Daniel Monzón

RED TEAM – SECURITY RESEARCHER

+34-645806289
daniel.monzonpeso@gmail.com
https://stark0de.com/
https://github.com/stark0de
https://www.exploit-db.com/?author=10335 (some of my exploits)

CERTIFICATIONS

- Offensive Security Certified Professional (OSCP)
- Offensive Security Wireless Professional (OSWP)
- CREST Certified Practitioner Security Analyst (CPSA) / CREST
- CRTPentesterAcademy - Certified Red Team Professional
- (CRTP) eLearnSecurity Mobile Application Penetration
- Tester (eMAPT) Pentester Academy - Cloud Security Professional (PACSP)
- Pentester Academy - Certified Azure Red Team Professional (CARTP)
- Offensive Driver Development – Zeropoint
- Malware Development Advanced – Sektor7
- Accelerated Windows API for Software Diagnostics
- Currently preparing for CRTO2 (specific for red teaming and AV/EDR evasion) and CARTE as well as researching about OS internals on my own.

ABOUT ME

Cybersecurity enthusiast, I have been learning and growing in the field for years. I am motivated by different areas such as red teaming and OS internals. Lately I've been focusing on malware development and learning about Windows internals. My goal is to become a great security researcher.

TALKS

- **Weaponizing 0days: From code analysis to massive exploitation**
  - HoneyCON (2020)
  - WorldParty (2020)
- **Hacking Kubernetes**
  - DragonJARCON (2021)
- **Smart Contract hacking**
  - Worldparty (2021)
  - BSides Barcelona (2021)
- **Introduction to Windows Internals**
  - Hackon (2023)
- **Advanced phishing talk (Worldparty 2023)**
- **macOS Security talk (Rooted Málaga 2024)**
- **Fuzzing workshop (hack0n -2024)**
- **Electron-legacy: reviewing the security of your desktop apps (hack0n -2025)**

LANGUAGES

- Spanish - Native
- English - C1 (IELTS (British Council)

STUDIES

- Bachillerato of Science - IES El Pinar

PROFESSIONAL EXPERIENCE

Red Team operator | Siemens – Jan 24 - Now

- Execution of red team exercises, thick client pentesting. Researching about AI red teaming.

Pentester | Innotec Security - Jul 21 – Dec 23

- Infrastructure hacking, web hacking, mobile app hacking, internal penetration tests, endpoint hacking, Wi-Fi networks hacking, phishing campaigns.
- Red Team exercises, code analysis, noise tests in AWS, Kubernetes clusters hacking, SAP audits.

Pentester | Atalanta Evolution - Mar 20 - May 21

- Teaching (Masters in Ethical Hacking San Pablo CEU).
- Red Team exercises, code analysis (NodeJS, C#, PHP, Ruby, Python, Java, Apex).
- Writing articles for the company's website
- Web audits, mobile, infrastructures, APIs, ICS-SCADA, IoT-systems.

SKILLS

- Windows internals mainly (but also macOS and Linux)
- Reverse engineering (IDA Pro, Ghidra)
- Python tooling development
- C/C++ coding
- Code analysis (NodeJS, PHP, C#, C++, Java, etc)
- Active Directory pentests and red teaming
- Web application assessments
- Mobile application pentesting (Android and iOS)
- Azure, AWS and GCP pentesting
- AI pentesting (LLMs)
- Wi-Fi pentesting
- Thick client pentesting
- Infrastructure pentesting
- OT (ICS) pentesting
- Endpoint security assessments
- Phishing campaigns delivery
- Kubernetes clusters pentesting

ACHIEVEMENTS

- Outside Talent winner - https://www.entelgy.com/divisiones/innotec-security/innotec-security-actualidad/innotec-security/noticias-corporativas-innotecsecurity/entelgy-innotec-security-presenta-a-los-ganadores-de-la-4-edicion-del-outside-talent
- As of today I've found 25 vulnerabilities in products (18 with CVE ID assigned), some of them are:

  - Lotus Core CMS v.1.0.1 Local File Inclusion (CVE-2020-8641) SEOPanel 4.6.0 Remote Code Execution (CVE-2020-27461)
  - Wordpress Plugin Media Library Assistant v2.81 Local File Inclusion (CVE-2020-11372)
  - ZenTao Pro 8.8.2 – Command injection (CVE-2020-7361)
  - Multiple vulnerabilities in rConfig (https://ssd-disclosure.com/ssd-advisory-rconfig-unauthenticated-rce/)

- Finally, I've published some tools (like Nginxpwner, regsave and the PE-tools) useful for tasks such as binary analysis and web hacking and articles (such as https://deephacking.tech/como-cargarse-windows-defender-y-explorer-exe-sin-querer-research/), which describes the way I found it was posible to kill Windows Defender (which is a PPL) by suspending the process.