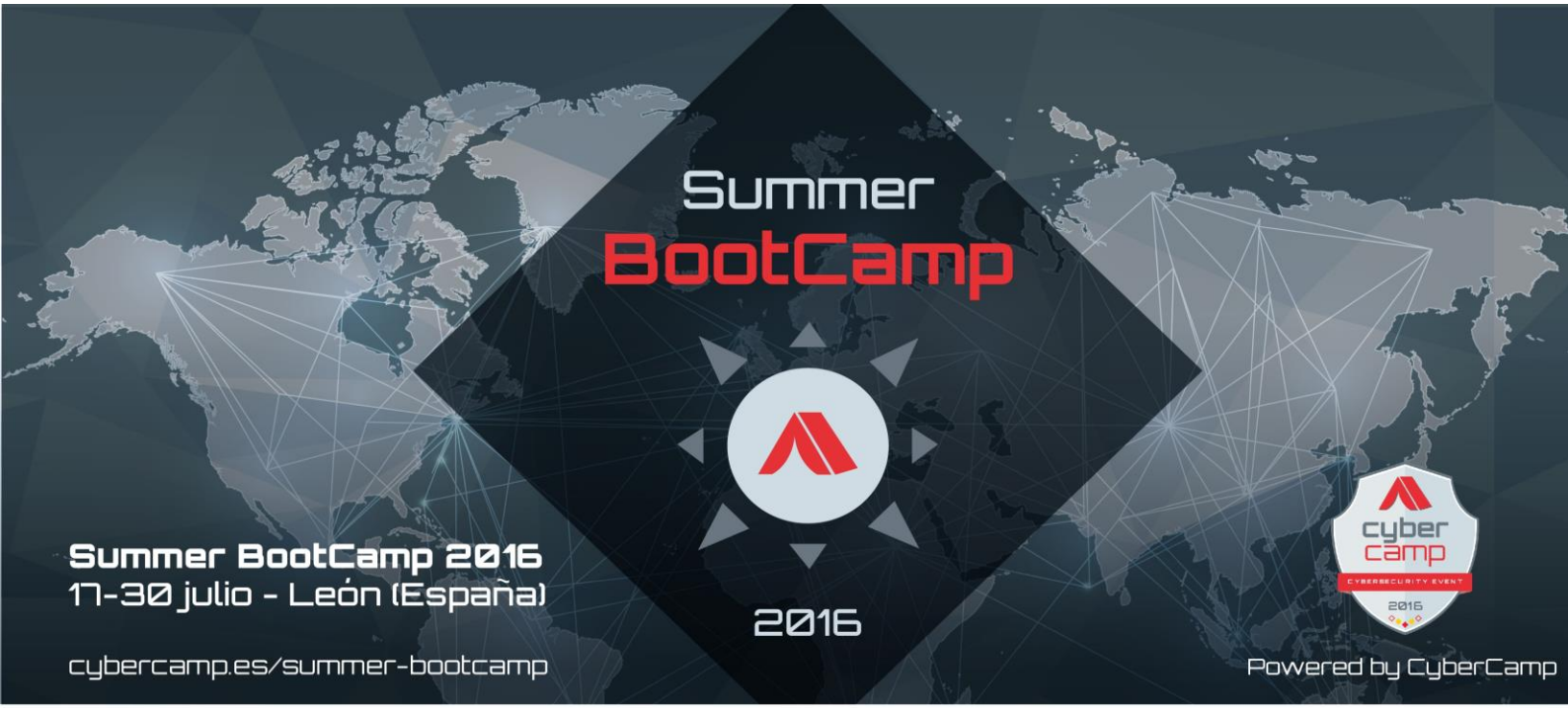

DOSSIER INFORMATIVO

summer bootcamp

LEÓN - 2016

Organizan:

GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR

10 incibe_ 2006-2016 TRABAJANDO POR LA CONFIANZA DIGITAL

GOBIERNO DE ESPAÑA MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

CNPIC CENTRO NACIONAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

Organización de los Estados Americanos | Más derechos para más gente

Colaboran:

universidad de león

AYUNTAMIENTO DE LEÓN

León Cuna del Parlamentarismo

EUROPOL EC3 European Cybercrime Centre

FIRST Improving Security Together

ÍNDICE

1. ANTECEDENTES

La falta de profesionales cualificados en ciberseguridad es una realidad, tal y como dejan patentes informes como el de CISCO en el 2014, según el cual hacen falta más de un millón de profesionales en ciberseguridad[1] a nivel mundial o el de ISACA de 2015 que tasa en 2Millones los puestos vacantes en ciberseguridad de cara al 2019[2]. Es por esto que grandes potencias en ciberseguridad, como son EEUU y UK están poniendo en marcha programas formativos de alta capacitación práctica (formato BootCamp) para formar a los profesionales en diversas materias relacionadas con la ciberseguridad.

Algunas de las iniciativas a destacar[3] están llevadas a cabo por universidades del prestigio de San José State University y el SVBCC (Silicon Valley Big Data and Cybersecurity Center), la Universidad de Stanford, la universidad de Delaware a través del USCC (U.S. Cyber Challenge), la Universidad de James Madison, la universidad de Maryland, la UT de Dallas, el Lowcountry Tech Academy en Charleston, la universidad estatal de Pennsylvania a través de su campus Penn State Berks o la Norfolk State University o la Universidad de Montfort Leicester (DMU) en UK.

O bien por otro tipo de entidades tanto privadas como públicas como son el SANS cyber academy, la base aérea de Wright-Patterson o la NSA a través de 43 campus repartidos por todo EEUU.

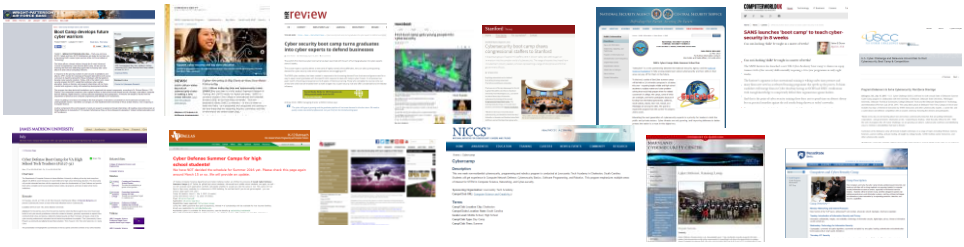

Ilustración 1 - Referencias de programas formativos de ciberseguridad en formato "BootCamp"

A la vista de lo anteriormente descrito, INCIBE va a organizar la primera edición de Summer BootCamp (powered by Cybercamp) en el verano de 2016, de manera que se proporcionarán actividades formativas y de entrenamiento específicas de Ciberseguridad, que actualmente se estaban haciendo en la edición de invierno de CyberCamp, a:

- Fuerzas y Cuerpos de Seguridad del Estado (FCSE).

[1] http://noticias.lainformacion.com/espana/espana-se-prepara-para-el-boom-de-los-empleos-de-ciberseguridad_3AyB6L7qgPXOPSI0Wx2g25/

[2] http://blog.firebrandtraining.co.uk/2016/02/2016-cyber-security-skills-gap.html

[3] Algunas referencias destacables:
http://www.hrreview.co.uk/hr-news/recruitment/cyber-security-boot-camp-turns-graduates-cyber-experts-defend-businesses/56444
http://www.computerworlduk.com/news/careers/sans-launches-boot-camp-teach-cyber-security-in-8-weeks-3607928/
http://www.wpafb.af.mil/news/story.asp?id=123262849
http://www.sjsu.edu/cybersecurity/
http://www.uscyberchallenge.org/2015/07/20/u-s-cyber-challenge-and-delaware-universities-to-host-cybersecurity-boot-camp-competition/
http://news.stanford.edu/news/2015/august/cyber-boot-camp-082415.html
http://www.dmu.ac.uk/about-dmu/news/2015/august/cyber-security-bootcamp-will-train-experts-of-the-future.aspx
http://www.jmu.edu/events/cs/2015/07/27-31-cyber-defense-boot-camp-va.shtml
https://www.nsa.gov/public_info/press_room/2015/gencyber_summer_camps.shtml
http://www.computerworlduk.com/news/careers/sans-launches-boot-camp-teach-cyber-security-in-8-weeks-3607928/
http://www.bbc.co.uk/newsbeat/article/19515213/first-boot-camp-gets-young-people-into-cybersecurity
http://cyber.umd.edu/education/cyber-defense
http://www.utdallas.edu/k12/cyber/
https://niccs.us-cert.gov/education/cyber-camps-clubs
http://www.bk.psu.edu/CE/computer-and-cyber-security-camp.htm
https://www.nsu.edu/cset/csetgraduate/cybersecurity/index

- Profesionales vinculados a la gestión y operación de equipos de respuesta a incidentes o CERTs

La organización de este Summer Bootcamp contribuirá a posicionar a la Ciudad León y a España como Centro de Referencia Mundial en formación en Ciberseguridad aprovechando la oportunidad actual de llevar a cabo el primer BootCamp en materia de ciberseguridad en habla hispana. Asimismo constará de grupos y presencia internacional con carácter global.

Para desarrollar esta iniciativa INCIBE aporta su posicionamiento nacional e internacional, su conocimiento y experiencia en la materia a través del diseño del programa, y profesorado de primer nivel tanto de su plantilla, como de las principales empresas españolas en la materia.

Además, para que este proyecto sea una realidad se requiere la colaboración de socios y entidades de referencia como son:

- Ministerio del Interior **(MINIT).**
- Ministerio de Asuntos Exteriores y Cooperación **(MAEC).**
- Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información **(SETSI).**
- Junta de Castilla y León **(JCyL)** a través de la Agencia de Desarrollo Económico **(ADE)**
- Organización de Estados Americanos **(OEA).**
- Oficina Europea de Policía **(EUROPOL).**
- Forum of Incident Response and Security Teams **(FIRST).**
- Ayuntamiento de León **(Ayto León)**.
- Universidad de León **(ULe).**
- Socios privados.

2. DESCRIPCIÓN DEL EVENTO

El Summer BootCamp 2016 se conforma como un evento internacional con formato eminentemente práctico, que tiene como objetivo formar y adiestrar en aspectos técnicos en las últimas técnicas para la lucha contra los ciberdelitos y la gestión de incidentes de Ciberseguridad a 100 especialistas de las fuerzas y cuerpos de seguridad (FCSE) y a 100 técnicos de CERTs públicos o personal de entidades públicas que trabajen temas relacionados directamente con la ciberseguridad.

El evento tendrá lugar en León (España) en 4 sedes dependiendo de las actividades a realizar.

- INCIBE (Instituto Nacional de Ciberseguridad): Talleres Técnicos (Grupos 1 y 2).
- CRAI-TIC (Universidad de León): Talleres Técnicos (Grupos 3 – 10).
- Auditorio Ciudad de León: Seminarios Magistrales.
- Auditorio Centro Cívico León Oeste: Revisión International CyberEx.

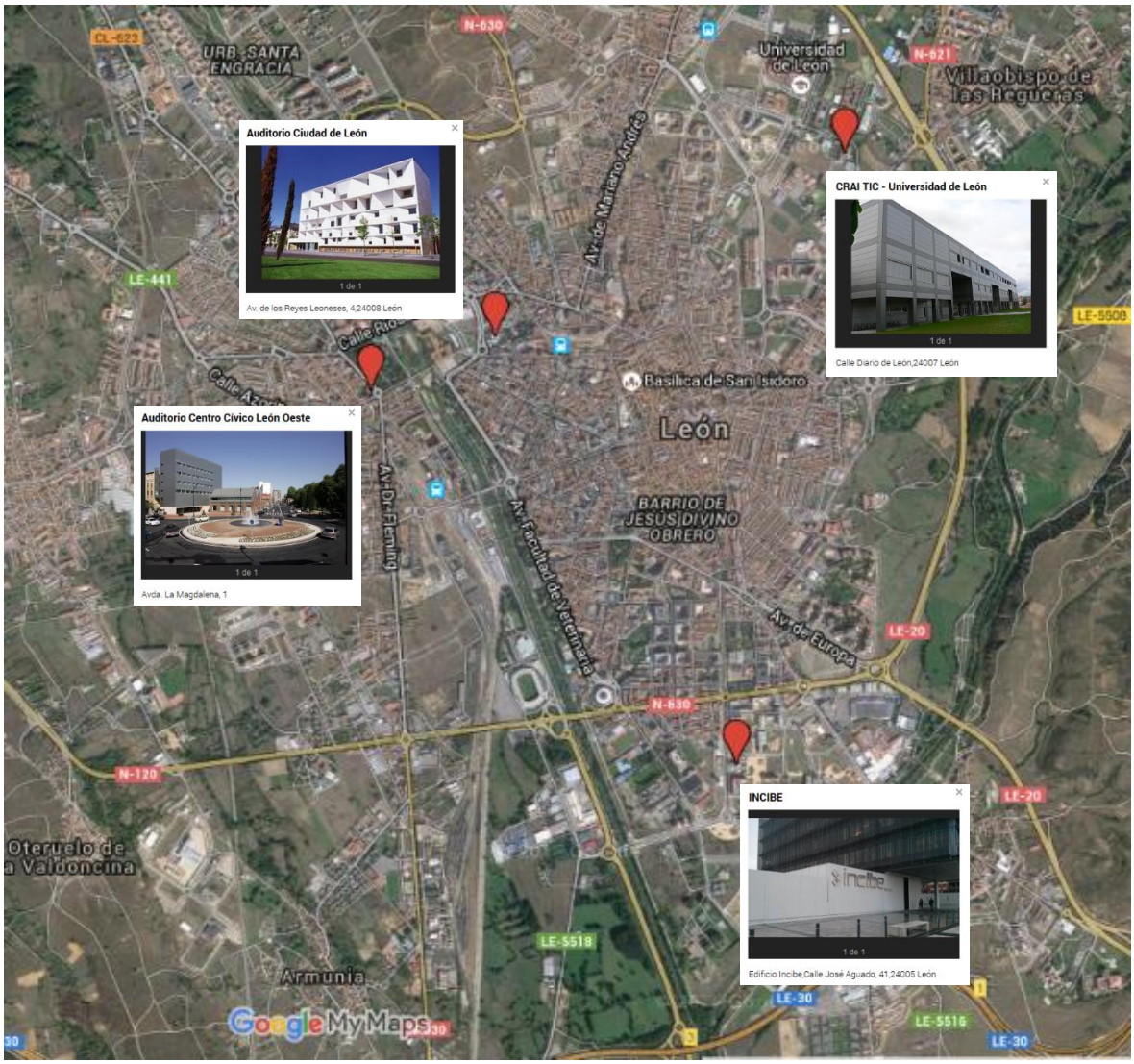

Ilustración 2 - Lugar de Impartición

Summer BootCamp 2016 se llevará a cabo la segunda quincena de julio (del 17 al 30 de julio) según el siguiente calendario:

	Julio '16						
	L	M	X	J	V	S	D
	11	12	13	14	15	16	17
Mañana							
Tarde							Inauguración
	18	19	20	21	22	23	24
Mañana	Talleres Técnicos y masterclass (FCSE / CERTs)			Talleres Técnicos (FCSE) TC FIRST (CERTs)	Revisión International CyberEX (CERTs) Seminarios Magistrales (FCSE / CERTs)		
Tarde				International CyberEX (CERTs)			
	25	26	27	28	29	30	31
Mañana	Talleres Técnicos y masterclass (FCSE / CERTs)				Seminarios Magistrales (FCSE / CERTs)	Clausura	
Tarde							

Ilustración 3 - Calendario Summer BootCamp 2016

El evento está dirigido a los siguientes públicos objetivos:

- Formación FCSE:
  - Personal en activo de FCSE que trabajen en unidades operativas relacionadas con la ciberseguridad.
- Formación CERTs:
  - Personal en activo de CERTs públicos de países latinoamericanos pertenecientes a la OEA**¡Error! Marcador no definido.**.
  - Personal en activo de entidades públicas que trabajen en temas relacionados directamente con ciberseguridad (profesores e investigadores de universidades, técnicos de ciberseguridad de entidades públicas, etc.) de países latinoamericanos pertenecientes a la OEA**¡Error! Marcador no efinido.**.
  - Otro personal relacionado directamente con las actividades de los CERTs y que trabajen en estas temáticas (tanto a nivel nacional como internacional).

Se crearán 5 grupos, de 20 personas para cada uno, que recibirán una formación avanzada y entrenamiento para los FCSE con un enfoque práctico sobre materias específicas para este colectivo y apoyado en herramientas enfocadas a la investigación tecnológica de ciberdelitos y ciberterrorismo.

Así mismo, se crearán otros 5 grupos, también de 20 personas cada uno, que recibirán formación avanzada y entrenamiento en la gestión de incidentes de nivel 2 y 3. Se incidirá principalmente en casos prácticos relacionados con el día a día de un operador de un CERT, en la resolución de incidentes relacionados con malware avanzado (APTs, Botnets, Ransomwares, etc.) y reversing, análisis forense, análisis de exploits, etc. Así mismo se realizará una introducción de retos o ciberejercicios o CTFs, basándose en la experiencia de INCIBE en los CYBEREX y Cybercamp 2014 y 2015.

Las clases se impartirán en inglés y en español, dependiendo del idioma de referencia de cada uno de los grupos, y las actividades conjuntas se impartirán en español contando con un servicio de traducción simultánea para los asistentes angloparlantes.

3. PROGRAMAS

Dado el carácter práctico de la formación, se ha elaborado un programa orientado la especialización en forma de talleres técnicos y prácticos de 5 horas de duración en los que se realizarán simulacros, retos y gran variedad de ejercicios prácticos. Para la realización de dichas dinámicas cada asistente contará con un equipo a su disposición para la realización de las mismas.

Por otra parte se incorporarán tanto seminarios magistrales de 2 horas de duración y que tendrán un componente más teórico orientado al total de los 200 asistentes como masterclass, impartidas por algunos de los colaboradores, orientadas a los públicos objetivos específicos.

Por último se realizarán una serie de actividades paralelas al evento como es un Technical Colloquium del FIRST.

Ambos cursos se convalidarán con 6 CTEs de la Universidad de León en calidad de curso de especialización y contarán con ponentes y formadores de primer nivel líderes a nivel nacional e internacional en las materias a impartir.

En la siguiente agenda se puede ver el detalle de los programas propuestos así como el contenido general para cada uno de los talleres[4]

[4] Dicho programa es provisional y puede estar sujeto a cambios a voluntad de la organización. Dichos cambios se notificarán convenientemente a través de los canales establecidos para ello.

CURSO DE ESPECIALIZACIÓN PARA FCSE

		Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
Domingo 17 Julio	**Tarde (16:30 - 21:30)**	**Inauguración**				
		Auditorio Ciudad de León				
Lunes 18 Julio	**Mañana (8:30 - 14:30)**	**Taller 1** OSINT: herramientas, técnicas de búsqueda y análisis de información Simón Roses	**Taller 3** Análisis de malware (I) Mikel Gastesi	**Taller 7** Cifrado, Navegación anónima y Deep Web Jesús Diaz Vico	**Taller 2** Análisis forense en dispositivos móviles Lorenzo Martínez	**Taller 8** Hacking Avanzado Félix Brezo Yaiza Rubio
		ULE 7	ULE 1	INCIBE 2	ULE 5	ULE 6
	Tarde (15:30 - 21:30)	**Seminario Magistral OEA** (2h)				
		Auditorio INCIBE				
Martes 19 Julio	**Mañana (8:30 - 14:30)**	**Taller 2** Análisis forense en dispositivos móviles Lorenzo Martínez	**Taller 4** Análisis de malware (II) Jose Miguel Esparza	**Taller 3** Análisis de malware (I) Mikel Gastesi	**Taller 1** OSINT: herramientas, técnicas de búsqueda y análisis de información Simón Roses	**Taller 7** Cifrado, Navegación anónima y Deep Web Jesús Diaz Vico
		ULE 5	ULE 2	ULE 1	ULE 7	INCIBE 2
	Tarde (15:30 - 21:30)	**Seminario Magistral FCSE Españoles** (3h)				
		Auditorio INCIBE				

		Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
Miércoles 20 Julio	**Mañana (8:30 - 14:30)**	**Taller 3** Análisis de malware (I) Mikel Gastesi	**Taller 8** Hacking Avanzado Félix Brezo Yaiza Rubio	**Taller 4** Análisis de malware (II) Jose Miguel Esparza		**Taller 1** OSINT: herramientas, técnicas de búsqueda y análisis de información Simón Roses
		ULE 1	INCIBE 2	ULE 2		ULE 7
	Tarde (15:30 - 21:30)				**Taller 5** Análisis forense de sistemas Windows (I) Pedro Sánchez	
		ULE 1 y ULE2			ULE 6	
Jueves 21 Julio	**Mañana (8:30 - 14:30)**	**Taller 4** Análisis de malware (II) Jose Miguel Esparza	**Taller 1** OSINT: herramientas, técnicas de búsqueda y análisis de información Simón Roses	**Taller 2** Análisis forense en dispositivos móviles Lorenzo Martínez	**Taller 6** Análisis forense de sistemas Windows (II) Juan Garrido	**Taller 5** Análisis forense de sistemas Windows (I) Pedro Sánchez
		ULE 2	ULE 7	ULE 5	ULE 4	ULE 6
	Tarde (15:30 - 21:30)	**Seminario Magistral EUROPOL** (3h)				
		Auditorio INCIBE				
Viernes 22 Julio	**Mañana (9:00 - 11:30)**	**Seminario Magistral 1** El negocio del cibercrimen Pendiente INTERPOL				
		Auditorio Ciudad de León				

		Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
	Mañana (12:00 - 14:30)	**Seminario Magistral 2** Seguridad ofensiva David Barroso				
		Auditorio Ciudad de León				
Lunes 25Julio	**Mañana (8:30 - 14:30)**	**Taller 7** Cifrado, Navegación anónima y Deep Web Jesús Diaz Vico	**Taller 5** Análisis forense de sistemas Windows (I) Pedro Sánchez	**Taller 1** OSINT: herramientas, técnicas de búsqueda y análisis de información Simón Roses	**Taller 8** Hacking Avanzado Félix Brezo Yaiza Rubio	
		INCIBE 2	ULE 6	ULE 7	ULE 1	
	Tarde (15:30 - 21:30)					**Taller 6** Análisis forense de sistemas Windows (II) Juan Garrido
						ULE 4
Martes 26 Julio	**Mañana (8:30 - 14:30)**	**Taller 8** Hacking Avanzado Félix Brezo Yaiza Rubio		**Taller 5** Análisis forense de sistemas Windows (I) Pedro Sánchez	**Taller 7** Cifrado, Navegación anónima y Deep Web Jesús Diaz Vico	**Taller 3** Análisis de malware (I) Mikel Gastesi
		ULE 3		ULE 6	INCIBE 2	ULE 1
	Tarde (15:30 - 21:30)		**Taller 6** Análisis forense de sistemas Windows (II) Juan Garrido			
			ULE 4			

		Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
Miércoles 27 Julio	**Mañana (8:30 - 14:30)**	**Taller 5** Análisis forense de sistemas Windows (I) Pedro Sánchez	**Taller 2** Análisis forense en dispositivos móviles Lorenzo Martínez		**Taller 3** Análisis de malware (I) Mikel Gastesi	**Taller 4** Análisis de malware (II) Jose Miguel Esparza
		ULE 6	ULE 5		ULE 1	ULE 2
	Tarde (15:30 - 21:30)			**Taller 6** Análisis forense de sistemas Windows (II) Juan Garrido		
				ULE 4		
Jueves 28 Julio	**Mañana (8:30 - 14:30)**	**Taller 6** Análisis forense de sistemas Windows (II) Juan Garrido	**Taller 7** Cifrado, Navegación anónima y Deep Web Jesús Diaz Vico	**Taller 8** Hacking Avanzado Félix Brezo Yaiza Rubio	**Taller 4** Análisis de malware (II) Jose Miguel Esparza	**Taller 2** Análisis forense en dispositivos móviles Lorenzo Martínez
		ULE 4	INCIBE 2	ULE 1	ULE 2	ULE 5
	Tarde (15:30 - 21:30)					

		Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
Viernes 29 Julio	**Mañana (9:00 - 14:30)**	**Seminario Magistral 3** APT: Casos de uso Vicente Díaz **Seminario Magistral 4** Ciberseguridad Industrial Elyoenai Egozcue				
		Auditorio Ciudad de León				
Sábado 30 Julio	**Mañana (11:30 - 15:30)**	**Clausura**				
		Auditorio Ciudad de León				

CURSO DE ESPECIALIZACIÓN PARA CERTs

		Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
Domingo 17 Julio	**Tarde (16:30 - 21:30)**	**Inauguración**				
		Auditorio Ciudad de León				
Lunes 18 Julio	**Mañana (8:30 - 14:30)**	**Taller 12** Análisis forense Windows y Linux (I) Juan Garrido		**Taller 9** Gestión de incidentes de seguridad Javier Berciano (INCIBE) Francisco Losada (INCIBE)	**Taller 10** Seguridad en redes (I) Raúl Siles	**Taller 3** Análisis de malware Ricardo J. Rodríguez
		ULE 4		ULE 2	INCIBE 1	ULE 3
	Tarde (15:30 - 21:30)		**Taller 2** Análisis forense en dispositivos móviles Lorenzo Martínez			
			ULE 5			
Martes 19 Julio	**Mañana (8:30 - 14:30)**	**Taller 13** Análisis forense Windows y Linux (II) Pedro Sánchez		**Taller 3** Análisis de malware Ricardo J. Rodríguez	**Taller 11** Seguridad en redes (II) *Pendiente*	**Taller 10** Seguridad en redes (I) Raúl Siles
		ULE 6		ULE 3	ULE 4	INCIBE 1
	Tarde (15:30 - 21:30)		**Taller 12** Análisis forense Windows y Linux (I) Juan Garrido			

		Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
			ULE 4			
Miércoles 20 Julio	**Mañana (8:30 - 14:30)**	**Taller 3** Análisis de malware Ricardo J. Rodríguez	**Taller 13** Análisis forense Windows y Linux (II) Pedro Sánchez	**Taller 2** Análisis forense en dispositivos móviles Lorenzo Martínez	**Taller 9** Gestión de incidentes de seguridad Javier Berciano (INCIBE) Francisco Losada (INCIBE)	**Taller 11** Seguridad en redes (II) *Pendiente*
		ULE 3	ULE 6	ULE 5	INCIBE 1	ULE 4
	Tarde (15:30 - 21:30)	**Seminario Magistral OEA** (2h)				
		Auditorio INCIBE				
Jueves 21 Julio	**Mañana (8:30 - 14:30)**	**TC FIRST** (8:00h - 15:30h)				
		Auditorio INCIBE				
	Tarde (15:30 - 21:30)	**International CyberEx** (8h en horario de tarde -- 16:00h - 00:00h) INCIBE				
		ULE				
Viernes 22 Julio	**Mañana (9:00 - 11:30)**	**Revisión International CyberEx** (1h) - (10:30-11:30) INCIBE				

		Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
		Centro Cívico León Oeste				
	Mañana (12:00 - 14:30)	**Seminario Magistral 2** Seguridad ofensiva David Barroso				
		Auditorio Ciudad de León				
Lunes 25Julio	**Mañana (8:30 - 14:30)**	**Taller 10** Seguridad en redes (I) Raúl Siles	**Taller 3** Análisis de malware Ricardo J. Rodríguez	**Taller 12** Análisis forense Windows y Linux (I) Juan Garrido	**Taller 2** Análisis forense en dispositivos móviles Lorenzo Martínez	**Taller 9** Gestión de incidentes de seguridad Javier Berciano (INCIBE) Francisco Losada (INCIBE)
		INCIBE 1	ULE 3	ULE 4	ULE 5	ULE 2
	Tarde (15:30 - 21:30)					
Martes 26 Julio	**Mañana (8:30 - 14:30)**	**Taller 11** Seguridad en redes (II) *Pendiente*	**Taller 10** Seguridad en redes (I) Raúl Siles		**Taller 12** Análisis forense Windows y Linux (I) Juan Garrido	**Taller 2** Análisis forense en dispositivos móviles Lorenzo Martínez
		ULE 7	INCIBE 1		ULE 4	ULE 5

		Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
	Tarde (15:30 - 21:30)			**Taller 13** Análisis forense Windows y Linux (II) Pedro Sánchez ULE 6		
Miércoles 27 Julio	**Mañana (8:30 - 14:30)**	**Taller 9** Gestión de incidentes de seguridad Javier Berciano (INCIBE) Francisco Losada (INCIBE) INCIBE 2	**Taller 11** Seguridad en redes (II) *Pendiente* ULE 7	**Taller 10** Seguridad en redes (I) Raúl Siles INCIBE 1		**Taller 12** Análisis forense Windows y Linux (I) Juan Garrido ULE 4
	Tarde (15:30 - 21:30)				**Taller 13** Análisis forense Windows y Linux (II) Pedro Sánchez ULE 6	
Jueves 28 Julio	**Mañana (8:30 - 14:30)**		**Taller 9** Gestión de incidentes de seguridad Javier Berciano (INCIBE) Francisco Losada (INCIBE) INCIBE 1	**Taller 11** Seguridad en redes (II) *Pendiente* ULE 7	**Taller 3** Análisis de malware Ricardo J. Rodríguez ULE 3	**Taller 13** Análisis forense Windows y Linux (II) Pedro Sánchez ULE 6
	Tarde (15:30 - 21:30)	**Taller 2** Análisis forense en dispositivos móviles Lorenzo Martínez ULE 5				

		Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
Viernes 29 Julio	**Mañana (9:00 - 14:30)**	**Seminario Magistral 3** APT: Casos de uso Vicente Díaz **Seminario Magistral 4** Ciberseguridad Industrial Elyoenai Egozcue				
		Auditorio Ciudad de León				
Sábado 30 Julio	**Mañana (11:30 - 15:30)**	**Clausura**				
		Auditorio Ciudad de León				

SIMÓN ROSES

Licenciado en Informática por Suffolk University (Boston), Postgrado en E-Commerce, Harvard University (Boston) y Executive MBA, Instituto de Empresa (IE, Madrid). En la actualidad es el Fundador y CEO de VULNEX. Anteriormente formó parte de Microsoft, PriceWaterhouseCoopers y @Stake.
Creador y colaborador en varios proyectos de código abierto de seguridad como OWASP Pantera y LibExploit, además de publicar avisos en seguridad de conocidos productos.
Ha obtenido una beca del DARPA Cyber Fast Track (CFT) para investigar sobre seguridad en el ciclo de desarrollo de software.
Ponente habitual en eventos del sector de seguridad incluyendo Black Hat, RSA, OWASP, DeepSec, SOURCE, AppSec y Technets de seguridad de Microsoft.
CISSP, CEH y CSSLP.

TALLER 1

OSINT: herramientas, técnicas de búsqueda y análisis de información

Descripción

Internet es un mar de información de todo tipo, lista para ser recolectada, analizada, visualizada e interpretada. Este curso altamente práctico emplea las últimas tendencias en análisis de fuentes abiertas para identificar la información relevante (OSINT).

Mediante una serie de ejercicios prácticos los alumnos utilizarán potentes herramientas de OSINT e incluso desarrollarán las suyas propias para explorar fuentes de información en Internet.

Temario

- Introducción al OSINT
- El Internet de las API
- Uso de herramientas OSINT
- Recolección y visualización de información
- Análisis de ficheros y metadatos
- Ejercicio final

LORENZO MARTÍNEZ

Lorenzo es ingeniero informático, CTO (Chief Technology Officer) de la empresa Securízame (https://www.securizame.com), perito informático forense, miembro de ANCITE (Asociación Nacional de Ciberseguridad y Pericia Tecnológica), asociación de la que forma parte de la junta directiva. Escritor y cofundador en Security By Default (www.securitybydefault.com), uno de los blogs más importantes sobre seguridad informática de habla hispana.
Reconocido ponente en congresos nacionales e internacionales (España, México, Colombia, Chile, Argentina, Bolivia, entre otros), ha sido profesor en materias relacionadas con seguridad informática y forense en másteres de diversas universidades, Colegios de Ingenieros, así como otras instituciones, entre las que destacan el Grupo de Delitos Telemáticos de la Guardia Civil y el CERT (Computer Emergency Response Team) de INCIBE.

TALLER 2

Análisis Forense en Dispositivos Móviles

Descripción

Los smartphones y tablets se han convertido en una herramienta indispensable en el día a día de los usuarios. Estos dispositivos no solo son capaces de almacenar información referente a la agenda de contactos, fotografías, mensajes, música o vídeos, sino que también pueden almacenar una gran cantidad de información que puede resultar de especial relevancia en casos de investigaciones y/o análisis forense.
Precisamente el uso extendido de los dispositivos móviles, y en muchas ocasiones sin grandes medidas de seguridad en el acceso a los mismos por parte de todos, incluidos los cibercriminales, habilita una vía de obtención de información que puede resultar decisiva en el desenlace de una investigación policial.
Por ello, esta sesión pretende profundizar en el conocimiento necesario para la realización de un análisis forense a dispositivos móviles y mostrar el correcto uso de herramientas que faciliten la realización de este análisis, con el fin de extraer la información sensible a ser utilizada en un caso real.

Temario

- Conceptos forenses y estándares
- Fases de un análisis forense de un dispositivo móvil y cadena de custodia. Gestión de evidencias.
- Formas de adquisición de evidencias
  - Dispositivo encendido
  - Dispositivo apagado
  - Backup
  - Nube
- Adquisición de evidencias en Android
- Adquisición de evidencias en IOS

RICARDO RODRÍGUEZ

Ricardo J. Rodriguez tiene un Máster y un Doctorado en Ciencias Informáticas por la Universidad de Zaragoza, España, en 2010 y 2013 respectivamente. Su exposición del Doctorado versaba en el análisis del comportamiento y optimización de recursos en sistemas críticos, con un foco especial en técnicas de modelado de redes Petri. Actualmente es profesor adjunto de la Universidad de Zaragoza, España. También es profesor invitado en la Universidad Seconda de Nápoles, en el segundo semestre del 2016.
Sus campos de investigación incluyen análisis de comportamiento y dependencia, optimización de sistemas amplios y distribuidos, análisis de códigos binarios y seguridad en tarjetas inalámbricas.
Ha participado como ponente (y formador) en numerosas conferencias de seguridad como NoConName, Hack.LU, RootedCON, Hack en Paris, MalCON, o Hack en el Box Amsterdam, entre otras. El Dr. Rodríguez también ha participado en trabajos de revisión de conferencias y medios de comunicación internacionales.

TALLER 3

Análisis de malware (I)

Descripción

Actualmente, los problemas de ciberseguridad relacionados con código malicioso o malware continúan creciendo. De hecho, muchas organizaciones todavía consideran que el código malicioso es su principal fuente de ataque.
El objetivo de esta sesión es realizar una aproximación al malware para que los agentes de los cuerpos y fuerzas de seguridad del estado sepan de los conocimientos básicos en el análisis de malware y dispongan de los procedimientos y buenas prácticas recomendadas en caso de que tengan que gestionar incidentes de ciberseguridad relacionados con código malicioso.
También se presentarán herramientas y aplicaciones que permiten obtener información relevante del malware.

Temario

- Introducción al malware
  - Características, tipos y evolución del malware
  - Ataques masivos vs ataques dirigidos.
  - Vectores de infección
- Cazando el malware
  - Detección y búsqueda del malware
  - Obtención de información
- Análisis estático de malware
  - Preparación del entorno de trabajo, aislamiento
  - Procedimiento de análisis
  - Técnicas y utilidades
  - Utilidades de terceros
- Este taller se complementará con el taller 4.

JOSE MIGUEL ESPARZA

Jose Miguel Esparza es un investigador de seguridad que lleva trabajando como Threat Analyst desde 2007, especializado en botnets, malware y cibercrimen. Después de trabajar durante varios años en S21sec e-crime se incorporó a la compañía holandesa Fox-IT, donde actualmente lidera el equipo de inteligencia conocido como InTELL. Es el autor de la herramienta de seguridad peepdf y suele escribir en eternal-todo.com sobre seguridad y amenazas en Internet cuando el tiempo lo permite. Ha tomado parte en diversas conferencias locales e internacionales como RootedCon, Source, Black Hat, Troopers y Botconf, entre otras. Se le puede encontrar fácilmente en Twitter, @EternalToDo, hablando sobre seguridad.

TALLER 4

Análisis de malware (II)

Descripción

Con el objetivo de reforzar y extender las lecciones aprendidas en el Taller 3 - Análisis de malware (I): Introducción, herramientas, preparación de entornos y análisis estático esta sesión se centrará en el análisis dinámico de malware en sistemas Windows, mostrando otra forma de extraer información útil al ejecutar código malicioso.

Temario

- Preparación del laboratorio de malware
- Monitorización del código malicioso
  - Extracción y análisis de Indicadores de Compromiso (IOCs)
    - Archivos del sistema
    - Registro de Windows
    - Tráfico de red
  - Técnicas de anti-análisis y anti-VM
- Depuración de código malicioso (dependiendo del nivel del grupo)

PEDRO SÁNCHEZ

Responsable del Equipo de Cyber Incident Response de Deloitte. Pedro ha trabajado en importantes empresas como consultor especializado en Computer Forensics, Honeynets, detección de intrusiones,redes trampa y pen-testing. Ha implantado normas ISO 27001, CMMI (nivel 5), PCI-DSS y diversas metodologías de seguridad especialmente en el sector bancario durante mas de diez años.
Colaborador habitual sobre seguridad, peritaje y análisis forense informático con diversas organizaciones comerciales y con las fuerzas y empresas de seguridad del estado, especialmente con el Grupo de Delitos Telemáticos de la Guardia Civil (GDT), la Unidad de Investigación Tecnológica de la policía nacional (UIT), INCIBE y Ministerio de Defensa.
Ha participado en las jornadas JWID/CWID organizadas por el ministerio de defensa, en donde obtuve la certificación OTAN SECRET.
Actualmente es miembro de la Spanish Honeynet Project , fundador del blog Conexión Inversa y trabaja como responsable del servicio de "incident response & DDoS protection" en Deloitte.También es Perito Judicial Informático adscrito a la Asociación Nacional de Ciberseguridad y Pericia Tecnológica (ANCITE) https://honeynet-es.org/
http://conexioninversa.blogspot.com.es/
http://www.ancite.es/w3/

TALLER 5

Análisis forense de sistemas Windows (I)

Descripción
Finalizado este módulo, el asistente dispondrá de conocimientos y capacidades para poder llevar a efecto un análisis forense digital, tanto en el ámbito de los sistemas operativos, como en el de las aplicaciones soportadas. Para ello se le hará conocedor de las arquitecturas internas de los sistemas operativos, así como su operativa. Finalizado el módulo, igualmente será conocedor de las posibilidades y metodologías para la localización de evidencias y su posterior análisis.
En el desarrollo del módulo se capacitará al asistente para el desarrollo de análisis forenses desde diversas perspectivas: Sistema operativo Windows 7/8, procesos y ficheros LOG fundamentalmente.

Temario

- Sistema operativo Windows
  - Diferencias entre Windows 7 y Windows 8
- Tratamiento de las evidencias
  - Análisis de navegación
  - Análisis temporal de la información
  - Búsquedas basadas en firmas
  - Análisis de la papelera de reciclaje
  - El registro del sistema
- Análisis Forense de procesos
  - Procesos en Windows
  - Tipos de cuentas en Windows
  - Análisis y correlación de procesos
  - Relación de procesos, puertos y conexiones realizadas
- Análisis Forense de logs
  - Análisis de registros
  - CLas auditorías de los sistemas
  - onsolidación del logs
  - Correlación y forense

JUAN GARRIDO

Juan Garrido es un apasionado de la seguridad. Trabaja en la firma de seguridad Grupo NCC como consultor especializado en evaluaciones de seguridad y respuesta a incidentes. En sus más de nueve años como profesional de seguridad, también ha trabajado en diferentes proyectos de seguridad e investigaciones judiciales. Juan ha escrito varios libros técnicos y herramientas de seguridad. Es autor de la herramienta de seguridad VOYEUR y también escribe con frecuencia en diversas revistas técnicas Españolas como Trade Press y Digital Media.
Juan ha sido reconocido como MVP, Microsoft Most Valuable Professional, en Seguridad Corporativa, actualmente renombrada a Gestión de la Nube y Centros de Datos. Ha participado como ponente en muchas conferencias como RootedCon, GsickMinds, DEFCON, Troopers, BlackHat, etc.
Puedes encontrarle hablando de seguridad en Twitter @tr1ana, o en su blog Security By Default

TALLER 6

Análisis forense de sistemas Windows (II)

Descripción
Finalizado este módulo, el asistente dispondrá de conocimientos y capacidades avanzadas para poder llevar a efecto un análisis forense digital, desde la perspectiva de la memoria, así como de la red. Para ello se le hará conocedor de las arquitecturas internas de los sistemas operativos, así como su operativa interna. Durante el desarrollo del módulo se incluirá un punto específico sobre técnicas anti-forense. Finalizado el módulo, igualmente será conocedor de las posibilidades y metodologías para la localización de evidencias y su posterior análisis.
En el desarrollo del módulo se capacitará al asistente para el desarrollo de análisis forenses desde diversas perspectivas: Sistema operativo Windows 7/8, procesos, memoria RAM, análisis de Red y técnicas anti-forense. En los puntos finales del módulo se analizarán aquellas acciones que puedan ir dirigidas a la eliminación de evidencias o a dificultar en algún término las tareas de análisis, así como posibles metodologías que permitan eliminar estas dificultades en el desarrollo del análisis forense digital.

Temario

- Sistema operativo Windows
  - Diferencias entre Windows 7 y Windows 8
- Análisis Forense de memoria RAM
  - Procesos en Windows
  - Tipos de cuentas en Windows
  - Relación de procesos, puertos y conexiones realizadas
  - Extracción de memoria en Windows
  - Uso y utilización de volatility Framework
- Análisis Forense de memoria RAM
  - Las auditorías de los sistemas
  - Análisis de registros
  - Consolidación del logs
  - Correlación y forense
- Antiforense
  - Las técnicas antiforense
  - Ocultación de evidencias
  - Eliminación de datos
  - Alteración de la información
  - Detección de trazas antiforense
- Análisis de tráfico de Red
  - Tipos de ataque
  - Pentest Fingerprint
  - Análisis de protocolos
  - Mapas y gráficos de conexiones

JESÚS DÍAZ

Jesús Díaz Vico es arquitecto software en BEEVA, especializado en criptografía y en tecnología blockchain. Ha trabajado y colaborado como investigador en criptografía en varios laboratorios (UAM, UPM y Columbia) y en compañías como el Instituto Nacional de Ciberseguridad (INCIBE). Es ingeniero en informática por la UAM desde 2007, máster en tecnologías de la información por la UPM desde 2010 y doctor en informática por la UAM desde 2015. Entre sus campos de investigación e interés destaca la criptografía aplicada al anonimato y a la privacidad, el análisis de seguridad de protocolos de comunicaciones, los sistemas distribuidos y la descentralización de la confianza.

TALLER 7

Cifrado, Navegación anónima y Deep Web

Descripción

Internet es la red global compuesta por cientos de miles de ordenadores a la cual solemos acceder a través de un navegador (Firefox, Chrome, Safari...) y ayudados por un buscador (Google, Bing, DuckDuckGo...). No obstante, la información que podemos obtener a través de estos mecanismos "comunes" no es más que una pequeña porción del total. Términos como deep web y dark web son cada vez más frecuentes en el mundo tecnológico, especialmente después de escándalos como Silk Road y otros mercados ilegales o del apoyo recibido por activistas de la privacidad como Edward Snowden o Julian Assange. En este curso, estudiaremos sus orígenes, conceptos fundamentales, funcionamiento y mecanismos de análisis.

Temario

- Introducción al curso.
  - Motivación y resumen de contenidos.
- Internet, deep web y dark web.
  - Resumen, definiciones y comparación.
- Conceptos básicos:
  - Recordatorio de protocolos de comunicaciones.
  - Hashes.
  - Criptografía simétrica.
  - Criptografía asimétrica.
  - Intercambio de claves.
  - Protocolos criptográficos.
- Tor en detalle:
  - Orígenes y propiedades.
  - Creación de circuitos.
  - Servicios ocultos.
- Otras sistemas de anonimato, usos y aplicaciones:
  - I2P, Freenet, Crowds, proxies anonimizadores, etc.
  - Mercados ilegales, protección anti-censura.
  - Relación con criptomonedas.
- Análisis:
  - Revisión de los distintos ataques a Tor y otras redes de anonimato.

YAIZA RUBIO

Licenciada en Ciencias de la Información, Máster en Análisis de Inteligencia y Máster en Logística y Economía de la Defensa. Miembro del Instituto de Ciencias Forenses de la UAM, desde mayo de 2013 ejerce como analista de inteligencia para Eleven Paths tras haberlo hecho en empresas como S21sec e Isdefe, además de ser colaboradora del Centro de Análisis y Prospectiva de la Guardia Civil.
Es docente a nivel universitario en cursos de postgrado sobre análisis de inteligencia, seguridad y fuentes abiertas y también se dedica a la publicación de contenidos científico-técnicos.

FÉLIX BREZO

Félix Brezo es Ingeniero en Informática e Ingeniero en Organización Industrial, Máster en Seguridad de la Información, Máster en Análisis de Inteligencia y Doctor en Ingeniería Informática y Telecomunicación.
Hasta junio de 2013, investigador en seguridad informática en el S3Lab de la Universidad de Deusto y, a partir de entonces, analista de inteligencia para Eleven Paths, además de colaborador del Centro de Análisis y Prospectiva, docente a nivel universitario sobre análisis de inteligencia y seguridad y divulgador de contenidos científico-técnicos.

TALLER 8

Hacking Avanzado: Técnicas de hacking en la era OSINT

Descripción

Hoy, el problema para los que trabajan en la industria de la seguridad no es la falta de información, sino discernirla y procesarla entre la disponible. Además, gracias al proceso de traspaso y fagocitación por parte de la nube (otras empresas que en realidad ofrecen los servicios), cada vez es menos eficaz recabar información que puedan ofrecer los propios servidores o recursos de una organización o individuo, sino que es necesario tomarla de los sistemas globales públicos desde donde está dispersa. Es posible que tenga más valor hoy día conocer el perfil de un administrador en una red social, que los puertos que mantiene abiertos en sus supuestos servidores.
El taller se centrará en uno de los temas más relevantes relativos al hacking avanzado: la búsqueda, análisis y síntesis de la información; el tratamiento eficaz que permita una investigación productiva. Para conseguirlo, son necesarias herramientas que permitan no solo recoger, sino procesar y comprender los datos que provienen de fuentes de información tan extensas como las redes sociales. Una vez conseguido, en una capa superior liderada por el analista, será necesario construir sistemas que le permitan operar cómodamente y detectar esa anomalía, relación, patrón o información que realmente le interesa.

Temario

-Hacking. Introducción. (2 horas).
-Análisis y procesado avanzado de información en la web. (1'5 horas).
-Análisis y procesado de información en el mundo móvil. (1'5 horas).

JAVIER BERCIANO

Javier Berciano es el responsable de respuesta a incidentes en el CERT de Seguridad e Industria (antes INTECO-CERT), liderando al equipo y realizando tareas de gestión de incidentes, análisis forense, detección, análisis y monitorización de amenazas. Lleva más de una década dedicándose profesionalmente a la seguridad informática y posee diversas certificaciones relacionadas con el mundo de la seguridad TIC como CISSP, GCFA y CISA entre otras.
Ha participado como ponente en múltiples conferencias internacionales como FIRST Conference y Symposiums, Microsoft DCC, National CSIRT meetings, TF-CSIRT, Trusted Introducer, Microsoft DCU Threat Intelligence, Foro ABUSES, ENISE, etc.

FRANCISCO LOSADA

D. Francisco LOSADA es coordinador de Operaciones de Ciberseguridad en el Instituto Nacional de Ciberseguridad. Desempeña sus funciones como parte del equipo técnico del CERT de Seguridad e Industria (CERTSI) focalizándose en la respuesta a incidentes y análisis forenses relacionados con amenazas a infraestructuras críticas. Entre sus tareas se encuentra también la coordinación de ciber ejercicios para las entidades que proporcionan los servicios esenciales a nuestra sociedad. Antes de unirse a INCIBE, D. Francisco Losada formó parte del equipo de ISDEFE que presataba servicios para el CERT del entonces Instituto Nacional de Tecnologías de la Comunicación. El Sr. LOSADA posee diversas certificaciones técnicas en el área de seguridad e investigación forense (GIAC, EC-Council, Cellebrite…). Desde el año 2013 pertenece a la Asociación Nacional de Ciberseguridad y Pericia Tecnológica.

TALLER 9

Gestión de incidentes de seguridad

Descripción

La misión principal de un CERT es la de proporcionar un servicio de apoyo en la gestión
de incidentes de seguridad. Los compromisos y la violación de la seguridad TIC de una organización son una realidad. Cuando los incidentes ocurren, los CERT deben estar preparados para realizar una adecuada gestión a nivel técnico y organizativo. Para ello es importante conocer en detalle las diferentes fases del ciclo de vida de un incidente y como abordar cada una de ellas, antes, durante y después de que se produzca el incidente.

Durante este curso se profundizará de manera práctica y mediante el uso de herramientas sobre supuestos incidentes, con la intención de poder ofrecer un soporte y respuesta adecuados en todas las fases del incidente.

Temario

- Aspectos formales de los CERT

- Fases de la gestión de incidentes:
  - Preparación
  - Identificación
  - Contención
  - Erradicación
  - Recuperación
  - Lecciones aprendidas

RAÚL SILES

Raúl Siles es fundador y analista de seguridad senior de DinoSec. Durante más de una década, ha aplicado su experiencia en la realización de servicios de seguridad técnicos avanzados y ha innovado soluciones ofensivas y defensivas para grandes empresas y organizaciones en diversas industrias de todo el mundo. A lo largo de su carrera, a partir de una sólida formación técnica, ha trabajado como experto en
seguridad en Hewlett Packard, como consultor independiente, y en sus propias empresas, Taddong
y DinoSec .

TALLER 10

Seguridad en redes (I)

Descripción

Una de las actividades más comunes en la investigación de incidentes de seguridad consiste en el análisis de la presencia y del estado de múltiples equipos y servicios en las redes de comunicaciones de datos, así como de su tráfico de red, con el objetivo de obtener la máxima información sobre el tipo de ataque, los activos implicados y las posibles acciones de remediación. Para ello se debe conocer con mucho detalle los dispositivos y servicios existentes en una red, su comportamiento y obtener información adicional a través del tráfico de red asociado.

El objetivo de este taller es profundizar de manera práctica, mediante herramientas como nmap, wireshark, o proxies de interceptación web, en los aspectos técnicos asociados al funcionamiento y comportamiento de TCP/IP para el descubrimiento e identificación de equipos, el escaneo activo de redes, y el análisis e interceptación de tráfico.

Temario

-Funcionamiento y comportamiento de TCP/IP
-Descubrimiento de la red y de sus elementos
-Filtrado de tráfico
-Escaneos de red activos
  Identificación de equipos
  Escaneos de puertos
  Identificación de SO y servicios
-Análisis del tráfico de red
  4 W
-Interceptación de tráfico
  Protocolos web: HTTP, HTTP2, WebSockets…
-Descifrado de tráfico
-Tráfico de redes inalámbricas Wi-Fi

JUAN GARRIDO

Juan Garrido es un apasionado de la seguridad. Trabaja en la firma de seguridad Grupo NCC como consultor especializado en evaluaciones de seguridad y respuesta a incidentes. En sus más de nueve años como profesional de seguridad, también ha trabajado en diferentes proyectos de seguridad e investigaciones judiciales. Juan ha escrito varios libros técnicos y herramientas de seguridad. Es autor de la herramienta de seguridad VOYEUR y también escribe con frecuencia en diversas revistas técnicas Españolas como Trade Press y Digital Media.
Juan ha sido reconocido como MVP, Microsoft Most Valuable Professional, en Seguridad Corporativa, actualmente renombrada a Gestión de la Nube y Centros de Datos. Ha participado como ponente en muchas conferencias como RootedCon, GsickMinds, DEFCON, Troopers, BlackHat, etc.
Puedes encontrarle hablando de seguridad en Twitter @tr1ana, o en su blog Security By Default

TALLER 12

Análisis forense Windows y Linux (I)

Descripción
Finalizado este módulo, el asistente dispondrá de conocimientos y capacidades para poder llevar a efecto un análisis forense digital bajo arquitecturas Windows o Linux. Para ello se le hará conocedor de las arquitecturas internas de los sistemas operativos, así como su operativa. Finalizado el módulo, igualmente será conocedor de las posibilidades y diversas metodologías para la localización de evidencias y su posterior análisis.
En el desarrollo del módulo se capacitará al asistente para el desarrollo de análisis forenses desde una perspectiva de *análisis en vivo*: Procesos y ficheros, extracción de memoria RAM, principales artifacts en cada uno de los sistemas operativos, etc...

Temario

-Sistema operativo
- Diferencias entre Windows 7 y Windows 8
- Arquitectura de Linux

-Kits de respuesta ante incidentes
- Basados en Agente
- Sin Agente

-Extracción de evidencias
- Navegación
- Conexiones de red
- Aplicaciones
- Sistema de ficheros
- Módulos

-Análisis de línea temporal
- Cuándo un sistema ha sido actualizado, arrancado, parado, etc...
- Análisis de creación/Modificación de ficheros (Malware)
- Ocultación & Ex-filtración de datos
- Relación de procesos, puertos y conexiones realizadas

-Análisis Forense de logs
- Las auditorías de los sistemas
- Análisis de registros
- Consolidación del logs
- Correlación y forense

PEDRO SÁNCHEZ

Responsable del Equipo de Cyber Incident Response de Deloitte.
Pedro ha trabajado en importantes empresas como consultor especializado en Computer Forensics, Honeynets, detección de intrusiones,redes trampa y pen-testing. Ha implantado normas ISO 27001, CMMI (nivel 5), PCI-DSS y diversas metodologías de seguridad especialmente en el sector bancario durante mas de diez años.
Colaborador habitual sobre seguridad, peritaje y análisis forense informático con diversas organizaciones comerciales y con las fuerzas y empresas de seguridad del estado, especialmente con el Grupo de Delitos Telemáticos de la Guardia Civil (GDT), la Unidad de Investigación Tecnológica de la policía nacional (UIT), INCIBE y Ministerio de Defensa.
Ha participado en las jornadas JWID/CWID organizadas por el ministerio de defensa, en donde obtuve la certificación OTAN SECRET.
Actualmente es miembro de la Spanish Honeynet Project , fundador del blog Conexión Inversa y trabaja como responsable del servicio de "incident response & DDoS protection" en Deloitte.También es Perito Judicial Informático adscrito a la Asociación Nacional de Ciberseguridad y Pericia Tecnológica (ANCITE).
https://honeynet-es.org/
http://conexioninversa.blogspot.com.es/
http://www.ancite.es/w3/

TALLER 13

Análisis forense Windows y Linux (II)

Descripción
Finalizado este módulo, el asistente dispondrá de conocimientos y capacidades para poder llevar a efecto un análisis forense digital bajo arquitecturas Windows o Linux. Para ello se le hará conocedor de las arquitecturas internas de los sistemas operativos, así como su operativa. Finalizado el módulo, igualmente será conocedor de las posibilidades y diversas metodologías para la localización de evidencias y su posterior análisis.
En el desarrollo del módulo se capacitará al asistente para el desarrollo de análisis forenses desde una perspectiva de *análisis offline*: Procesos y ficheros, análisis de memoria RAM, principales artifacts en cada uno de los sistemas operativos, etc...

Temario

-Sistema operativo
- Diferencias entre Windows 7 y Windows 8
- Arquitectura de Linux

-Kits de respuesta ante incidentes
- Basados en Agente
- Sin Agente

-Montaje de evidencias
- Montaje de evidencias en Linux
- Montaje de evidencias en Windows

-Análisis de línea temporal
- Cuándo un sistema ha sido actualizado, arrancado, parado, etc...
- Análisis de creación/Modificación de ficheros (Malware)
- Ocultación & Ex-filtración de datos
- Relación de procesos, puertos y conexiones realizadas

-Análisis Forense de RAM con volatility
- Perfiles de volatility
- Análisis de registros
- Análisis de procesos
- Recuperación de la memoria de un proceso
- Detección de Malware

DAVID BARROSO

David Barroso lleva más de 15 años trabajando en seguridad, en aspectos tan diferentes como respuesta ante incidentes, inteligencia, o seguridad en las redes y sistemas. Actualmente es el fundador de CounterCraft, cuyo objetivo es ayudar a empresas y gobiernos de todo el mundo a definir y desplegar campañas de contra-inteligencia digital. Anteriormente, ha sido el CTO De ElevenPaths, la empresa de seguridad de Telefónica y Responsable de Inteligencia de Seguridad en Telefónica Digital.
Antes de incorporarse a Telefónica, fue el coordinador de Seguridad en AT&T para España y Portugal, y posteriormente el Director de e-crime de S21sec, donde contaba con un equipo de más de 30 personas para combatir el cibercrimen, ayudando a compañías y gobiernos de todo el mundo a prevenir y responder ante cualquier amenaza.
David es un conferenciante habitual sobre temas de seguridad, riesgos en dispositivos móviles, cibercrimen, botnets, malware, DDoS, etc., y participa en numerosos grupos y eventos de seguridad por todo el mundo como BlackHat, RSA Conference, e-crime congress, APWG, FIRST, NATO, ENISA, Segurinfo, RootedCon o ICCyber entre otras.

SEMINARIO MAGISTRAL 2

Seguridad ofensiva.

Descripción
Cualquier empresa o gobierno es objetivo de ataques de forma sistemática; algunos ataques son oportunistas, otros aleatorios o, incluso, dirigidos. La gran mayoría de estrategias de seguridad se centran enteramente en la defensa y protección de nuestros activos, pero muy pocas exploran los beneficios de ser más activos. Durante la sesión, explicaremos en qué consiste la defensa activa, así como sus principales beneficios:

- Conseguir que al atacante le sean más costosos sus esfuerzos (minimizar su Retorno de Inversión (ROI))
- Aprovechar su momentum e inercia en nuestro beneficio
- Obtener la máxima información del atacante
- Alertar de forma temprana compromisos o fases iniciales de un ataque

> SEMINARIO MAGISTRAL

VICENTE DÍAZ

Vicente se incorporó al equipo de Kaspersky Lab's Global Research & Analysis en noviembre del 2010. Está especializado en Threat Intelligence y también investiga malware y fraude en la región Europea, lo que incluye troyanos bancarios, amenazas en redes sociales, redes de ciberdelincuentes y malware en móviles. Además, Vicente lidera proyectos técnicos de investigación y proporciona soporte técnico a clientes.
Anteriormente a su incorporación en Kaspersky Lab, Vicente trabajó como Desarrollador Software en IT&C y Actaris, después de lo cual accedió a un puesto de investigación en la Universidad Politécnica de Cataluña (UPC). Posteriormente pasó al mundo de la ciberseguridad en S21Sec, trabajando primero como pentester y luego como gestor de e-crimen. Vicente es autor de diferentes herramientas software aparte de ser un miembro activo en el entorno de las conferencias, tanto como organizador como ponente. Fue miembro del consejo asesor de Source Conference y es co-fundador de Edge-Security, un grupo de seguridad dedicado a la investigación y organización de eventos sin ánimo de lucro.
Vicente es Ingeniero Informático y tiene un máster en inteligencia artificial.

SEMINARIO 3

APT: Casos de uso

Descripción

Esta ponencia proporciona información acerca de las APTs que están en máximo apogeo en la actualidad y sobretodo cómo se investigan. Se trata de dar consejos útiles, ejemplos reales de uso de herramientas, y descripción de cómo se aplican en la práctica, así como proporcionar un contexto completo de aplicación y referencias. La agenda sería:

- Introducción a APTs modernas: descripción de grupos, técnicas utilizadas, actores e intereses de los mismos.
- Investigación de APTs: técnicas y herramientas para el descubrimiento de APTs, análisis de evidencias, correlación de datos, gestión de TTPs y generación de inteligencia
- Gestión de inteligencia: almacenamiento, compartición y correlación de información, indicadores y TTPs para la gestión de inteligencia.
- Resumen, consejos, conclusiones, materiales adicionales.

> SEMINARIO MAGISTRAL

NOMBRE APELLIDO

Ingeniero superior de telecomunicación por la Universidad Pública de Navarra (UPNA), realizó su proyecto fin de carrera sobre calidad de servicio (QoS) en redes IP sobre WDM en la Universidad Libre de Bruselas BUV. Fue investigador de seguridad en S21sec Labs entre 2006 y 2008, donde trabajó en varios proyectos punteros de consultoría en RFID, MPLS, ciberinteligencia y biometría. Entre 2008 y 2011, fue responsable técnico de varios proyectos de investigación a nivel nacional y europeo sobre los sistemas digitales de control utilizados en infraestructuras críticas, incluyendo entre otros el proyecto INSPIRE del 7º Programa Marco. Entre 2011 y 2013 fue Project Manager de distintos proyectos, tanto de investigación como para cliente final, en ICS/SCADA y seguridad Smart Grid. Entre ellos destacan servicios de consultoría tecnológica, de cumplimiento y auditoría para plantas nucleares e infraestructuras de distribución de gas y electricidad, y contadores inteligentes. Ha colaborado activamente con ENISA, tanto a nivel personal como profesional, liderando en este caso varios proyectos en seguridad ICS/SCADA y Smart Grid. Desde 2014 es manager de la línea de negocio de servicios de Ciberseguridad en IACS/SCADA y Smart Grids de S21sec.

SEMINARIO 4

Ciberseguridad Industrial

Los contenidos se estructurarán como sigue:

Primera parte (30'): La problemática de la ciber(in)seguridad industrial

- Entorno de TI vs entorno de TO: objetivos de seguridad, vulnerabilidades, perfiles de las amenazas, riesgos.
- Presentación de los sistemas informáticos industriales en diferentes industrias.
- Presentación de los principales actores y sus roles: fabricantes, operadoras e ingenierías.

Segunda parte (50'): Técnicas de ataque y buenas prácticas de seguridad

- Repaso a los principales incidentes y grupos criminales en el ámbito de la seguridad industrial: lecciones aprendidas.
- Factores limitantes en la adopción de estrategias y tecnologías de seguridad de TI en el ámbito industrial.
- Buenas prácticas a nivel técnico y tecnológico: control de accesos, segmentación de red, criptografía, registro de eventos de seguridad, etc.
- Buenas prácticas a nivel organizativo: personas, procesos y procedimientos.

Tercera parte (40'): Soluciones tecnológicas y aproximación de los fabricantes industriales a la seguridad industrial

- Principales tecnologías de seguridad industrial
- Soluciones de fabricantes de nicho
- Soluciones de grandes fabricantes de seguridad
- Aproximación de los fabricantes industriales a la seguridad industrial

> SEMINARIO MAGISTRAL


GOBIERNO
DE ESPAÑA
MINISTERIO
DE INDUSTRIA, ENERGÍA
Y TURISMO


incibe_
2006-2016
TRABAJANDO POR
LA CONFIANZA DIGITAL