summer bootcamp

LEÓN - 2016

Organizan:

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

10 incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

CNPIC
CENTRO NACIONAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

Organización de los Estados Americanos

Con el apoyo de:

universidad de león

AYUNTAMIENTO DE LEÓN

ÍNDICE

1. ANTECEDENTES 3
2. DESCRIPCIÓN DEL EVENTO 5
3. PROGRAMAS 8
3.1. Taller 1 - OSINT: herramientas, técnicas de búsqueda y análisis de información 12
3.2. Taller 2 - Análisis forense en dispositivos móviles 12
3.3. Taller 3 - Análisis de malware (I): Introducción, herramientas, preparación de entornos y análisis estático 13
3.4. Taller 4 - Análisis de malware (II): Introducción, herramientas, preparación de entornos y análisis dinámico 14
3.5. Taller 5 - Análisis forense de sistemas Windows (I): Introducción y toma de evidencias 14
3.6. Taller 6 - Análisis forense de sistemas Windows (II): Análisis y documentación de evidencias 15
3.7. Taller 7 - Cifrado, navegación anónima y Deep Web. 15
3.8. Taller 8 – Hacking Avanzado. 16
3.9. Taller 9: Gestión de incidentes de seguridad. 16
3.10. Talleres 10 y 11: Seguridad en redes. 16
3.11. Talleres 12 y 13: Análisis forense dispositivos Windows y Linux. 16
4. REGISTRO 18

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:

- Organización de Estados Americanos **(OEA).**
- Oficina Europea de Policía **(EUROPOL).**
- Forum of Incident Response and Security Teams **(FIRST).**
- Ministerio de Asuntos Exteriores y Cooperación **(MAEC).**
- Ministerio del Interior **(MINIT).**
- 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)**
- 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 (FCSE / CERTs)			Talleres Técnicos (FCSE)	Revisión International CyberEX (CERTs) Seminarios Magistrales (FCSE / CERTs)		
Tarde			Presentación HELIOS (FCSE Españolas) Presentación International CyberEX (CERTs)	International CyberEX (CERTs)			
	25	26	27	28	29	30	31
Mañana	Talleres Técnicos (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 de países pertenecientes a la OEA[4].
  - Personal en activo de FCSE que trabajen en unidades operativas relacionadas con la ciberseguridad de países pertenecientes a EUROPOL[5].
  - Personal en activo de FCSE del territorio español que trabajen en unidades operativas relacionadas con la ciberseguridad[6].
- Formación CERTs:
  - Personal en activo de CERTs públicos de países latinoamericanos pertenecientes a la OEA[4].
  - 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[4].

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

[4] En este caso el acceso al curso requerirá de una validación previa por parte de la OEA.

[5] En este caso el acceso al curso requerirá que la solicitud provenga de la entidad competente del país perteneciente a EUROPOL

[6] En este caso el acceso al curso requerirá de una validación previa por parte de la Oficina de Coordinación Cibernética (OCC) del CNPIC.

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 seminarios magistrales de 2 horas de duración y que tendrán un componente más teórico orientado al total de los 200 asistentes.

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[7]

[7] 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

Fecha		Actividad Grupo 1	Actividad Grupo 2	Actividad Grupo 3	Actividad Grupo 4	Actividad Grupo 5
Semana 1	**Lunes 18**	**Taller 1** OSINT: herramientas, técnicas de búsqueda y análisis de información	**Taller 3** Análisis de malware (I)	**Taller 7** Cifrado, Navegación anónima y Deep Web	**Taller 2** Análisis forense en dispositivos móviles	**Taller 8** Hacking Avanzado
	Martes 19	**Taller 2** Análisis forense en dispositivos móviles	**Taller 4** Análisis de malware (II)	**Taller 3** Análisis de malware (I)	**Taller 1** OSINT: herramientas, técnicas de búsqueda y análisis de información	**Taller 7** Cifrado, Navegación anónima y Deep Web
	Miércoles 20	**Taller 3** Análisis de malware (I)	**Taller 8** Hacking Avanzado	**Taller 4** Análisis de malware (II)	**Taller 5** Análisis forense de sistemas Windows (I)	**Taller 1** OSINT: herramientas, técnicas de búsqueda y análisis de información
		Para las FCSE españolas en horario de tarde seminario práctico de presentación de HELIOS				
	Jueves 21	**Taller 4** Análisis de malware (II)	**Taller 1** OSINT: herramientas, técnicas de búsqueda y análisis de información	**Taller 2** Análisis forense en dispositivos móviles	**Taller 6** Análisis forense de sistemas Windows (II)	**Taller 5** Análisis forense de sistemas Windows (I)
	Viernes 22	**Seminario Magistral 1** El negocio del cibercrimen **Seminario Magistral 2** Seguridad ofensiva				
Semana 2	**Lunes 25**	**Taller 7** Cifrado, Navegación anónima y Deep Web	**Taller 5** Análisis forense de sistemas Windows (I)	**Taller 1** OSINT: herramientas, técnicas de búsqueda y análisis de información	**Taller 8** Hacking Avanzado	**Taller 6** Análisis forense de sistemas Windows (II)
	Martes 26	**Taller 8** Hacking Avanzado	**Taller 6** Análisis forense de sistemas Windows (II)	**Taller 5** Análisis forense de sistemas Windows (I)	**Taller 7** Cifrado, Navegación anónima y Deep Web	**Taller 3** Análisis de malware (I)

Fecha		Actividad Grupo 1	Actividad Grupo 2	Actividad Grupo 3	Actividad Grupo 4	Actividad Grupo 5
	Miércoles 27	**Taller 5** Análisis forense de sistemas Windows (I)	**Taller 2** Análisis forense en dispositivos móviles	**Taller 6** Análisis forense de sistemas Windows (II)	**Taller 3** Análisis de malware (I)	**Taller 4** Análisis de malware (II)
	Jueves 28	**Taller 6** Análisis forense de sistemas Windows (II)	**Taller 7** Cifrado, Navegación anónima y Deep Web	**Taller 8** Hacking Avanzado	**Taller 4** Análisis de malware (II)	**Taller 2** Análisis forense en dispositivos móviles
	Viernes 29	**Seminario Magistral 3** APT: Casos de uso **Seminario Magistral 4** Ciberseguridad Industrial				

CURSO DE ESPECIALIZACIÓN PARA CERTs

Fecha		Actividad Grupo 1	Actividad Grupo 2	Actividad Grupo 3	Actividad Grupo 4	Actividad Grupo 5
Semana 1	**Lunes 18**	**Taller 12** Análisis forense Windows y Linux (I)	**Taller 2** Análisis forense en dispositivos móviles	**Taller 3 y 4** Análisis de malware	**Taller 10** Seguridad en redes (I)	**Taller 9** Gestión de incidentes de seguridad
	Martes 19	**Taller 13** Análisis forense Windows y Linux (II)	**Taller 12** Análisis forense Windows y Linux (I)	**Taller 9** Gestión de incidentes de seguridad	**Taller 11** Seguridad en redes (II)	**Taller 10** Seguridad en redes (I)
	Miércoles 20	**Taller 9** Gestión de incidentes de seguridad	**Taller 13** Análisis forense Windows y Linux (II)	**Taller 2** Análisis forense en dispositivos móviles	**Taller 3 y 4** Análisis de malware	**Taller 11** Seguridad en redes (II)
		Presentación International CyberEx				
	Jueves 21	International CyberEx (8h en horario de tarde) INCIBE				

Fecha		Actividad Grupo 1	Actividad Grupo 2	Actividad Grupo 3	Actividad Grupo 4	Actividad Grupo 5
	Viernes 22	Revisión International CyberEx **Seminario Magistral 2** Seguridad ofensiva				
Semana 2	**Lunes 25**	**Taller 10** Seguridad en redes (I)	**Taller 9** Gestión de incidentes de seguridad	**Taller 12** Análisis forense Windows y Linux (I)	**Taller 2** Análisis forense en dispositivos móviles	**Taller 3 y 4** Análisis de malware
	Martes 26	**Taller 11** Seguridad en redes (II)	**Taller 10** Seguridad en redes (I)	**Taller 13** Análisis forense Windows y Linux (II)	**Taller 12** Análisis forense Windows y Linux (I)	**Taller 2** Análisis forense en dispositivos móviles
	Miércoles 27	**Taller 3 y 4** Análisis de malware	**Taller 11** Seguridad en redes (II)	**Taller 10** Seguridad en redes (I)	**Taller 13** Análisis forense Windows y Linux (II)	**Taller 12** Análisis forense Windows y Linux (I)
	Jueves 28	**Taller 2** Análisis forense en dispositivos móviles	**Taller 3 y 4** Análisis de malware	**Taller 11** Seguridad en redes (II)	**Taller 9** Gestión de incidentes de seguridad	**Taller 13** Análisis forense Windows y Linux (II)
	Viernes 29	**Seminario Magistral 3** APT: Casos de uso **Seminario Magistral 4** Ciberseguridad Industrial				

3.1. Taller 1 - OSINT: herramientas, técnicas de búsqueda y análisis de información

La sociedad de la información es un concepto del siglo XX nacido de la integración de las nuevas tecnologías (TIC) en las relaciones humanas y sociales. Internet y toda la información que contiene es un claro ejemplo de cómo las personas deseamos compartir pensamientos, ideas, sucesos, etc. Desde 2005, la UNESCO ha decidido elevar el concepto hacia la sociedad del conocimiento, pues el reto ya no es conseguir que fluya la información, sino que ésta aporte valor a las civilizaciones. Es así como saber buscar la información adecuada y analizarla puede ayudarnos a construir verdadero conocimiento que facilite la toma de decisiones en una organización y en nuestra propia vida.

En esta sesión se utilizarán algunas técnicas utilizadas para encontrar información en fuentes abiertas en Internet. También se hablará de algunas herramientas imprescindibles para localizar aquello que resulte de interés. Además, se tratará la importancia de utilizar métodos y técnicas propios del análisis de inteligencia para procesar la información proveniente de Fuentes Abiertas y metodologías específicas para la detección de tendencias y la interpretación de la realidad como el Time Line y los Mapas Mentales.

Los contenidos son los siguientes:

- Descripción y casos prácticos de uso
- Fases del proceso
    - Requisitos
    - Fuentes de información
    - Adquisición
    - Procesamiento
    - Análisis
    - Inteligencia
- Herramientas comunes
    - Búsquedas parametrizadas en buscadores
    - Buscadores de personas
    - Herramientas específicas
        - TheHarvester
        - Tinfoleak
        - Cree.py
        - API de redes sociales
        - Maltego
        - Palantir
- Profiling de usuarios

3.2. Taller 2 - Análisis forense en dispositivos móviles

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.

- Introducción
  - Conceptos clave en análisis forense. Particularización a dispositivos móviles.
  - Características de las plataformas móviles.
    - Android
    - iOS
    - Otras: BlackBerry y Windows Phone
- Procedimientos de análisis forense aplicados a entorno móvil
  - Fases de un análisis forense
  - Cadena de custodia
  - Gestión de evidencias
- Clonado de datos
  - Android, iOS, Windows Phone, Blackberry
  - Herramientas
- Análisis de la información recuperada
  - Análisis de memoria volátil
  - Análisis de memoria no volátil
    - Ficheros
    - Espacio libre
  - Recuperación y análisis de ficheros borrados
  - Herramientas

3.3. Taller 3 - Análisis de malware (I): Introducción, herramientas, preparación de entornos y análisis estático

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.

Los puntos alrededor de los que se estructurará la sesión son:

- Introducción al malware
- Características, tipos y evolución del malware

- Ataques masivos vs ataques dirigidos.
- Vectores de infección
- Respuesta ante un equipo infectado
- Fortificación de equipos. Técnicas para evitar infecciones
- Análisis estático de malware
    - Preparación del entorno de trabajo, aislamiento
    - Procedimiento de análisis
    - Búsqueda de información sobre el malware
    - Utilidades y herramientas del sistema
    - Utilidades de terceros

3.4. Taller 4 - Análisis de malware (II): Introducción, herramientas, preparación de entornos y análisis dinámico

Como complemento al Taller 3 - Análisis de malware (I): Introducción, herramientas, preparación de entornos y análisis estático los puntos alrededor de los que se estructurará la sesión son:

- Análisis dinámico de malware
    - Preparación del entorno de trabajo, aislamiento
    - Procedimiento de análisis
    - Búsqueda de información sobre el malware
    - Utilidades y herramientas del sistema
    - Utilidades de terceros
    - Análisis del tráfico de red generado por el malware

3.5. Taller 5 - Análisis forense de sistemas Windows (I): Introducción y toma de evidencias

El concepto de análisis forense digital hace referencia a un conjunto de procedimientos de recopilación y análisis de evidencias que se realizan con el fin de responder a un incidente relacionado con la seguridad informática y que, en ocasiones, deben de servir como pruebas ante un tribunal. Mediante este procedimiento se pretende responder a las siguientes preguntas: ¿qué?, ¿dónde?, ¿cuándo?, ¿por qué?, ¿quién? y ¿cómo?

Su uso está extendido por muy diversos campos, entre los que destacan:

- Persecución de delitos como fraude financiero, evasión de impuestos, acoso o pornografía infantil
- Casos de discriminación o acoso
- Investigación de seguros
- Recuperación de ficheros eliminados
- Casos de robo de la propiedad intelectual
- Ciberterrorismo
- Asegurar la resiliencia de las empresas, es decir, la capacidad de recuperación frente a ataques

Los puntos alrededor de los que se estructurará la sesión son:

- Fases del análisis forense

- Preservación
- Adquisición
  - Adquisición de la memoria RAM
  - Adquisición del registro Windows
  - Adquisición del tráfico de red.
- Documentación
- Cadena de custodia

3.6. Taller 6 - Análisis forense de sistemas Windows (II): Análisis y documentación de evidencias

Como complemento al Taller 5 - Análisis forense de sistemas Windows (I): Introducción y toma de evidencias los puntos alrededor de los que se estructurará la sesión son:

- Fases del análisis forense
  - Análisis
    - Análisis de la memoria RAM
    - Análisis del registro Windows
    - Análisis del tráfico de red.
  - Documentación
  - Presentación
  - Cadena de custodia

3.7. Taller 7 - Cifrado, navegación anónima y Deep Web.

La Deep Web es una región de Internet difícilmente rastreable cuyo tamaño se estima que es mucho mayor que la llamada Internet conocida, que es indexada de manera automática por los motores de búsqueda como Google o Bing. Dentro de esta Deep Web se encuentran las redes o sistemas que usan el Proyecto Tor, el cual fue concebido para garantizar el anonimato a través de técnicas de cifrado proporcionado privacidad de sus usuarios, características por las cuales está siendo usada por criminales para ocultar sus identidades y llevar a acabo multitud de delitos.

El objeto de esta sesión es definir qué es la Deep Web, así como los principales métodos o protocolos de navegación anónima que existen y los diferentes usos tanto legítimos como ilegítimos para los que son usados. Y por último una detallada descripción de la estructura y funcionamiento de TOR, al ser la red anónima más conocida

- Deep Web
- Cifrado y su importancia en el anonimato
- Navegación anónima: TOR, I2P, Freenet
  - Usos de la Deep Web
- TOR
  - Funcionamiento
  - Estructura
  - Usos de TOR ilegítimos
    - Sinergia TOR-Bitcoins: Mercado negro
      - SilkRoad
      - SilkRoad Reloaded
    - Botnets
  - Ataques de desanonimización

3.8. Taller 8 – Hacking Avanzado.

Pendiente de desarrollar.

3.9. Taller 9: Gestión de incidentes de seguridad.

La misión principal de un CERT es la de proporcionar un servicio de apoyo en la gestión de incidentes de seguridad, encargado de facilitar tanto medidas técnicas como organizativas que trabajen en las distintas fases de existencia del incidente. Para ello se revisarán las mejores prácticas y herramientas a utilizar en la gestión de incidentes.

- Aspectos formales de los CERT
- Fases de la gestión de incidentes:
  - Preparación
  - Identificación
  - Contención
  - Erradicación
  - Recuperación
  - Lecciones aprendidas

3.10. Talleres 10 y 11: Seguridad en redes.

Una de las actividades más comunes en la mitigación e investigación de incidentes consiste en el análisis de los dispositivos de red, con el objetivo de obtener la máxima información sobre el tipo de ataque, activos implicados y posible remediación. Para ello se debe conocer con mucho detalle los dispositivos implicados en la seguridad de una red y el análisis de las trazas que muestran.

- Detección de Intrusos
- Servicios de conexión segura
- Seguridad perimetral y segmentación segura
- Eventos de seguridad
- Redes Inalámbricas y de VoIP

3.11. Talleres 12 y 13: Análisis forense dispositivos Windows y Linux.

Windows dispone de mecanismos que dejan rastro de la actividad de los usuarios, de los programas que se utilizan, los accesos, conexiones y aplicaciones, si han navegado, descargado o ejecutado algún programa. Cuando se realiza un análisis forense, toda esta información es de vital importancia. Asimismo, dada la amplia presencia de ataques hacia servidores con sistema operativo Linux, se analizarán las actividades a realizar en este tipo de arquitecturas.

Los contenidos a abordar son los siguientes:

- Fases del análisis forense
  - Preservación
  - Adquisición
    - Adquisición de la memoria RAM
    - Adquisición del registro Windows

        - Adquisición del tráfico de red.
    - Análisis
        - Análisis de la memoria RAM
        - Análisis del registro Windows
        - Análisis del tráfico de red.
    - Documentación
    - Presentación
    - Cadena de custodia

4. REGISTRO

El registro para asistir al evento Summer BootCamp 2016 se realizará a través de la página web del evento https://cybercamp.es/summer-bootcamp (disponible a partir del 20 de abril de 2016).

Para el registro se deberá remitir el formulario PDF que se encontrará en la página de registro al contacto contacto_summerBC@incibe.es

La admisión en el curso se realizará por estricto orden de inscripción previa validación del organismo competente para cada uno de los públicos objetivos:

- Formación FCSE:
  - Personal en activo de FCSE que trabajen en unidades operativas relacionadas con la ciberseguridad de países pertenecientes a la OEA → Validación por parte de la OEA.
  - Personal en activo de FCSE que trabajen en unidades operativas relacionadas con la ciberseguridad de países pertenecientes a EUROPOL → Se remitirá la lista de participantes desde EUROPOL en coordinación con los países de origen y las entidades competentes de cada país determinadas desde EUROPOL.
  - Personal en activo de FCSE del territorio español que trabajen en unidades operativas relacionadas con la ciberseguridad → Se remitirá la lista de participantes desde la Oficina de Coordinación Cibernética (OCC) del CNPIC
- Formación CERTs:
  - Personal en activo de CERTs públicos de países latinoamericanos pertenecientes a la OEA → Validación por parte de la OEA.
  - 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 → Validación por parte de la OEA.

Desde INCIBE se realizarán las acciones necesarias para la validación de las inscripciones recibidas directamente con la entidad competente y notificará posteriormente su admisión o no en el curso correspondiente.


GOBIERNO
DE ESPAÑA
MINISTERIO
DE INDUSTRIA, ENERGÍA
Y TURISMO


incibe_
2006-2016
TRABAJANDO POR
LA CONFIANZA DIGITAL