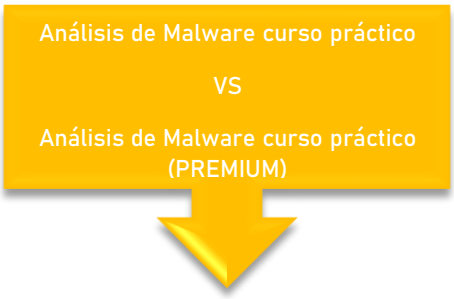
ENLACE A VERSIÓN PREMIUM

- ENLACE DE ACCESO “Análisis de Malware curso práctico (PREMIUM)” CON UN GRAN DESCUENTO POR TIEMPO LIMITADO: https://www.udemy.com/course/draft/3556017/?couponCode=DESC_TIEMPO_LIMITADO
- Recuerda que los objetivos de aprendizaje de cada curso son independientes, puedes tomar cada curso por separado sin ningún problema.



LECCIONES

Análisis de Malware curso práctico	Análisis de Malware curso práctico (PREMIUM)	Descripción
Introducción al Análisis de Malware	**Introducción al Análisis de Malware**	**En esta sección enseñaremos algunos conceptos básicos pero necesarios, reducimos la teoría al mínimo para enfocarnos en las prácticas.**
¿Qué es malware? Vectores de infección, ¿Por qué se realiza análisis de malware?	¿Qué es malware? Vectores de infección, ¿Por qué se realiza análisis de malware?	
Tipos de malware, Componentes de un malware, Centro de Comando y Control	Tipos de malware, Componentes de un malware, Centro de Comando y Control	
¿Cómo se infecta una máquina? Métodos de prevención, Análisis Estático/Dinámico	¿Cómo se infecta una máquina? Métodos de prevención, Análisis Estático/Dinámico	
Configurando el Laboratorio de pruebas	**Configurando el Laboratorio de pruebas**	**En esta sección configuraremos un laboratorio de pruebas para ejecutar con seguridad cualquier tipo de malware.**
Configurando Windows 10 virtual machine	Configurando Windows 10 virtual machine	
Configurando Inetsim en Kali Linux virtual machine	Configurando Inetsim en Kali Linux virtual machine	
Configurando Inetsim en Windows 10 virtual machine	Configurando Inetsim en Windows 10 virtual machine	
Virtual Box extras	Virtual Box extras	
Internet y Windows 10 virtual machine	Internet y Windows 10 virtual machine	
Consideraciones antes de iniciar prácticas	Consideraciones antes de iniciar prácticas	
Precauciones	Precauciones	
Análisis Estático	**Análisis Estático**	**En esta sección aprenderás varias técnicas para realizar Análisis Estático**
Portable Executable (PE)	Portable Executable (PE)	
Tipo de archivo/File type	Tipo de archivo/File type	
Huella de identificación/Fingerprinting	Huella de identificación/Fingerprinting	
Cadenas/Strings	Cadenas/Strings	
x	Ofuscación/Obfuscation	
Análisis Dinámico	Análisis Dinámico	

¿Cómo se realiza un Análisis Dinámico?	¿Cómo se realiza un Análisis Dinámico?	
Análisis Estático y Dinámico en práctica	**Análisis Estático y Dinámico en práctica**	**En esta sección aprenderás como funciona la ingeniería social con un ejemplo real que incluye código. También aprenderás a capturar malware en tu sistema operativo y red.**
Ingeniería social y Downloaders	Ingeniería social y Downloaders	
Capturando Keyloggers	Capturando Keyloggers	
Capturando el tráfico de un Keylogger 1/2	Capturando el tráfico de un Keylogger 1/2	
x	Capturando el tráfico de un Keylogger 2/2	
X	**Malware en Dlls**	**En esta sección aprenderás que es una dll y como funcionan, técnicas para inyectar dlls maliciosas y como codificar una dll maliciosa.**
X	¿Qué es una dll?, Imports Exports y apis, Introducción a "Dll Injection"	
X	Técnicas de "Dll injection", "Remote Code Injection" en detalle	
X	Codificando "Remote Dll Injection".	
X	Codificando malware dentro de una dll.	
X	**Analizando DLLs maliciosas**	**En esta sección aprenderás a capturar y analizar una dll maliciosa**
X	Analizando DLLs con rundll32	
X	Analizando DLLs con x32dbg	
X	Analizando DLLs combinando x32dbg, rundll32 y procmon	
X	Analizando DLLs con Noriben	
X	**Codificando Keyloggers**	**En esta sección aprenderás a analizar y codificar un Keylogger básico usando una api de windows. También aprenderás a analizar y codificar un Keylogger avanzado con un filtro para capturar actividad de Facebook y casi cualquier sitio web.**
Revisión de código Keylogger TotalAware3	Revisión de código Keylogger TotalAware3	
X	Presentación del Keylogger TotalAware2	
X	Módulo espía para Facebook de TotalAware2 1/2	
X	Módulo espía para Facebook de TotalAware2 2/2	
X	Delegados en C#	
X	Módulo "keyboard listener" de TotalAware2 1/2	
X	Módulo "keyboard listener" de TotalAware2 2/2	
X	**Codificando Ransomware**	**En esta sección aprenderás a desarrollar y analizar un Ransomware, aprenderás conceptos y que hacer en caso de infección, creación**

		de un programa desencriptador y más.
X	¿Qué es Ransomware? Síntomas de infección, Pasos Ransomware dentro del sistema	
X	Estoy infectado ¿Qué puedo hacer?, Flujograma de nuestro Ransomware "Rams1"	
X	Revisión del código de Rams1 1/3	
X	Revisión del código de Rams1 2/3	
X	Revisión del código de Rams1 3/3	
X	Revisión del código DecryptRams1	
X	Analizando Rams1 con wireshark	
X	Añadiendo capas de seguridad a Rams1 1/2	
X	Añadiendo capas de seguridad a Rams1 2/2	
X	**Sacando más provecho a las prácticas**	**En esta sección aprenderás a sacar Indicadores de Compromiso (IoC) y resumiremos algunos conceptos para potenciar lo aprendido.**
X	Los componentes de malware descifrados	
X	Obteniendo indicadores de compromiso	

Nota: Los objetivos de aprendizaje de cada curso son independientes, puedes tomar cada curso por separado sin ningún problema.

- ENLACE DE ACCESO "Análisis de Malware curso práctico (PREMIUM)" CON UN GRAN DESCUENTO POR TIEMPO LIMITADO: https://www.udemy.com/course/draft/3556017/?couponCode=DESC_TIEMPO_LIMITADO

RECURSOS

Análisis de Malware curso práctico	Análisis de Malware curso práctico (PREMIUM)	Descripción
X	Rams1 código fuente	Es una muestra de **Ransomware** completo, funcional y con su código fuente, se proporciona con fines académicos.
Rams1 ejecutable		Es un Ransomware ejecutable, funciona solo para realizar prácticas de análisis.
	Rams1 ejecutable	Es un Ransomware ejecutable capaz de encriptar una variedad de archivos.
X	DecryptRams1	Software para **descifrar archivos cifrados por nuestro Ransomware** (código completo proporcionado para fines académicos).
X	Ayuda de ransomware	Es un pequeño documento que te ayudará si estás infectado.
TotalAware2 ejecutable		Es un Keylogger ejecutable, funciona solo para realizar prácticas de análisis.

	TotalAware2 ejecutable	Es un **Keylogger** ejecutable capaz de robar credenciales y datos de Facebook (y otros sitios web) y conectarse a un Centro de Comando y Control.
X	TotalAware2 código fuente	Es un Keylogger capaz de robar credenciales y datos de Facebook (y otros sitios web) y conectarse a un Centro de Comando y Control (código completo proporcionado para fines académicos).
TotalAware3 código fuente	TotalAware3 código fuente	Es un Keylogger codificado en C ++. (código completo proporcionado para fines académicos).
X	Injector7	**Inyecta código malicioso** en un proceso legítimo de Windows (código completo proporcionado con fines académicos).
X	Dll4	Es un ejemplo **de malware codificado en un dll** (el código completo se proporciona con fines académicos).
X	Dll8	Muestra cómo utilizar la función de exportación en una dll (código completo proporcionado para fines académicos).
Prácticas	Prácticas	Es un documento que contiene la guía de ejercicios de laboratorio.
Requisitos de laboratorio y guía rápida	Requisitos de laboratorio y guía rápida	Es un documento que te ayudará a configurar un laboratorio seguro para el Análisis de Malware.
Recursos web	Recursos web	Es un documento con páginas web que se utilizarán a lo largo del curso.

Nota: Los objetivos de aprendizaje de cada curso son independientes, puedes tomar cada curso por separado sin ningún problema.

- ENLACE DE ACCESO “Análisis de Malware curso práctico (PREMIUM)” CON UN GRAN DESCUENTO POR TIEMPO LIMITADO: https://www.udemy.com/course/draft/3556017/?couponCode=DESC_TIEMPO_LIMITADO