Guangning Li

guangning.li@outlook.com | Portfolio: 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. Strong communicator with hands-on experience driving cross-functional security initiatives in high-availability environments.

Professional Experience

Teaching Assistant Sep 2024 – Apr 2025

University of Victoria Victoria, BC

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

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 financial data between enterprise systems and banking partners
- Led risk assessments, identified system vulnerabilities, proposed mitigations, and maintained the organization's risk database

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, UFW – host-based), Network Segmentation, VLANs, VPNs (IPSec, SSL), IDS/IPS Systems (network-based), Load Balancing, Wireshark (network traffic analysis)

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

Scripting & Automation for Security:
Python, PowerShell, Bash (for security tasks, log parsing, automation of security checks)

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 (Excel, Word, PowerPoint, Outlook), Technical Writing, Report 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

Relevant Courses

Cyber-System Security • Advanced Network Security • Firewalls and Intrusion Prevention Systems

Information Security and Privacy • Data Mining • Digital Forensics Methodologies

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, ensuring secure communication while maintaining service availability.

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 while minimizing false positives, strengthening the network's defense posture.

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.

Digital Forensics Methodologies:
Studied the principles and processes of digital forensics, including evidence collection, preservation, and analysis of digital and network data. Gained understanding of forensic tools, evidence sources (residual and non-obvious data), and investigative techniques applied in criminal, civil, and corporate contexts, following best practices for legal admissibility and integrity.

Capstone Project – Phishing Email Detection Using Machine Learning:
Developed a phishing email detection system by applying machine learning (ML) and deep neural networks (DNN) to extract patterns from unstructured email data. Conducted descriptive analysis, feature extraction (e.g., TF-IDF, link presence), and model training to enable real-time classification and improve detection accuracy against evolving phishing tactics.