MARK SAVIOUR FARRUGIA

London, UK • +44 7555 536794 • marksaviourfarrugia@proton.me • LinkedIn • GitHub • Portfolio

EDUCATION

King's College London **London, UK**
Master of Science in Cybersecurity – In Progress *Sep 2025 – Sep 2026*

- Dissertation (in progress): Designing and evaluating alternative post-quantum key-agreement handshakes for the Signal protocol, benchmarked against Signal's current PQXDH design based on performance, bandwidth and security guarantees.
- Relevant modules: Cryptography, Security Engineering, Machine Learning, Agent Reasoning, Cybercrime & Forensics, Network Security, Security Management.

University of Wolverhampton **Pembroke, Malta**
BSc (Hons) Cybersecurity – First-Class Honours *Sep 2022 – Jun 2025*

- Dissertation: "Exploring Different 2FA Methods and Their Vulnerabilities". A comparative security analysis of different authentication methods was conducted using a testing ground created as the artefact.
- Relevant modules: Ethical Hacking, Digital Forensics, Risk Management, Networking Security & Principles, Databases, Object-Oriented Programming, Web Development.

NCC Education **Pembroke, Malta**
Level 4 Diploma in Computing – Merit *Sep 2022 – Jul 2023*

PROFESSIONAL EXPERIENCE

St. John's Pharmacy & Medical Centre **Xewkija, Malta**
IT Security & Infrastructure Engineer (Summer Engagement) *Jun 2025 – Sep 2025*

- Reduced the organisation's external attack surface across all company endpoints by deploying endpoint detection and response (EDR), establishing centralised endpoint protection where none previously existed.
- Implemented Zero Trust Network Access (ZTNA) using Twingate to secure internal systems, replacing implicit-trust connectivity with identity-verified access for remote and on-site staff.
- Managed 5 device categories (networking, servers, storage, endpoints, AV) and minimised operational downtime by introducing proactive maintenance and monitoring, ensuring uninterrupted daily operations.
- Served as primary responder for all IT and security incidents during daily operations and events, resolving issues to maintain business continuity.

RSM Malta **Zebbug, Malta**
IT Intern *Jun 2023 – Mar 2024*

- Cut new-employee onboarding time by 70% (from 2.5 hours to 45 minutes) by designing and deploying a Windows Golden Image tailored to the organisation's needs.
- Strengthened endpoint security across 100% of company devices by managing Sophos endpoint protection (EDR), maintaining consistent threat-defence coverage organisation-wide.
- Improved support efficiency as part of a 3-person team by streamlining incident-management workflows in Freshdesk and maintaining audit-ready asset records through the full hardware lifecycle in Xeox.
- Enforced least-privilege access by administering user accounts in Active Directory, applying identity and access management (IAM) principles to staff onboarding and offboarding.

TECHNICAL SKILLS

Offensive Security: Penetration Testing, Web Application Security Testing (Burp Suite), Vulnerability Assessment, Exploitation & Reverse Engineering, Kali Linux

Defensive Security: Endpoint Detection & Response (Sophos), Zero Trust Network Access (ZTNA), Firewall Configuration (iptables/Netfilter), Intrusion Detection (Snort), Active Directory & IAM

Digital Forensics: Autopsy, OSForensics, John the Ripper, Wireshark, Evidence Handling & Chain of Custody

Frameworks & Standards: ISO/IEC 27001, ISO/IEC 27005, NIST SP 800-30, NIST SP 800-86, ACPO

Networking & Platforms: Mininet, Cisco Packet Tracer, hping3, Windows (Client & Server), Linux/Unix, VMware

Programming: PHP, HTML/CSS, Bootstrap, Python, Java, C, C#, Rust, Swift, SQL

PROJECTS

Risk & Cybersecurity Assessment – BSc, Wolverhampton *ISO 27005, NIST SP 800-30, ISO 27001*

- Produced a full risk and cybersecurity management assessment for a case study using ISO/IEC 27005 and NIST SP 800-30, identifying 28 distinct risks and recommending an ISO 27001-aligned ISMS, privileged access management, and a Cyber-Security Incident Response Plan (CSIRP) that cut projected aggregate risk exposure by an estimated 54%.

Digital Forensic Investigation – BSc, Wolverhampton *Autopsy, OSForensics, John the Ripper*

- Conducted an end-to-end forensic investigation of a compromised Linux host, recovering evidence of privilege escalation and prohibited activity by cracking the /etc/shadow hash with John the Ripper and reconstructing user activity in Autopsy and OSForensics, then documenting findings in a court-admissible expert report aligned to NIST SP 800-86 and ACPO chain-of-custody principles.

Collaborative SwiftUI Application – BSc, Wolverhampton *Swift, SwiftUI, Xcode, Google Calendar API, Git*

- Served as the security engineer in a five-person Agile team across two sprints, delivering an iOS appointment-booking app — implementing secure password hashing for user credentials, integrating the Google Calendar API, and supporting the team's risk assessment, test planning, and version control.

Network Engineering, Attack & Defence – BSc & MSc Network Security *Cisco Packet Tracer, Mininet, Wireshark*

- Simulated and mitigated denial-of-service attacks in a team-based environment by launching ICMP and TCP SYN floods (including IP spoofing) via hping3 against a Mininet network, then deploying iptables firewall rules that blocked ~56M malicious packets and reduced attacker traffic reaching the server to 0%, verified through Wireshark analysis.
- Built, configured, and hardened enterprise networks across a dozen Cisco Packet Tracer labs and mini-projects — spanning IPv6, VLAN trunking, GRE tunnelling, DHCPv4, and inter-AS routing, plus secure designs featuring router hardening, a zone-based policy firewall, and IDS on critical servers — complemented by Linux firewall and Snort intrusion-detection configuration.

Off-Sec & Web Penetration Testing – BSc Labs & CTF KCL Security Testing *Burp Suite, Kali Linux, Python*

- Captured all 10 flags in a web-application penetration-testing challenge by identifying and exploiting XSS, UNION-based SQL injection, OS command injection, and IDOR vulnerabilities, escalating to Java applet decompilation and binary reverse engineering (objdump plus a custom Python XOR decryptor) using Burp Suite Repeater and Intruder.
- Completed a ten-part ethical-hacking lab series covering the full offensive lifecycle in a controlled VM environment — OSINT reconnaissance, Nmap scanning and enumeration, web exploitation (SQLi/XSS/CSRF), Metasploit exploitation and post-exploitation, social engineering/phishing simulation, and privilege escalation to gain unauthorised access to Linux and Windows hosts.