Universidad de Alcalá

Estudio Propio: **EXPERTO EN MALWARE**

Código Plan de Estudios: **EL35**

Año Académico: **2018-2019**

ESTRUCTURA GENERAL DEL PLAN DE ESTUDIOS:

CURSO	Obligatorios		Optativos		Prácticas Externas	Memoria/ Proyecto	Créditos
	Créditos	Nº Asignaturas	Créditos	Nº Asignaturas	Créditos	Créditos	
1º	18	5					18
2º							
3º							
ECTS TOTALES	**18**	**5**					**18**

PROGRAMA TEMÁTICO:

ASIGNATURAS OBLIGATORIAS

Código Asignatura	Curso	Denominación	Carácter OB/OP	Créditos
702215	1	EXPERIMENTACIÓN EN CIBERDEFENSA (CD&E)	OB	3
702219	1	ANÁLISIS DE MALWARE	OB	3
702220	1	RECUPERACIÓN Y ANÁLISIS DE DATOS	OB	3
702223	1	AMENAZAS AVANZADAS PERSISTENTES (APT'S)	OB	3
702224	1	HACKING ÉTICO	OB	6

Carácter: OB - Obligatoria; OP – Optativa

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2018-2019	
Estudio	Experto en Malware (EL35)	
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	

1. 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

2. 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.

3. 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.

4. 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	2018-2019	
Estudio	Experto en Malware (EL35)	
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	

1. 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

2. 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.

3. 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.

4. 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.

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2018-2019	
Estudio	Experto en Malware (EL35)	
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	

1. 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

2. CONTENIDOS (Temario)

3. EVALUACIÓN

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.

4. 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	2018-2019	
Estudio	Experto en Malware (EL35)	
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	

1. 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

2. 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.

3. 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.

4. 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 e 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	2018-2019	
Estudio	Experto en Malware (EL35)	
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	

1. 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

2. 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.

3. 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.

4. 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.