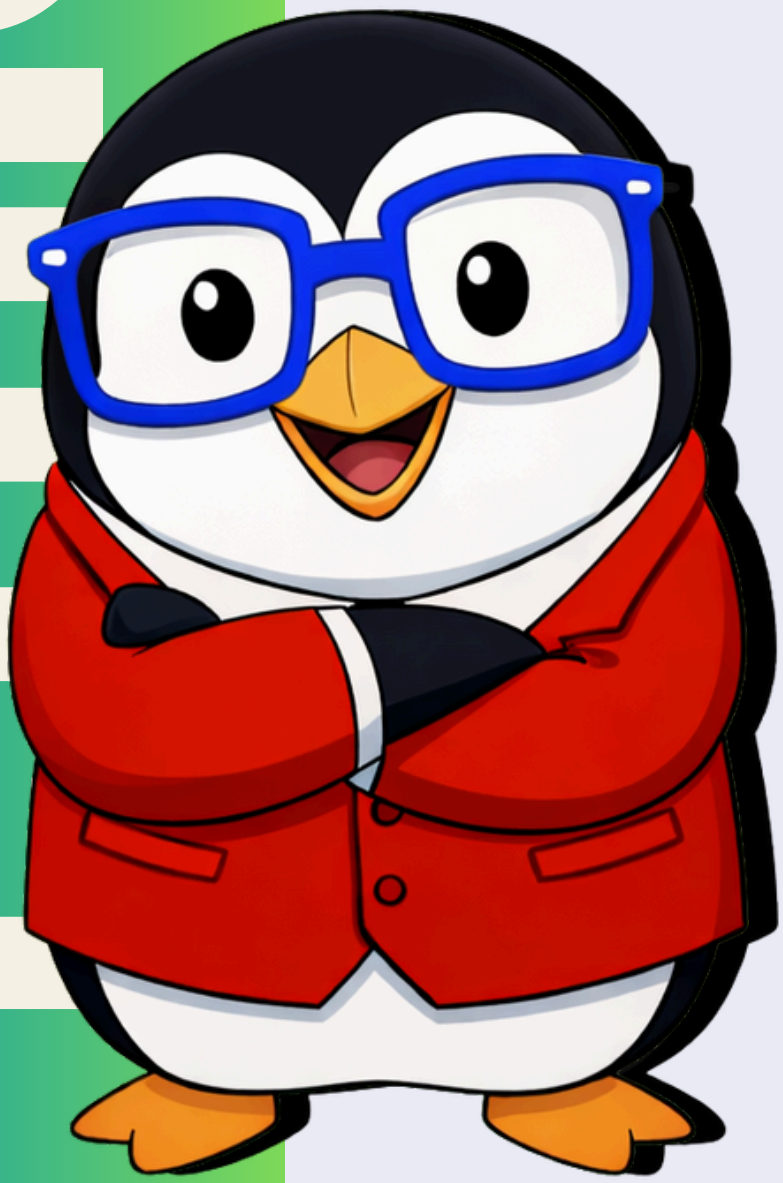
aulaútil

# ETHICAL

## CENTRO DE CAPACITACIÓN ESPECIALIZADO EN CURSOS DE INFORMÁTICA

CON SERVIDORES VPS PARA CADA ALUMNO

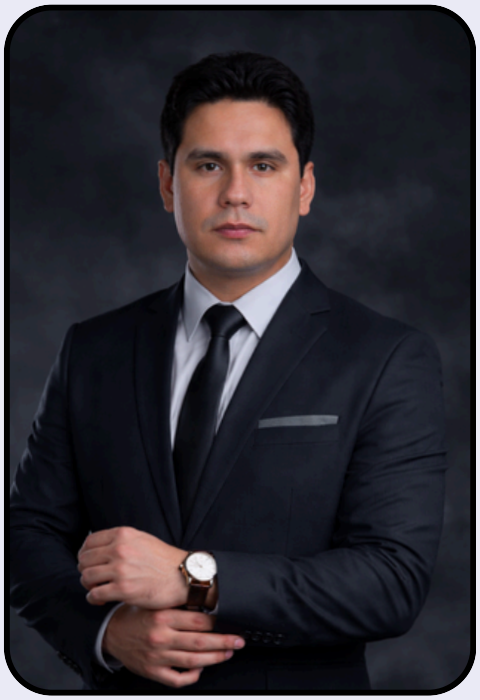


CURSOS ALTAMENTE ESPECIALIZADOS EN LINUX, OPEN SOURCE, CLOUD COMPUTING, PROGRAMACIÓN, SEGURIDAD, IA Y TELEFONÍA IP

aulaútil

# ING. JUAN OLIVA

## TRAINER OFICIAL DE MILE2



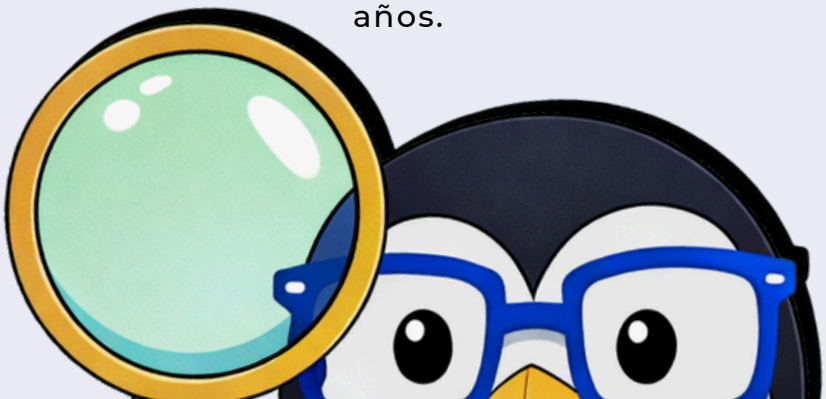
- Certified Ethical Hacking C|EH
- CertIfied Penetration Testing Engineer C)PTE
- Certified Secure Web Application
- Engineer C)SWAE
- Brainbench Network Security

Consultor en Ciberseguridad y VoIP con más de 15 años de experiencia en el campo, altamente involucrado en proyectos de Ethical Hacking, análisis y explotación de vulnerabilidades, pruebas de ingeniería social, seguridad física, revisión de código, entre otras tareas relacionadas con la seguridad informática.

Desarrolla proyectos de implementación e integración de plataformas VoIP, basadas en Asterisk, incluyendo proyectos de call center y aseguramiento de plataformas de telefonía IP.

Ha liderado y participado en proyectos en Sudamérica y Europa, y cuenta con certificaciones vigentes en Ethical Hacking, Linux y Telefonía IP.

Se desempeña como instructor de cursos de Ethical Hacking, Linux y VoIP, habiendo realizado capacitaciones tanto en el Perú como en el extranjero. Es investigador de vulnerabilidades y creador de contenido técnico, publicado en su blog personal jroliva.net, el cual mantiene activo desde hace más de 6 años.



Ha participado como ponente en múltiples conferencias y eventos internacionales, entre los que destacan:

- BSides Colombia 2019 – Pentesting de APIs y Microservicios
- II Congreso Internacional de Tecnología en Informática 2019 – Ecuador – Hacking de Aplicaciones Web
- Semana de la Ingeniería – CIP-CD Piura 2019 – Perú – Hacking de Aplicaciones Móviles
- OWASP Latam Tour Perú 2019 – Perú – Hacking de APIs y Microservicios
- Seminario Internacional de Seguridad en Desarrollo de Software 2018 – Ecuador – Hacking a Web Services
- Peru Hack 2018 – Perú – Attack in Depth for Web Applications
- OWASP Latam Tour Perú 2018 – Perú – Pentesting de Aplicaciones Node.js
- VII Villatel UNFV 2017 – Perú – Alta Disponibilidad en Issabel PBX
- Google DevFest Lima 2017 – Perú – Ethical Hacking a Web Services
- BeFree 2017 – México – Issabel: una relación segura
- CONECIT 2017 – Tingo María, Perú – Hacking a Redes Corporativas
- Global Azure BootCamp – Lima, Perú – Ethical Hacking desde Azure
- UbuntuCon Latinoamérica 2016 – Cifrado de Comunicaciones con Software Libre
- CyberSecurity Bank & Government 2016 – Lima – Evadiendo Antivirus: técnicas y herramientas
- Peru Hack 2015 – Lima – UTMs: ¿Seguridad al 100%?
- Elastix World 2015 – Colombia – Uso del módulo PIKE en Elastix MT
- Peru Hack 2014 – Lima – Crazy Shellshock Vectors & Attacks
- Elastix World 2014 – Chile – Seguridad en VoIP Open Source: poniendo el punto sobre la “i”
- Elastix BeFree 2014 – México – SBC: protección efectiva de seguridad VoIP
- Elastix World 2013 – México – Extending Elastix security with Snort IDS/IPS

aulaútil

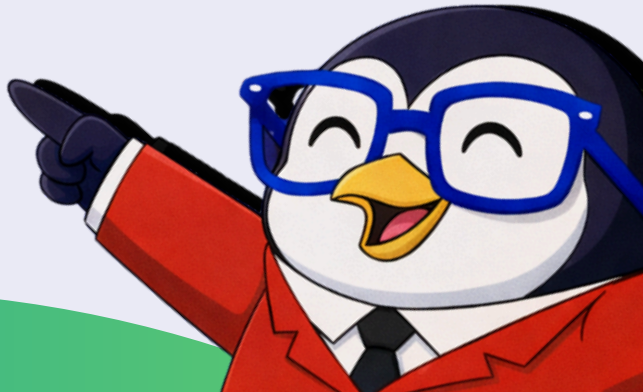
# CURSO DE ETHICAL HACKING Y SEGURIDAD OFENSIVA

## MÓDULO 1 – INTRODUCCIÓN A UN PROYECTO DE ETHICAL HACKING

- Introducción al Ethical Hacking.
- Tendencias actuales: Dónde apuntan los ataques hoy, Riesgos y Componentes Asociados, Nuevos Riesgos.
- Metodologías de Penetration Testing - Ethical Hacking , Introducción a OSSTM, OWASP, CVSS.
- Difinir el alcance de un proyecto y/o servicio de Ethical Hacking, documentación y formatos requeridos.

## MÓDULO 2 – ETHICAL HACKING NETWORKING

- Introducción a Linux para Pentesters
- Footprint y reconocimiento con Google Hacking e Interrogación DNS .
- Escaneo de red redes con Nmap.
- Enumeración de servicios.
- Detección de vulnerabilidades con scripts de Nmap.
- Ataques a servicios de red, password craking, divulgación de información.
- Detección y Explotación de vulnerabilidades en SNMP, SMTP, SSH, RDP, FTP, RPC.



aulaútil

## MÓDULO 3 - EXPLOITS Y VULNERABILIDADES

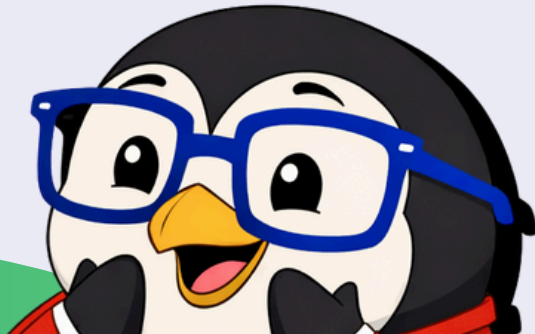
- Introducción a la explotación manual de vulnerabilidades dentro de un proyecto de Pentesting.
- Trabajando con exploits.
- Uso Metasploit como framework de ataque.
- Ataques a sistemas operativos Windows 7 y 10.
- Ataques del lado Cliente.
- Creando ejecutables infectados (Virus), para conseguir control de Windows.

## MÓDULO 4 – ESCANEO Y ANÁLISIS DE VULNERABILIDADES

- Instalación y personalización de Nessus.
- Escaneo de Vulnerabilidades avanzada con Nessus a nivel de Plataforma y aplicaciones.
- Análisis de reportes de Nessus , detección de falsos positivos y falsos negativos.
- Explotación de vulnerabilidades desde los reportes de Nessus.

## MÓDULO 5 – ACTIVE DIRECTORY PENTESTING

- Instalación y configuración de un entorno común de Active Directory.
- Escaneo de reconocimiento y enumeración de un entorno de A.D.
- Ataques de Password Spraying.
- Ataques de fuerza bruta hacia cuentas en A.D.
- Captura de credenciales mediante consultas LLMNR y NBT-NS
- Kerberoasting attack
- Exfiltración de datos.

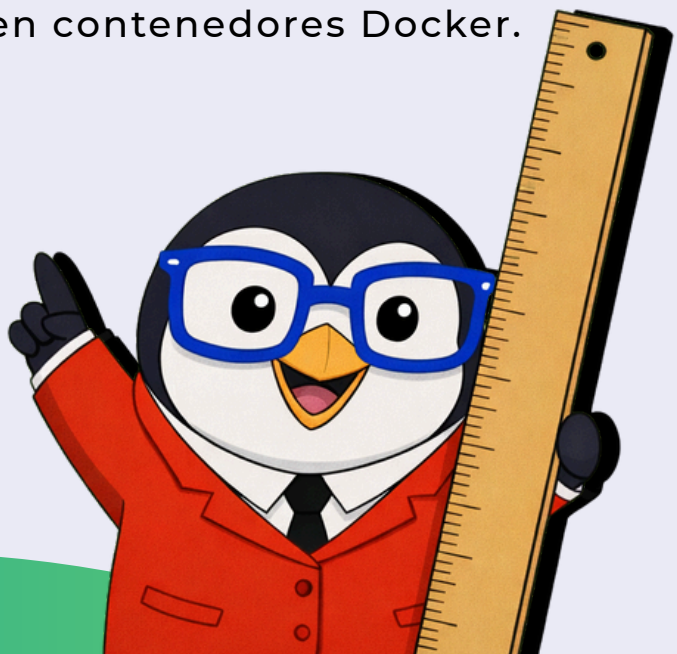


## MÓDULO 6 - ETHICAL HACKING A APLICACIONES WEB

- Introducción al OWASP TOP 10 WEB Aplication Security Risk.
- Uso de proxys de interceptación con Burp Suite, ZAP Proxy.
- Detección de vulnerabilidades de forma manual.
- Ataques a servidores Web con Sql Inyection.
- Explotando vulnerabilidades XSS, LFI, RFI, Upload, SQLI POST, evasión de Login, HTML inyection, Ataques de fuerza bruta contra formularios de autenticación, Acceso inseguro de objetos.
- Ataques de robo de sesión o session hijacking
- Haciendo un defacement (defaceo) de una pagina web y conociendo la superficie de la vulnerabilidad.

## MÓDULO 7 - ETHICAL HACKING DE API, SERVICIOS WEB Y CONTENEDORES

- Introducción al OWASP API SECURITY TOP 10.
- Introducción a la arquitectura de Contenedores, APIs y Microservicios.
- Ataques contra API REST, divulgación de información, Roptura de acceso, Inyecciones de SQL, devibilidad en token JSON, Mongo inyection, API google Hacking.
- Ataques contra microservicios en contenedores Docker.



aulaútil

## MÓDULO 8 - ETHICAL HACKING A APLICACIONES MÓVILES

- Introducción al OWASP MOBILE TOP10 Risks.
- Metodologías Mobile Appsec Verification / Mobile Security Testing Guide.
- Como implementar laboratorios para Android e iOS
- Instalación de emulador para aplicaciones Android.
- Análisis, descarga y descompresión de APK.
- Crear archivos .java y análisis de métodos de la aplicación.
- Capturar credenciales mediante log de la aplicación.
- Análisis de bases de datos SQLITE.
- Análisis de almacenamiento externo.
- Ataques de inyeccion de SQL.
- Captura de paquetes con ZAP Proxy
- Análisis dinámico de aplicaciones móviles con Frida.

## MÓDULO 9 – PENTESTING con IA.

- Introducción a la inteligencia artificial
- Tipos de IA ,modelos , definicion de LLM.
- OWASP top 10 para aplicaciones LLM
- Programación python para LLM
- Pentesting con Ollama, Ollamacode , PentestGTP
- Damn Vulnerable LLM agent

## EVALUACIÓN FINAL

- Prueba de conocimiento de todo lo aprendido.