



2
Sesiones

6
Horas

En vivo,
Virtual, o
Personalizado



Alonso Eduardo Caballero Quezada

Tengo más de veintidós años de experiencia, y desde hace dieciocho años realizo capacitaciones y consultorías en Hacking, Forense, OSINT, CiberSeguridad, y GNU/Linux

Redes Sociales

[LinkedIn](#)

[X \(Twitter\)](#)

[YouTube](#)

[Facebook](#)

[Sitio Web](#)

[e-mail](#)

[WhatsApp](#)

Presentación

El avance de la tecnología e Internet ha revolucionado la forma en la cual las organizaciones realizan sus negocios. Esta evolución consecuentemente genera también actividades maliciosas. La creciente amenaza de los ciberataques contra infraestructuras críticas, centros de datos, sector privado y público, defensa, energía, gobierno y finanzas, son un reto para todos los involucrados, desde una persona hasta las grandes empresas. Estos ciberataques utilizan software malicioso (también conocido como Malware) para realizar robo financiero, espionaje, sabotaje, robo de propiedad intelectual, o por motivos políticos.

Dado el hecho los ciberdelincuentes son cada vez más sofisticados y realizan ataques de malware avanzados, detectar y responder a estas intrusiones es fundamental para los profesionales en ciberseguridad. El análisis de malware se ha convertido en una habilidad imprescindible para enfrentar el malware avanzado y los ataques dirigidos. El análisis de malware requiere un conocimiento equilibrado de muchas habilidades y temas diferentes.

Este curso proporciona los conceptos, herramientas y técnicas para comprender el comportamiento y las características de malware para Windows, realizando análisis de malware. Para comprender mejor los conceptos, se utilizan ejemplos y demostraciones prácticas durante todo el curso. Además se proporciona suficiente información para comprender los conceptos necesarios. Este curso ayuda a iniciarse en el ámbito del análisis de Malware, o si tiene experiencia en este campo, ayudará a mejorar conocimientos.



Temario

¿Qué es Malware?
¿Qué es el Análisis de Malware?
¿Porque Análisis de Malware?
Tipos de Análisis de Malware
REMnux
theZoo
Análisis Estático
Determinar el Tipo de Archivo
Identificar Tipo de Archivos con Métodos Manuales
Huella del Malware
Generar Hashes Criptográficos utilizando Herramientas
Escaneo con Múltiples Antivirus
Escanear Archivo Sospechoso VirusTotal Factores / Riesgos a Considerar
Extraer Cadenas
Extracción de Cadenas utilizando Herramientas
Decodificar Cadenas Ofuscadas con FLOSS
Determinar Ofuscación del Archivos Packets y Cryptos
Detectar Ofuscación de Archivos
Inspeccionar la Información de la Cabecera PE
Inspeccionar Dependencias e Importación del Archivo
Inspeccionar Exportación
Examinar Tabla de Sección y Secciones PE
Examinar Marca de Tiempo de Compilación
Examinar Recursos PE
Comparar y Clasificar Malware
Clasificar Malware utilizando Hashes Difusos
Clasificar Malware utilizando Hashes Importados
Clasificar Malware utilizando Hashes de Sección
Clasificar Malware utilizando YARA
Análisis Dinámico
Vigilancia del Sistema y Red
Herramientas para el Análisis Dinámico
Determinar la Interacción del Sistema
Registrar las Actividades del Sistema
Capturar Tráfico de Red
Etapas para un Análisis Dinámico
Análisis de las DLLs
Porque los Atacantes utilizan DLLs
Analizar DLLs

Beneficios

- Acceso al aula virtual por 60 días
- Acceso a las sesiones en vivo
- Video de las dos (2) sesiones
- Acceso libre a las sesiones en vivo de los siguientes cursos a dictarse
- Material utilizado durante el desarrollo del curso
- Dos (2) horas de asesoría personalizada en vivo por videoconferencia
- Libro "Fundamentos de Hacking Ético" escrito por el instructor
- Certificado digital de participación
- Certificado digital de aprobación por una duración total de 16 horas

Inversión

Perú: S/. 225 Soles

- Depósito o transferencia interbancaria a Scotiabank
- Pago mediante YAPE o PLIN

Otros países: \$ 70 Dólares

- Pago mediante PayPal

Escriba un mensaje al WhatsApp <https://wa.me/51949304030> para proporcionarle los datos pertinentes.

Información

Para obtener más información sobre este curso tiene a su disposición los siguientes mecanismos de contacto.

WhatsApp: <https://wa.me/51949304030>

Correo electrónico: reydes@gmail.com