TEMARIO
CERTs nivel básico

Cybersecurity
Summer
BootCamp
2017

Cybersecurity Summer BootCamp 2017
18-29 julio - León (España)
www.incibe.es/summer-bootcamp

Organizado por:

GOBIERNO DE ESPAÑA · MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

OEA OAS

Con la colaboración de:

universidad de León

AYUNTAMIENTO DE LEÓN

León Cuna del Parlamentarismo

GOBIERNO DE ESPAÑA · MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACIÓN

Santander

BID Banco Interamericano de Desarrollo

EUROPOL EC3 European Cybercrime Centre

INTERPOL

PROFESOR

Leonardo Amor

Taller 1

Creación de un CERT

Duración: 5 horas

Descripción

La misión principal de un CERT es la de proporcionar un servicio de apoye en la gestión de incidentes de seguridad. Los compromisos y la violación de la seguridad TIC de una organización son una realidad. Cuando sucede un incidente los CERT deben estar preparados para realizar una adecuada gestión a nivel técnico y organizativo

Temario

1. ¿Qué es un CERT?
- Tipos de CERTS
- Servicios que se pueden prestar desde un CERT
- Evento vs Incidente
- La importancia de la parte reactiva en el CERT

2. Planificación inicial del CERT
- Objetivos
- Expectativas
- Horario atención / 24*7

3. Respuesta ante incidentes
- Procesos y procedimientos
- Preparación / Entrenamiento
- Plan de coordinación / Comunicación
- Gestión de la crisis
  - Mitigación
  - Cadena de custodia
  - Lecciones aprendidas
- Herramientas

4. Métricas

5. Comunidad
- Comunicación / relación con otros CERT's
- FIRST / Terena Geant
- Incibe
- El uso de estándares
- PGP/GPG key Signing Ceremony

PROFESOR

Luis Jurado

Taller 2

Aspectos legales y cooperación

Duración: 5 horas

Descripción

Este curso está orientado a formar en su globalidad sobre cooperación jurídica internacional penal. El temario está orientado a que sea eminentemente útil en la práctica diaria de los asistentes al mismo. Dada la enorme variabilidad de situaciones y cauces legales a nivel internacional en la aplicación de medidas de cooperación en el ámbito penal, se procurará -siempre que sea posible- adaptarlos a los países de los alumnos asistentes.

Temario

1. Extradición
2. Orden Europea de Detención y Entrega
3. Reconocimiento mutuo de resoluciones penales en la Unión Europea
4. Sujetos e instituciones de cooperación judicial
5. Auxilio judicial en particular dentro del marco de la investigación penal
6. Medios de cooperación específica
7. Intercambio de información sobre antecedentes penales y consideración de una condena de otro Estado al amparo del principio de reconocimiento mutuo
8. Transmisión de procedimientos y cesión de jurisdicción
9. Medidas cautelares
10. Ejecución de resoluciones judiciales: Decomiso
11. Ejecución de resoluciones judiciales: Penas privativas de libertad
12. Cooperación judicial internacional fuera de la UE
13. Cooperación judicial internacional en Iberoamérica
14. Jurisdicción universal y cooperación con la Corte Penal Internacional
15. Cooperación policial
16. Valor probatorio de las actuaciones en el extranjero

PROFESOR

David Gallardo

Taller 3

Operaciones

Duración: 10 horas

Descripción

Los incidentes de seguridad de la información son inevitables, antes o después cualquier organización tendrá uno por lo que, si se quiere minimizar su impacto en el negocio, es necesario estar preparados y contar con unos mecanismos adecuados que permitan identificar, evaluar y gestionar la respuesta de un modo eficiente y planificado.

Una adecuada gestión de incidentes debe estar siempre presente pues permitirá reducir su impacto en el negocio en el corto y largo plazo. A la larga las ventajas incluirán, entre otras, una mayor robustez del plan de continuidad de negocio, una mejora de la reputación y un incremento de la confianza por parte de los usuarios/clientes así como una mayor protección contra pérdidas económicas y una reducción de los riesgos.

En el taller se combinará teoría con ejercicios prácticos para analizar los principales elementos que componen la gestión de incidentes y cómo éstos interaccionan entre sí y con terceros.

Temario

1. **Gestión de incidentes**
   - Conceptos
   - Objetivos de la gestión de incidentes
   - Gestión de incidentes vs. respuesta a incidentes
   - Metodologías
   - Herramientas
   - Ciclo de vida de un incidente
2. **Incidentes críticos**
   - Valoración de la criticidad
   - Niveles
3. **Avisos de seguridad**
   - Servicios reactivos: alertas y advertencias
   - Servicios proactivos: Comunicados y anuncios
   - Otros
   - Procesos asociados
4. **Fuentes de información**
   - Avisos de seguridad
   - Otras fuentes: logs, registros, eventos
5. **Role-play**
   - Utilidad
   - Toma de decisiones

PROFESOR

José Miguel Esparza

Taller 4

Análisis de amenazas

Duración: 10 horas

Descripción

Actualmente, la cantidad de ciberataques y amenazas registrados por los diferentes CERTs a nivel mundial es abrumador. Sin embargo, no hay previsión de que estas cifras remitan, sino más bien todo lo contrario, ya que se estima que seguirán incrementándose a lo largo de los años. Con este escenario de "guerra" cibernética en mente es crucial que los equipos encargados de dar respuesta a incidentes estén familiarizados de forma mínima con los diferentes tipos de amenazas y cómo analizarlas.

Durante el desarrollo de esta formación se ahondará en los tipos de amenazas que nos podemos encontrar, cómo identificarlas y cómo preparar un entorno adecuado para su análisis. Se hará hincapié en la introducción al análisis de malware desde el punto de vista dinámico, dejando la parte estática para otros cursos más avanzados.

Temario

1. **Introducción a los tipos de amenazas y vectores de infección**
2. **Diferencias entre análisis estático y dinámico**
3. **Preparación del entorno de trabajo**
    - Herramientas necesarias
    - Anti-análisis y ocultación de máquinas virtuales
    - Aislamiento
4. **Introducción al análisis de malware**
    - Identificación de una máquina infectada
    - Recolección de indicadores de compromiso (IOCs)
    - Clasificación del malware
    - Identificación del malware en memoria
    - Análisis de tráfico de red

PROFESOR

Juan Garrido

Taller 5

Introducción al análisis forense

Duración: 10 horas

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, así como de análisis de tipo offline*: Procesos y ficheros, extracción de memoria RAM, principales artifacts en cada uno de los sistemas operativos, etc...

Temario

1. **Sistema operativo**
   - Diferencias entre Windows 7, Windows 8 y Windows 10
   - Arquitectura de Linux
2. **Kits de respuesta ante incidentes**
   - Basados en agente
   - Sin agente
3. **Extracción de evidencias**
   - Navegación
   - Conexiones de red
   - Aplicaciones
   - Sistema de ficheros
   - Módulos
4. **Nuevos *artifacts* en Windows 10**
   - Asistente personal CORTANA
     - Introducción
     - Integración en Windows 10
     - Captura y análisis de información
   - Integración de aplicaciones
     - Centro de notificaciones
     - Geo-localización en Windows 10
5. **Análisis de línea temporal**
   - Cuándo un sistema ha sido actualizado, arrancado, parado, etc.
   - Análisis de creación/modificación de ficheros (malware)
   - Ocultación y ex-filtración de datos
   - Relación de procesos, puertos y conexiones realizadas