MOURAD MAACHA

443-760-7788 | mmaachaus11@gmail.com
LinkedIn| Website | GitHub

SUMMARY

Current Cybersecurity student who has completed coursework in Intrusion Detection, Digital Forensics, Advanced Network Defense, Networking, Linux System Administration, Network Security, and SQL & Database Design. Hands-on experience in SIEM-based monitoring, vulnerability assessment, and incident response. Seeking a security-related entry-level or internship opportunity.

TECHNICAL SKILLS

- **Security & Forensics:** SIEM (Wazuh, Splunk), Log analysis, Endpoint forensics (FTK Imager, Autopsy, OSForensics, ProDiscover Basic, Paraben E3), digital evidence handling & Chain of custody, malware analysis, phishing detection.
- **Detection & Response**: Intrusion Detection & Prevention (Snort IPS/IDS), SIEM rule tuning, alert triage, threat identification, incident response workflows, incident documentation, containment, remediation, and familiarity with NIST incident response processes.
- **Penetration & Vulnerability Testing**: Nessus, OpenVAS, Nmap, Metasploit, SQLMap, Hydra, John the Ripper, Hashcat, vulnerability scanning, exploit validation, basic web app testing, and penetration testing methodologies.
- **Networking & Infrastructure**: Strong knowledge in Cisco routers, multilayer switching (L2/L3), ASA firewalls (ACLs, NAT, security zones), VLANs, OSPF, EIGRP, static routing, HSRP, DHCP, DNS, RADIUS, VPNs, DMZ architecture, EtherChannel, port security, network segmentation, and secure network design.
- **Systems & Hardening**: Windows and Linux system hardening (patching, service restriction, password policy enforcement, secure boot, UEFI), macOS security, Authentication and Group Policy, system patching, service hardening, BitLocker, secure configuration management.
- **Tools & Utilities:** Wireshark, PuTTY, Tera Term, Cisco Packet Tracer, VirtualBox, VMware, UTM, Sysinternals, APTSimulator, PowerShell scripting for automation & log parsing.
- **Frameworks & Compliance**: NIST SP 800 series, NIST RMF Concepts, MITRE ATT&CK & D3FEND, HIPAA & FISMA awareness, CIS Controls, Lockheed Martin Kill Chain, PCI DSS, FIAR fundamentals, ISO/IT governance concepts, COBIT, ITIL, Security governance, Acceptable Use & credential policy development.
- **Languages**: English, French, Arabic, Amazigh.

SECURITY-RELATED PROJECTS

Wazuh & Sysmon SIEM Lab | ***GitHub: Wazuh-SIEM-Lab***

Configured a full open-source SIEM environment to monitor Windows and Linux systems. Configured Sysmon for detailed event logging, developed custom detection rules and alert pipelines in Wazuh. Simulated cyberattacks using APTSimulator and Kali Linux to test detections. Analyzed and documented SIEM alerts and tuning recommendations in a public repository on GitHub.

Enterprise Network Infrastructure Lab | *GitHub:* ***Secure-Enterprise-Network-Design***

Deployed a secure, multi-tier enterprise network environment featuring VLAN and subnet segmentation, inter-VLAN routing, dynamic routing with OSPF, and high-availability failover using HSRP. Implemented Cisco ASA firewall protections, including security zones, ACLs, NAT, and traffic inspection policies. Built out core services—DHCP, DNS, wireless LANs, and VoIP—while applying security controls such as port security, management-plane protection, SSH hardening, and AAA/RADIUS authentication. Designed DMZ segmentation, VPN support, EtherChannel uplinks, and server-room topology to ensure resilient, scalable, and defense-in-depth network operations. Fully documented configurations and diagrams in a GitHub repository.

Cybersecurity Research & Writing | *Personal Website:* ***MouradMaacha.com*** **Jan 2025 - Present**

Publish weekly articles on mouradmaacha.com about recent vulnerabilities, malware campaigns, and industry incidents. Track and explain CVEs, attack trends, and intrusion techniques in clear language for a broad audience. (Published 30+ blog posts to date, demonstrating subject-matter expertise and communication skills.)

RELATED TECHNICAL EXPERIENCE

Carroll Community College | *Teacher Assistant - Technology Programs* **Sep 2025 - Present**

- Support Cisco Networking courses by guiding students through labs and troubleshooting technical issues.
- Create instructional materials and hands-on lab exercises to reinforce core networking concepts.
- Provide one-on-one tutoring to help students understand course material.

EDUCATION

University of Maryland Global Campus *Adelphi, MD*
Major in Cyber Operations **Currently Enrolled**

Carroll Community College *Westminster, MD*
Associates of Applied Science in Cybersecurity **Dec, 2025**

Baltimore Cyber Range *Baltimore, MD*
Cybersecurity Workforce Accelerator **Fall 2025**

CERTIFICATIONS

CompTIA Security +
Credentials: D78008JZ9V3LPS12

Baltimore Cyber Range SOC OPERATIONS ANALYST 1
Credentials: 166052963

PROFESSIONAL ASSOCIATION

Carroll Technology & Innovation Council

ISSA

Carroll Cyber Club Member