

# Guangning Li

guangning.li@outlook.com | 672-995-0081 | Portfolio: [gnli.net](https://gnli.net) | Victoria BC – **Willing to Relocate**

## Summary

---

Master's student in Telecommunications and Information Security at the University of Victoria with over two years of experience in cybersecurity operations, scripting, and infrastructure support. Skilled in log analysis, vulnerability management, incident response, and technical documentation.

## Professional Experience

---

### IT Systems Administrator

Sep 2021 – Apr 2024

Inner Mongolia Power (Group) CO., LTD

Inner Mongolia, China

- Monitored and analyzed daily security events using firewall logs, IDS/IPS, and SIEM tools; responded to 5–10 monthly incidents, driving improvements in threat identification, containment, and recovery
- Ran weekly Nessus vulnerability scans and took the lead on hardening and patching 100+ Windows and Linux servers, reducing weaknesses by 60% and boosting system uptime and security compliance
- Collaborated with cross-functional teams (development, networking, operations) to optimize firewall rules and network segmentation for secure cross-site connectivity
- Created and maintained 50+ security documentation artifacts, including audit reports, incident logs, and compliance checklists, ensuring readiness for internal and external audits
- Improved threat detection, forensic analysis, and secure coding skills by competing in national CTF competitions, placing in the top 10% of teams
- Used AES, RSA, and key rotation to protect sensitive data between enterprise systems and banking partners
- Led risk assessments, identified system vulnerabilities, proposed mitigations, and maintained the s risk database

### Teaching Assistant

Sep 2024 – Apr 2025

University of Victoria

Victoria, BC

- Collaborated with professors to enhance academic systems and grading processes for a class of 100+ students

## Technical Skills

---

**Security Operations & Analysis:** Threat Detection, Incident Response, Log Analysis, SIEM (concepts and tools), Phishing Analysis, Vulnerability Scanning (Nessus, Zenmap), IDS/IPS (alert analysis & response)

**Network Security:** Firewall Technologies & Policy Management (Cisco ASA, Palo Alto NGFW), Network Segmentation, VLANs, VPNs (IPSec, SSL), IDS/IPS Systems (network-based), Load Balancing, Wireshark

**Endpoint Security & Identity Management:** System Hardening, Role-Based Access Control, Authentication & Authorization, Active Directory & Group Policy

**Scripting & Automation for Security:** Python, PowerShell, Bash

**Systems & Cloud Platforms:** Windows Server, Linux (Ubuntu, Debian, CentOS/RHEL), AWS, Azure, Office 365

**Programming & Development Tools:** SQL, Java, C, C++, Node.js, Git

**Productivity & Documentation:** Microsoft Office Suite, Technical Documentation

## Education

---

### University of Victoria - GPA 8.4/9 (93%)

Victoria, BC

- Master of Engineering in Telecommunications and Information Security

Sep 2024 – Present

### Northeastern University

Shenyang, China

- Bachelor of Software Engineering

Sep 2017 – Jun 2021

## Certifications

---

AWS Solutions Architect Associate • CompTIA Security+ • CompTIA Network+

## Relevant Coursework / Projects

---

### Firewalls and Intrusion Prevention Systems:

Designed and configured a virtualized zero-trust network using Palo Alto NGFW and Cisco ASA; implemented firewall rules, HTTPS inspection, URL filtering, antivirus scanning, and PAN-OS IPS to secure inter-segment traffic. Simulated attacks using Metasploit to test and reinforce defenses against SMB exploits.

### Advanced Network Penetration Testing and Defense (Kali Linux, Snort IDS, IPTables):

Conducted penetration testing on a simulated corporate network, including reconnaissance (Nmap, Nessus), exploitation (Metasploit), data exfiltration, and decryption of sensitive files. Designed and implemented custom Snort IDS rules to detect specific attack patterns and applied IPTables firewall rules to block exploits.

### Information Security and Privacy (CISSP-Aligned Coursework):

Gained comprehensive knowledge of enterprise security architecture, risk management, cryptography, secure network design, incident response, privacy, and business continuity planning, applying CISSP-aligned frameworks to understand organizational security strategy and governance.