

Entre las 15:00 del viernes 27 y las 23:59 del domingo 29 de Junio de 2025 tuvo lugar la competición internacional de ciberseguridad **Industrial Intrusion**, organizada por la plataforma **TryHackMe**. El evento consistió en 37 desafíos tipo CTF (Capture The Flag), con temáticas que abarcaron desde protocolos industriales y análisis forense hasta seguridad web, elevación de privilegios, Active Directory, Samba, shells reversos, redes y múltiples aspectos del ámbito IT y OT.



El escenario planteado por la competición nos introducía a una narrativa envolvente (del inglés):

«Tres meses después del ataque de malware a la Planta de Control de Agua de Virelia, la instalación reanudó sus operaciones gracias a un “reestablecimiento completo”. Sin embargo, los operadores comenzaron a notar sensores que parpadeaban, presiones de válvulas inconsistentes y alertas automáticas que no podían vincularse a ningún proceso activo. Una investigación más profunda reveló que el atacante había dejado un mecanismo de persistencia en forma de implante encubierto de segunda fase, que restableció el control a través de puertas traseras OT pasadas por alto y se observó un portal web comprometido. Como especialista de red team contratado por la empresa Black Echo tu misión es infiltrarte en los sistemas infectados antes de que el atacante active su interruptor de apagado y se pierda toda la información sobre su autoría.»

Este texto ya anticipaba un escenario técnico e inmersivo **centrado en la ciberseguridad industrial**, en el que debíamos rastrear la actividad del atacante, descubrir sus persistencias y neutralizar sus implantes.

La competición se desarrolló en **equipos de hasta cinco integrantes**, con la participación de **más de 5.500 equipos** de todo el mundo. Fue un éxito rotundo, tanto en términos técnicos como organizativos, y dejó el listón muy alto para futuras competiciones de nivel internacional.

Mi equipo estaba formado por compañeros del Instituto de Educación Superior **Zubiri Manteo**, donde recientemente finalicé mi formación reglada en informática: tanto el ciclo superior de Administración de Sistemas Informáticos en Red (ASIR) como la especialización en Ciberseguridad (CETI). Cuatro de los miembros habían sido compañeros míos en el aula de ciberseguridad, y el quinto, aunque especializado en desarrollo de aplicaciones, también estudió en el mismo centro.

Haciendo honor a quién fue nuestro **rival más duro** en la **CyberLehia 2025**, pusimos al grupo el nombre **HackTxoko**. Sin duda un nombre que retrata esos espacios de la casa (o del mundo) donde nos encerramos a presionar teclas durante horas.



Si bien es cierto que por momentos llegamos a escalar hasta el puesto **30, de 5698 equipos apuntados**, nuestro resultado final fue la posición **164**, situándonos dentro del **top 3%** mundial. Esto significa que superamos al 97% de los equipos participantes, entre los que había no sólo estudiantes sino profesionales del sector con años de experiencia, incluyendo potentes equipos de países como Estados Unidos, China, India o Israel.



A diferencia de mi participación en la CyberLehia, en esta ocasión opté por un enfoque más versátil: en lugar de centrarme solo en los desafíos más difíciles, intenté resolver **la mayor cantidad posible**. Esta estrategia se reflejó de manera positiva en la distribución de flags resueltas por cada miembro del equipo:

MIEMBRO	FLAGS RESUELTA
NiPeGun (Nico)	16
NanoGrep (Asier)	8
LilBr0 (Alejandro)	4
Starke (Dani)	3
SirCoconut72 (Eneko)	1

La siguiente imagen muestra el desglose de las flags obtenidas por cada miembro del equipo. Al hacer click sobre ella, se abrirá en una nueva pestaña donde se podrán ver mejor los detalles.



Con esta participación **cierro con orgullo mi etapa de formación** académica en informática y ciberseguridad. Soy consciente de que aún queda mucho por mejorar para alcanzar el codiciado **top 1% mundial**, pero encaro el futuro con mentalidad combativa, listo para enfrentar cada nuevo reto que el universo de ceros y unos tenga preparado para mí.

