Universidad de Alcalá

Estudio Propio: **EXPERTO EN CIBERINTELIGENCIA**

Código Plan de Estudios: **EL34**

Año Académico: **2020-2021**

ESTRUCTURA GENERAL DEL PLAN DE ESTUDIOS:

CURSO	Obligatorios		Optativos		Prácticas Externas	Memoria/ Proyecto	Créditos
	Créditos	Nº Asignaturas	Créditos	Nº Asignaturas	Créditos	Créditos	
1º	18	6					18
2º							
3º							
ECTS TOTALES	**18**	**6**					**18**

PROGRAMA TEMÁTICO:

ASIGNATURAS OBLIGATORIAS

Código Asignatura	Curso	Denominación	Carácter OB/OP	Créditos
702214	1	CIBERAMENAZAS A LA INFRAESTRUCTURAS CRÍTICAS	OB	3
702217	1	DETECCIÓN Y DEFENSA FRENTE A AMENAZAS CIBERNÉTICAS	OB	3
702218	1	RESPUESTA A INCIDENTES. ANÁLISIS FORENSE	OB	3
702222	1	CIBERINTELIGENCIA Y FUENTES ABIERTAS	OB	3
702225	1	ATAQUES DE DENEGACIÓN DE SERVICIO	OB	3
702226	1	INGENIERÍA SOCIAL	OB	3

Carácter: OB - Obligatoria; OP – Optativa

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2020-2021	
Estudio	Experto en Ciberinteligencia (EL34)	
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	2020-2021	
Estudio	Experto en Ciberinteligencia (EL34)	
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	2020-2021	
Estudio	Experto en Ciberinteligencia (EL34)	
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	2020-2021	
Estudio	Experto en Ciberinteligencia (EL34)	
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	2020-2021	
Estudio	Experto en Ciberinteligencia (EL34)	
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	2020-2021	
Estudio	Experto en Ciberinteligencia (EL34)	
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].