ROMAIN GERARD

French National | Software Engineering Researcher
Software Engineering (M.Eng), USTC
Suzhou, Jiangsu
LinkedIn | Github | Website
159 0560 1208 | gerarromain@gmail.com

EDUCATION

University of Science and Technology of China (USTC) **Hefei/Suzhou, China**
M.Eng. in Electronic Information - Major: Software Engineering *2025 - Present*
Coursework/Focus: Information Security, Compiler Engineering, Blockchain Technologies, Information Theory & Coding, Ubiquitous OS, HarmonyOS Development, Artificial Intelligence
Current GPA: 3.54/4.0 (First Semester)

University of Rouen Normandy **Rouen, France**
Associate + Bachelor of Science (B.Sc.) equivalent in Multimedia & Internet Technologies *2020 - 2024*
GPA: Top of Class – 16.07/20 (4.0 equivalent)

WORK EXPERIENCE

Prescott (Internship) **Paris, France**
Webmaster & Graphic Designer *April 2024 – July 2024*
- Managed updates for an existing WordPress platform; Produced product visuals and Figma prototypes.

JKDS Renovation (Internship) **Paris, France**
Artistic Creation Lead & Front-End Developer *April 2022 – July 2022*
- Designed the company's complete visual identity and built its WordPress website.
- Created digital/print assets and optimized site UX for new customer acquisition.

PROJECT EXPERIENCE

HexStrike-AI | LLM Security Research Framework | Link **Suzhou, China**
Security Researcher & Lead Developer *February 2026 - Present*
USTC Suzhou Institute – Information Security Lab | Engineering Project (Credited)
Supervisor: Prof. Guo Yan (郭燕)
- Extended a Python/Flask pentest framework exposing 150+ security tools via MCP, researching why LLM agents underutilize available tools and designing an improved architecture.
- Ran controlled experiments comparing Claude and DeepSeek across 4 AI clients (Claude.ai, RooCode, 5ire, TRAE) on PicoCTF challenges, measuring tool-selection behavior across 3 variants: baseline preference, ranking compliance, and forced compliance.
- Built a 529-prompt benchmark corpus across 7 CTF categories × 3 difficulty levels × 2 LLMs × 3 clients for reproducible behavioral analysis.
- Deployed an OpenAI-compatible LLM proxy to intercept and log tool call chains across clients; defined 3 core metrics: ranking compliance rate, selection frequency bias, and decision divergence rate.

2026 Software System Security Competition (National) **Suzhou, China**
Security Researcher / CTF Competitor *March 2026*

- Participated in the 2026 Software System Security Competition, a national attack-defense cybersecurity competition.
- Solved challenges across forensics, reverse engineering, and cryptography.

OS Engineering Labs – Ubiquitous Computing Course **Suzhou, China**
Graduate Coursework *Dec 2025*

- Implemented a custom Linux kernel syscall in C using RCU locking for deadlock-safe process/group ID traversal; validated via kernel logs and /proc filesystem.
- Cross-compiled Linux 5.4.250 for x86 and ARM64 using GCC and QEMU; built minimal initramfs with BusyBox and custom init scripts.
- Built a buddy memory allocator in C with XOR-based partner indexing, block splitting, and cascading merge on free.
- Deployed openEuler 22.03 LTS on a two-node cluster; loaded HMDFS kernel module and validated 9 distributed filesystem behaviors including cross-node sync and write conflict detection.

SEED Labs – Network Security Practicum **Suzhou, China**
Security Researcher / Graduate Coursework *Oct 2025 – Nov 2025*

- Performed ARP cache poisoning (request, reply, gratuitous) in Docker environments using Scapy to enable MITM attacks on Telnet and Netcat sessions with live traffic modification.
- Exploited 32/64-bit buffer overflows via shellcode injection and GDB-assisted offset calculation, achieving root privilege escalation through Set-UID programs.
- Developed Linux kernel modules using Netfilter hooks to filter traffic by protocol, IP, and port; validated enforcement dynamically against live DNS and ICMP traffic.
- Executed ICMP redirect attacks to hijack victim routing tables, followed by TCP-layer payload interception and modification using Scapy.

Stardew Dashboard (Personal Project) **Paris, France**
Full-Stack AI Developer *Feb 2024 - Apr 2025*

- Co-developed an intelligent dashboard analyzing Stardew Valley game saves using ReactJS and PHP.
- Built Python scripts with scikit-learn to categorize in-game data and improve user navigation.
- Added automated filtering and recommendation features, enhancing functionality and user experience.

Monarchy Mayhem (Awarded) **Paris, France**
Game Developer *Nov 2023 - Feb 2024*

- Built a full game in Unity (C#) with a team; awarded 3rd place at Festival MMI France.
- Engineered enemy AI using state machines and pathfinding, enabling realistic NPC behaviors.
- Designed adaptive difficulty mechanics based on player performance analytics to improve engagement.

SKILLS & LANGUAGES

Security: Nmap, Burp Suite, Wireshark, x86 Assembly, Scapy, GDB

Dev & Infra: Python, Flask, JavaScript, PHP, C, C#, Docker, Git, Linux/Bash

Languages: French (Native), English (C1 - IELTS 7.5), Spanish (B1), Mandarin (A1 - HSK1)