe2CKB2E.

3. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas. Método. Ministerio de Hacienda y Administraciones Públicas.
   - Describe algunas técnicas utilizadas en análisis y gestión de riesgos
   - http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.U2_oe2CKB2E.

4. Herramienta PILAR de análisis de riesgos de uso obligatorio en la Administración pública de España, y oficial en la OTAN (Organización del Tratado del Atlántico Norte).
   - Manual de usuario de la herramienta de análisis de riesgos PILAR
   - Herramienta de análisis de riesgos de la Administración pública del Estado. Español y oficial en la OTAN (Organización del Tratado del Atlántico Norte). Permite analizar los riesgos en varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad (accountability).
   - http://www.ar-tools.com/es/index.html
   - https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar/pilar.html

5. CIGITAL's architectural risk analysis process.
   - Método de análisis de riesgo arquitectónico para aplicaciones.

https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/architecture/10-BSI.html

6. ASSET (Automated Security Self-Evaluation Tool). National Institute on Standards and Technology (NIST).
   - Método de análisis de riesgos del NIST de los EEUU.

http://csrc.nist.gov/archive/asset/index.html

7. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation). SEI de la Universidad Carnegie Mellon.
   - Método de análisis de la Universidad Carnegie Mellon.

http://www.sei.cmu.edu/library/abstracts/reports/99tr017.cfm

8. CRAMM. CCTA Risk Analysis and Management Method.
   - Metodología de análisis de riesgos del Reino Unido
   - http://www.cramm.com/

9. Ron Ross, Stu Katzke, Arnold Johnson, Marianne Swanson, Gary Stoneburner, George Rogers. Guía NIST SP 800-53. Recommended Security Controls for Federal Information Systems.
   - Contiene un catálogo de salvaguardas.
   - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

10. NIST 800-30 rev1 Risk Management Guide for Information Technology Systems, 2012.
    - Guía del NIST para la realización de análisis de riesgos. 2012
    - http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

Vídeos recomendados y complementarios

1. Lección 11: Análisis y gestión de riesgos (intypedia)

- Video que indica los pasos que hay que seguir para realizar un correcto análisis de las amenazas a las que puede enfrentarse un sistema de información, su impacto y la consiguiente gestión de riesgos, recomendando algunas metodologías.

https://www.youtube.com/watch?v=EgiYIIJ8WnU

2. SGSI - 07 Los activos de Seguridad de la Información.
   - La implantación de un SGSI tiene como objetivo proteger la información, el activo más importante en una empresa. Para ello una de las tareas principales en su implantación es analizar las dependencias y la relevancia de los activos.

https://www.youtube.com/watch?v=THnQ2FH7NtU

3. SGSI - 08 Análisis y valoración de riesgos. Metodologías.
   - Video del INTECO. Un negocio debe hacer frente al análisis y valoración de riesgos a los que está expuesto. Esta tarea, aplicando las distintas metodologías, permitirá delimitar claramente las áreas que deben ser protegidas así como el impacto económico y la probabilidad realista de que ocurra un incidente de cada uno de ellos. También se realiza una demostración de los ataques populares.

https://www.youtube.com/watch?v=g7EPuzN5Awg

4. SGSI - 09 Gestión y tratamiento de los riesgos
   - Video del INTECO. A la hora de implantar un Sistema de Gestión de la Seguridad de la Información (SGSI) es necesario conocer en qué consiste la gestión de riesgos y cómo se deben escoger y documentar los controles que se van a aplicar.

https://www.youtube.com/watch?v=9T9X0q2y6vQ

5. SGSI - 10 Seguimiento, monitorización y registro de las operaciones de sistema.
   - Video del INTECO. Uno de los requisitos más importantes de la Norma UNE/ISO-IEC 27001 es la revisión que la dirección de la organización debe realizar con una cierta periodicidad, como mínimo anual, al Sistema de Gestión de Seguridad de la Información.

https://www.youtube.com/watch?v=Z5vaQn7bGhA

6. SGSI - 11 Gestión de la continuidad de negocio
   - Video del INTECO. Con el fin de no comprometer la actividad normal de una empresa se desarrollan diseños que constan de varias tareas encaminadas a la obtención de un plan de continuidad eficaz y viable que permita a la organización recuperarse tras un incidente.

https://www.youtube.com/watch?v=KbwhvivHNDI

7. SGSI - 12 Proceso de certificación.
   - Video del INTECO. Certificar un SGSI según la Norma UNE/ISO-IEC 27001 significa obtener un "Documento" que reconoce y avala la correcta adecuación del Sistema de Gestión de Seguridad de la Información mejorando la confianza de clientes y proveedores.

https://www.youtube.com/watch?v=OQCVpiVCR9k

8. Threat Modeling Tool 2014 Demo
   - Emil Karafezov explica las nuevas características de nueva herramienta de modelado de amenazas: Microsoft Modeling Tool 2014.

https://www.youtube.com/watch?v=G2reie1skGg

9. Threat Modeling Tool principles
   - Interesante vídeo sobre la herramienta de modelado de amenazas de Microsoft.

https://www.youtube.com/watch?v=wUt8gVxmO-0

Bibliografía recomendada y complementaria

1. Marta Castellaro, Susana Romaniz, Juan Carlos Ramos, Carlos Feck, Ivana Gaspoz. Aplicar el Modelo de Amenazas para incluir la Seguridad en el Modelado de Sistemas. Argentina, Universidad Tecnológica Nacional, Facultad Regional Santa Fe. Disponible: http://docplayer.es/1665552-Aplicar-el-modelo-de-amenazas-para-incluir-la-seguridad-en-el-modelado-de-sistemas.htmlmodelado-de-sistemas.html

2. Carlos Ignacio Feck. Modelado de Amenazas, una herramienta para el tratamiento de la seguridad en el diseño de sistemas. UTN – Facultad Regional Santa Fe. Disponible en: http://www.criptored.upm.es/cibsi/cibsi2009/docs/Papers/CIBSI-Dia2-Sesion3(2).pdf

3. Daniel P.F. Análisis y Modelado de Amenazas. Una revisión detallada de las metodologías y herramientas emergentes. Metal AT/DOT hacktimes.com. Año 2006. Disponible: https://fortinux.com/wp-content/uploads/2010/12/Analisis-y-Modelado-de-Amenazas.pdf

4. M. Castellaro, S. Romaniz, J.C. Ramos,C. Feck e I. Gaspoz, "Aplicar el Modelo de Amenazas para incluir la Seguridad en el Modelado de Sistemas", CIBSI, 2009.

5. A. Shostack, "Experiences Threat Modeling at Microsoft", Microsoft, 2008. Disponible: http://www.homeport.org/~adam/modsec08/Shostack-ModSec08-Experiences-Threat-Modeling-At-Microsoft.pdf

6. Presentación de Microsoft. Introduction to Microsoft® Security Development Lifecycle (SDL) Threat Modeling. Disponible: http://www.microsoft.com/en-us/download/details.aspx?id=16420

7. Gary McGraw. Software Security: Building Security In. Addison Wesley Professional. Año 2005. ISBN-10: 0-321-35670-5.

8. ISO/IEC 17799:2005 – 27002:2005. Code of practice for information security management

9. UNE 71502:2004. Especificaciones para los sistemas de gestión de la seguridad de la información

10. ISO/IEC 17799:2000 | UNE-ISO/IEC 17799:2002. Código de buenas prácticas para la Gestión de la Seguridad de la Información.

11. ISI/IEC 27000 (ISMS). Information technology – Security techniques – Information security management systems

    - 200x: 27000: Glossary [GMITS-1 y 2 – MICTS-1]
    - 2005: 27001: Requirements [BS 7799-2 – UNE 71502]
    - 2005: 27002: Code of practice for information security management [BS 7799-1 – 17799:2000 – UNE 17799:2002 – 17799:2005]
    - 200x: 27003: Implementation guidance
    - 200x: 27004: Measurements
    - 200x: 27005: Risk management
    - xxx: 27006 – 27009:

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2022-2023	
Estudio	Máster en Ciberdefensa (EH70)	
Nombre de la asignatura	DETECCIÓN Y DEFENSA FRENTE A AMENAZAS CIBERNÉTICAS	
Carácter (Obligatoria/Optativa)	OB	
Créditos (1 ECTS=25 horas)	3	
Modalidad (elegir una opción)		Presencial
		Semipresencial
	x	On-line
Profesor responsable	Iván Marsá Maestre	
Idioma en el que se imparte	Español	

DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)	
Número de horas presenciales/on-line asistencia profesor	30
Número de horas de trabajo personal del estudiante	45
Total horas	75

CONTENIDOS (Temario)

UD1. DEFENSA EN PROFUNDIDAD
- Introducción. Concepto de defensa en profundidad.
- Controles de Ciberdefensa.
- Vulnerabilidades y riesgos.
- Principios de diseño seguro.

UD2. MECANISMOS DE DETECCIÓN
- Introducción.
- Seguridad perimetral. Cortafuegos y proxies. Sistemas de DLP.
- Sistemas de detección de Intrusiones.
- Otras herramientas de detección: escáneres.

UD3. SISTEMAS SIEM
- Sistemas SIEM.
- Correlación de eventos.

EVALUACIÓN

La evaluación de los alumnos se realiza teniendo en cuenta las siguientes valoraciones:
- Unidades Didácticas: 70% de la nota total de la asignatura. Controles de seguimiento conformados por una sala de debate, un test por cada unidad y un caso práctico por cada unidad
- Examen Final: 30% de la nota total de la asignatura.

BIBLIOGRAFÍA

1. The Critical Security Controls for Effective Cyber Defense
   - Documento en el que se definen los controles de ciber defensa presentados en la UD.
   - https://www.sans.org/media/critical-security-controls/CSC-5.pdf

2. Agent-Based Modeling of User Circumvention of Security
    - Artículo sobre cómo los usuarios tienden a saltarse los mecanismos de seguridad que son "incómodos"
    - http://publish.illinois.edu/science-of-security-lablet/files/2014/05/Agent-Based-Modeling-of-User-Circumvention-of-Security.pdf
    - http://dl.acm.org/citation.cfm?id=2602948

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2022-2023	
Estudio	Máster en Ciberdefensa (EH70)	
Nombre de la asignatura	RESPUESTA A INCIDENTES. ANÁLISIS FORENSE	
Carácter (Obligatoria/Optativa)	OB	
Créditos (1 ECTS=25 horas)	3	
Modalidad (elegir una opción)		Presencial
		Semipresencial
	x	On-line
Profesor responsable	Manuel Martínez García	
Idioma en el que se imparte	Español	

DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)	
Número de horas presenciales/on-line asistencia profesor	30
Número de horas de trabajo personal del estudiante	45
Total horas	75

CONTENIDOS (Temario)

UD1. INTRODUCCIÓN A LA RESPUESTA A INCIDENTES Y AL ANÁLISIS FORENSE

- Introducción a los CSIRTs/CERTs.
- Estrategias de planificación y creación de un CSIRT.
- Introducción al Análisis Forense.
- Objetivos de un Análisis Forense.
- Etapas de un Análisis Forense.
- Aspectos jurídicos de la Informática Forense.

UD2. RECOLECTAR Y PRESERVAR

- Aspectos técnicos de la recolección de evidencias digitales.
- Tipos de evidencia y orden de volatilidad.
- Acotar la escena del crimen.
- Adquisición de evidencias.

UD3. ANÁLISIS Y PRESENTACIÓN

- Introducción a los Sistemas de Ficheros.
- Estructura e información de los archivos.
- Esquema general de un Análisis Forense.
- Artefactos de interés.
- Análisis de la memoria RAM.
- Estructura de un informe pericial.
- Redacción y conclusiones de un informe pericial.

EVALUACIÓN

La evaluación de los alumnos se realiza teniendo en cuenta las siguientes valoraciones:

- Unidades Didácticas: 70% de la nota total de la asignatura. Controles de seguimiento conformados por una sala de debate, un test por cada unidad y un caso práctico por cada unidad
- Examen Final: 30% de la nota total de la asignatura.

BIBLIOGRAFÍA

Enlaces de la UD

Servicio de seguridad de RedIRIS (IRIS-CERT). El servicio de seguridad de RedIRIS (IRIS-CERT) tiene como finalidad la detección de problemas que afecten a la seguridad de las redes de centros de RedIRIS, así como la actuación coordinada con dichos centros para poner solución a estos problemas. También se realiza una labor preventiva, avisando con tiempo de problemas potenciales, ofreciendo asesoramiento a los centros, organizando actividades de acuerdo con los mismos, y ofreciendo servicios complementarios.

http://www.rediris.es/cert/

Portal CCN- CERT. Portal de Equipo de Respuesta a Incidentes del Centro Criptológico Nacional (CCN). Incluye secciones sobre vulnerabilidades, contiene guías de bastionado de todo tipo de software en idioma español, herramienta de análisis de riesgo Pilar, herramientas, etc. Se incluye otro enlace del sitio web relacionado específicamente con las infraestructuras críticas.

https://www.ccn-cert.cni.es/

Instituto Nacional de Ciberseguridad (INCIBE). El Instituto Nacional de Ciberseguridad (INCIBE), como entidad de referencia para el desarrollo de la ciberseguridad y de confianza digital, tiene entre sus cometidos fomentar la cultura de seguridad entre los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores estratégicos. Uno de los elementos que utiliza INCIBE para fomentar esta cultura de la seguridad es la creación de guías y estudios sobre temas relacionados con la ciberseguridad.

https://www.incibe.es/CERT/guias_estudios/

Distribuciones Linux Forenses. Estas son algunas de las distribuciones Linux Forenses más utilizadas.

http://www.deftlinux.net
https://www.kali.org/
http://www.caine-live.net/

Bibliografía recomendada y complementaria

Computer evidence: Collection and preservation. De Christopher Brown, publicado por primera vez en 2009. ISBN-13: 978-1584506997.

ISO/IEC 27037. Esta norma ISO proporciona directrices para las actividades específicas en el manejo de la evidencia digital.

Handbook for Computer Security Incident Response Teams (CSIRTs). Guía publicada por el Instituto de Ingeniería del Software de Carnegie Mellon para la creación y gestión de un CSIRT.

http://www.sei.cmu.edu/reports/03hb002.pdf

Guía de Seguridad (CCN-STIC-810). Guía de creación de un CERT / CSIRT publicada por el Centro Criptológico Nacional (CCN).

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-CSIRT.pdf

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2022-2023	
Estudio	Máster en Ciberdefensa (EH70)	
Nombre de la asignatura	ANÁLISIS DE MALWARE	
Carácter (Obligatoria/Optativa)	OB	
Créditos (1 ECTS=25 horas)	3	
Modalidad (elegir una opción)		Presencial
		Semipresencial
	x	On-line
Profesor responsable	Javier Bermejo Higuera	
Idioma en el que se imparte	Español	

DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)	
Número de horas presenciales/on-line asistencia profesor	30
Número de horas de trabajo personal del estudiante	45
Total horas	75

CONTENIDOS (Temario)

UD1. FUNDAMENTOS ANÁLISIS DE MALWARE
- Introducción.
- Capacidad "Análisis de Malware".
- Tipos de Malware.
- Caracterización de Malware (MAEC)
- Conocimientos de base
- Fundamentos de ingeniería inversa
- Introducción a la herramienta IDRA PRO

UD2. HERRAMIENTAS Y MÉTODOS DE ANÁLISIS DE MALWARE
- Técnicas y métodos de análisis de Malware.
- Herramientas de análisis de Malware.

UD3. METODOLOGÍA, ANÁLISIS Y SISTEMAS DE OBTENCIÓN DE MALWARE
- Obtención del Malware. Honeynet.
- Arquitectura laboratorio análisis de Malware.
- Metodología de análisis: clasificación, análisis de código dinámico o de comportamiento.

EVALUACIÓN

La evaluación de los alumnos se realiza teniendo en cuenta las siguientes valoraciones:
- Unidades Didácticas: 70% de la nota total de la asignatura. Controles de seguimiento conformados por una sala de debate, un test por cada unidad y un caso práctico por cada unidad
- Examen Final: 30% de la nota total de la asignatura.

BIBLIOGRAFÍA

Enlaces

1. Malware Attribute Enumeration and Characterization (MAEC)
    - Página web que introduce y define un lenguaje para la caracterización de malware basado en sus comportamientos, artefactos, y los patrones de ataque.
    - https://maec.mitre.org/
2. Enciclopedia Virus Kaspersky:
    - Página web donde se pueden consultar las diferentes características de los diversos tipos de malware detectados por la empresa Kasperky, hasta la fecha.
    - www.viruslist.com/eng/
3. Enciclopedia Virus Symantec:
    - Página web donde se pueden consultar las diferentes características de los diversos tipos de malware detectados por la empresa Symantec, hasta la fecha.
    - http://securityresponse.symantec.com/avcenter/vinfodb.html
4. Enciclopedia Virus Trend Micro:
    - Página web donde se pueden consultar las diferentes características de los diversos tipos de malware detectados por la empresa Trend Micro, hasta la fecha.
    - www.trendmicro.com/vinfo/virusencyclo/

Lecturas complementarias

1. Programming from the Ground Up
    - Libro para aprender lenguaje ensamblador.
    - http://security.di.unimi.it/sicurezza1314/papers/Assemblerprogramming.pdf

2. PC Assembly Language
    - Libro para aprender lenguaje ensamblador.
    - http://www.ic.unicamp.br/~pannain/mc404/aulas/pdfs/Assembly_Language.pdf

3. Brochure. Malware Attribute Enumeration and Characterization - MAEC™ A Standardized Language for Attribute-Based Malware Characterization.
    - Descripción del estándar de caracterización y clasificación de malware MAEC.
    - http://makingsecuritymeasurable.mitre.org/docs/maec-intro-handout.pdf

4. White Paper. Ivan Kirillov, Desiree Beck, Penny Chase, Robert Martin. Malware Attribute Enumeration and Characterization. MITRE Corporation.
    - Documento que presenta y define un lenguaje para caracterizar malware sobre la base de sus comportamientos, artefactos, y dibujos de ataque.
    - http://maec.mitre.org/about/docs/Introduction_to_MAEC_white_paper.pdf

5. Informe de McAfee sobre amenazas: Segundo trimestre de 2012.
    - Informe que describe las tendencias del malware ocurridas durante el segundo trimestre del 2012.
    - http://www.mcafee.com/es/resources/reports/rp-quarterly-threat-q1-2012.pdf
6. INTECO. Cuaderno de notas del Observatorio. Amenazas silenciosas en la Red: rootkits y botnets.
    - Artículo realizado por el INTECO, acerca de malware tipo rootkits y botnet. Se recomienda su lectura.
    - https://www.incibe.es/file/o958020emUS5f1Ez5MwRMA

7. INTECO. Cuaderno de notas del Observatorio. Desmontando el Malware.
    - Artículo realizado por el INTECO, que trata en profundidad los diferentes tipos de malware y se presentarán algunos ejemplos de renombre.
    - https://www.incibe.es/file/18H7L9lQPedm-YRQlNJucQ

Videos recomendados y complementarios

1. Windows Assembly Language Megaprimer

- Grupo de nueve videos de un curso de Lenguaje Ensamblador para Windows.
- http://www.securitytube.net/groups?operation=view&groupId=6

2. Assembly Language Megaprimer for Linux
   - Grupo de once videos de un curso de Lenguaje Ensamblador para linux.
   - http://www.securitytube.net/groups?operation=view&groupId=6
3. Real Advances in Android Malware
   - Conferencia sobre lo que los autores de malware y delincuentes están haciendo para mejorar la eficacia y la capacidad de evasión de su código malicioso en sistemas Android.
   - http://www.brighttalk.com/community/it-security/webcast/7651/59047

Bibliografía recomendada y complementaria

1. Michael Hale Ligh, Steven Adair, Blake Hartstein, Matthew Richard. Malware Analyst's Cookbook and DVD. Tools and Techniques for Fighting Malicious Code. Wiley Publishing, Inc. Año 2011.
   - Libro que contiene una serie de soluciones y tutoriales diseñados para mejorar el conjunto de habilidades y capacidades analíticas de quienes realizan análisis de malware.
2. Sikorski, M., & Honig, A. (2012). PRACTICAL MALWARE ANALYSIS. The Hands-On Guide to Dissecting Malicious Sofware. San Francisco: No Starch Press.
   - Uno de los mejores libros sobre análisis de malware.
3. Michael Davis, Sean Bodmer, Aaron Lemasters. Hacking Exposed™ Malware & Rootkits: Security Secrets & Solutions. McGraw-Hill. Año 2010.
   - Libro que trata en profundidad los malware tipo rootkits.
4. Ed Tittel. PC Magazine® Fighting Spyware, Viruses, and Malware. Wiley Publishing, Inc. Absolute Beginner's Guide to Security, Spam, Spyware & Viruses (Absolute Beginner's Guide)
   - Guía para principiantes que ayuda a defenderse de spam, spyware y virus etc.

GUÍA DOCENTE

Año académico	2022-2023	
Estudio	Máster en Ciberdefensa (EH70)	
Nombre de la asignatura	RECUPERACIÓN Y ANÁLISIS DE DATOS	
Carácter (Obligatoria/Optativa)	OB	
Créditos (1 ECTS=25 horas)	3	
Modalidad (elegir una opción)		Presencial
		Semipresencial
	x	On-line
Profesor responsable	Miguel Ángel Sicilia Urbán	
Idioma en el que se imparte	Español	

DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)	
Número de horas presenciales/on-line asistencia profesor	30
Número de horas de trabajo personal del estudiante	45
Total horas	75

CONTENIDOS (Temario)

UD1. INTRODUCCIÓN AL ANÁLISIS DE DATOS DE CIBERDEFENSA
- El análisis de datos en las diferentes fases.
- Dos enfoques para la detección.
- Diferentes tipos de datos.
- Una exploración en los datos en bruto.
- Uso de bases de datos externas.
- Una mirada a los patrones de ataque.

UD2. CAPTURA, AGREGACIÓN Y RECUPERACIÓN
- Sistemas de captura de logs.
- Sistemas de gestión de logs.
- Recuperación de información.
- El caso de Graylog.

UD3. INTRODUCCIÓN AL ANÁLISIS DE DATOS Y APRENDIZAJE AUTOMÁTICO
- Aprendizaje supervisado.
- Aprendizaje no supervisado.

UD4. CASOS DE ANÁLISIS DE DATOS Y APRENDIZAJE AUTOMÁTICO

UD5. FUSIÓN DE DATOS
- ¿Por qué fusión en la ciberseguridad?
- La fusión tiene lugar a diferentes niveles.
- Un ejemplo de fusión de nivel II/III
- Técnicas de agregación y fusión de datos.

EVALUACIÓN

La evaluación de los alumnos se realiza teniendo en cuenta las siguientes valoraciones:

- Unidades Didácticas: 70% de la nota total de la asignatura. Controles de seguimiento conformados por una sala de debate, un test por cada unidad y un caso práctico por cada unidad
- Examen Final: 30% de la nota total de la asignatura.

BIBLIOGRAFÍA

Enlaces

1. Snort Intrusion Detection System
   - Snort es un IDS open source muy utilizado. El interés en la asignatura es utilizarlo como fuente de datos, dado que se pueden obtener de él conjuntos de reglas que actúan como firmas en la detección de ataques.
   - https://www.snort.org/
2. National Vulnerability Database (NVD):
   - Un repositorio de conocimiento y estándares de ciberseguridad del gobierno americano. Cuenta con bases de datos como CVE que se utilizan a nivel mundial como referencia, y con muchos otros estándares que se mencionan en la asignatura. Es importante conocerlo a nivel general porque se utiliza mucho como fuente de clasificación y relación de datos de seguridad (por ejemplo, para identificar vulnerabilidades asociadas a tipos de malware).
   - https://nvd.nist.gov/

Lecturas complementarias

1. "At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues", NRC, National Academies Press, 2014.
   - Proporciona un marco de definiciones interesantes para clarificar la terminología, y explica la naturaleza adversaria del dominio.
   - Sirve como un repaso de conceptos para aproximarnos al tipo de análisis de datos del módulo.
   - Disponible en: http://www.ncbi.nlm.nih.gov/books/NBK223221/
2. "Common cyberattacks: reducing the impact", CERT-UK
   - En el apartado 3 describe a alto nivel las fases genéricas de un ciberataque: survey, delivery, breach, affect. Es útil como lectura inicial para comprender el concepto de patrón de ataque.
   - Disponible en: https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

Vídeos recomendados y complementarios

1. "Creating Snort rules", Philip Craiger
   - El video es un tutorial sobre la estructura de las reglas de Snort. Son un buen ejemplo para entender cómo se construyen firmas en este popular IDS. Aunque no se pide escribir reglas de Snort, comprender su sintaxis es útil para entender el tipo de alertas que recoge y cómo las dispara a nivel de paquete.
   - https://www.youtube.com/watch?v=RUmYojxy3Xw

Bibliografía complementaria

1. Jacobs, J., & Rudis, B. (2014). Data-driven Security: Analysis, Visualization and Dashboards. John Wiley & Sons.

El capítulo I nos da una introducción a conceptos muy genéricos del análisis de datos, incluido un poco de historia. No es específico de los contenidos de la asignatura, pero puede ser interés.

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2022-2023	
Estudio	Máster en Ciberdefensa (EH70)	
Nombre de la asignatura	CONCIENCIA DE LA SITUACIÓN Y COMPARTICIÓN INFORMACIÓN	
Carácter (Obligatoria/Optativa)	OB	
Créditos (1 ECTS=25 horas)	3	
Modalidad (elegir una opción)		Presencial
		Semipresencial
	x	On-line
Profesor responsable	Miguel Ángel Pérez Sánchez	
Idioma en el que se imparte	Español	

DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)	
Número de horas presenciales/on-line asistencia profesor	30
Número de horas de trabajo personal del estudiante	45
Total horas	75

CONTENIDOS (Temario)

UD1. CAPACIDADES DE EXPLOTACIÓN. Parte I
- Introducción.
- La conciencia situacional
- Concepto de empleo de la conciencia de la situación cibernética.

UD2. CAPACIDADES DE EXPLOTACIÓN. Parte II
- Enfoque conceptual de la conciencia de la situación cibernética.
- Necesidades de la conciencia de la situación cibernética.
- Conciencia situacional para la ciberdefensa.

UD3. CAPACIDADES DE EXPLOTACIÓN. Parte III
- La conciencia situacional cibernética en apoyo al planeamiento.
- Visualización de la información.
- Colaboración y compartición de la información.

EVALUACIÓN

La evaluación de los alumnos se realiza teniendo en cuenta las siguientes valoraciones:
- Unidades Didácticas: 70% de la nota total de la asignatura. Controles de seguimiento conformados por una sala de debate, un test por cada unidad y un caso práctico por cada unidad
- Examen Final: 30% de la nota total de la asignatura.

BIBLIOGRAFÍA

Documentación complementaria
1. Enlaces de interés sobre Conciencia de la situación
https://www.dhs.gov/sites/default/files/publications/Using%20Social%20Media%20for%20Enhanced%20Situational%20Awareness%20and%20Decision%20Support.pdf
http://www.esri.com/library/whitepapers/pdfs/situational-awareness.pdf
https://www.raes-hfg.com/crm/reports/sa-defns.pdf
https://www.nap.edu/read/6173/chapter/9
http://wikiofscience.wikidot.com/quasiscience:situational-awareness
https://www.stratfor.com/weekly/practical-guide-situational-awareness
http://www.skybrary.aero/index.php/Situational_Awareness
https://www.nap.edu/read/6173/chapter/9#182
https://www.army.gov.au/our-future/blog/situational-awareness
https://es.wikipedia.org/wiki/Consciencia_situacional

2. Textos sobre temas relativos a conciencia de la situación
a. A Review of Situation Awareness Literature Relevant to Pilot Surveillance Functions. John Uhlarik. DIANE Publishing, 2002
b. Situational Awareness. Eduardo Salas. Routledge, Julio 2017
c. Human Performance, Workload, and Situational Awareness Measures Handbook, Second Edition. Valerie J. Gawron. CRC Press, 2008

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2022-2023	
Estudio	Máster en Ciberdefensa (EH70)	
Nombre de la asignatura	CIBERINTELIGENCIA Y FUENTES ABIERTAS	
Carácter (Obligatoria/Optativa)	OB	
Créditos (1 ECTS=25 horas)	3	
Modalidad (elegir una opción)		Presencial
		Semipresencial
	x	On-line
Profesor responsable	Diego López Abril	
Idioma en el que se imparte	Español	

DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)	
Número de horas presenciales/on-line asistencia profesor	30
Número de horas de trabajo personal del estudiante	45
Total horas	75

CONTENIDOS (Temario)

UD1. CIBERINTELIGENCIA
- Introducción
- Ciclo de Inteligencia
- Disciplinas Ciberinteligencia
- Proceso OSINT
- Herramientas OSINT

UD2. FUENTES ABIERTAS (PARTE I)
- Proceso OSINT. Recopilación y Monitorización.
- Herramientas del Ciclo OSINT. Planificación, Obtención, Almacenamiento, Análisis.
- Implementación de un entorno OSINT. Herramientas, Arquitectura y Flujos de datos.

UD3. FUENTES ABIERTAS (PARTE II)
- Enmascaramiento de red. Ingeniería social. Metadatos.
- Implementación de un entorno OSINT. MongoDB.
- Implementación de un entorno OSINT. Twitter y Kibana.

EVALUACIÓN

La evaluación de los alumnos se realiza teniendo en cuenta las siguientes valoraciones:
- Unidades Didácticas: 70% de la nota total de la asignatura. Controles de seguimiento conformados por una sala de debate, un test por cada unidad y un caso práctico por cada unidad
- Examen Final: 30% de la nota total de la asignatura.

BIBLIOGRAFÍA

Enlaces

1. Ciber Inteligencia
   - Blog sobre artículos de ciberguerra.

http://www.securityartwork.es/2012/02/08/cyberwarfare-connecting-the-dots-in-cyber-intelligence/

   - Conociendo a nuestros atacantes antes de que nos conozcan

http://www2.deloitte.com/content/dam/Deloitte/pa/Documents/risk/2015-01-Pa-Riesgo-CiberSeguridad.pdf

2. Fuentes Abiertas: artículos y herramientas
   - Articulo periódico Público.es. Los espías se apuntan a las redes sociales Los servicios de inteligencia intentan aprovechar las ventajas de las denominadas "fuentes abiertas"

http://www.taringa.net/posts/info/14073215/Los-espias-se-apuntan-a-las-redes-sociales.html

   - Andrew McLaughlin. "El espionaje en redes sociales es la forma más efectiva de control estatal en Internet". Las redes sociales no son sólo el lugar para coordinar esfuerzos contra gobiernos represores. Según el ex asesor en tecnología de Barack Obama, Andrew McLaughlin, son una fabulosa fuente de información para los que espían a sus ciudadanos.

http://www.ieco.clarin.com/tecnologia/espionaje-sociales-efectiva-control-Internet_0_545345712.html

   - Sitio Web de la empresa S21sec, donde se describe la herramienta de obtención de información de fuentes abiertas Vigilancia Digital.

http://www.s21sec.com/es/productos/digital-surveillance.

3. Google Hacking
   - Tutoriales de Google hacking:

https://www.youtube.com/watch?v=Ft5gND96EBk
http://antoniogonzalezm.es/tag/intitleindex-of-index-of-password-txt/

4. Bases de Datos de vulnerabilidades
   - CVE, Common Vulnerabilities and Exposures.

http://cve.mitre.org/

   - CVSS, Common Vulnerability Scoring System,

http://www.first.org/cvss/

   - CPE, Common Platform Enumeration.

http://cpe.mitre.org/

   - CCE, Common Configuration Enumeration.

http://cce.mitre.org/

   - CAPEC, Common Attack Pattern Enumeration and Classification.

http://capec.mitre.org/

   - CWE, Common Weakness Enumeration.

http://cwe.mitre.org/

   - OVAL, Open Vulnerability and Assessment Language.

http://oval.mitre.org/

Lecturas complementarias

1. Leslie D. Cumiford, PhD. Situation Awareness for Cyber Defense. 2006 CCRTS
   - Documento que trata de la aplicación de la Conciencia situacional al dominio cibernético como medio de mejorar las capacidades.
   - http://www.dtic.mil/dtic/tr/fulltext/u2/a463389.pdf
2. The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.0.
   - Guía muy completa del NIST, que especifica el protocol SCAP.
   - http://csrc.nist.gov/publications/nistpubs/800-126/sp800-126.pdf
3. Design and Operational Guide to Protect Against "Advanced Persistent Threats", November 2011.

- Interesante documento que explica la realidad de las “Advanced Persistent Threats" y cómo diseñar y operar redes y sistemas para contrarrestarlas.
- http://www.ipa.go.jp/files/000017299.pdf

Vídeos recomendados y complementarios

1. Making Security Intelligence Real: Delivering Insight with Agility
   - Además de los pequeños delincuentes y defraudores, hacktivistas y organizaciones cibercriminales mediante malware tipo APT amenazan ahora a muchas empresas. En respuesta, las organizaciones están utilizando técnicas de inteligencia de Ciberdefensa (IC) para ganar visibilidad de 360 grados y lograr una postura de seguridad más proactiva. El enfoque IC utiliza datos más amplios y más inteligentes de análisis, tales como la detección de anomalías, para obtener un conocimiento más preciso. Construido con la próxima generación de sistemas SIEM, las técnicas de inteligencia de Ciberdefensa evitan los inconvenientes de la primera generación de productos: lentos y costoso de implementar, difíciles de manejar e incapaces de evolucionar. En su lugar, se utiliza un enfoque modular y flexible y una aplicación de análisis de datos de seguridad de una forma muy manejable. En esta sesión se comparten en el mundo real.

https://www.brighttalk.com/webcast/8273/53267

2. Seven Stages of Advanced Threats & Data Theft
   - Los ataques dirigidos mediante APT son una de las amenazas cibernéticas más peligrosas para las organizaciones y además sus defensas tradicionales no proporcionan contención contra el robo de datos y delitos informáticos. Además, las aplicaciones en la nube, la movilidad y los usuarios remotos están aumentando el uso de SSL que es a menudo un punto ciego para muchas defensas. El cambio es constante en el mundo de la seguridad informática y los nuevos escenarios de amenazas exigen defensas eficaces.

https://www.brighttalk.com/webcast/7365/56903

3. Top Strategies to Capture Security Intelligence for Applications
   - Los profesionales de seguridad tienen años de experiencia en el registro y seguimiento de los eventos de seguridad de la red para identificar actividades no autorizada o maliciosa. Desafortunadamente, muchos de los ataques de hoy se centran en la capa de aplicación, donde la fidelidad del registro de eventos de seguridad es menos robusta. La mayoría de los registros de aplicaciones se suelen utilizar para ver los errores y el estado interno del sistema, no eventos que pueden ser interesantes desde el punto de vista de seguridad. En esta presentación, John Dickson presenta una discusión sobre lo que deben contener los registros de aplicaciones para ayudar a entender las amenazas y ataques.

https://www.brighttalk.com/webcast/288/53007

4. Combating Advanced Threats 2.0 – Moving Into Mature Cyber Intelligence
   - Ahora que las APT y otras amenazas avanzadas están siendo frecuentemente utilizadas por organizaciones cibercriminales, es absolutamente crítico para profesionales de la seguridad de tener un plan para obtener una defensa eficaz. El logro de este objetivo requiere un fuerte compromiso con la excelencia y dominio en numerosas áreas de operaciones cibernéticas y de inteligencia de seguridad. En esta sesión se basa en la experiencia directa del hablante con muchas de las organizaciones líderes en la lucha contra las amenazas avanzadas para delinear los factores esenciales de éxito, y un plan de acciones e hitos de la lucha contra las amenazas avanzadas utilizando impulsadas por técnicas de inteligencia de ciberdefensa.

https://www.brighttalk.com/webcast/288/52955

Bibliografía recomendada y complementaria

1. Monografía 126 CESDEN “El Ciberespacio. Nuevo Escenario de Confrontación. Año 2012
   - La Monografía se orienta principalmente hacia aspectos relacionados con la ciberdefensa considerada como una cuestión básicamente militar, en el sentido de que se interesa por

facetas que involucran a instituciones, organizaciones o profesiones militares, en todo o en parte. No considera sin embargo, al menos explícita y detalladamente, otros aspectos también importantes para el ciudadano, como el robo de datos personales, el ciberdelito económico, etc., y otros, seguramente de interés nacional general, como el ciberespionaje industrial o el uso malicioso de otras herramientas «corrientes» de Internet, como redes sociales, blogs o simples portales web (o medios de comunicación on-line) para hacer apología extremista o sembrar dudas de confianza o reputación de una economía, una nación, una empresa, etc.

2. Endsley M. R. Towards a Theory of Situation Awareness in Dynamic Systems; Human Factors; Año 1995.
    - Libro de obligada lectura para el que quiera profundizar en los conceptos asociados a la conciencia situacional.
3. Endsley M. R., Garland D. J.; Theoretical underpinnings of situation awareness: a critical review; (Book) Situation Awareness Analysis and Measurement. Lawrence Erlbaum, Mahwah, NJ. Año 2000.
    - Libro de obligada lectura para el que quiera profundizar en los conceptos asociados a la conciencia situacional.
4. Cuadernos de Estrategia Instituto Español de Estudios Estratégicos Instituto Universitario “General Gutiérrez Mellado”. Cuaderno de Estrategia 149. Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio. Diciembre 2010.

Cuaderno que contempla los aspectos más importantes de ciberespacio desde el ámbito de seguridad y defensa. Realizado por seis ponentes expertos en diferentes áreas que bajo la dirección

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2022-2023	
Estudio	Máster en Ciberdefensa (EH70)	
Nombre de la asignatura	AMENAZAS AVANZADAS PERSISTENTES (APT'S)	
Carácter (Obligatoria/Optativa)	OB	
Créditos (1 ECTS=25 horas)	3	
Modalidad (elegir una opción)		Presencial
		Semipresencial
	x	On-line
Profesor responsable	Javier Bermejo Higuera	
Idioma en el que se imparte	Español	

DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)	
Número de horas presenciales/on-line asistencia profesor	30
Número de horas de trabajo personal del estudiante	45
Total horas	75

CONTENIDOS (Temario)

UD1. INTRODUCCIÓN A LAS APT
- Introducción a las APT.
- Antecedentes y principales ciberincidentes relacionados con las APT.
- Características Principales de un APT.
- Fases de un Ataque de un APT.
- Estrategias de defensa frente a las APT.

UD2. TÉCNICAS DE OFUSCACIÓN
- Introducción.
- Ofuscación de los especímenes ejecutables.
- Restricción de los entornos de ejecución.

UD3. CASO DE ESTUDIO: FLAME Y OCTUBRE ROJO
- Introducción.
- Estudio del malware.
- Estudio del malware Octubre Rojo.

EVALUACIÓN

La evaluación de los alumnos se realiza teniendo en cuenta las siguientes valoraciones:
- Unidades Didácticas: 70% de la nota total de la asignatura. Controles de seguimiento conformados por una sala de debate, un test por cada unidad y un caso práctico por cada unidad
- Examen Final: 30% de la nota total de la asignatura.

BIBLIOGRAFÍA

Enlaces

1. How to combat advanced persistent threats: APT strategies to protect your organization.
   - Artículo de Computer Weekly de cómo reducir riesgos frente a los ataques de los APTs.
   - http://www.computerweekly.com/feature/How-to-combat-advanced-persistent-threats-APT-strategies-to-protect-your-organisation

2. Equation APT Group Attack Platform A Study in Stealth - See more at:

   - Intervención en un block acerca del grupo de ataque Equation APT Group Attack Platform.
   - https://threatpost.com/equation-apt-group-attack-platform-a-study-in-stealth/111550/

3. Answering APT Misconceptions:
   - Varios Post de Richard Bejtlich que aclara muchos conceptos sobre APT y que incluye muchos datos y enlaces sobre las mismas.

http://taosecurity.blogspot.com.es/search?q=APT

4. https://en.wikipedia.org/wiki/Advanced_persistent_threat:
   - Página web de WIKIPEDIA sobre la APT que incluye informaciones sobre su concepto, antecedentes, características y ciclo de vida. Además incluye bastantes referencias y enlaces.
   - https://en.wikipedia.org/wiki/Advanced_persistent_threat

Lecturas complementarias

1. Detección de APTs.
   - Informe elaborado por el Instituto Nacional de Ciberseguridad (INCIBE) y el Centro de Seguridad TIC de la Comunidad de Valenciana (CCSIRT-CV), con objeto de concienciar sobre la importancia de una detección precoz de las APTs.
   - https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/deteccion_apt.pdf

2. Informe de Mandiant APT1.
   - Con este informe la mpresa Mandiant, da a conocer al la existencia de los ataques tipo de APT que están siendo patrocinados por distintos gobiernos para obtener información ventajosa sobre actividades y tecnologías de terceros.
   - http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

3. A Detailed Analysis of an Advanced Persistent Threat Malware
   - Artículo del Sans Institute, que muestra el análisis de comportamiento y el código realizado a una APT.
   - https://www.sans.org/reading-room/whitepapers/malicious/detailed-analysis-advanced-persistent-threat-malware-33814

4. Design and Operational Guide to Protect Against "Advanced Persistent Threats", Noviembre 2011.
   - Interesante documento que explica la realidad de las “Advanced Persistent Threats" y cómo diseñar y operar redes y sistemas para contrarrestarlas.

http://www.ipa.go.jp/files/000017299.pdf

Vídeos recomendados y complementarios

1. Cómo defenderse de los APT - Advanced Persistent Threats (Pablo Lopez).
   - Pablo López desarrolla un esquema de protección contra APT planteado desde Check Point, basado en sensores, información integrada de diferentes fuentes de datos de amenazas y con un proceso inteligente de recopilación, procesamiento y detección.

https://www.youtube.com/watch?v=pZzZvq3F9mY

2. Combating Advanced Threats 2.0 – Moving Into Mature Cyber Intelligence

   - Ahora que las APT y otras amenazas avanzadas están siendo frecuentemente utilizadas por organizaciones cibercriminales, es absolutamente crítico para profesionales de la seguridad de tener

un plan de defensa eficaz. El logro de este objetivo requiere un fuerte compromiso con la excelencia y dominio en numerosas áreas de operaciones cibernéticas y de inteligencia de seguridad. Esta sesión se basa en la experiencia directa del autor en muchas de las organizaciones líderes en la lucha contra las amenazas avanzadas para perfilar un plan de acción e hitos contra su lucha, utilizando técnicas de inteligencia de ciberdefensa.

https://www.brighttalk.com/webcast/288/52955

3. Seven Stages of Advanced Threats & Data Theft
    - Los ataques dirigidos mediante APT son una de las amenazas cibernéticas más peligrosas para las organizaciones. Sus defensas tradicionales no proporcionan contención contra el robo de datos y delitos informáticos. Además, las aplicaciones en la nube, la movilidad y los usuarios remotos están aumentando el uso de SSL que es a menudo un punto ciego para muchas defensas. El cambio es constante en el mundo de la seguridad informática y los nuevos escenarios de amenazas exigen defensas eficaces.

https://www.brighttalk.com/webcast/7365/56903

4. Making Security Intelligence Real: Delivering Insight with Agility
    - Además de los pequeños delincuentes y defraudores, hacktivistas y organizaciones cibercriminales mediante malware tipo APT amenazan ahora a muchas empresas. En respuesta, las organizaciones están utilizando técnicas de inteligencia de Ciberdefensa (IC) para ganar visibilidad de 360 grados y lograr una postura de seguridad más proactiva. El enfoque IC utiliza datos más amplios y más inteligentes de análisis, tales como la detección de anomalías, para obtener un conocimiento más preciso. Construido con la próxima generación de sistemas SIEM, las técnicas de inteligencia de Ciberdefensa evitan los inconvenientes de la primera generación de productos: lentos y costoso de implementar, difíciles de manejar e incapaces de evolucionar. En su lugar, se utiliza un enfoque modular y flexible y una aplicación de análisis de datos de seguridad de una forma muy manejable. En esta sesión se comparten en el mundo real.

https://www.brighttalk.com/webcast/8273/53267

5. Introduction to Malware Analysis – Free Recorded Webcast
    - Introducción práctica de las técnicas de ingeniería inversa para el análisis de malware en un sistema Windows. Estudia los tipos de análisis de comportamiento y código, para hacer de este tema accesible incluso a los individuos con una exposición limitada a conceptos de programación. https://zeltser.com/malware-analysis-webcast/

Bibliografía recomendada y complementaria

1. Michael Gregg. Build Your Own Security Lab: A Field Guide for Network Testing. Wiley Publishing, Inc. Año 2008.
    - Interesante libro que describe como construir un laboratorio de seguridad para la realización de pruebas de sistemas. Incluye un capítulo de malware muy completo.
2. Michael Hale Ligh, Steven Adair, Blake Hartstein, Matthew Richard. Malware Analyst's Cookbook and DVD. Tools and Techniques for Fighting Malicious Code. Wiley Publishing, Inc. Año 2011.
    - Libro que contiene una serie de soluciones y tutoriales diseñados para mejorar el conjunto de habilidades y capacidades analíticas de quienes realizan análisis de malware.
3. Sikorski, M., & Honig, A. (2012). PRACTICAL MALWARE ANALYSIS. The Hands-On Guide to Dissecting Malicious Sofware. San Francisco: No Starch Press.
    - Uno de los mejores libros sobre análisis de malware.

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2022-2023	
Estudio	Máster en Ciberdefensa (EH70)	
Nombre de la asignatura	HACKING ÉTICO	
Carácter (Obligatoria/Optativa)	OB	
Créditos (1 ECTS=25 horas)	6	
Modalidad (elegir una opción)		Presencial
		Semipresencial
	x	On-line
Profesor responsable	Enrique de la Hoz de la Hoz	
Idioma en el que se imparte	Español	

DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)	
Número de horas presenciales/on-line asistencia profesor	60
Número de horas de trabajo personal del estudiante	90
Total horas	150

CONTENIDOS (Temario)

UD1. INTRODUCCIÓN AL HACKING ÉTICO
- Hacking ético y auditoria.
- Tipos de auditorías.
- Metodologías, recomendaciones y estándares.
- Aspectos legales y éticos.

UD2. FASES DE UNA PRUEBA DE PENETRACIÓN: PLANIFICACIÓN Y DESCUBRIMIENTO
- El modelo de cuatro fases de un test de penetración.
- Fases de planificación.
- Fase de descubrimiento: etapas.
- Fase de descubrimiento: reconocimiento.
- Fase de descubrimiento: mapeo de Red.
- Fase de descubrimiento: enumeración.
- Fase de descubrimiento: análisis de vulnerabilidades.

UD3. FASES DE UNA PRUEBA DE PENETRACIÓN (II)
- Hacking ético y auditoria.
- Tipos de auditorías.
- Metodologías, recomendaciones y estándares.
- Aspectos legales y éticos.

UD4. AUDITORÍA Y SEGURIDAD DE REDES IP
- El modelo de cuatro fases de un test de penetración.
- Fases de planificación.
- Fase de descubrimiento: etapas.

- Fase de descubrimiento: reconocimiento.
- Fase de descubrimiento: mapeo de Red.
- Fase de descubrimiento: enumeración.
- Fase de descubrimiento: análisis de vulnerabilidades.

UD5.AUDITORIA DE REDES INALÁMBRICAS

- Redes WiFi: un repaso a 802,11
- WEP: auditoria y limitaciones
- El estándar de seguridad inalámbrica 802,11i.
- Auditoria de redes WPA/WP2 – PSK.

UD6. SEGURIDAD Y AUDITORIA DE APLICACIONES WEB

- Obtención del Malware. Honeynet.
- Arquitectura laboratorio análisis de Malware.
- Metodología de análisis: clasificación, análisis de código dinámico o de comportamiento.

EVALUACIÓN

La evaluación de los alumnos se realiza teniendo en cuenta las siguientes valoraciones:

- Unidades Didácticas: 70% de la nota total de la asignatura. Controles de seguimiento conformados por una sala de debate, un test por cada unidad y un caso práctico por cada unidad
- Examen Final: 30% de la nota total de la asignatura.

BIBLIOGRAFÍA

Enlaces

1. Mapa de la Enseñanza de la Seguridad en España versión 2.0
   - http://www.criptored.upm.es/mesi/mesi2/mesi2ES.html
2. PTES Technical Guidelines.
   - http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

Lecturas complementarias

1. Hillary Clinton Says China Is “Trying to Hack Into Everything That Doesn’t Move’’.
   - http://time.com/3946275/hillary-clinton-china-hacking-cyberwarfare-usa/
2. Chinese Hackers Pursue Key Data on U.S. Workers
   - https://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html?search-input-2=Chinese+Hackers+Pursue+Key+Data+on+U.S.+Workers%92
3. National Cybersecurity and Communication Integration Center, ‘Combating the Insider Threat’
   - https://www.us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat_0.pdf
4. “(ISC)² Code Of Ethics”
   - https://www.isc2.org/ethics/default.aspx
5. Anthony D. Bundschuh, ‘Ethics in the IT Community’. SANS Whitepaper
6. Herzog, P. (2008). Open source security testing methodology manual (OSSTMM). Retrieved from Institute for Security and Open Methodologies Web site:
   - http://www.isecom.org/research/osstmm.html
7. Information Systems Security Group. (2006). Information Systems Security Assessment Framework (ISSAF) Draft 0.2.1B. Retrieved from Open Information Systems Security Group Web site:
   - http://www.oissg.org/files/issaf0.2.1B.pdf

Bibliografía recomendada y complementaria

1. Verizon Data Breach Investigations Report (DBIR, 2014).
2. Richard O. Mason, 'Four ethical issues of the information age', MIS Quarterly, v.10 n.1, p.5-12, March 1986.
3. Sean-Philip Oriyano, 'CEH: Certified Ethical Hacker Version 8 Study Guide', Ed. Sybex, 2014.
4. Karen Scarfone and Murugiah Souppaya, Amanda Cody and Angela Orebaugh. NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, 2008.
5. Engebretson Patrick. The Basics of Hacking and Penetration Testing. 2011. © 2011 Elsevier Inc. All rights reserved. ISBN: 978-1-59749-655-1.
6. Project Management Institute. (2008). A guide to the project management body of knowledge (4th ed.). Newtown Square, PA: Author.
7. PMI Project Management Institute. (2012). A guide to the project management body of knowledge (5th ed.). Newtown Square, PA: Author.
8. Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, and Terron Williams. "Gray Hat Hacking. The Ethical Hacker's Handbook". Third Edition. ISBN: 978-0-07-174256-6.
9. Wilhelm T (2010), "Professional Penetration Testing", Ed. Elsevier. ISBN: 978-1-59749-425-0.
10. Institute for Security and Open Methodologies. OSSTMM 2.1.Open-Source Security Testing Methodology Manual.
11. Lee Allen; Kevin Cardwell. (2016)"Chapter 1: Penetration Testing Essentials" En: 'Advanced Penetration Testing for Highly-Secured Environments" Pack Publishing. Second Edition.
12. Institute for Security and Open Methodologies. OSSTMM 2.1.Open-Source Security Testing Methodology Manual.
13. Lee Allen; Kevin Cardwell. (2016)"Chapter 1: Penetration Testing Essentials" En: 'Advanced Penetration Testing for Highly-Secured Environments" Pack Publishing. Second Edition.

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2022-2023	
Estudio	Máster en Ciberdefensa (EH70)	
Nombre de la asignatura	ATAQUES DE DENEGACIÓN DE SERVICIO	
Carácter (Obligatoria/Optativa)	OB	
Créditos (1 ECTS=25 horas)	3	
Modalidad (elegir una opción)		Presencial
		Semipresencial
	x	On-line
Profesor responsable	Juan Ramón Bermejo Higuera	
Idioma en el que se imparte	Español	

DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)	
Número de horas presenciales/on-line asistencia profesor	30
Número de horas de trabajo personal del estudiante	45
Total horas	75

CONTENIDOS (Temario)

UD1. ATAQUES DE DENEGACIÓN DE SERVICIO
- Introducción. Tipos de ataques de denegación de servicio.
- Ataques DOS.
- Herramientas DOS.

UD2. ATAQUES DE DENEGACIÓN DE SERVICIO DISTRIBUIDOS DDOS
- Tipos de ataques DDOS.
- Botnets.
- Herramientas DDOS.

UD3. DEFENSAS CONTRA ATAQUES DDOS
- Introducción.
- Tipos de defensas contra ataques DDOS.
- Implementaciones y configuraciones específicas anti DDOS.

EVALUACIÓN

La evaluación de los alumnos se realiza teniendo en cuenta las siguientes valoraciones:
- Unidades Didácticas: 70% de la nota total de la asignatura. Controles de seguimiento conformados por una sala de debate, un test por cada unidad y un caso práctico por cada unidad
- Examen Final: 30% de la nota total de la asignatura.

BIBLIOGRAFÍA

Enlaces

1. **Ataques DDOS.**
   - Resumen de ataques DOS: http://www.tic.udc.es/~nino/blog/lsi/documentos/5-ddos.pdf
   - Gabriel Verdejo Alvarez: Ataques de denegación de servicio DOS/DDOS: https://sites.google.com/site/gabrielverdejoalvarez/DEA-es-2DOS-DDOS.pdf?attredirects=0
   - DDOSpedia RADWARE: https://security.radware.com/ddos-knowledge-center/ddospedia/

   - INCIBE. DOS capa de infraestructura. Accedida el 16 de marzo de 2016. https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/DoS_Capa_Infraestructura

   - Ataques DOS Flooding. http://www.tic.udc.es/~nino/blog/lsi/reports/flood.pdf

   - DDOS attacks for dummies: http://www.ireo.com/fileadmin/docs/documentacion_de_productos/Corero/Corero%20-%20DDoS%20for%20dummies.pdf

2. **Herramientas DOS.**
   - Página web de InfosecInstitute que resume características de herramientas DOS-DDOS: http://resources.infosecinstitute.com/dos-attacks-free-dos-attacking-tools/
   - Herramienta hping3. Accedida el 16 de marzo de 2016. Sitio web: http://www.hping.org/hping3.html
   - Herramienta Goldeneye. Accedida el 16 de marzo de 2016. Sitio web: https://sourceforge.net/directory/os:windows/?q=goldeneye
   - Herramienta UDPFlood. Accedida el 16 de marzo de 2016. Sitio web: http://www.mcafee.com/us/downloads/free-tools/udpflood.aspx
   - Anatomía del ataque Hackivist. Accedida el 16 de marzo de 2016. Sitio web: http://www.imperva.com/docs/WP_The_Anatomy_of_a_Hacktivist_Attack.pdf
   - Slowloris. Accedida el 16 de marzo de 2016. Sitio web:
     - https://github.com/llaera/slowloris.pl
     - http://www.acunetix.com/blog/articles/slow-http-dos-attacks-mitigate-apache-http-server/
     - http://www.funtoo.org/Slowloris_DOS_Mitigation_Guide
   - Slowhttptest. Accedida el 16 de marzo de 2016. Sitio web: https://github.com/shekyan/slowhttptest

Lecturas complementarias

1. Simulacro de: Ataque Distribuido de Denegación de Servicio (DDoS) mediante reflección NTP, desde y contra una red científica. http://www.flu-project.com/2014/02/simulacro-de-ataque-distribuido-de.html

2. Ataque DoS WiFi
http://hacking-etico.com/2013/03/13/ataque-dos-wifi/#more-1772

3. Killapache CVE-2011-3192
https://www.exploit-db.com/exploits/17696/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192

4. Estadísticas ataques DOS-DDOS. Akamai's State of the Internet: Q3 2015 Report.
https://www.stateoftheinternet.com/resources-connectivity-2015-q3-state-of-the-internet-report.html

5. UDP Port Denial-of-Service Attack 1997:
http://www.cert.org/advisories/CA-1996-01.html

6. SLOWHTTPTEST:
http://www.blackmoreops.com/2015/06/07/attack-website-using-slowhttptest-in-kali-linux/

7. Protección contra ataques HTTP SLOW:
https://blog.qualys.com/securitylabs/2011/11/02/how-to-protect-against-slow-http-attacks

8. Estado del arte de los ataques DDOS:
http://www.ijircce.com/upload/2013/october/25ASurvey.pdf

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2022-2023	
Estudio	Máster en Ciberdefensa (EH70)	
Nombre de la asignatura	INGENIERÍA SOCIAL	
Carácter (Obligatoria/Optativa)	OB	
Créditos (1 ECTS=25 horas)	3	
Modalidad (elegir una opción)		Presencial
		Semipresencial
	x	On-line
Profesor responsable	Diego López Abril	
Idioma en el que se imparte	Español	

DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)	
Número de horas presenciales/on-line asistencia profesor	30
Número de horas de trabajo personal del estudiante	45
Total horas	75

CONTENIDOS (Temario)

UD1. FUNDAMENTOS DE LA INGENIERÍA SOCIAL – RECOPILACIÓN

- Introducción a la Ingeniería Social.
- Tipos de Ingenieros Sociales.
- Técnicas y métodos de Ingeniería Social.
- El papel de la ingeniería social en la recopilación de información.

UD2. HERRAMIENTAS Y MÉTODOS UTILIZADOS – ANÁLISIS

- Casos o incidentes de ingeniería social ocurridos.
- Análisis de información – Bases de datos de grafos.

UD3. APLICACIÓN Y DEFENSA EN LA INGENIERÍA SOCIAL

- Aplicación de la Ingeniería Social a la Ciberdefensa. Operaciones psicológicas.
- Utilización de herramientas para la realización de ataques de Ingeniería Social.
- Medidas defensivas.

EVALUACIÓN

La evaluación de los alumnos se realiza teniendo en cuenta las siguientes valoraciones:

- Unidades Didácticas: 70% de la nota total de la asignatura. Controles de seguimiento conformados por una sala de debate, un test por cada unidad y un caso práctico por cada unidad
- Examen Final: 30% de la nota total de la asignatura.

BIBLIOGRAFÍA

Enlaces

1. Instalación Maltego
   - Decargarlo de la página web.

- https://www.paterva.com/web6/products/download2.php [Último acceso: 4 enero 2018].

2. Espionaje y Metadatos
   - Artículos que hablan sobre los metadatos y sus peligros.
   - http://www.libertaddigital.com/opinion/jorge-alcalde/no-me-toques-los-metadatos-69865/ [Último acceso: 4 enero 2018].
   - https://lignux.com/instalar-mat-metadata-anonymisation-toolkit-en-debian-o-ubuntu/ [Último acceso: 4 enero 2018].
   - http://blogs.lavanguardia.com/tecladomovil/espionaje-y-metadata-59754 [Último acceso: 4 enero 2018].

Lecturas complementarias

1. El arte de la intrusión de Kevin Mitnick.
   - Libro de obligada lectura para profundizar en los conceptos asociados a la ingeniería social.

2. Social Engineering: The Art of Human Hacking de Christopher Hadnagy.
   - Otro libro muy importante para profundizar en los conceptos asociados a la ingeniería social.

3. PENTEST: Recolección de Información (Information Gathering). Inteco.
   - Documento de recomendado, realizado por INTECO que recoge de manera profunda y acertada las técnicas existentes de recolección de información.
   - http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_information_gathering.pdf [Último acceso: 4 enero 2018].

4. Anubis.
   - Herramienta de fingerprinting Anubis.
   - https://github.com/fluproject/Anubis [Último acceso: 4 enero 2018].

5. Manual de FOCA.
   - Manual oficial para aprender en profundidad el uso de la herramienta de fingerprinting FOCA.
   - http://www.elladodelmal.com/2010/07/foca-25-free-manual-de-usuario-1-de-6.html [Último acceso: 4 enero 2018].

6. Guía Usuario de Maltego
   - Manual oficial en español para aprender en profundidad el uso de la herramienta Maltego y del uso de las transformaciones.
   - http://www.paterva.com/malv3/303/M3GuideGUI.pdf
   - http://www.paterva.com/malv3/303/M3GuideTransforms.pdf
   - http://www.paterva.com/malv3/303/Maltego3TDSTransformGuideAM.pdf

[Último acceso: 4 enero 2018].

Vídeos recomendados y complementarios

1. Introducción a la Ingeniería Social
   - Video de Introducción a la ingeniería social
   - https://www.youtube.com/watch?v=eMJLK8aJMbU [Último acceso: 4 enero 2018].
2. Tutorial de la Herramienta Maltego.
   - Excelente videotutorial de la herramienta de figerprinting maltego.
   - https://www.youtube.com/watch?v=3zlbUck_BLk&feature=share&list=PLC9DB3E7C258CD215 [Último acceso: 4 enero 2018].
3. Ingeniería social - la última frontera

- Video donde se definen las características de un ataque de Ingeniería Social. Tácticas, ejemplos prácticos, conceptos y definiciones que nos permiten detectar y prevenir ataques, analizando algunos casos históricos y recientes.
- https://www.youtube.com/watch?v=TL9ipoBAeUU [Último acceso: 4 enero 2018].

4. Top Strategies to Capture Security Intelligence for Applications
   - Los profesionales de seguridad tienen años de experiencia en el registro y seguimiento de los eventos de seguridad de la red para identificar actividades no autorizada o maliciosa. Muchos de los ataques de hoy se centran en la capa de aplicación, donde la fidelidad del registro de eventos de seguridad es menos robusta. La mayoría de los registros de aplicaciones se suelen utilizar para ver los errores y el estado interno del sistema, eventos que pueden ser interesantes desde el punto de vista de seguridad. Presentación de John Dickson que presenta una discusión sobre lo que deben contener los registros de aplicaciones para ayudar a entender las amenazas y ataques.

https://www.brighttalk.com/webcast/288/53007 [Último acceso: 4 enero 2018].

Bibliografía recomendada y complementaria

1. Web de Ingeniería Social
   - Framework de Ingeniería Social
   - www.social-engineer.org [Último acceso: 4 enero 2018].
2. Kevin Mitnick
   - El hacker más famoso del mundo, objeto de innumerables noticias, películas y artículos de revistas publicados en todo el mundo.
   - https://www.mitnicksecurity.com/ [Último acceso: 4 enero 2018].
   - https://es.wikipedia.org/wiki/Kevin_Mitnick [Último acceso: 4 enero 2018].

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2022-2023	
Estudio	Máster en Ciberdefensa (EH70)	
Nombre de la asignatura	TRABAJO FIN DE MÁSTER	
Carácter (Obligatoria/Optativa)	OB	
Créditos (1 ECTS=25 horas)	6	
Modalidad (elegir una opción)		Presencial
		Semipresencial
	x	On-line
Profesor responsable	Miguel Ángel Sicilia	
Idioma en el que se imparte	Español	

DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)	
Número de horas presenciales/on-line asistencia profesor	60
Número de horas de trabajo personal del estudiante	90
Total horas	150

CONTENIDOS (Temario)

Temática de la asignatura sobre la que se realiza el TFM

EVALUACIÓN

- Evaluación del tutor 60% de la nota final
- Evaluación del tribunal de defensa 40 % de la nota final

BIBLIOGRAFÍA

Varios