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. Proven ability to implement enterprise-grade security tools in lab environments and communicate technical concepts clearly. Strong foundation in Cybersecurity and Networking. Seeking a security-related entry-level or internship opportunity.

TECHNICAL SKILLS

- **Security & Forensics:** SIEM platforms (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 experience.
- **Networking & Infrastructure**: Strong knowledge in Cisco routers, multilayer switching (L2/L3), ASA firewalls, 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, Standards & Governance**: 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*

Designed an end-to-end SIEM and incident response lab using Wazuh to simulate enterprise security monitoring. Deployed a centralized Wazuh manager on Linux with Windows endpoint telemetry collected via a Wazuh agent and Sysmon, enabling detailed visibility into process execution, file activity, network connections, authentication events, and registry changes. Architected an isolated NAT and host-only network to safely simulate adversary behavior using APTSimulator and manual attacks from Kali Linux, then validated detection coverage through custom Wazuh rules and alert tuning. Performed alert triage, threat analysis, and evidence collection by correlating Sysmon and Windows Event logs with SIEM alerts, exporting forensic artifacts, hashing evidence for integrity, and documenting incident timelines aligned with NIST incident response practices. This project demonstrates practical experience in security monitoring, detection engineering, adversary emulation, and SOC-style incident handling.

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

Designed and implemented a secure, enterprise-scale network architecture simulating a multi-department organization with over 600 users using Cisco Packet Tracer. Architected a hierarchical, highly available infrastructure featuring dual ISP connectivity, redundant Cisco ASA firewalls, multilayer switching, and segmented security zones (Inside, Outside, DMZ). Implemented VLAN-based network segmentation, inter-VLAN routing, OSPF and static routing, HSRP for gateway redundancy, EtherChannel for link aggregation, and STP hardening. Deployed and secured core enterprise services, including DHCP, DNS, Active Directory, RADIUS, VoIP, wireless LAN controllers, and public-facing DMZ servers, with firewall inspection policies and access controls aligned to defense-in-depth principles. Designed a scalable IP addressing scheme, enforced network hardening controls, and documented end-to-end configuration and security decisions following industry best practices. 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 - Dec 2025**

- Served as a Teaching Assistant for 2 college-level Cisco Networking course sections meeting twice weekly, providing technical instruction, supervising labs, and offering academic support to students.
- Facilitated hands-on labs using real Cisco networking equipment, promoting collaboration and accountability, and improving lab completion rates, efficiency, and overall course comprehension.

- Developed practice exercises covering theoretical knowledge, which helped students prepare for the course examination.
- Provided one-on-one tutoring sessions using Cisco Packet Tracer for students needing extra support, helping them gain the knowledge and the confidence to configure physical equipment and pass the course.
- Coordinated a complex, 6-rack network deployment involving the entire class to simulate real-world scenarios and strengthen teamwork, troubleshooting skills, and performance on practical configuration exams.
- Recognized for technical proficiency, professionalism, and peer leadership.

EDUCATION

University of Maryland Global Campus — *Adelphi, MD*
Major in Cyber Operations — **Dec, 2027**

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