

MOHAMED YASSINE GADHGADHI

CYBER SECURITY AND SYSTEMS ENGINEER

Tunis, Tunisia | mohamedyassinegadhgadhi@gmail.com

<https://www.linkedin.com/in/mohamed-yassine-gadhgadhi-3a4006228/> | Personal Portfolio : <https://woodjooe.github.io>

EXPERIENCE

● System Administrator at KPIT engineering

August 2024 - Present

With a multicultural team, performed a range of infrastructure and security tasks:

- ❖ Deployed and maintained various Linux servers for specialized purposes:
 - ELK for data monitoring (e.g., Netflow traffic), Security-Onion to monitor Linux and Windows servers.
 - File sharing server, SonarQube for code quality analysis, and version control systems (e.g., GitLab).
- ❖ Monitored ESET antivirus across both servers and employee workstations (1000+).
- ❖ Troubleshoot and resolved network issues, including configuring Mikrotik firewall rules.
- ❖ Automated tasks that leverage APIs securely with Python scripts and Ansible playbooks.
- ❖ Developed PowerShell scripts to streamline Active Directory and DNS tasks.
- ❖ Worked with Devops team to solve issues and automate tasks
- ❖ Mentored interns in Phishing Detection/Threat Intelligence PFE Project.
- ❖ Mentored Interns in Traffic Monitoring using traditional tools including Zeek/Suricata and newly developed tools with AI.
- ❖ Mentored Intern to leverage AI to test Captcha security.

● Cyber security Intern at Talan

February 2024 - June 2024

- ❖ Graduation Project titled "SOC Detection Capacity Assessment Tool":
 - Designed and implemented an open-source adversary emulation framework to evaluate SOC detection capabilities, in order to identify security detection gaps and improve.

● Cyber security Intern at DefensyLab

July 2023 - September 2023

- ❖ Worked on Active Directory Penetration Testing:
 - Set up an AD lab with vagrant (IaC) to perform penetration testing and harden the AD security.

EDUCATION

● Computer Engineering at National Engineering School of Sfax (ENIS)

September 2021 - June 2024

● Preparatory School for Engineering Studies of Tunis - Physics/Chemistry (IPEIT)

September 2019 - June 2021

EXTRACURRICULAR ACTIVITIES

● Founded SecurITNets ENIS cyber security university club

- Organized a team of cyber security enthusiasts whose goal is to gain and spread knowledge.
- Prepared and presented multiple cyber security workshops.

CERTIFICATIONS

- RedHat Certified System Administrator (RHCSA)
- Microsoft Certified : Azure Fundamentals (AZ-900)
- Microsoft Certified : Security, Compliance and identity fundamentals (SC-900)
- HTB Certified Junior CyberSecurity Associate - CJCA (Expected in October)
- CyberTalents Certified : SOC Analyst (Blue Team Scholarship 2023)
- CyberTalents Certified : Threat Hunter (Blue Team Scholarship 2023)

COMPETITIONS

- CyberSphere 6 Advanced CTF 2025 | 1 / 60+ teams
- HTB Cyber Apocalypse CTF 2024 | 107 / 5694 teams
- HackFest Finals CTF 2024 | 5 / 15 Finalist teams
- Engineers Spark CTF 2024 | 2 / 60+ teams
- Arab Security CWG CTF 2023 | top 30 / 738 teams

PROJECTS

- AD + SOC LAB
 - Monitor AD with Universal Forwarder to forward data to Splunk for indexing and Zeek and Suricata to analyze traffic
- Malware Development and Analysis
 - Developed with Win32 assembly and C++, analyzed with VirusTotal.
- Cyber Security CTF competitions Author
 - CybererTek CTF V2 / CyberTek CTF / CTF Kareem / Tekup Mini CTF

SKILLS & TOOLS

- Active Directory
- Linux
- Windows
- Docker
- Mikrotik
- Ansible
- Salt
- Python
- Powershell
- Bash
- VMware Vsphere
- ESET
- WireShark
- Veeam
- SAN storage server

LANGUAGES

- Arabic (Native)
- English (Fluent)
- French (Intermediate)
- German (Beginner)