

# MOGHEES AHMAD

Highly Motivated Computer Science Graduate with Passion for Cybersecurity and Penetration Testing. A motivated team player looking to excel

Phone# (+92) 336-7403919 | Email: [mogheesahmad244@gmail.com](mailto:mogheesahmad244@gmail.com) | [github.com/Moghees244](https://github.com/Moghees244) | [linkedin.com/in/moghees-ahmad-064a94188/](https://linkedin.com/in/moghees-ahmad-064a94188/)

## Professional Summary

As a recent graduate, I possess a strong interest in the field of cybersecurity, with a particular focus on penetration testing. My academic background in computer science, combined with practical experience gained through participation in Capture the Flags (CTF) and personal projects, has equipped me with the necessary skills to identify vulnerabilities and implement effective solutions. I am committed to continuous professional development and strive to stay updated with the latest advancements in security technologies and best practices. With a deep passion for cybersecurity, I am dedicated to honing my expertise and making a meaningful contribution to the industry.

## Education

**BS Computer Science**

**FAST-NUCES**

*September. 2020 - June 2024*

**Relevant Courses:** DSA, COAL, OS, Computer Networks, Information Security, AI, Machine Learning, Data Science, Web Programming

## Achievements

Dean's List of Honor Certificate: Received Dean's List certificate in 7<sup>th</sup> semester at FAST NUCES for achieving 3.6 SGPA.

## Skills

- **Penetration Testing:** Web Applications, API, Active Directory
- **Computer Networks and Traffic Analysis**
- **Machine Learning & Deep Learning**
- **LLM Fine Tuning**
- **Programming:** C++, Python
- **Web Development:** Flask

## Selected Projects

### Droid Deceptor (Final Year Project)

*Machine Learning, Adversarial Attacks*

[Github](#)

- Developed dataset from Drebin Dataset and trained multiple Machine Learning models for Malware Detection
- This tool generates adversarial attacks to fool Android Malware Detection Systems based on Static Features.
- It uses FGSM algorithm to find most effective features that are added to malware apk file which deceives the machine learning and Deep learning models.
- It provides complete report of static analysis and adversarial attack results.

### Capture The Flags Reports

*Penetration Testing*

[Github](#)

- Completed 50+ Capture the flags on different platforms related to Web Exploitation and Active Directory
- All the reports of these labs are in present in the repository

### Development and Hosting of a Cybersecurity Hackathon

*Penetration Testing, Forensics (Private)*

- Jeopardy Style Capture the Flag event.
- Developed 10+ challenges of different categories including Web Exploitation, Forensics, Binary Exploitation and Misc.
- Deployed CTFd website and challenges on a local server as docker containers (each team can start a separate instance of challenge).
- Walkthroughs and challenges will be uploaded on platforms like TryHackMe and HackTheBox once hackathon finishes.

## Certifications

- **HackTheBox Certified Penetration Testing Specialist (Ongoing)**  
by *Hack the Box*
- **Practical Ethical Hacking**  
by *TCM Security*. Credential ID cert\_xbmm1j12
- **API Penetration Testing**  
by *APIsec University*. [Link](#)
- **Practical Malware Analysis and Triage**  
by *TCM Security*. Credential ID cert\_8483xvcm
- **Supervised Machine Learning: Regression and Classification**  
by *Coursera*. [Link](#)
- **Advanced Learning Algorithms**  
by *Coursera*. [Link](#)

## Co-Curricular Activities

- President of FAST Society of Cybersecurity
- Technical Team Member Google Student Developer Club
- Member of Table Tennis Team of FAST Sports Society