

NIZAR LAHMAR

XXX-XXX-XXXX | xxxxxxxx@nizarlahmar.com | linkedin.com/in/nizar-lahmar | github.com/nizarlahmar | nizarlahmar.com

SUMMARY

Cybersecurity student (B.S., Dec. 2026) focused on security operations and detection. Built a segmented SOC lab with Wazuh SIEM and a fully documented, end-to-end attack chain; rooted 19 Hack The Box machines (rank: Skilled). Security+ and CySA+ certified; technical write-ups at nizarlahmar.com.

TECHNICAL SKILLS

Security Operations & Detection: SIEM (Wazuh), Log Analysis, Threat Detection, Attack-Chain Analysis, Incident Documentation
Networking & Cloud: TCP/IP, DNS, Subnetting, Network Segmentation, Packet Capture, Azure VNets, NSGs, IAM, SSO (OpenID)
Systems: Linux (daily — CachyOS, Kali, Ubuntu, Debian), Windows, Windows Server, Proxmox, QEMU/KVM
Tools: Burp Suite, Metasploit, Nmap, Nessus, Impacket, Gobuster, Wireshark, Git
Offensive Security: Web Application Exploitation, Privilege Escalation, Lateral Movement, Reconnaissance, Password Cracking, CVE Exploitation, PCAP Analysis
Development: C++ (C++17), Python, Bash, PowerShell, CMake, BSD Sockets, POSIX Threading
GRC: PCI-DSS, GDPR, Access-Control Policy, RBAC
Languages (fluent): English, French, Arabic

PROJECTS

SOC Detection Lab | *Wazuh, QEMU/KVM, Burp Suite, DVWA, Linux* 2026
– Designed a segmented virtual network (DMZ + internal tiers) with Wazuh SIEM agents on every host, modeling a corporate monitoring environment on QEMU/KVM.
– Executed a full attack chain (file-upload web shell for initial access, sudo misconfiguration for privilege escalation, NIC misconfiguration for lateral movement, then anonymous FTP and credential reuse on internal targets); capturing the host and auth-log artifacts.
– Engineered a custom Wazuh detection rule (mapped to MITRE T1505.003) flagging web-shell execution (GET requests for uploaded PHP files in an upload directory) layered on the default Apache ruleset and confirmed firing on live SIEM traffic.

C2 Framework (basic-c2) | *C++17, BSD Sockets, CMake, Linux* 2026
– Built a pull-based TCP C2 framework in C++17 directly on the BSD socket API (~600 LOC, no higher-level networking libraries): outbound-only agents poll a queue, execute commands, and return output; an agent-initiated model that minimizes inbound detection surface. Documented on GitHub.
– Implemented length-prefixed framing to handle partial TCP sends/receives, an XOR stream cipher for transport obfuscation, and POSIX threading with mutex-guarded session state; resolved a blocking-recv deadlock and rebuilt the console I/O loop to separate beacon output from the operator prompt.
– Executed the implant on an internal host (simulating a drive-by delivery) and confirmed that beaconing and routine post-exploitation commands generated no Wazuh alerts under default rules; demonstrating the host-based monitoring gap against outbound-only C2.

CTF & Vulnerability Exploitation | *Hack The Box, TryHackMe, picoCTF, pwn.college* Ongoing
– Rooted 19 Hack The Box machines (rank: Skilled) plus TryHackMe and picoCTF challenges; exploiting SQLi, XSS, CSRF, SSTI, SSRF, LFI, Shellshock, race conditions, Jenkins Script Console RCE, misconfigured S3 buckets, WPS/WiFi and more; publishing methodology write-ups at nizarlahmar.com.
– Working through pwn.college (26 modules, 31 challenges solved), building assembly-level program analysis and gdb debugging.

Infrastructure Deployment & Hardening Lab | *Linux, Docker, Nginx, LAMP, Azure* 2025
– Deployed multi-VM web infrastructure (Rocky Linux + Ubuntu): Ghost CMS on Docker behind an Nginx reverse proxy and a full LAMP/WordPress stack with MySQL under least-privilege scoped accounts.
– Hardened the stack defense-in-depth (file permissions, protected `wp-config.php`, firewall controls) and provisioned segmented Azure VNets with NSGs and load balancing; documented each control as vulnerability/configuration/validation.

GRC & Compliance Documentation | *PCI-DSS, GDPR, Active Directory, RBAC* 2025
– Authored audit-ready security policies for a simulated enterprise: credential lifecycle, ADUC-based reset workflows across five role types, exception handling, and enforcement escalation.
– Co-authored a PCI-DSS compliance policy (cardholder-data encryption at rest and in transit, RBAC/MFA, tokenization, log-retention, and CDE segmentation) with controls mapped to PCI-DSS and GDPR obligations.

CERTIFICATIONS & EDUCATION

Certifications: CompTIA A+, Security+, CySA+ | INE eJPT v2 | Cisco CCNA (in progress)

Full Sail University, Winter Park, FL — B.S. Cybersecurity (GPA 4.00), expected Dec. 2026; A.S. Information Technology (GPA 4.00), 2025.

EXPERIENCE

Full Sail University Winter Park, FL
Campus Tour Guide Oct. 2025 – Present
– Led campus tours and presentations for prospective students and families, tailoring technical program details to non-technical audiences.