

DAVID PADRON

Cyber Threat Intelligence Analyst | OSINT | Seguridad Ofensiva

Buenos Aires, Argentina

Tel: +54 9 2226 554793

Email: davidpadron.cyber@gmail.com

LinkedIn: linkedin.com/in/david-padron-9a74aa323

GitHub: github.com/FeathersMcgr4w

Portfolio: feathersmcgr4w.github.io/cyber-portfolio/

PERFIL PROFESIONAL

Analista de Cyber Threat Intelligence con experiencia en OSINT ofensivo, reconocimiento avanzado y apoyo a equipos de Red Team. Especializado en la recolección de información, mapeo de infraestructuras, identificación de vectores de ataque y automatización de tareas en Linux. Experiencia en análisis de amenazas, IOCs, modelado de riesgos, estándares MITRE ATTACK, NIST y OWASP. Desarrollo de herramientas personalizadas en Bash y Python para inteligencia, scraping, scripting y análisis técnico.

EXPERIENCIA PROFESIONAL

Cyber Threat Intelligence Analyst

Pentesting Al Palo

01/2024 – Actualidad

- Ejecución de OSINT para la fase de reconocimiento en auditorías de pentesting web.
- Identificación de activos, subdominios, tecnologías y potenciales vectores de ataque.
- Uso de MITRE ATTACK, CVE, CVSS, NIST y OWASP para análisis técnico.
- Desarrollo de herramientas de automatización en Bash y Python para inteligencia y scraping.
- Elaboración de informes técnicos, análisis de riesgo y modelado de amenazas.
- Gestión de credenciales en KeePassXC y Bitwarden.
- Implementación de políticas de seguridad basadas en NIST 800-53.
- Tareas de backup, administración básica de infraestructura y hardening.
- Configuración de entornos virtualizados en VirtualBox y VMware.
- Consultoría de seguridad a equipos de desarrollo (AppSec).

Instructor de Seguridad Informática

Encode S.A

05/2025 – 06/2025

- Diseño e impartición de capacitación en seguridad informática al personal de desarrollo de software y líderes.
- Temas: fundamentos de seguridad, amenazas, buenas prácticas, introducción al desarrollo seguro y políticas de seguridad.

Técnico de Soporte Informático

Autónomo

2020 – 2024

- Instalación de sistemas operativos Windows y Linux.
- Análisis y limpieza de malware.
- Optimización de sistemas y mantenimiento preventivo.
- Armado de computadoras empresariales y hogareñas.
- Armado de rigs para minería de criptomonedas.
- Instalación de impresoras y equipos para comercios.

EDUCACIÓN Y CURSOS

Cisco Networking Academy

- Introduction to Cybersecurity
- Networking Basics
- Network Devices and Initial Configuration
- Endpoint Security
- Network Defense
- Cyber Threat Management

Hack The Box

- Más de 20 laboratorios de pentesting web

Udemy

- Análisis dinámico de malware en Windows
- Análisis estático de malware en Windows

OSINT y Ciberinteligencia

- EVILSEC – Técnicas de Investigación e Inteligencia OSINT
- XSEC – Curso de Ciberinteligencia

HABILIDADES TÉCNICAS

Sistemas Operativos: Linux, Windows

Lenguajes y Scripting: Python, Bash, JavaScript, C/C++, SQL, MongoDB

OSINT y Pentesting: BurpSuite, Nmap, Wireshark, Shodan, FOFA, Spiderfoot, Subfinder, Katana, DNSX, HTTPX, Wfuzz, Exiftool, Espoofer, Sherlock

Threat Intelligence: Hybrid Analysis, VirusTotal, URLScan, AbuseDB

Análisis de Malware: ProcMon, ProcExp, Autoruns, ESET SysInspector, Detect It Easy, PE-bear, CFF Explorer, Ghidra

Frameworks: MITRE ATTACK, CVE/CVSS, OWASP Top 10, NIST 800-53

Virtualización: VirtualBox, VMware

Especialidades: OSINT ofensivo, Seguridad Ofensiva, Red Team Recon, AppSec, Threat Intelligence

HABILIDADES BLANDAS

Creatividad, Autodidacta, Análisis, Investigación, Trabajo en equipo, Resolución de problemas.

IDIOMAS

Inglés B1 – Cambridge Assessment English