NORMAN RENTERIA
San Antonio, TX 78247
(719) 433-3548 | nrenteria2331@gmail.com
www.linkedin.com/in/norman-renteria-95a9a618b/

PROFESSIONAL SUMMARY

Aspiring Cybersecurity Specialist and United States Army Veteran with an Active Secret Security Clearance and over 5+ years of proven experience working in live enterprise and tactical network environments. Skilled in network administration, vulnerability scanning, network hardening, and digital security consulting. Experience orchestrating software, hardware, and information technology support, managing configurations, and system integration. Possesses applicable knowledge in network and software troubleshooting, security implementation, network configurations, systems architecture, diagnostics, server administration, vulnerability assessments, and active directory configuration derived from implementing communication security protocols and adhering to risk mitigation strategies. Career supported with a Bachelor of Business Administration in Cybersecurity.

- Research and Discovery
- Network Security
- Information Systems
- Security Solution
- Technical Support
- NOS Patches & Updates
- Cybersecurity
- Training and Development
- System Configuration

TECHNICAL COMPETENCIES

Systems: Linux, UNIX, Windows 10/11/Server, macOS, iOS, Android OS
Software: Microsoft Office 365, MySQL, Wireshark, Splunk, Nmap, Snort, Metasploit
Applications: Active Directory, VMWare, Java, JavaScript+, Eclipse IDE, MS Visual Studio, HTML, MATLAB
Networking: LAN, WAN, Wireless, Cisco, DHCP, Ethernet, Hubs/Switches, Routers, TCP/IP, VoIP, Wi-Fi

EDUCATION AND CERTIFICATIONS

Bachelor's degree in Business Administration in Cybersecurity | University of Texas at San Antonio | May. 2024
Google Cybersecurity Certificate | Coursera | Expected Sept. 2024
CompTIA Security+ | Autodidact | Expected Dec. 2024
CompTIA A+ & ITF| NPower | Excepted Dec. 2024

PROFESSIONAL EXPERIENCE

University of Texas at San Antonio | San Antonio, TX **Jan 2019 – May 2024**
Student

- Developed and implemented a secure network architecture as part of a capstone project, demonstrating the practical application of cybersecurity principles.
- Learned concepts covered in CompTIA ITF, A+, Sec+ and Googles Cybersecurity Modules.
- Gained hands-on experience in cybersecurity labs, working with tools such as Wireshark, Metasploit, and Nessus to identify and mitigate security vulnerabilities.
- Collaborated with peers on group projects and team-based assignments, fostering a collaborative approach to solving complex cybersecurity problems.

G4S | San Antonio, TX **Apr 2016 – Dec 2019**
Resident Supervisor

- Utilized conflict resolution skills to address disputes among residents and prevent the escalation of tensions within the facility.
- Maintained detailed and accurate records of resident's behavior, incidents, and daily activities, producing reports for documentation and administrative purposes.
- Monitored residents' activities, ensuring compliance with rules and regulations, and intervening in conflicts to prevent disturbances.
- Implemented and enforced camp policies and procedures, ensuring all residents adhered to established rules and guidelines.

Sterling Global Operations | San Antonio, TX **Feb 2014 – May 2016**
UXO Tech II

- Performed manual, technical, and mechanically assisted duties involved with the production, storage, receipt, shipment, inspection, maintenance, or testing of explosive ordnance items or components
- Operated mobile equipment such as MHE, vehicles for transporting personnel, tools, equipment, ammunition components, or machines used in the manufacture or demilitarization of munitions.
- Conducted thorough site surveys to identify and assess potential UXO hazards in both military and civilian environments.
- Trained in the identification, detection, and disposal of unexploded ordnance (UXO) and explosive remnants of war (ERW).
- Skilled in various demolition techniques to safely and effectively dispose of UXO, ensuring minimal impact on the surrounding area.

United States ARMY | Various Locations **Sept 2010 – Jan 2014**
Team Leader

- Maintained 100% accountability of all his team's tactical equipment, weapons, and sensitive items while conducting dismounted training exercises and night live fire training with zero losses.
- Assumed the role of team leader and quickly earned the trust and respect of other individuals while continuing to accomplish his assigned tasks with no faults.
- Stepped up in the absence of the section supervisor and performed admirably in his inherited responsibility of 10 other personnel providing impeccable leadership traits.
- Supervised a group of 10 Soldiers leading to significant knowledge and skills growth and ensured every individual training opportunity was maximized, 100% first time go on all training assigned.
- Received and implemented combat orders and directed deployment of personnel in offensive, defensive, and retrograde operations.

PROJECTS AND LABS

Event Analysis Lab

- PCAP files provided as part of a project to analyze network traffic using industry-standard tools such as Network Miner, Snort, and Wireshark.
- Employed software tools to swiftly identify crucial information, including host computer details, potential attackers, and operating systems in use.
- Utilized tool functionalities to pinpoint the timing and volume of data transmission, uncovering anomalies leading to transmission spikes.
- Detected and analyzed security threats within the network, including instances of IP spoofing, attempted session hijacking, and phishing attempts targeting bank credentials.

Malware Analysis Lab

- Leveraged backdoor vulnerability to enter the compromised system, ensuring minimal disruption to evidence integrity.
- Created an image of the compromised system and used MD5 hash to maintain image integrity.
- Transferred forensic image to a designated analysis machine for further examination using file transfer protocol (FTP).
- Conducted forensic analysis of suspicious files within the compromised system, preserving evidence for further investigation.

Hunting In Memory Lab

- Employed Volatility toolset to analyze memory dumps, determining the operating system version and running processes.
- Generated a comprehensive timeline of the incident by correlating findings from memory analysis, aiding in the reconstruction of events leading up to and following the security incident.