**MARCO MARSHALL**

Huntington, WV | marco.marshall@marshall.edu | 304-696-2370

Linkedin.com/in/marcomarshall

Cybersecurity | Network Security | IT Support | Risk Analysis

**SUMMARY OF QUALIFICATIONS**

Recent graduate in Computer and Information Security, with a strong foundation in cybersecurity principles, network defense, and ethical hacking. Proficient in security tools and technologies including firewalls, intrusion detection systems (IDS), and vulnerability assessment tools. Skilled in securing network infrastructures, monitoring system integrity, and responding to security incidents. Excellent analytical skills and a proactive problem solver, with hands-on experience in both academic and real-world IT environments.

**TECHNICAL SKILLS**

* Operating systems: Windows, Linux (Kali, Ubuntu), Mac OS
* Security Tools: Wireshark, Nmap, Nessus, Metasploit, Splunk, pfSense
* Networking: TCP/IP, VPN, DNS, DHCP, Firewalls, IDS/IPS
* Programming: Python, Bash, SQL, HTML
* Applications: Microsoft Office, TeamViewer, anti-virus software, network monitoring tools
* Certifications: CompTIA Security+ (Expected August 2024), CPR/AED Certified

**EDUCATION**

Marshall University Huntington, WV

Bachelor of Science, Computer and Information Security May 2024

*Emphasis: Network Security | Minor: Cyber Defense*

GPA: 3.6

***Relevant Coursework:*** *Ethical Hacking, Cybersecurity Policy, Cryptography, Network Security, Information Assurance, Risk Management*

**PROJECTS**

Network Security Audit Simulation

* Conducted a simulated network security audit for a mock organization, identifying vulnerabilities and recommending mitigation strategies.
* Utilized Nmap and Nessus to scan for open ports and assess system weaknesses.
* Prepared a comprehensive report on findings and presented recommendations to faculty.

**WORK EXPERIENCE**

Marshall University Information Security Office Huntington, WV

IT Security Intern January 2024 – Present

* Assisted with monitoring and analyzing network traffic for potential security threats.
* Supported the implementation of firewall policies and user access controls.
* Helped conduct vulnerability scans and documented security incidents.
* Provided support for university-wide security awareness training initiatives.