ERMAND MANI

Cyber Security Graduate | Glasgow | 07494 196195
hi@ermand.uk | ermand.uk | linkedin.com/in/ermandmani | github.com/CodeEvent

PROFESSIONAL SUMMARY

BEng (Hons) Cyber Security graduate from the University of the West of Scotland with hands-on experience across blockchain security, digital forensics, penetration testing, network security, and secure programming. Dissertation project SmartGuard, a Slither-based DeFi fraud detection tool, was accepted for presentation at SIGiST 2026 in London, achieving 100% precision, recall, and F1 against a 17-contract evaluation dataset, with findings corroborated by a professional BlockSec audit. Actively seeking roles in SOC analysis, penetration testing, DFIR, application security, or blockchain security.

KEY ACHIEVEMENTS

- **SIGiST 2026 London**: Research paper accepted for presentation
- SmartGuard: **100% precision, recall, and F1** on 17-contract blockchain dataset
- BlockSec STRATOS-2024-001: 2 of 12 HIGH-severity audit findings independently corroborated
- Operation FishNet: ACPO-compliant digital forensic investigation producing 50+ court-ready exhibits
- Network Security (COMP10014): **Grade A2, First-class band** (80-89%)
- Web Application Security: **89/100** across two penetration testing courseworks (45/50 and 44/50)

EDUCATION

BEng (Hons) Cyber Security | *University of the West of Scotland* 2022 – 2026
Lanarkshire Campus | Supervised by Dr. Althaff Irfan Cader Mohideen | Student ID: B00249469

Module	Grade	Classification
Honours Dissertation: SmartGuard	**First**	First-class
Network Security (COMP10014)	**A2**	First-class band (80-89%)
Web Application Security (COMP09109)	**89/100**	Distinction
Secure Programming (COMP10068)	**A2**	First-class band (80-89%)
Programming for Cyber Security (COMP08101)	**A2**	First-class band (80-89%)

PROJECTS & RESEARCH

SmartGuard: Blockchain Security Dissertation | *University of the West of Scotland* 2025 – 2026

- Designed and built a Slither plugin extending its static analysis engine with three custom detectors targeting intent-based DeFi fraud: unlimited minting, token name impersonation, and unprotected critical functions.
- Evaluated against 17 Ethereum smart contracts (7 fraudulent, 10 legitimate) achieving 100% precision, recall, and F1 with zero false positives.
- Corroborated 2 of 12 HIGH-severity findings from professional BlockSec audit report STRATOS-2024-001, validating detector accuracy against an independent commercial standard.
- Accepted for presentation at SIGiST 2026, London, the Software Testing special interest group conference.
- Stack: Python 3.10.11, Slither 0.11.5, Solidity 0.8.0, solc-select.

Operation FishNet: Digital Forensic Investigation | *University of the West of Scotland* Nov – Dec 2025

- Conducted an ACPO 2012-compliant forensic examination of two seized devices including disk images (E01) and volatile memory dumps (RAW).
- Identified DarkComet RAT as an active process in volatile memory using Volatility 2.6 (pslist, malfind, netscan plugins).

- Confirmed illegal image possession on Device 2 via MD5 hash comparison against a reference database; confirmed zero matches on Device 1.
- Recovered email evidence from Mozilla Thunderbird local storage establishing deliberate coordination between device users.
- Produced a court-standard report with 50+ numbered exhibits and full chain of custody documentation.
- Tools: Autopsy 4.21.0, FTK Imager 4.7.1, Volatility 2.6, RegRipper 3.0, Registry Explorer.

OWASP Web Application Penetration Testing | *University of the West of Scotland* 2024 – 2025

- Part A (45/50): Demonstrated broken access control, cryptographic failures, SQL injection authentication bypass, and security misconfiguration against Mutillidae II using Burp Suite.
- Part B (44/50): Chained SQL injection to extract TOTP secret and bypass 2FA on OWASP Juice Shop; demonstrated stored and reflected XSS with session cookie theft on Mutillidae II; exploited CSRF via image-tag payload on Security Shepherd; deployed OSSEC HIDS for logging and monitoring failure demonstration.
- Tools: Burp Suite Community Edition 2025.2.4, Kali Linux, OWASP Juice Shop, Mutillidae II, Security Shepherd, OSSEC v3.7.0.

Network Security Labs: COMP10014 | *University of the West of Scotland* 2025 – 2026

- ARP poisoning and MITM attack using Ettercap; HTTP traffic interception via tcpdump; detection with Arpwatch (flip-flop alerts).
- Snort IDS deployment with custom rules; traffic mirroring via iptables TEE to transition from HIDS to NIDS.
- GRE tunnelling configuration using Linux kernel and OpenVSwitch; Layer 2/3 encapsulation analysis in Wireshark.
- OpenVPN PKI deployment using EasyRSA: CA creation, certificate signing, Diffie-Hellman parameters, secure credential transfer via SCP.
- FreeRADIUS 3.0 AAA server configuration: client setup, user authentication, Attribute Value Pairs, radclient testing.

SEI CERT C++ Remediation: COMP10068 | *University of the West of Scotland* 2025 – 2026

- Analysed five noncompliant C++17 programs against the SEI CERT C++ Coding Standard; produced compliant fixes without modifying protected main() functions.
- Rules addressed: DCL50-CPP (C-style variadic to template), STR50-CPP (buffer over-read fix), MEM51-CPP (RAII via unique_ptr), MSC51-CPP (std::random_device seeding), ERR55-CPP (false noexcept removal).
- Built a Hangman game in Rust from a bare Hello World template, demonstrating memory-safe systems programming with HashSet deduplication, ownership semantics, and idiomatic Rust patterns.

WORK EXPERIENCE

Event Security & Staff Management | *OVO Hydro, Glasgow* 2022 – Present

- Managed security and staff operations across four hub zones (South, East, West, Hydro Club) at one of Europe's largest indoor arenas.
- Responsible for coordinating sign-in procedures, role slot management, and real-time staff deployment across live events.
- Developed internal tooling including colour-coded Excel staff planning workbooks and designed specification for a React/Node.js/SQLite live staff management web application with PIN-based authentication and real-time tracking.

TECHNICAL SKILLS

Offensive Security	Burp Suite, Metasploit, Nmap, Ettercap, Wireshark, SQLi, XSS, CSRF, 2FA bypass
Digital Forensics	Autopsy 4.21, Volatility 2.6, FTK Imager, RegRipper 3.0, E01 imaging, ACPO 2012
Network Security	Snort IDS, OpenVPN 2.4, FreeRADIUS 3.0, GRE tunnelling, iptables, Arpwatch, Wireshark
SIEM & Monitoring	Wazuh, OSSEC v3.7.0, Snort custom rules, log analysis, alert correlation

Blockchain Security	Slither 0.11.5, Solidity 0.8.0, DeFi taxonomy, taint analysis, smart contract AST
Languages	Python 3.10.11, Rust, C++17, Solidity, Bash, PowerShell
Platforms	Kali Linux, Tails OS, Ubuntu 20.04, VirtualBox, Docker, Git
Secure Coding	SEI CERT C++ (DCL50 STR50 MEM51 MSC51 ERR55), RAII, memory safety, type safety

ADDITIONAL INFORMATION

- GitHub Portfolio: github.com/CodeEvent: SmartGuard, Network-Security, Operation-FishNet, OWASP-Pentest-Suite, Secure-Programming, Programming-for-Cyber-Security
- SIGiST 2026 Speaker: presenting SmartGuard research at Software Testing special interest group conference, London
- Website: ermand.uk