Nour Alhouseini

Cybersecurity Professional — Red Teaming — Adversary Simulation
+1 (708) 882 7784 | nohous20@outlook.com | linkedin.com/n0ur | 0xlumos.github.io

Summary

Cybersecurity specialist with hands-on experience in red teaming, adversary simulation, vulnerability assessments, and exploit development. Proficient in scripting and tooling for offensive security operations, with a passion for applying threat intelligence and communicating technical risks effectively to technical and non-technical audiences.

Education

DePaul University — Chicago, IL
Masters in Cybersecurity (Computer Security) — *Aug 2024 – Jun 2026*

Coventry University — Coventry, United Kingdom
Bachelor of Science in Computer Science — *Sep 2018 – May 2022*

Experience

Junior Penetration Tester — Mar 2024 – Aug 2024
Palestinian Higher Education — *Ramallah, Palestine*

- Led internal/external red team assessments uncovering 7 critical vulnerabilities, reducing risk exposure by 60%.
- Simulated adversary techniques including lateral movement and privilege escalation using custom scripts and known TTPs.
- Delivered actionable technical reports and executive summaries for remediation and board-level review.

IT Specialist — Oct 2023 – Mar 2024
digitized — *Dubai, UAE*

- Secured network environments across 3 healthcare sites; conducted wireless testing and incident response readiness reviews.
- Implemented secure VPN access and ACLs to protect sensitive medical data and support 24/7 critical system uptime.

Junior Cyber Security Consultant — Sep 2022 – Sep 2023
Provention — *Milton Keynes, UK*

- Performed risk-based assessments on client environments using tools like Nessus, Burp Suite, and Metasploit.
- Supported ISO 27001/Cyber Essentials+ compliance through control assessments, documentation, and gap analysis.
- Facilitated security training workshops, translating technical threats into accessible concepts for 100+ end-users.

Projects

Nonprofit Red Team Simulation Project *DePaul University course (10 weeks)*

- Conducted vulnerability scans using open-source tools; identified RCE in SSH and insecure VLAN segmentation.
- Assessed security posture by leading efforts on network scanning, web app hardening, incident response, and password policy development, identifying critical vulnerabilities and misconfigurations.

gRPC-based File Retrieval System | GitHub

- Engineered a multi-threaded gRPC system in Java for secure file indexing and retrieval under load-balanced client conditions.
- Integrated performance benchmarks and error handling for resilient communication over large data payloads.

Static Code Analysis Tool | GitHub

- Built a Java static analyzer detecting concurrency flaws, performance issues, and insecure coding patterns in source and bytecode.
- Designed rule engine for automated security scanning and extensible rulesets for CI pipeline integration.

Skills

Red Team Ops: Adversarial Emulation, C2 Frameworks, Social Engineering, Assumed Breach Testing, Purple Teaming
Security Tools: Burp Suite, Metasploit, Nmap, Nessus, Cobalt Strike, Wireshark, Ghidra, Hashcat
Languages & Scripting: Python, Bash, PowerShell, Java, JavaScript, C/C++
Protocols & Systems: TCP/IP, DNS, HTTP/HTTPS, SMB, SSH, FTP, Wireless Security, VPN, Firewalls
Frameworks: MITRE ATT&CK, OSSTMM, PTES, NIST SP 800-30