Sam Yoo

604-418-0954 | syoo28@my.bcit.ca
Website: https://www.sam-yoo.com LinkedIn: https://www.linkedin.com/in/sam-yoo-bb50b1206/ GitHub: https://github.com/syoo0295

TECHNICAL SKILLS

Cybersecurity	Wireshark, Metasploit, Snort, Ettercap, Nmap, hping3, Netcat, Malware Analysis, Social Engineering Toolkit (SET), Firewall/IDS/IPS Management, Vulnerability Assessment & Penetration Testing (VAPT), Threat Intelligence, Incident Response
IT Technologies	Networking, Linux/Windows/macOS, Computer Architecture, Packet Analysis, OSI Model, Log Management, Virtual Private Network (VPN) Configuration, Secure Shell (SSH), Network Protocols (TCP/IP, UDP, IPv4/IPv6), Security Protocols (SSL/TLS,HTTP/HTTPS)
Tools	MS Office, MS Azure, Git, VMware/VirtualBox, UTM
Languages	Python, Java, C, C++, SQL, Bash

EDUCATION

Bachelor of Science in Applied Computer Science Jan. 2024 – Dec. 2026. (expected)
Network Security Applications Development
British Columbia Institute of Technology

Computer Systems Technology, Diploma Sep. 2020 – Dec. 2022
Programming Paradigms option
British Columbia Institute of Technology

PROJECTS

Phishing Website and USB Attack Simulation Sep. 2024

- Developed a phishing website to perform credential harvesting through phishing emails
- Simulated phishing attacks by creating realistic phishing emails to capture user credentials
- Implemented a USB attack simulation to demonstrate how malicious payloads can be delivered through removable media
- Technology used: **Social Engineer Toolkit, Metasploit**

Analysis of Stuxnet Sep.2024

- Analyzed the Stuxnet attack by breaking down its lifecycle into the 7 stages of the Cyber Kill Chain framework
- Explored the significance and functionality of each phase in the Cyber Kill Chain (Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control, Actions on Objectives)
- Assessed cybersecurity measures that could have counteracted or mitigated Stuxnet at each phase of the kill chain

Reliable UDP Server with Network Simulation and Visualization Apr. 2024

- Developed a server, client, and proxy for UDP communication with TCP-like reliability, specifically designed for Linux environments
- Created a proxy server to simulate network unreliability, including delays and packet loss
- Designed a GUI for real-time visualization of packets sent, received, and retransmitted
- Technology used: **Python**

Packet Manipulation and Intrusion Detection Mar. 2024

- Manipulated network packets to simulate various types of attacks, observing traffic patterns and analyze
- Created iptables rules to counteract the manipulated packets, improving network defense strategies
- Configured Snort to log and analyze attack attempts, providing detailed intrusion detection insights
- Technology used: **hping3, Wireshark, iptables, snort**