DAVID PADRON

DIGITAL INVESTIGATOR | OSINT | CYBER INTELLIGENCE | ETHICAL HACKER

Buenos Aires, Argentina
Email: davidpadron.cyber@gmail.com | LinkedIn: linkedin.com/in/david-padron-9a74aa323
GitHub: github.com/FeathersMcgr4w | Portfolio: davidpadron.info

PROFESSIONAL SUMMARY

Digital investigator and ethical hacker specializing in cyber intelligence, OSINT, and offensive security. Experienced in web security assessments and penetration testing alongside Red Team teams, as well as digital investigations involving scams, fraud, police reports, and corporate data leaks.

My work combines open-source intelligence techniques, digital footprint analysis, web application vulnerability identification, and intelligence gathering to identify threats, investigate suspicious activity, and help resolve real-world problems.

PROFESSIONAL EXPERIENCE

Cyber Intelligence Analyst

Pentesting Al Palo | December 2025 – Present

- Identity investigations: Query and analyze government databases and available information sources to reconstruct investigated subjects' physical identities and establish potential links to their digital identities.
- OSINT reconnaissance and investigations: Apply OSINT, SOCMINT, WEBINT, IMINT, and GEOINT techniques to trace digital footprints, identify information assets, and connect data from different open sources.
- Social media analysis: Identify and correlate profiles, relationships, activity patterns, behaviors, location indicators, and potential risks. Extract and analyze metadata and unique identifiers associated with profiles and usernames.
- Digital identifier correlation: Analyze email addresses, phone numbers, usernames, domains, IP addresses, and platform identifiers to link records and build digital profiles from converging evidence.
- Technical Gmail identifier analysis: Extract and analyze the Gaia ID associated with Gmail accounts to support identity correlation and digital footprint tracing.
- Image-based geolocation (IMINT): Analyze photographs obtained during investigations to identify visual references, environmental features, and geographic clues that help determine or narrow down where they were taken.
- Geospatial intelligence (GEOINT): Create investigative maps by plotting and correlating locations identified through open sources, supporting spatial analysis of findings.
- Digital fraud and scam investigations: Analyze online activity traces, profiles, identifiers, and digital evidence to reconstruct events, establish potential links among involved parties, and document relevant findings.
- Digital investigations with potential legal relevance: Collect, analyze, and organize digital information related to alleged criminal activity to reconstruct events and document findings that may contribute to legal investigations.
- Private cyber intelligence and digital investigation reports: Document evidence and digital identities in cases involving sexual harassment, scams, and e-commerce fraud; collect and correlate information to support affected individuals and potential legal proceedings; identify and document fraudulent online stores for reporting to platform providers; and report corporate data leaks found on cybercrime forums, documenting the identification, acquisition, and validation of exposed material for affected organizations.

Security Research Analyst

Pentesting Al Palo | January 2024 – Present

- Corporate intelligence and target reconnaissance: Research company profiles, tax information, trademark records, leadership structures, and digital presence to identify relevant assets and contextualize security assessments.
- Infrastructure and attack surface reconnaissance: Enumerate domains, subdomains, IP addresses, and DNS records; identify web technologies; perform URL crawling and directory fuzzing; and conduct port scanning to map exposed services and identify potential entry points.
- Vulnerability assessment and classification: Analyze identified vulnerabilities, estimate severity using CVSS, and assess technical risks to prioritize findings by potential impact and relevance to infrastructure security.
- Threat analysis and risk modeling: Apply MITRE ATT&CK;, CVE, CVSS, and NIST standards to contextualize threats, map vulnerabilities to potential attack techniques, and support security recommendations.
- Corporate email security assessment: Analyze SMTP infrastructure and domain authentication mechanisms, including SPF, DKIM, and DMARC, to identify misconfigurations and potential email spoofing scenarios.
- Corporate information exposure research: Analyze metadata from files accessible through web servers to identify potential information leaks. Collect corporate email addresses and review public LinkedIn profiles of employees and executives as part of organizational reconnaissance.
- Technical validation of attack vectors: Identify potential exploitation paths and develop controlled proof-of-concept (PoC) tests to verify the existence and impact of vulnerabilities in assessed systems.
- Tool development and automation: Create Bash and Python scripts and utilities to automate reconnaissance, scrape data, and support technical vulnerability validation.
- Technical and executive cybersecurity reporting: Produce infrastructure and attack surface reconnaissance reports for Red Team operators; technical penetration testing reports detailing vulnerabilities, CVSS severity ratings, PoCs, validation procedures, and remediation recommendations; executive reports presenting web application security status through graphical indicators and CIDA ratings; risk assessment reports covering asset identification and valuation, risk prioritization, and remediation levels; and practical cybersecurity guides to strengthen organizational security awareness.

Information Security Instructor

Encode S.A. | *May 2025 – July 2025*

- Designed and delivered information security training for software development staff and team leaders.
- Topics: Security fundamentals, threats, development best practices, introduction to secure development, and security policies.

IT Support Technician

Self-employed | *2020 – 2024*

- Installed Windows and Linux operating systems.
- Performed malware analysis and cleanup.
- Optimized systems and performed preventive maintenance.
- Assembled computers for business and home use.
- Assembled cryptocurrency mining rigs.
- Installed printers and equipment for retail businesses.

EDUCATION & TRAINING

Certifications & 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

Hands-on Labs — Hack The Box

- More than 20 web penetration testing labs.

Completed Courses — Udemy

- Dynamic Malware Analysis on Windows.
- Static Malware Analysis on Windows.

OSINT & Cyber Intelligence

- Advanced Cyber Intelligence Techniques (TACINT) — Hefin.
- Ivan Castañeda — OSINT and Cybercrime Mentoring.
- EVILSEC — OSINT Investigation and Intelligence Techniques.
- XSEC — Cyber Intelligence Course.

TECHNICAL SKILLS

Operating systems: Linux, Windows.

Programming and scripting: Python, Bash, JavaScript, C/C++, SQL.

OSINT and cyber intelligence: Maltego, SpiderFoot, Shodan, FOFA, Sherlock, Holehe, GHunt, OSINT Industries, Gephi.

Web reconnaissance and penetration testing: Burp Suite, Nmap, Subfinder, Katana, DNSx, HTTPx, Nuclei, Wfuzz, Ghauri.

Network and traffic analysis: Wireshark.

Metadata and digital footprint analysis: ExifTool and digital identifier investigation tools.

Threat and malware analysis: VirusTotal, Hybrid Analysis, URLScan, ProcMon, Process Explorer, Autoruns, Detect It Easy, OleTools, Ghidra, Malcat, ESET SysInspector.

Open databases: Dateas, Nosis, ARCA, BCRA, ANSES, ARBA.

Security and risk assessment: MITRE ATT&CK;, CVE, CVSS, NIST, and OWASP.

SOFT SKILLS

Creativity, self-directed learning, analytical thinking, research, teamwork, and problem-solving.

LANGUAGES

English: B1 — Cambridge Assessment English