



Gracias a



[openwebinars.net/cert/RYgLK](https://openwebinars.net/cert/RYgLK)



OpenWebinars certifica que

**MIGUEL JESÚS GARCÍA SÁNCHEZ**

Ha superado con éxito

**Curso de Metasploit Framework**

Duración del curso

**10 horas**

Fecha de expedición

**03 enero 2022**

A handwritten signature in black ink, appearing to read 'Manuel Agudo', positioned over a large, light gray watermark of the OpenWebinars logo.

CEO de OpenWebinars

**Manuel Agudo**

## Contenido

# Curso de Metasploit Framework

### 1. INTRODUCCIÓN A METASPLOIT

Presentación

¿Qué es Metasploit?

### 2. INSTALACIÓN DE METASPLOIT FRAMEWORK

Instalación de Metasploit en Linux

Instalación de Metasploit en Microsoft Windows

### 3. CONFIGURACIÓN Y FUNDAMENTOS DE METASPLOIT FRAMEWORK

Ejecutar servicios de Metasploit

Comandos msfconsole

Exploits y tipos de Payloads

Generando Payloads

Bases de datos

Shell Meterpreter

### 4. INFORMATION GATHERING (RECOPIACIÓN DE INFORMACIÓN)

Escaneo de puertos

Usando Metasploit para descubrir vulnerabilidades MSSQL

Identificación de servicios

### 5. ESCÁNER DE VULNERABILIDADES

Nmap Scripts

Nessus: escáner de vulnerabilidades

### 6. ATAQUES DEL LADO DEL CLIENTE

Troyano para Linux

Phishing



PDF Malicioso

## **7. POST EXPLOTACIÓN**

Escalada de privilegios

Persistencia con NetCat

Capturando tráfico

Captura de pantalla

Buscando contenido en máquinas comprometidas

John the Ripper: rompiendo Hashes

## **8. METERPRETER SCRIPTING**

Personalización del Payload Meterpreter

## **9. MANTENIMIENTO DE ACCESO**

Keylogin

Shell Meterpreter persistente

## **10. USO AVANZADO DE METASPLOIT**

Backdorizando archivos .EXE

## **11. ENTORNO GRÁFICO DE METASPLOIT FRAMEWORK**

Armitage GUI

Módulos auxiliares