# William Gao

williamgao101@gmail.com | 585-348-1319 | linkedin.com/in/gao-william | github.com/gao-william

## EDUCATION

**Rochester Institute of Technology** **Rochester, NY**
*Bachelor of Science (BS) in Cybersecurity* **Expected Graduation May 2028**
**Relevant Coursework:** Reverse Engineering Fundamentals, Network Services, Programming for Information Security, System Administration I, Routing & Switching, Database & Data Modeling, Cybersecurity Policy & Law.

## SKILLS

**Programming & Data:**
C, Python, Java, PowerShell, Bash, SQL/MySQL, Git/GitHub, data structures, dynamic memory, debugging, relational data modeling, UML, joins, primary/foreign keys.

**Reverse Engineering & Security:**
Malware Analysis, IDA, x32dbg, x86 Assembly, Windows PE/API Analysis, Static/Dynamic Analysis, Disassembly/Control Flow Analysis, Binary Patching, Process Monitor, Regshot, Wireshark, Scapy.

**Networking & Systems:**
Cisco IOS, pfSense, firewalls, ACLs, VLANs/802.1Q, OSPF, IPv4 subnetting, NAT, DNS/BIND, DHCP relay/failover, AD DS, GPO, SSH/SCP/SFTP, Windows Server, Rocky Linux, Kali Linux, Windows Admin Center.

## PROJECTS

**SystemBC Malware Analysis |** *IDA, x32dbg, Procmon, Regshot, Windows PE* **Mar 2026 - May 2026**

- Performed basic/advanced static and dynamic analysis of a SystemBC sample from MalwareBazaar in an isolated Windows VM, examining PE headers, imports, resources, strings, and runtime artifacts.
- Assessed packing and obfuscation indicators with UPX and IDA; inspected PE metadata and NSIS-style resources using PEview and Resource Hacker.
- Correlated IDA cross-references, Regshot, and Procmon to trace Run-key persistence logic, scheduled-task artifacts, silent execution, and randomized executables under C:\ProgramData.
- Set API breakpoints in x32dbg and OllyDbg and inspected stack, register, and memory data to validate randomized directory/executable paths; documented IOCs, analysis limitations, and remediation steps.

**Enterprise Network Services & Protocol Analysis |** *Cisco IOS, BIND, DHCP, VoIP, Scapy, Wireshark* **Jan 2026 - May 2026**

- Deployed authoritative BIND DNS and Linux/Windows DHCP services with forward/reverse zones, resource records, scopes, reservations, relay, and failover.
- Configured Cisco CME, inter-VLAN routing, DHCP Option 150, and TFTP for IP phones; analyzed SCCP, SIP/SDP, and RTP traffic.
- Crafted and inspected custom IPv4, ICMP, and TCP packets with Scapy; diagnosed TCP loss, SACK/duplicate ACKs, retransmissions, fragmentation, and controlled SYN-flood behavior.
- Administered Rocky Linux through OpenSSH and SCP/SFTP; generated server host keys and investigated SSH fingerprint and known_hosts behavior.

**File Metadata Ledger CLI & Tamper-Evident History |** *C, Data Structures, Hashing, Pointers* **Sep 2025 - Dec 2025**

- Built a C CLI using dynamic memory management, hashing, and input validation to manage tamper-evident file history.
- Tested deletion, modification, and hash-tampering scenarios; debugged memory and command-handling failures.

**Windows Domain Services & Automation |** *pfSense, Windows Server, GPO, WAC, Rocky Linux* **Sep 2025 - Dec 2025**

- Built a pfSense-backed Windows domain with AD DS, DNS, and DHCP services for Windows 11 and Rocky Linux clients.
- Automated organizational units, users, domain joins, and policy hardening using PowerShell, Group Policy, and Windows Admin Center.

**Vulnerability Assessment Project |** *Network Topology Analysis, Threat Modeling, Risk Assessment* **Oct 2024 - Dec 2024**

- Threat-modeled a simulated enterprise network and prioritized vulnerabilities using risk matrices and CVSS.
- Researched CVEs across DNS, web, WordPress, and pfSense; prioritized patching and hardening by business impact.