

Alejandro Fernández Castrillo

29 years old.

Madrid, Madrid

Email : **afernandezca8@gmail.com**

Proactive, self-taught, patient and responsible. Thirsty for knowledge.

I love Computer Science. One of my hobbies is spending time in front of the PC learning hacking techniques and solving CTFs. Currently I'm focused in AD vulnerabilities and exploitation, but web and reversing binaries challenges are always welcome.

EDUCATION

- 2010-2012 High School**
«IES Ornia» (La Bañeza)
- 2012-2016 Computer Science degree (Project : Remote management of a drone by using hands gestures)**
«Universidad Pontificia de Salamanca» (Salamanca)
- 2016-2018 Cybersecurity research master's degree (Project : Android malware detection using artificial intelligence model)**
«Universidad de León» (León).

ADDITIONAL EDUCATION

- 2016 BigData expert**
«Non-official Universidad Pontificia de Salamanca master's degree»
- 2021 OSCP (Offensive Security Certified Professional) – Offensive Security – “OS-101-43071”.**
- 2022 CRTP (Certified Red Team Professional) – Pentester Academy – “ADLID3625”.**
- 2022 CRTE (Certified Red Team Expert) – Pentester Academy – “RTLID1532”.**
- 2022 “OFFSHORE” ProLabs – Hack The Box – “HTBCERT-2AB879A4A3”.**
- 2023 “CYBERNETICS” ProLabs – Hack The Box – “HTBCERT-ACDAEB4373”.**
- 2023 “ZEPHYR” ProLabs – Hack The Box – “HTBCERT-0742FFC6DB”**

Technical:

- C, C++, Python, Java
- Software Analysis (x86, ARM)
- Reversing (gHidra, IDA)
- Debugging (GDB, radare2, ollydbg...)
- Fuzzing, Taint Analysis
- Sandboxing (Cuckoo). Qemu/KVM
- Windows and Active Directory. Networks and systems pentesting. Red team & Blue team.
- Burp, OpenVas, Nikto, Nessus, Metasploit and other C2 frameworks
- Data Analysis (searching, storing, preparation/cleaning, processing). Machine Learning with Python (Scikit Learn)
- Windows and Linux forensinc analysis

- DevOps (Docker and Kubernetes)
- ...

EXPERIENCE

July 2017- January 2018 Instituto Nacional de Ciberseguridad - Incibe. (National Cybersecurity Institute)

Department: Cybersecurity services for professionals and companies

Duties:

- Cybersecurity advices for both professionals and industrial control systems, cybersecurity-related event blogs, blog articles for both companies and professionals, layout of the websites incibe.es and INCIBE Cert
- MOOCs review
- Vulnerabilities translation and review

November 2018 – June 2019 Capgemini Asturias

Department: SOC

Duties:

- Monitoring of SIEMs (ArcSight, McAfee), firewall management (CheckPoint, PaloAlto, Fortimanager) as well as Cisco-Asa (VPN), antivirus, IPS/IDS, WAFs and various SOC tools. Ticketing (ServiceNow, Cherwell)
- Web and Networks pentesting

July 2019 – Currently in the company Epoche and Espri, a DEKRA company

Department: Testing y pentesting

Duties:

- "Common Criteria". ATE and AVA
- Verify software functionalities indicated by the manufacturer for subsequent certification. Testing of different interfaces (TFSIs). Protocol analysis using different techniques (payloads manipulation...). Fuzzing. Code analysis (radare2 and GDB)
- Vulnerability scanning and exploitation. Exploit development
- Android and Web pentesting
- Network auditing, including Windows AD.
- FIPS 140-2 and FIPS 140-3. Cryptographic algorithm testing

Others:

- Industrial Control systems (PLCs and RTUs) IEC 62443-4-1/4-2