Jia Hu

Edmonton, AB • LinkedIn | Notion | THM Top 6% • jhu26@ualberta.ca

EDUCATION

University of Alberta | Edmonton AB Sept. 2023 - Apr. 2025
Master of Science in Internetworking GPA: 3.8/4.0

Taiyuan University of Technology | Jinzhong Shanxi Sept. 2019 – Jun. 2023
Bachelor of Engineering, Computer Science WA: 86.53/100

SKILLS SUMMARY

Digital Forensics: Wireshark, Yara, Volitilit, CAPA, Flare, Snort, Procmon, PEStudio, CFF Explore, Shodan

Vulnerability Management: Burp Suite, Rapid7, SentinelOne, EDR, ELK SIEM, SOAR, IDS/IPS, Firewall

Reverse Engineering: Ghridra, IDA, Radare2, VirusTotal, Flare, REMnux (Olemdump)

Network Pentesing: Nmap, Netcat, Metasploit, Bloodhound, Mimikatz, Crackmapexec, Kerberoasting

Application sSecurity: OWASP Top 10, Metasploit , John, Hydra, SQLMap, SAST/DAST (Snyk)

Risk & Compliance: MITRE ATT&CK Framework, Cyber Kill Chain, NIST, ISO 27001, PCI-DSS, HIPAA

Operating System/Virtualization: Window, Kali linux, Ubuntu, VMware, Docker, Kubernets

Programming/Scripting Languages: Python, Java, C/C++, Bash, PowerShell, SQL, C#, CSS

Cloud Security: AWS, Azure, GCP

WORKING EXPERIENCE

Graduate Teaching Assistant – Information Security Sept. 2024 - present
University of Alberta, Edmonton, AB, CA

- Collaborate with Principal Security Architect to deliver MINT 719 Advanced Security Course
- Design and validate **PCAP** files for TCP flooding, NTP, LDAP, Tor attacks
- Rebuild Heartbleed VM to simulate a **memory injection** attack on SSL/TLS and solve persistent keyboard layout issue
- Designe and validate a **Windows Defender Firewall** lab, configuring both NAT and Bridged networks for PC and smart devices, and implementing rules to manage **inbound and outbound traffic**
- Conduct sessions on common attacks targeting communication networks, including POODLE, BEAST, FREAK, and man-in-the-middle attacks.
- Demonstrate mitigation techniques for **DDoS** attacks, including protocol abuse, resource exhaustion methods, and various mitigation strategies.

WiCys & SANS & Target Security Training Jul. 2024 - Present
USA, remote

- Complete **87 labs** on TryHackMe (**THM)** covering Digital Forensics, Log Analysis, Security Operations, Web Exploit, Cryptography, OSINY and Network Penetration Testing
- Conduct **malware analysis** using **FalreVM**, accurately identifying file types, **IoCs** of PE files
- Analyze **memory images** using **Volatility** to identify, extracting specific artifacts such as running processes, network connections, loaded modules, and registry hives, for forensic investigations.
- Use VBA and PowerShell scripting to extract **Macros** from Word documents, uncovering malicious code and decoding obfuscated threats via **CyberChef**
- Secure a corporate perimeter by utilizing Suricata **IDS** for recon, alert triage and rapid incident response
- Develop and optimize **SIEM** queries/rules for **Microsoft Sentinel** and Splunk, improving threat detection across multiple **MITRE ATT&CK** tactics and log sources.

- Threat Hunting using **OpenCTI**, identifying abnormal activities and optimizing **YARA** detection rules, reducing false positives by 70-90%
- Execute advanced **red teaming**, including credential harvesting, phishing campaign development, EDR bypass, data exfiltration, DNS tunnelling analysis and JWT token hijacking.

Co-op Software Developer Intern Feb. 2022 - May. 2022
Chengdu Suncaper Date Ltd.

- Collaborated with team members to design and develop an Online Shopping Mall project using Java, Spring, SpringMVC, Mybatis-plus Java, React, and Vue.js
- Implemented key functionalities including CRUD operations, data visualization, file downloading, and file uploading to enhance user experience
- Utilized deployment tools such as Maven, Git, IntelliJ IDEA, SQLyog, VirtualBox, MobaXterm for efficient project management, testing, and deployment

PROJECT EXPERIENCE

- **Cisco EDR Capstone:** Use the Cisco Cloud Dashboard to configure agent policies and simulate advanced persistent threats (**APTs**) attempting to bypass Cisco AMP. Analyzed **quarantined files** using Telemetry, mapped attack techniques to the **MITRE ATT&CK** framework, and generated detailed reports to enhance understanding of the threats and improve security defenses. Sept. 2024 - Present
- **Active Directory Lab**: Configured AD domain controllers, users, shares and group polies with lease privileges. Conducted OSINT and **Internal and External penetration tests**, exploited network vulnerabilities, and **debriefed to clients** with mitigations Mar. 20224 - Jul. 2024
- **Networking Lab:** Established seamless connectivity between **Cisco, Juniper, and Nokia** routers and switches, optimized network performance, and designed and troubleshot complex networks in **EVE-NG** with hybrid protocols like BGP, RIP, OSPF, and IS-IS, while implementing networking concepts such as VLAN segmentation, STP, MST, NAT, and PAT, and conducting **packet analysis** with Wireshark for protocols including ARP, DHCP, DNS, ICMP, IPv4, and TCP/UDP. Sep. 2023 - Jan. 2024

LEADERSHIP EXPERIENCE

Director of Communication and Digital media Sep. 2023 - May. 2024
Computer Science Graduate Student Association (CSGSA), University of Alberta

- Assisted with Associate dean and faculty members to publicize announcements like scholarship, leaning, working and volunteering opportunities
- Managed and updated CCSGSA website and respond to high inquiries from CS students
- Coordinated with president and other executives to organize various events, setting priorities to achieve team objectives

CERTIFICATIONS

- TCM Security certified Practical Network Penetration Tester (PNPT) Jul. 2024
- TCM Security certified Practical Junior Penetration Tester (PJPT) May. 2024
- CompTIA Security+ Mar. 2024
- AWS Certified Cloud Practitioner Jan. 2024

ACHIEVEMENTS

- BSides Edmonton CTF 2024: Individual work, ranked **16** out of 52 Sep. 2024
- SANS Bootup CTF Player: Ranked **88** out of 1300+ Sep. 2024
- Target Cyber Defense Challenge: Ranked **27** out of 900+ players Aug. 2024