Joel William Kommu

(478)305-4710 | joelwilliamkommu@gmail.com

OBJECTIVE

Information Technology student with strong foundation in networking, systems, and cybersecurity, proficient in Linux, Windows, Python, and network analysis tools. Hands-on experience configuring and troubleshooting firewalls, AWS architectures, and analyzing network traffic with Wireshark. Demonstrated problem-solving and communication skills through lab projects. Seeking a Intern role to deliver high-quality remote hardware and software support.

EDUCATION

Georgia Southern University | *Bachelor of Science, Information Technology* (GPA: 3.6)Dec 2026

SKILLS

- **Programming Languages:** C#, PowerShell, Java, Python, HTML, CSS, SQL
- **Tools and Software:** Microsoft Office, Google Workspace, Linux, Windows, Network Analyzers, SIEM Tools, VirtualBox, Wireshark, Cisco Packet Tracer, VMware, Office365
- **Soft Skills:** Troubleshooting, Communication, Teamwork, Attention to Detail

CERTIFICATIONS

- **Google Cybersecurity Professional Certificate**
- (In Progress) - CompTIA Security+, CompTIA Network +

PROJECTS

AWS Transit Gateway Hub-and-Spoke Network Lab (Terraform, AWS)

- Built a hub-and-spoke multi-VPC architecture on AWS using Transit Gateway and Terraform, enabling inter-VPC routing and centralized internet egress via a hub NAT gateway.
- Deployed EC2 instances in spoke VPCs to validate private cross-VPC connectivity and secure internet access through the hub, with multi-AZ subnets for high availability and resilience.

pfSense Firewall & Networking Lab

- Installed and configured pfSense firewall in VMware Workstation with dual-NIC design (WAN via NAT, LAN via Host-Only).
- Set up LAN interface with static IP, DHCP services, and secure WebGUI access for management.
- Verified connectivity by configuring Windows 11 client VM to obtain IP/DNS via pfSense and successfully tested local and outbound traffic.
- Troubleshot WAN/LAN interface assignments, DHCP, and NAT to ensure proper packet flow and client internet access.
- Implemented VPN (OpenVPN/WireGuard) and hybrid-cloud simulation to model secure on-prem cloud connectivity.

Data Communications – Wireshark Protocol Analysis

- Captured and analyzed live network traffic with Wireshark, focusing on HTTP, DNS, ICMP, and NAT protocols.
- Interpreted packet structures (Ethernet, IP, TCP/UDP, application-layer) to trace client-server interactions such as HTTP GET/200 OK exchanges and DNS queries/responses.
- Conducted hands-on experiments with Ping and Traceroute, examining ICMP Echo, TTL-exceeded, and error messages to map end-to-end packet flow.
- Constructed and interpreted NAT translation tables by comparing home-side vs. ISP-side traces, demonstrating how private-to-public IP mappings occur.
- Tools: Wireshark, TCP/IP, HTTP, DNS, ICMP, NAT, Packet Capture & Analysis