Curso Análisis de Malware 2022

Domingos 11 y 18 de Setiembre del 2022. De 9:00am a 12:00am (UTC -05:00)

Este curso virtual ha sido dictado a participantes residentes en los siguientes países:

Presentación

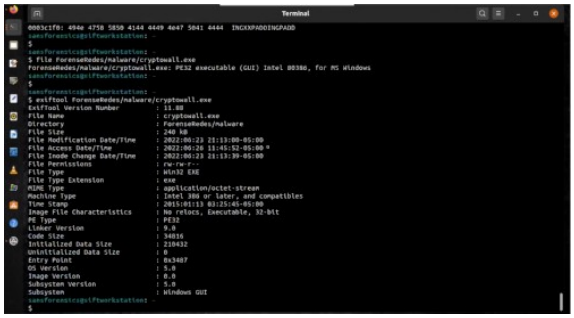
El avance de la tecnología e Internet ha revolucionado la forma en la cual las organizaciones realizan sus negocios. Esta evolución consecuentemente genera también actividades maliciosas. La creciente amenaza de los ciberataques contra infraestructuras críticas, centros de datos, sector privado y público, 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.

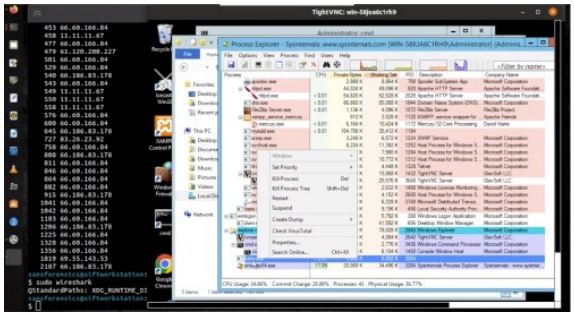
Este curso proporciona los conceptos, herramientas y técnicas para comprender el comportamiento y las características de malware para Windows, realizando análisis de malware. Para comprender mejor los conceptos, se utilizan ejemplos y demostraciones prácticas durante todo el curso. Además se proporciona 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
- Fuentes de Malware
- Análisis Estático
- Determinar el Tipo de Archivo
- Identificar Tipo de Archivos con Métodos Manuales
- Huella del Malware
- Generar Hashes Criptográficos
- Escaneo con Múltiples Antivirus
- Escanear el Archivo Binario Sospechoso
- Extraer Cadenas
- Determinar Ofuscación del Archivo
- Packers y Cryptos
- Inspeccionar la Información de la Cabecera PE
- Comparar y Clasificar Malware



- Análisis Dinámico
- Vigilancia del Sistema
- Vigilancia de la Red
- Herramientas para el Análisis Dinámico
- Determinar la Interacción con el Sistemas
- Registrar Actividades en el Sistemas
- Capturar Tráficos de Red
- Etapas para un Análisis Dinámico
- Analizar un Malware Ejecutable
- Análisis de las DLLs



Material

Todos los participantes al Curso Virtual de Análisis de Malware tendrán la posibilidad de descargar los videos de cada sesión, un día después de impartida la misma.

- **REMnux:**
  Link de Descarga: https://docs.remnux.org/install-distro/get-virtual-appliance

Fechas y Horario

El Curso Virtual de Análisis de Malware tiene una duración total de seis (6) horas, las cuales se dividen en dos (2) sesiones de tres (3) horas cada una.

- **Fechas:**

  Domingos 11 y 18 de Setiembre del 2022

- **Horario:**

  De 9:00 am a 12:00 pm (UTC -05:00). 6 horas en total.

[*] El Curso se dicta sin ningún requisito mínimo en el número de participantes.

Inversión y Forma de Pago:

Acceso a todos los videos y material:

S/. 175 Soles o $ 55 Dólares

Acceso al aula virtual por 30 días, todos los videos, material, evaluaciones, certificado de participación y certificado de aprobación.

S/. 260 Soles o $ 80 Dólares

El pago del curso se realiza mediante alguno de los siguientes mecanismos:

Residentes en Perú	Residentes en Otros Países
Deposito bancario o transferencia interbancaria en la siguiente cuenta: Scotiabank ScotiaBank Cuenta de Ahorros en Soles: 324-0003164 A nombre de: Alonso Eduardo Caballero Quezada CCI: 009-324-203240003164-58	Transferencia de dinero mediante Western Union y MoneyGram o pago por Paypal: MoneyGram · Western Union · PayPal Escriba por favor un mensaje de correo electrónico a caballero.alonso@gmail.com para proporcionarle los datos requeridos.

Confirmado el pago se enviará al correo electrónico del participante, los datos necesarios para conectarse hacia la plataforma, además de toda la información pertinente para su participación en el curso

El curso se realiza utilizando el sistema para video conferencias de nombre Anymeeting. El cual proporciona transmisión de audio y video HD en alta calidad, tanto para el instructor y los participantes, entre otras características ideales para el dictado de cursos virtuales o en línea.

INTERMEDIA ANYMEETING

Más Información

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

Correo electrónico: caballero.alonso@gmail.com

Teléfono: +51 949 304 030

Sitio Web: https://www.reydes.com

Instructor

Alonso Eduardo Caballero Quezada. EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures, Pen Testing, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS) y OPEN-SEC Ethical Hacker (OSEH). He sido instructor, expositor y conferencista en el OWASP LATAM Tour, OWASP Perú Chapter Meeting, OWASP LATAM at Home, PERUHACK, PERUHACKNOT, 8.8 Lucky Perú, Ekoparty University Talks Perú. Cuento con más de diecisiete años de experiencia en el área y desde hace trece años laboro como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital. Pertenecí por muchos años al grupo internacional RareGaZz y grupo Peruano PeruSEC. He dictado cursos para España, Ecuador, México, Bolivia y Perú, presentándome también en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux y Software Libre.