Título: Análisis de Malware para Administradores de Sistemas

Fecha: 31 de octubre – 9:30 a 20:00h

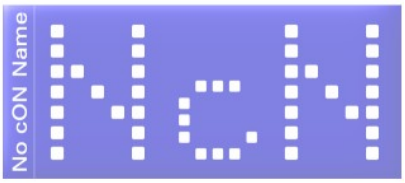
Formador: Juan Garrido (Silverhack)

Temario

Descripción y objetivos:
En el desarrollo de este curso se abordará el análisis de Malware desde la perspectiva de un administrador de sistemas. Para ello se mostrará una metodología basada en diferentes formas de análisis. Entender qué información es útil y dónde conseguir esta información para que de un determinado análisis se pueda dar respuesta a todas las cuestiones planteadas.
El curso, eminentemente práctico, abordará la posibilidad de poder realizar un análisis de Malware utilizando todos los elementos, herramientas y conocimientos comunes que pueda disponer un administrador de sistemas.
Finalizado el módulo el asistente conocerá múltiples variantes de malware, así como las diferentes vías de infección, siendo capaz llevar a efecto su detección y análisis. Estará también capacitado para realizar tareas básicas de mitigación y limpieza de amenazas.

Contenidos

1. Teoría del Malware
    a. Tipos de Malware
    b. Métodos comunes de infección
2. La figura del Administrador de IT en una organización
    a. Perdiendo el miedo ante un posible análisis
    b. Aplicación de conocimientos de IT en la mitigación de amenazas
    c. Elección de un laboratorio de análisis
        i. Virtualización total de un laboratorio
        ii. Virtualización parcial de un laboratorio
3. Metodologías de análisis
    a. Tipos de metodologías
    b. Elección del tipo de metodología
    c. Integración de metodologías en la empresa
4. Fuentes de información pública
    a. Tipos de fuentes de información
    b. Análisis de Malware utilizando sólamente fuentes públicas
    c. Automatización de análisis con TRIANA (Threat Intelligent Analysis)
5. Ocultación
    a. Ocultación basada en código
    b. Ocultación basada en tipo de Malware
    c. Ocultación basada en características del sistema operativo



6. Análisis de Malware con herramientas IT
    a. Identificación de Packers
    b. Identificación de conexiones
    c. Análisis del Registro
    d. Análisis de procesos
    e. Análisis basado en comportamiento
    f. Análisis de documentos ofimáticos, código embebido (JS), etc...
7. Análisis del tráfico de Red
    a. Utilizaciónd de Wireshark
    b. Filtros útiles para el análisis de Malware
    c. Aislamiento de una red
    d. Crea tu propio Internet para analizar Malware
8. El rol de un Sandbox
    a. Tipos de Sandbox
    b. Elección del tipo de Sandbox para la empresa
    c. Do it Yourself!

Duración: 8h

Público objetivo: Administradores de Sistemas, Administradores de red, profesional de la seguridad informática, analistas forenses

Conocimientos previos: Conocimientos básicos en Windows y redes
Requisitos tecnológicos: PC portátil para tomar notas y realización de demos. Conexión a internet

Precio: 210€ (impuestos incluidos). Incluye desayuno y bufet libre.

La inscripción y pago de todas las formaciones incluyen la entrada gratuita al Congreso No cON Name edición 2012. Para efectuar el pago los solicitantes deben hacer su inscripción a través de la web: http://www.noconname.org