Inor Wang

(210) 529-5399 | inorwang@gmail.com | linkedin.com/inorwang | github.com/inorw | inorw.com

Education

The University of Texas at San Antonio Expected Graduation: May 2026

Bachelor of Business Administration in Cybersecurity, Minor in Computer Science *GPA: 3.95*

- **Certificates:** CompTIA ITF+
- **Relevant Coursework:** Digital Forensic Analysis I/II - Intrusion Detection & IR - Network Security - Data Structures - Information Assurance & Security - OS Security - Cyber Attack & Defend I - C Programming

Experience

Cybersecurity Operations Analyst Intern | *UT San Antonio* Jan 2026 - Present

- Monitored SOC alert queues and executed playbooks to triage alerts and identify escalation paths
- Correlated evidence across Splunk, Microsoft Defender for Endpoint, ExtraHop, Infoblox, Duo Admin, enterprise asset inventory, and user identity directory to scope activity and support investigations
- Documented findings in ServiceNow tickets and refined playbooks to improve consistency and escalation workflows

Cybersecurity Lab Intern | *UT San Antonio* Jan 2026 - Present

- Supported systems administrators in maintaining enterprise-style lab infrastructure, including virtualized environments (VMware/Proxmox) for cybersecurity coursework and research
- Provisioned and troubleshot Windows/Linux lab systems and network connectivity issues, documenting root cause and resolution steps for follow-up
- Assisted with patching and baseline configuration checks using a documented checklist

Data Analyst Intern | *Haven for Hope* Jun 2025 - Aug 2025

- Cleaned, standardized, and analyzed multi-year donor and fundraising datasets to identify patterns, anomalies, and drivers of retention/acquisition; delivered findings to stakeholders to support decision-making
- Applied statistical tests (Chi-square, Kruskal-Wallis, logistic regression); insights supported strategy tied to an 11.2% revenue lift
- Built clear, repeatable reporting deliverables, and presented key findings to stakeholders; improved stakeholder visibility into campaign performance and donor behavior

Social Media Lead | *RowdyHacks & ACM UTSA* Dec 2024 - Present

- Led a 12–14 person RowdyHacks & ACM media team; built an end-to-end content workflow (plan → brief → review → publish) that cut turnaround time by 40% and drove a +320% lift in engagement and +21.6% in follower growth semester-over-semester
- Implemented and standardized programs/services for team communication, collaboration, and asset sharing, reinforcing brand consistency and improving on-time delivery across channels

Projects

Windows 10 Encrypted Container & Payload Triage | *Autopsy, Volatility 3, Hashcat, VirusTotal* Dec 2025

- Performed memory + disk forensics on a Windows 10 VM: validated capture context, enumerated user activity (Edge, VeraCrypt, WSL/Kali), and correlated web + execution artifacts (Prefetch) to reconstruct behavior.
- Identified a high-entropy VeraCrypt container; extracted header bytes and executed a masked Hashcat attack to regain access, then hashed recovered artifacts and used VirusTotal evidence to classify the payload as a Meterpreter/Cobalt Strike-style stager.

Advanced Memory Forensics & Malware Analysis | *Volatility 3, FLOSS, capa, ClamAV* Nov 2025

- Analyzed Windows memory dumps using Volatility 3 to detect process injection, identify short-lived malware processes, and map C2 connections; utilized FLOSS, capa, and ClamAV to extract obfuscated strings, analyze capabilities, and identify Meterpreter payloads.
- Performed memory forensics to detect spoolsv.exe injection; extracted C2 IP addresses from memory regions and validated findings through multiple analysis tools.

Skills

Technical Skills: Python, Java, C, JS, Bash, PowerShell, SQL (MySQL), HTML/CSS, Linux, Windows, Git, AWS

Security Tools: Microsoft Defender for Endpoint, Splunk, ExtraHop, Duo Admin, ServiceNow, Volatility 3, Autopsy, KAPE, FTK Imager, Abnormal AI, Windows Event Log Analysis (EVTX), Velociraptor, Wireshark, Registry Explorer, FLOSS, capa, Hashcat