Cedric LIN

M.Sc. Computer Science (Double Degree), Cybersecurity. Available for internship beginning July 1, 2026.

✉ clin@etu.uqac.ca | ☎ +1 (581) 560-9210
ruohao.dev | linkedin.com/in/ruohaolin | github.com/Ruohao1

Profile

Master's student in a double-degree Computer Science program specializing in cybersecurity, with interests in secure system design, security controls, and technical security testing. Experienced in analyzing Linux-based environments, identifying architectural weaknesses, and developing automation for security validation and configuration management. Comfortable translating complex technical implementations into clear documentation and structured security improvements.

Technical Skills

Security & Risk: Threat modeling, attack surface analysis, vulnerability assessment, remediation, control mapping
Systems & Infrastructure: Linux, Proxmox, network segmentation, firewalling, CIS hardening
Offensive & Testing: Recon, enumeration, web exploitation, authentication and privilege escalation techniques
Programming: Python, Go, C, Bash
Automation & IaC: Ansible, Terraform (provisioning, compliance validation, configuration enforcement)
Tools: Nmap, Burp Suite, Nessus, Wireshark, Elastic Stack (ELK), Git

Professional Experience

Systems Security Intern — Wintics (Paris, France) *Jun – Aug 2025*

- Designed and developed a **Python** + **Ansible**-based compliance framework aligned with **CIS** and **ANSSI** benchmarks for Linux systems.
- Implemented automated auditing modules to validate configuration rules and detect benchmark deviations.
- Built remediation playbooks to enforce secure baselines and standardize system hardening.
- Produced operational documentation and troubleshooting guides for deployment and host-level issue resolution.
- Coordinated with system administrators to validate remediation outcomes and ensure benchmark conformity.

Projects

Security Testing & Architecture Lab (Homelab) *2025 – Present*

- Designed and operated a segmented virtual infrastructure on **Proxmox**, simulating enterprise-style network zones.
- Implemented perimeter routing and firewall rules using **OPNsense**, enforcing segmentation and access control.
- Secured remote access via **WireGuard VPN** with restricted management interfaces.
- Deployed **Traefik** reverse proxy for controlled service exposure and TLS termination; integrated **Pi-hole** for DNS-level filtering and monitoring.
- Currently developing **Terraform configurations** and **Ansible playbooks** to enable reproducible infrastructure deployment and compliance validation.

Offensive Security Practice & CTFs *2024 – Present*

- **TryHackMe Top 1%** worldwide; 2nd place NCC CTF; Hackfest 2025 (LAN) competitor.
- Completed advanced web exploitation labs (PortSwigger Web Security Academy), focusing on XSS, SSTI, authentication bypass, file upload abuse, and access control flaws.
- Built custom **Python** exploit scripts to automate lab vulnerabilities (token manipulation, payload generation).
- Developed a **Go**-based reconnaissance toolkit to automate recon including service enumeration, HTTP probing.
- Applied structured offensive methodology: enumeration, attack surface mapping, exploit development, privilege escalation, and post-exploitation analysis.
- Authored technical writeups documenting attack paths, root causes, and defensive remediation insights.

Education

Université du Québec à Chicoutimi (UQAC) — Canada *2025 – 2026*
MSc in Computer Science (Cybersecurity) — Double Degree with Télécom Nancy
Télécom Nancy — France *2023 – 2026*
Engineering / MSc-level program in Computer Science (Networks & Security)
Lycée Chaptal — Paris, France *2021 – 2023*
MPSI / MP* — Highly selective two-year pre-engineering program (intensive mathematics and physics)

Languages

French (native), English (C1 - TOEIC), Chinese (native)