Xin

Male | 25 | Personal site: xtar.pages.dev

Background

Lanzhou University of Technology 2021.09 – 2025.06

Bachelor's degree in Cybersecurity

- Published paper: *An Interactive Multimodal Tool for Extraction and Verification in Archaeological Reports* (ACM)
- Wrote several technical posts on CSDN; my personal WeChat Official Account has 800+ followers; my Yuque notes contain 80,000+ words of technical writing
- Freelance work: built the security baseline for a company from scratch (0 to 1). Designed and set up a network security architecture for 50+ Windows endpoints, isolating office, production, personal, guest, and data storage zones with VLAN/ACL. Built an AD domain controller on Windows Server 2025 and managed endpoint security policy with GPO. Set up endpoint monitoring and centralized log analysis with Sysmon and Wazuh, and added the open-source SOAR platform Shuffle to automate response, so that Wazuh alerts connect with asset, identity, and endpoint handling flows. Used automation scripts to join endpoints to the domain and deploy security agents/policies in bulk. Also planned long-term improvements around NAS data access, VPN access, 802.1X/RADIUS network admission control, and network traffic analysis, building a defense-in-depth system that covers assets, network, identity, endpoints, detection, response, and data access control.

Skills

- **Security Tools**: Skilled with Kali Linux; familiar with Nmap, Wireshark, Metasploit, Hashcat, Hydra, Burp Suite, SQLmap, and AWVS; has taken part in multiple offensive-defense drill red teams
- **Programming**: Skilled with Python (pygame, Matplotlib, pandas, requests); can build simple web scrapers, do data analysis, and develop small games; used Flask and FastAPI for backend work
- **AI & LLMs**: Familiar with major AI models, agent frameworks, and local AI apps (MetaGPT, LM-Studio, AnythingLLM); can deploy local LLMs, build knowledge bases, and write simple scripts
- **Security Basics**: Familiar with TCP/IP; can analyze packet captures with Wireshark; knows encryption algorithms such as RSA, CTF tools, file steganography, and common security scripts
- **DevOps**: Built a general-purpose local LLM knowledge base system; familiar with Linux, Docker, Git, and conda environments; has used Docker to deploy security lab environments, MaxKB, PaddleOCR, and similar tools

Work Experience

Credit Reference Center of PBOC – Qianxin (on-site) 2026.04 – Present

Security Operations Engineer

- Helped deploy and tune domestic WAFs, Tianyan and other security devices and platforms, including log collection, alert linkage, rule optimization, and endpoint security policy tuning
- Took part in the 2026 national-level financial offensive-defense exercise. Served as the internal and external contact person, coordinating staff and communication during the event; the project was completed smoothly
- Helped sort out internet-exposed assets and run penetration tests before the exercise. Used AI to help find hidden high-risk vulnerabilities in the frontend JS of the credit reference system, and wrote up the report and followed up on the fixes
- Took part in building internal security policies, introducing several SIEM platforms, network admission control, and a localization (Xinchuang) upgrade project. Can quickly understand the pain points on both sides and handle different kinds of unexpected situations

InsightSec/CloudFall (Shanghai) Information Technology 2025.10 – 2026.04

Security Analyst

- Took part in deploying an MDR platform for a large pharmaceutical company. Independently finished agent distribution, policy configuration, endpoint onboarding, and joint testing. Brought about 2000 endpoints online. Used InsightSec/CloudFall's own security platform to do correlation analysis on ELK logs, wrote and deployed alerting rules, and enabled abnormal behavior detection and early warning of security incidents
- Took part in rebuilding the security baseline for an energy company. Responsible for deploying the ELK tool chain, log collection components, and the SIEM platform, plus connecting device logs and tuning rules
- Used log analysis platforms such as Splunk and ELK for daily security checks: searching logs, analyzing abnormal behavior, writing daily/weekly security reports, and following up on alerting events
- Helped with multi-level protection (MLPS) security work for a company: assisted in writing security management rules, asset lists, network diagrams, and security remediation plans, plus part of the assessment materials
- Improved rules and analyzed logs on Microsoft Sentinel platforms for several foreign-invested clients. Used Shannon entropy to detect DGA domain requests and abnormal network behavior. Can analyze attack paths and assess risk based on real business scenarios. Has practical experience in security operations, threat detection, and reducing the attack surface
- Led internal and external penetration test projects for several foreign-invested clients. Covered the full flow: initial information gathering, vulnerability verification, attack chain building, risk analysis, and the final report. Delivered the project and followed up on remediation on my own
- During an internal network pentest at a foreign-invested company, found and exploited an SQL injection. Got the database type, username, several tables and their fields, and some sensitive data to prove impact. Also found leaked Swagger API docs and unauthorized access to its endpoints
- During an external pentest on a project, found SQL injection on several databases and successfully accessed sensitive data. Found an arbitrary file upload vulnerability in an upload endpoint on one site, and XSS on several systems
- During an internal network pentest at a foreign-invested company, found username brute force, directory listing, and sensitive information disclosure vulnerabilities

Internships

NSFOCUS 2025.04 – 2025.09

Penetration Testing Engineer (Intern)

- Took part in daily system testing for financial institutions, found vulnerabilities, and helped with fixes. Also tested the internet-exposed assets of some institutions that were assigned to us
- Submitted multiple medium and high severity vulnerabilities to the vuldb and edu platforms, including privilege escalation and unauthorized access issues

National-level Financial Offensive-Defense Exercise – Medium-level Analyst 2025.07 – 2025.08

Blue Team Analyst

- Did the preparation work: sorted out assets, ran risk checks, and did penetration testing on internet-exposed assets
- Analyzed about 150 alerts per day on average from the monitoring team. Traced back to 1 suspected attack team. Used Qingteng cloud and Moran honeypots and other devices to help with the tracing and forensics work

Gansu Province Education Offensive-Defense Exercise 2025.06 – 2025.06

Red Team Member

- Got into the internal networks of 3 universities. Captured the databases and OA system, and earned more than 3500 points
- Audited frontend JS and found a backend data API without proper authorization. Walked the API to pull over 100,000 sensitive records, which led to one university dropping out

Lanzhou Zhengtianhe Law Firm – Zhengyuan branch office 2024.04 – 2025.04

System Maintenance & Security Intern

- Responsible for daily maintenance of the main system, monitored operation logs, and ran simple attack-and-defense exercises
- Tried adding a new frontend module, tried deploying quantized LLMs locally, and improved the user interface and interaction experience

Shanghai Fujv Logistics 2024.06 – 2024.09

Security Engineer (Intern)

- Improved backend system features, helped harden the firewalls, and raised overall system security
- Wrote security test cases, detected system vulnerabilities, and gave fix suggestions

Lanzhou University of Technology – Gansu Education Offensive-Defense Exercise 2023.09 – 2023.10

Red Team Member. Took part in the Gansu Department of Education's offensive-defense exercise. Won the "Rising Star" award from the Gansu Department of Education

- Accessed an old, not-yet-retired login page of a university. After getting into the academic system, found unauthorized access that could walk through hundreds of thousands of sensitive records
- In a middle school's enrollment system, anyone could register with any identity, and the avatar upload allowed file upload. Got a shell and entered the internal network

Ningxia WX Chuang'an – Medical Offensive-Defense Exercise 2023.07 – 2023.08

Red Team Member. Took part in the Ningxia autonomous region's offensive-defense exercise. Team score: 5/13

- Scanned and exploited vulnerabilities with tools such as Burp Suite and SQLmap, helping the team complete the attack-and-defense tasks
- Penetrated the mini program and official account of a hospital. Found a privilege escalation bug in one of the hospital official account's APIs, which allowed downloading other patients' sensitive information

Ningxia Provincial-level Offensive-Defense Exercise 2022.07 – 2022.07

Red Team Member. Gathered information with fofa and hunter. Successfully found several target admin panels, OA and CMS systems

- Found weak passwords and historical vulnerabilities. Wrote PoCs to verify and exploit them. Captured several databases, dropped shells, and gained control of a large number of IoT devices on the internal network

Undergraduate Projects

Lanzhou University of Technology – AIGC Cutting-edge Tech: "Archaeology Document Extraction" 2023 – 2024

Deeply involved in developing a multi-role agent driven by MetaGPT. Responsible for the dynamic conversation module

- Deployed PaddleOCR to extract text and key information from paper archaeology documents
- Designed and developed the frontend of the data annotation page, and used the Vue framework to improve the code
- Implemented a single-agent (LLM + observe + think + act + memory) feature, with support for real-scene interaction
- Project link: sjys.lut.edu.cn/info/1039/6814.htm

CTF Competitions and Security Practice 2022 – 2024

Took part in many CTF competitions. Strong in cryptography, steganography, packet analysis, and web security

- Results: Haifeng Cup (17/46, 5/52), Palu Cup (top 20%), DESCTF (top 25%)
- In Palu Cup, got 2nd place on a cryptography question (RSA) and 2nd place on a misc question (steganography analysis). Used tools such as 010 and IDA to quickly pin down vulnerabilities
- Solved 3 web security questions in DESCTF. Used Burp Suite to find XSS and SQL injection bugs, and successfully read the flags through the vulnerabilities
- Wrote Python scripts to automate CTF packet analysis. Improved solving efficiency by about 30%