Noah Cosamano

5573 Rolling Meadows Way, Camillus, NY 13031 | (315) 663-4458 | njc3403@rit.edu | github.com/noahcosamano

Objective: Seeking a Cybersecurity co-op where I can apply systems programming, network protocol analysis, and threat detection skills to support secure infrastructure and real-time monitoring.

EDUCATION

Rochester Institute of Technology (RIT), Rochester, NY — Expected May 2028

Bachelor of Science, Cybersecurity

Related Courses: Programming for Information Security, Routing & Switching, Software Development and Problem Solving I & II, Introduction to Cybersecurity, Ethics in Computing, Discrete Mathematics for Computing, Reverse Engineering Fundamentals, Systems Administration

SKILLS

Programming Languages: Python, Java, C, C++, Assembly, SQL, Shell

Operating Systems: Linux, MS Windows, iOS, Cisco IOS

Tools & Platforms: Wireshark, Scapy, Nmap, Npcap/libpcap, PyQt6, PyTorch, Git, x32dbg, PuTTY, VS Code, Visual Studio, Ghidra, pe-bear, VMware, Metasploit, Active Directory, Powershell, FakeNet-NG, Airodump-NG

Concepts: Packet capture and analysis, Intrusion detection and prevention, multi-threaded systems, C/Python FFI (ctypes), TCP/IP protocol stack, reverse engineering, systems administration

PROJECTS

AmanoWatch — Real-Time Network Intrusion Detection System — March 2026 – Present

- Built a multi-threaded IDS in Python and C that captures live traffic via a custom Npcap/libpcap wrapper, sustaining multi-gigabit throughput with negligible packet loss on real systems.
- Designed a C extension (compiled to DLL) that parses Ethernet, IPv4, IPv6, TCP, UDP, ICMP, ARP, and IGMP headers and performs deep packet inspection to classify 15+ application-layer protocols (DNS, mDNS, TLS, QUIC, HTTP/HTTPS, SSDP, LLMNR, DHCP, SNMP, FTP, POP3, SMTP, Telnet, NFS, TFTP).
- Integrated the C layer with Python through ctypes using a batched packet-cache API with pcap timeout handling latency delivery regardless of traffic volume.
- Implemented six concurrent detection modules: fast/slow port scan detection (SYN, FIN, NULL, XMAS), ICMP sweep detection, ARP spoofing, DNS tunneling via Shannon entropy analysis, and honeypot monitoring.
- Optimized port scan detection from O(n) to O(1) per packet using sliding-window deques and incremental unique-port tracking, going from ~200mbps to ~2gbps ceiling
- Built a PyQt6 GUI with a live packet stream, per-detector toggles, real-time protocol statistics, threat alert panel with severity filtering, and automated firewall-rule-based IP blocking on Windows.
- Persisted detections to a SQLite database with IP geolocation and a daily purge routine forlow-severity entry.

Buffer Overflow Exploit Simulation — Class Project — August 2025 – December 2025

- Analyzed a C-based file server and discovered a stack buffer overflow caused by improper command parsing.
- Wrote Python scripts to send controlled input and locate the exact offset needed to overwrite the instruction pointer; used x32dbg to inspect CPU registers and control program execution.
- Redirected execution flow with a jmp esp command, built a NOP sled and custom shellcode, and simulated a reverseTCP connection for remote command execution.
- Researched and documented common defenses (ASLR, stack canaries, PIE, Control Flow Guard) and authored a formal vulnerability report detailing discovery, exploitation, and impact.

Network Packet Crafter — Personal Project — August 2025 – September 2025

- Built a Python CLI tool for crafting and sending custom network packets with user-defined source/destination IPs, MACs, ports, and payloads.
- Supported TCP, UDP, ARP, ICMP, and ICMPv6 with dynamic routing based on user input, validated packets in Wireshark during testing.
- Logged packet metadata to an SQL database with hashed IPv4, MAC, and payload fields for privacy-preserving audit trails.

WORK EXPERIENCE

McDonald's — Crew Member, Fairmount, NY — June 2025 – March 2026

- Delivered fast, high-quality customer service while managing multiple responsibilities under time pressure.