Cedric LIN

France · Luxembourg · Canada Driver's license
+33 7 82 98 58 39 ruohaolin@gmail.com linkedin.com/in/ruohaolin github.com/Ruohao1

Profile

Master's student in Cybersecurity at UQAC, pursuing a double degree with Télécom Nancy (France) in Computer Science. Enthusiastic about cybersecurity, with hands-on experience in system hardening, automation, and security standards. Motivated, rigorous, and eager to contribute technical expertise while continuing to grow as a cybersecurity professional.

Education

Université du Québec à Chicoutimi **2025 – 2026**
Master's in Computer Science, Cybersecurity specialization *Chicoutimi, Canada*

Télécom Nancy **2023 – 2026**
Master's in Computer Science, specialization in Internet, Connected Systems and Security *Nancy, France*

Lycée Chaptal **2021 – 2023**
Preparatory Classes MPSI / MP (Mathematics, Physics, Engineering)* *Paris, France*

Professional Experience

Wintics **June 2025 – Aug. 2025**
Operational Security Intern *Paris, France*

- Designed and developed an automation tool for Ubuntu system hardening using Python and Ansible, integrated with internal reporting and auditing dashboards.
- Implemented a complete set of CIS and ANSSI-compliant security controls, including authentication policies, SSH restrictions, logging, and firewall hardening, with plans for production deployment.
- Produced technical documentation and troubleshooting playbooks tailored for operations staff and interns to streamline adoption.

Super U **Nov. 2024 – May 2025**
Retail Associate *Maxéville, France*

- Reduced waste and improved efficiency by optimizing inventory tracking and restocking processes.
- Handled high-volume customer transactions, including refunds and conflict resolution, ensuring smooth checkout operations.
- Worked in a small team of 5, maintaining supply and cleanliness across all aisles.
- Entrusted with opening and closing procedures, cash reconciliation, and shift management, demonstrating reliability and autonomy.

Projects

Homelab Environment | *Proxmox, Tailscale, Ansible, ELK, Snort* **Ongoing**

- Deployed a Proxmox-based homelab with automated VM and container provisioning using Ansible playbooks.
- Configured a SIEM stack (ELK) with Snort IDS and firewall rules to monitor, detect, and analyze network threats.
- Implemented secure remote access via Tailscale, ensuring encrypted connectivity to services.
- Hosted and managed self-deployed services such as Nextcloud, Vaultwarden, and Jellyfin for practical system administration and security hardening practice.

TryHackMe Labs | *Offensive-focused: Web, Reverse, Linux* **Ongoing**

- Regularly complete offensive labs covering web exploitation, reverse engineering, and Linux privilege escalation.
- Produce detailed write-ups for completed rooms with step-by-step exploitation and remediation notes.
- Toolset: nmap, ffuf, Burp Suite, Metasploit, pwndbg — used for discovery, fuzzing, exploitation and post-exploitation.
- Ranked in the top 4% of TryHackMe users.

Technical Skills

Programming Languages: Python, Rust, C, TypeScript, Java, SQL
Web Technologies: Next.js, Node.js, HTML, CSS
Security & Systems: Linux (hardening, automation), Ansible, Docker, ELK, Snort, SIEM, Firewalls
Pentesting Tools: Nmap, FFUF, Burp Suite, Metasploit, pwndbg