Alejandro Fernández Castrillo
29 años
Residencia actual : Madrid, Madrid
Email : **afernandezca8@gmail.com**

Proactivo, autodidacta, paciente y responsable. Sediento de conocimiento.

ESTUDIOS

2010-2012 **Título de bachillerato**
«IES Ornia» (La Bañeza)

2012-2016 **Grado en Ingeniería Informática (TFG : Gestión remota gesticular de un dron)**
«Universidad Pontificia de Salamanca» (Salamanca)

2016-2018 **Máster Universitario de Investigación en Ciberseguridad (TFM: Desarrollo de un modelo predictivo de Malware para Android)**
«Universidad de León» (León).

FORMACIÓN COMPLEMENTARIA

2016 **Título de Experto en BigData**
«Titulo propio de la Universidad Pontificia de Salamanca» (Salamanca).

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"**

Conocimientos informáticos:

- C, C++, Python y Java.
- Análisis de software (x86, ARM). Reversing (ghidra, IDA). Debugging (gdb, radare2, ollydbdg…), Fuzzing, Taint Analysis… Sandboxing (Cuckoo). Qemu/KVM.
- Windows y Active Directory. Pentesting de redes y sitemas Windows. Red team y Blue team.
- Herramientas para auditorias, Burp, OpenVas, Nikto, Nessus, Metasploit y otros frameworks C2.
- Analisis de datos. (búsqueda, almacenamiento, preparación/limpieza, procesamiento). Machine Learning con Python (Scikit Learn)
- Análisis forense en Linux y Windows.
- Docker. (DevOps)
- …

Idiomas :

Inglés: **Hablado:** Medio
Escrito: Alto
Leido: Alto

EXPERIENCIA LABORAL

Julio 2017- Enero 2018 **Instituto Nacional de Ciberseguridad [Incibe]**

Sección: Servicios de Ciberseguridad para profesionales y empresas.

Funciones realizadas:

- Redacción de: avisos de ciberseguridad tanto para profesionales y como para sistemas de control industrial, bitácoras de eventos relacionados con la ciberseguridad, artículos de blog tanto para empresas como para profesionales, maquetación de las páginas web incibe.es y certsi.es.
- Revisión de MOOCs
- Traducción y revisión de vulnerabilidades

Otros:

- 3 publicaciones en el blog de Incibe e Incibe Cert.

Noviembre 2018 – Junio 2019 **Capgemini Asturias**

Sección: SOC

Funciones realizadas:

- Monitorización de SIEMs (ArcSight, Mcafee), gestión de firewalls (CheckPoint, PaloAlto, Fortimanager) además de Cisco-Asa (VPN), antivirus, IPS/IDS, WAFs y diversas herramientas propias de un SOC. Ticketing (ServiceNow, Cherwell).
- Pentesting web y redes.

Otros:

- Conocimientos básicos de Splunk

Julio 2019 – Actualidad **Epoche and Espri, a DEKRA company**

Sección: Testing y pentesting

Funciones realizadas:

- *"Common Criteria". ATE y AVA.*
- Verificar funcionalidades de software que indica el fabricante para su posterior certificación. Testing de las diferentes interfaces (TFSIs). Análisis de protocolos mediante diversas técnicas (Manipulación de 'payloads'…). Fuzzing. Analisis de código (radare2 y GDB).
- Busqueda de vulnerabilidades y posterior explotación, Desarrollo de 'exploits'. Pentesting. Auditoría.
- Python y C.
- FIPS 140-2 y FIPS 140-3. Testing de algoritmos criptográficos.
- Android y Web.

Otros:

- Sistemas de control industrial. (PLCs y RTUs) IEC 62443-4-1/4-2

Otra información:

- Carnet de Conducir B1. Vehículo propio.
- Licencia RPAS, con posibilidad de pilotar aeronaves no tripuladas de hasta 25 kg.