Ibrahim Mahamane

(224) 434-6324 | **iamahamane@gmail.com** | LinkedIn | GitHub | **iamibie.com**

EDUCATION & CERTIFICATIONS

DePaul Universit**y** | Chicago, IL | **MS Computer Science**	2023
CompTIA Security+ Certification	2022
Flatiron School | Online Bootcamp | Cybersecurity Engineering	2022
North Central College | Naperville, IL | BA Political Science & Philosophy	2019

SKILLS

- **Languages**: Python, JavaScript, Shell, Bash,
- **Cloud**: AWS, Azure, Google Cloud Platform
- **DevOps**: Docker, Kubernetes, Jenkins, Git, GitHub, Terraform, Ansible
- **Security**: Nessus, Wireshark, Metasploit, Snort, VirtualBox, Splunk SIEM, Rapid7, Nexpose, Checkmarx, Jira
- **Version Control**: Git/GitHub
- **OS**: Windows, Linux, Unix, Mac OS, Apple iOS
- **Server Management**: Remote Management, Virtual Machine, Backup
- **Networking**: DHCP, SMTP, LAN, VLAN, WAN, VPN, DNS, SSH, RDP, SSL, IDS/IPS, Honeypot, Nmap, Port Scanning
- **Compliance**: NIST 800-53, ISO 27001, HIPAA, GDPR, PCI-DSS, SOX
- **Wireless Security**: WEP, WPA, WPA2, AES

PROJECTS

Portfolio Website

- Developed a personal portfolio website with a REST API using JavaScript, Node.js, and MySQL.
- Deployed the application on an AWS EC2 Linux server. Configured domain name and SSL certificate using AWS Route 53 and Certbot.
- Created Bash scripts for process automation and set up a CI pipeline using Jenkins and GitHub. Configured webhooks in GitHub to trigger automated builds in Jenkins.
- Improved deployment time by 50% through automation. Ensured high availability with NGINX configuration.

Blog Application

- Built a blog application with CRUD functionality using the MERN stack.
- Containerized each service in the stack using Docker and deployed on an Ubuntu server on EC2. Configured NGINX as a reverse proxy.
- Configured domain name and SSL certificate using AWS Route 53 and Certbot.
- Enhanced security and performance by configuring NGINX and Docker. Achieved seamless deployment with automated processes.

E-commerce Application

- Created an e-commerce application with CRUD functionality using the MERN stack.
- Containerized each service in the stack using Docker, configured NGINX as a reverse proxy, and deployed the application on an EC2 server.
- Automated infrastructure provisioning on AWS using Terraform.
- Configured domain name and SSL certificate using AWS Route 53 and Certbot.
- Reduced deployment time by 60% with Terraform automation. Enhanced user experience with robust CRUD functionality.

Enterprise Network Threat Hunt:

- Investigated a simulated security breach for a major corporation, identified vulnerabilities, removed threats, and recommended threat prevention tactics to CISO.
- Technical Expertise: Firewalls, Rapid7 Nexpose (vulnerability scanner), Netmask, RK Hunter, Linux OS, Windows OS, digital forensics, malware analysis and defense.
- Performed cyber forensics to discover malware infected files, uncover root cause of issue, identify the threat actor, and determine a course of action for timely recovery.
- Set up firewalls and a honeypot to locate intruders by creating a Demilitarized Zone (DMZ).
- Performed a Rapid7 Nexpose vulnerability scan and conducted a full vulnerability audit to assess system weaknesses. Discovered vulnerable open ports and lack of risk mitigation awareness from company staff.
- Generated a 68-page report on the incident, including causes, details of the recovery process, and recommendations for prevention including technical fixes and employee risk education.

Network Traffic Analysis:

- Built Python scripts to capture and analyze network traffic using Wireshark APIs. Identified and mitigated potential security threats by analyzing packet payloads and traffic patterns.
- Built custom PowerShell scripts to extract geolocation information from Windows Event Viewer metadata using a third-party API. Configured Log Analytics workspace to receive custom logs with the geolocation data and created Sentinel workbooks to display RDP brute force attack data based on location and magnitude.

Vulnerability Assessment and Penetration Testing:

- Installed and configured Nessus Essentials to perform credentialed vulnerability scans. Performed penetration tests on web applications to identify and exploit security vulnerabilities. Documented findings and recommended remediation measures to enhance application security posture.
- Developed automated remediation processes to proactively deal with vulnerabilities from Windows updates and other third-party software.

Automated Security Compliance Checks:

- Created Ansible playbooks to automate security compliance checks against industry standards. Streamlined the process of auditing and remediating security configuration drifts across multiple servers.
- Created an integrity baseline using the SHA-512 hashing algorithm. Continuously compared files to the baseline, raising alerts if file integrity was compromised.

Network Security Monitoring with Azure Sentinel (SIEM):

- Used a custom PowerShell script to extract geolocation information from Windows Event Viewer metadata using a third-party API.
- Configured Log Analytics workspace to receive custom logs with the geolocation data and extracted custom fields in the workspace.
- Configured Sentinel workbook to display RDP brute force attack data on a world map based on location and magnitude.

Active Directory Administration:

- Created a virtual machine running a Windows 2019 server on Oracle VM VirtualBox. Configured Windows DNS and DHCP services, set up Remote Access Server (RAS) features to support NAT and PAT, and configured Windows domain name services.
- Developed and Ran a PowerShell script to provision and maintain 500 user accounts. Initialized a Windows 10 desktop client and configured it to receive DHCP services from the Domain Controller, ensuring it connects to the internet via the DC.

RELEVANT TRAINING

Cybersecurity Engineering Program, Flatiron School, November, 2021 – March, /2022

Coursework includes 15 weeks of intensive classroom and lab-based training in security concepts including:

- **Application Security** - OWASP Top 10, XSS, CSRF, CORS, SQLi, Fuzzing, Command Injection, DoS & DDoS, Vulnerability Scanning
- **Cryptography** - Stream & Block Ciphers, OpenSSL, Certificate Management, Symmetric and Asymmetric Cryptography, Cryptocurrencies
- **Governance, Risk and Compliance (GRC)** - Frameworks, Tools, Artifacts (Strategy, Policies, Standards, Guidelines and Procedures), Risk Management, Business Continuity, Incident Response; Plans and policies concerning GRC requirements including HIPAA, PCI-DSS, NIST 800-53, FedRAMP, Cyber Kill Chain, and FISMA
- **Networking** - OSI & TCP/IP Models, Hardware, Routing, Protocols, Encapsulation, Framing, NAT Networks, VLANs
- **Network Security** - Wireshark & Filters, Port Forwarding, VPNs, Port Scanning, Bind & Reverse Shells, IDS / IPS, Firewalls and WAFs, Rule Writing, Vulnerability Management, MITM Attacks, DNS Security
- **Logs and Detection** - SIEMs (Splunk), IoCs, Log Types, Databases, Normalization, Regular Expressions (RegEX), Hunting, Alarms & Reports, Investigations, User and Process Monitoring
- **Threat Intelligence** - CTI Sources and Methods, Threat Actors, Social Engineering, CTI Cycle and Process, Cyber Kill Chain, CTI Diamond Model, Cyber Mission Analysis
- **Strategy and Analysis** - Strategic Planning, Leadership, Operational Design, Decision Making Cycle
- **Systems** - VMs, x86/ARM Architecture, Linux, Windows, Memory, Storage, Python, Cloud
- **Systems Administration** - Windows, Unix/Linux, VyOS
- **Systems Security** - OWASP Secure Coding Practices, Input Validation, Session Management, Encoding, Debugging, Buffer Overflows, Code Injection, Cloud Security Infrastructure, Hypervisors