Arsh Imtiaz Jamadar
Cyber Security Engineer
Coventry, United Kingdom

arshjamadar5@gmail.com | +44 (0) 74482 94298
https://arshimtiaz.github.io | https://linkedin.com/in/arsh-imtiaz | https://github.com/c0ncatenate

Profile Summary

Cyber Security Engineer with hands-on experience across penetration testing, threat modelling, secure architecture review, and regulatory-aligned security verification. Strong background in analysing complex systems end-to-end at system, application, and protocol layers; identifying trust boundaries and translating risk into actionable engineering controls.
Experienced across Linux and embedded platforms, network protocols, cloud environments, and automotive systems, with a balance of offensive testing and defensive design. Comfortable supporting secure-by-design development and audit readiness across complex platforms.

Core Skills

- **Security Engineering:** Threat modelling (STRIDE, TARA), secure architecture review, trust-boundary analysis, abuse-case driven design
- **Offensive Security:** Manual penetration testing, protocol-level testing, service enumeration, exploit PoCs, traffic manipulation
- **Networking:** TCP/IP, TLS, DNS, protocol analysis (Wireshark, tcpdump), custom traffic crafting
- **Cloud Security:** AWS IAM, S3 policy analysis, logging, and cloud architecture risk assessment
- **Defensive & Platform Security:** Secure-by-design reviews, security requirements validation, logging and detection reasoning
- **Operating Systems:** Linux security internals (permissions, services, hardening), Windows fundamentals
- **Automation & Tooling:** Python and Bash for testing, analysis, and security tooling
- **Embedded & Automotive Security:** Protocol analysis, platform security assumptions, regulatory-aligned verification
- **Governance & Compliance:** ISO 27001, ISO/SAE 21434, UN R155/R156-aligned evidence review and audit preparation

Professional Experience

Penetration Tester
McLaren Automotive Ltd (Contract via Tata Technologies)
Woking, UK | Aug 2025 – Present

- Led cybersecurity verification activities for regulatory audit readiness, including reviewing requirements, validating evidence, and confirming coverage against approved cybersecurity work products.
- Assessed cybersecurity architecture and identified control gaps through threat-based reasoning, supporting remediation planning ahead of regulatory assessment.
- Produced structured verification reports and audit-ready documentation for submission to the Vehicle Certification Agency (VCA), ensuring alignment with regulatory expectations and internal quality standards.
- Collaborated with feature owners, architects, and technical teams to close gaps, improve documentation quality, and streamline verification workflows ahead of external assessment.
- Analysed security test results and supporting evidence to assess system-level coverage, traceability, and completeness across multiple components.
- Additionally supported penetration testing activities, including protocol-level testing, service enumeration, traffic manipulation, and vulnerability identification.
- Provided remediation guidance through technical reports and proof-of-concept demonstrations, contributing to platform security hardening.

Cyber Security Engineer
Tata Technologies Ltd
Warwick, UK | July 2025 – Present

- Supported secure-by-design reviews and threat modelling activities, contributing to architectural risk identification and security requirement definition across multiple systems.
- Developed custom Bash and Python tooling to support manual penetration testing, protocol analysis, and vulnerability validation.
- Contributed to governance processes and cross-team security alignment across engineering and security stakeholders.

Client Assignment
Aston Martin Lagonda (via Tata Technologies)
Gaydon, UK | August 2024 – September 2024

- Completed a one-month on-site assignment at Aston Martin supporting their infotainment engineering team.
- Developed an automated Diagnostic Trouble Code (DTC) parser to accelerate debugging and log analysis workflows.
- Created a Python-based debugging tool for AMP audio issues, which helped diagnose and reproduce a random pop sound occurring during system runtime.
- Collaborated with infotainment and software engineers to analyse logs, isolate triggers, and improve troubleshooting efficiency.

Cybersecurity Engineer (Early Career)
Tata Technologies Ltd
Warwick, UK | July 2023 – October 2024

- Gained exposure to engineering workflows across ER&D and ESS departments, supporting early-stage security activities.
- Wrote attack scripts in Bash and Python for penetration testing tooling.
- Created documentation, test plans, and risk assessments.

Education

BSc (Hons) Ethical Hacking and Cyber Security – First Class Honours
Coventry University | 2021 – 2025

Projects

- Built and currently maintaining a portfolio and cybersecurity blog website.
- Designed and maintained a personal cybersecurity lab to simulate real-world attack paths, protocol-level abuse, and multi-system trust relationships using Linux, virtualisation, and network tooling.
- Designed a secure distributed communication prototype using decentralised principles, with a blockchain background.
- Developed threat simulation PoCs targeting authentication, messaging, and protocol weaknesses to validate assumptions and document exploitation paths.
- Focused on understanding system trust boundaries, attacker assumptions, and failure modes rather than tool-driven testing.

References

Available upon request.