Vicente Garrigues-Trenor

CIBERSEGURIDAD

649 334 830

garriguestrenorblanc@gmail.com

linkedin.com/in/vicentegarrigues-trenor

trenor13.github.io

Valencia

Herramientas

Blue Team / Detección y SIEM:
Splunk (fundamentos), IBM QRadar (básico), CrowdStrike (conocimientos generales), detección de amenazas, revisión de logs, análisis de eventos, Sysmon, Sigma Rules.

Análisis de tráfico y Red:
Wireshark, TCPDump, Snort, Suricata, Responder, Ettercap, Socat, Netcat.

OSINT y Reconocimiento:
Shodan, theHarvester, Maltego, SpiderFoot, Recon-ng, Hunter.io, WhatWeb, Wappalyzer, Nmap, AutoRecon, Gobuster, Dirbuster.

Post-explotación y Escalada:
LinPEAS, WinPEAS, GTFOBins, Chisel.

Pentesting / Explotación:
Metasploit, msfvenom, Hydra, SQLmap, CrackMapExec, Commix, Burp Suite, Nikto, FFUF, Hashcat, CeWL, John the Ripper.

Forense y Evidencia:
Autopsy, Volatility, ExifTool.

Scripting y Automatización:
Bash, Python (básico).

Hardening y Seguridad en SO:
Nociones de SELinux, seguridad en sistemas operativos.

Sistemas operativos:
Linux (Kali, Debian), Windows.

Idiomas

Inglés
B1

Sobre mí

Apasionado por la ciberseguridad, con formación práctica en Red Team y Blue Team a través del máster intensivo de The Bridge (Valencia). He trabajado en entornos simulados aplicando técnicas ofensivas y defensivas, análisis forense, respuesta ante incidentes y protección de infraestructuras.
Me considero una persona proactiva, resiliente y con alta tolerancia al estrés, que disfruta enfrentando retos técnicos, aprendiendo de forma constante y colaborando en equipo. Destaco por mi capacidad de adaptación, organización del tiempo y aplicación de buenas prácticas en entornos técnicos, así como por el compromiso con la mejora continua, el cumplimiento de objetivos y el crecimiento progresivo en el ámbito de la ciberseguridad.

Formación

Master en Ciberseguridad
EDEM | Escuela de Empresarios, valencia
Septiembre 2024 - Mayo 2025

Programa intensivo con enfoque práctico especializado en ciberseguridad ofensiva y defensiva. Pentesting, defensa activa, análisis de sistemas reales, resolución de retos tipo CTF, y escenarios Red Team / Blue Team.
Incluye prácticas con herramientas SIEM reales como Splunk y QRadar, análisis forense, respuesta ante incidentes y simulación de ataques.

Certificación eJPTv2
INE Security | eLearnSecurity Junior Penetration Tester
Abril 2025

Pentesting práctico centrado en todo el flujo de un test de intrusión real: reconocimiento de red, escaneo y enumeración activa, análisis de servicios, explotación manual de vulnerabilidades, obtención de shells, escalada básica, análisis de tráfico con Wireshark, pivoting en red interna, y uso de herramientas como Nmap, Gobuster, Netcat y Metasploit.

Security Operations Center (SOC)
Cisco | Coursera
Junio 2025

Operaciones clave en un SOC: detección de amenazas, automatización, SIEM (Splunk), respuesta a incidentes y análisis de eventos. Incluye prácticas con herramientas reales como Splunk y CrowdStrike, gestión de alertas, registros y flujos de trabajo defensivos.

Certificado Profesional en Ciberseguridad
Google | Coursera
Mayo 2025

Fundamentos de ciberseguridad: Certificación profesional en detección de amenazas, análisis de vulnerabilidades, SIEM, Linux, SQL, Python y respuesta a incidentes.

Curso: Introducción a Splunk
El Rincón del Hacker | Mario Álvarez Fernández
Mayo 2025

Análisis de eventos con Splunk: Formación práctica en lenguaje SPL, creación de dashboards, correlación de datos y detección de amenazas en entornos defensivos. Curso impartido por experto en ciberseguridad, enfocado en el uso de Splunk como herramienta clave en operaciones SOC.

Experiencia

Casos prácticos durante mi formación
The Bridge | Más de 500 horas aplicadas en entornos simulados

Durante mi formación en The Bridge, completé más de 500 horas prácticas en entornos simulados Red Team y Blue Team, con foco en explotación de vulnerabilidades en Linux y Windows, escalada de privilegios y post-explotación. Simulé ataques OWASP Top 10 (SQLi, XSS, webshells) y utilicé Snort y Suricata para detección de tráfico malicioso. Trabajé con Splunk para análisis de eventos (consolidado en el curso SOC de Cisco), exploré EDRs como CrowdStrike y participé en respuesta a incidentes, análisis forense básico y hardening de sistemas.