Eng. Mohamed Nofal *Penetration Tester*

✉ mohammedsfnofal@gmail.com

☎ +971501667123

in Mohamed-Nofal

Vaxene

Abu Dhabi

Github

Blog

Profile

Since 2017, I have been deeply passionate about **cybersecurity**, building hands-on expertise in both **offensive and defensive security practices**. I have actively engaged in **red and blue team operations**, leveraging my skills to assess, fortify, and defend digital infrastructures against evolving cyber threats. My ability to navigate the ever-changing landscape of cybersecurity is complemented by a strong foundation in **scripting languages** like **Python, PowerShell, and Bash**, allowing me to create robust tools and automation processes that enhance security and streamline workflows. To bolster my technical acumen, I hold **CompTIA Network+ KLCP (Kali Linux Certified Professional)** and **OSWP (Offensive Security Wireless Professional)** certifications. Currently, I am pursuing industry-renowned certification—**OSCP (Offensive Security Certified Professional)**

Beyond cybersecurity, I am equally invested in the **DevOps domain**, applying modern practices to improve operational efficiency and align security with agile development lifecycles. My experience spans developing CI/CD pipelines, automating deployments, and ensuring compliance with cybersecurity standards throughout the software development process.

Certificates

Network+
CompTIA

OSCP
Offensive Security

OSWP
Offensive Security

KLCP
Offensive Security

Introduction to Cybersecurity
Cisco

Education

06/2021 – present
Abu Dhabi, UAE

Cybersecurity Engineering
Abu Dhabi University

Skills

- CI/CD Pipelines
- Active Directory Attacks
- Vulnerability management
- Linux Systems Configuration
- Penetration Testing
- Infrastructure as Code
- JavaScript & TypeScript
- Python Scripting
- Vulnerability Scanning
- Analytical Skills
- Threat Intelligence
- Containerization
- SIEM Tools (SPLUNK)
- Java

Awards

2024

Intersec Best Innovative start-up
Intersec
Won the best innovative startup award at Intersec Dubai 2024.

2023

ADUx5ire Hackathon Winner
5ire
Won the hackathon organized by Abu Dhabi University and 5ire Company and showcased dedication towards a more sustainable future.

Projects

05/2024 – present

Web Application Penetration Testing Lab

Multiple Platforms

- What ensues after this is an outline of the project, where I go on to describe and implement a series of web applications with a frontend back-end, particularly as a testing ground for research on security and penetration testing methodologies. The implemented technologies used in developing the application included:
- Front-end Development: It is built using TypeScript because of the robust typing system; it enhances code quality and maintainability. These interfaces were built using one of the most popular UI libraries, React, along with Next.js, a framework for server-side rendering and static site generation. For styling, this integrates Tailwind CSS to build custom designs very quickly without ever leaving your HTML.
- I conducted complete penetration testing for all the applications basically to find any possible way that I could attack the system. I attacked it, actually, to test the defense mechanisms in place. The tests spanned the following, among other security dimensions: SQL injection, cross-site scripting (XSS), and privilege escalation.

#Main Accomplishments:

- Full-Stack Development Competency: Can work with front-end and back-end development in web-based projects to ensure that integration and functionality
- Web Application Security Expertise: This can be stated as practical knowledge obtained on the identification and mitigation of vulnerabilities in web applications such that this has further solidified my understanding of the web security landscapes.
- Analytical and Problem-Solving Skills: Each step in the penetration testing process had to be planned very carefully to get results not just in exploiting the vulnerabilities but in taking defensive measures as well.
- This project has not only technically reinforced me in most domains but also reminded me of the importance of security throughout the software development life cycle.

2022 – present

Ethical Hacking Home lab

AD & Linux penetration testing

A high-tech lab for ethical hacking mimics real-life networking situations with seven virtual machines: four are primarily for Active Directory surroundings, and three emulate different Linux distributions. This arrangement promotes thorough penetration testing, allowing users to pinpoint and correct weaknesses in both AD and Linux configurations. Perfect for sharpening hands-on cybersecurity abilities in a managed environment.

2024

VaxLabs

Startup

- Designed and implemented scalable, automated infrastructure solutions using **Terraform**, **Docker**, and **Ansible**, ensuring seamless deployment and efficient management of resources.
- Developed and managed CI/CD pipelines using **Jenkins** and **GitHub Actions**, enabling rapid and reliable software delivery.
- Streamlined deployment processes, reducing lead times and enhancing operational efficiency.
- Ensured system reliability and security by automating monitoring, backups, and infrastructure updates.
- Collaborated with cross-functional teams to align DevOps strategies with business objectives, fostering innovation and growth.
- Delivered robust solutions for infrastructure-as-code (IaC), container orchestration, and automated configurations to support VaxLabs' mission of technological excellence.