DAVID PADRON

Threat Intelligence Researcher | OSINT | Offensive Security
Buenos Aires, Argentina
Email: davidpadron.cyber@gmail.com
LinkedIn: linkedin.com/in/david-padron-9a74aa323
GitHub: github.com/FeathersMcgr4w

Portfolio: davidpadron.info

PROFESSIONAL PROFILE

Threat intelligence researcher with experience in offensive OSINT, advanced attack surface reconnaissance, and working with Red Teams to conduct web penetration testing. Specialized in gathering information from open (OSINT) and closed sources, mapping web infrastructures, and identifying attack vectors. Experienced in threat analysis, IOCs, and risk modeling under MITRE ATTACK, NIST, and OWASP standards. Develops custom tools in Bash and Python to exploit vulnerabilities, perform data scraping, and execute automated scripting. Utilizes artificial intelligence (AI) models such as Gpt, Gemini, and Copilot to process data and develop actionable intelligence for generating reports and graphs that inform future decision-making. Performs corporate intelligence tasks, including background checks, digital fingerprinting, image intelligence (IMINT), social media intelligence (SOCMINT), and monitoring phishing campaigns and leaks on the deep and dark web to protect corporate branding.

PROFESSIONAL EXPERIENCE

Cyber Intelligence Analyst

Pentesting Al Palo
12/2025 – Present

- Corporate intelligence.
- Investigating individuals.
- Cyber profiling and digital footprint tracking.
- Image intelligence (IMINT).
- Social media intelligence (SOCMINT).
- Investigating personal data breaches.
- Geospatial intelligence and geolocation.

Threat Intelligence Researcher

Pentesting Al Palo
01/2024 – Present

- Advanced attack surface reconnaissance in web penetration testing.
- Data collection using open-source intelligence (OSINT) and closed-source intelligence.
- Mapping of web infrastructure, servers, applications, and firewalls (WAFs).
- Identification of attack vectors and exploitation using proof-of-concept (POC) tests.
- Threat and risk analysis based on MITRE ATTACK, CVE, CVSS, and NIST standards.
- Development of tools using Bash and Python for vulnerability exploitation, data scraping, and scripting.
- Monitoring of cyberattack and web phishing campaigns.
- Monitoring of data breaches on the deep and dark web.
- Preparation of technical reports for web penetration testing audits.
- Security consulting for software development teams (AppSec).
- Implementation of security policies based on NIST 800-53.
- Backup tasks, basic infrastructure administration, hardening, and server and virtual machine management.

Information Security Instructor

Encode S.A
05/2025 – 07/2025

- Design and delivery of cybersecurity training to software development staff and team leaders.
- Topics: security fundamentals, threats, best practices, introduction to secure development, and security policies.

IT Support Technician

Autonomous
2020 – 2024

- Installation of Windows and Linux operating systems.
- Malware analysis and removal.
- System optimization and preventative maintenance.
- Assembly of business and home computers.
- Assembly of cryptocurrency mining rigs.
- Installation of printers and equipment for businesses.

EDUCATION AND COURSES

Cisco Networking Academy

- Introduction to Cybersecurity
- Networking Basics
- Network Devices and Initial Configuration
- Endpoint Security
- Network Defense
- Cyber Threat Management
- Junior Cybersecurity Analyst Exam (CCNA Certification)

Hack The Box

- More than 20 web pentesting labs

Udemy

- Dynamic malware analysis on Windows
- Static malware analysis on Windows

OSINT and Cyber intelligence

- Advanced techniques in Cyber Intelligence (TACINT) – Hefin
- Ivan Castañeda – OSINT and Cybercrime Mentoring
- EVILSEC – OSINT Investigation and Intelligence Techniques
- XSEC – Cyber Intelligence Course

TECHNICAL SKILLS

Operative Systems: Linux, Windows
Languages and 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, Holehe, Ghunt.
Threat Intelligence: Hybrid Analysis, VirusTotal, URLScan, AbuseDB, OpenCTI, Maltego, Gephi.

Cybercrime Investigation: BreachForums, DarkForum, Telegram, Twitter
Malware Analysis: ProcMon, ProcExp, Autoruns, ESET SysInspector, Detect It Easy, OleTools, Ghidra, Malcat.
Frameworks: MITRE ATTACK, CVE/CVSS, OWASP, NIST 800-53
Virtualization: VirtualBox, VMware
Specialties: offensive OSINT, Offensive Security, Red Team Research, AppSec, Threat Intelligence, Cyber Intelligence Analyst.

SOFT SKILLS

Creativity, Self-taught, Analysis, Research, Teamwork, Problem solving.

LANGUAGES

English B1 – Cambridge Assessment English