NIKHIL SANKHLA

+61-449-812-858 | nikhilsankhla.cybersec@gmail.com | LinkedIn | Sydney, Australia

Software developer turned security practitioner with 2.5 years of industry experience. Currently pursuing a Master's in Cyber Security at UNSW, specialising in offensive security, binary exploitation, wireless security, and web application pentesting.

Education

The University of New South Wales — Sydney, Australia
Master's in Information Technology (Major: Cyber Security) — *2025 – Present*

Experience

Software Developer — Jul 2023 – Dec 2024
Experis IT (Client: Dell Technologies) — *Bengaluru, India*

- Embedded automated vulnerability scans (SAST, dependency checks) into CI/CD pipelines, reducing insecure code merges.
- Migrated two ML monolithic applications to secure microservices with fine-grained access control and monitoring.
- Strengthened authentication by implementing token-based login across microservices architecture.

IT Officer — Jul 2022 – Jul 2023
JK Cement — *Gurugram, India*

- Implemented APIs with data validation and integrity checks to protect ML workloads from tampering.
- Built access-controlled automation applications with full audit trails for internal IT processes.

Projects

Automated Black-Box Fuzzer | *Python, Linux, ELF Binary Analysis*

- Engineered a fuzzer to detect memory corruption vulnerabilities (Heap UAF, Invalid Writes) in 64-bit Linux ELF binaries applicable to embedded and firmware security testing.
- Implemented hybrid mutation strategies (bit-flipping, null-byte injection) and format-specific mutators for JSON, XML, PDF, JPEG, and ELF inputs.

Wireless Attack Simulation Lab | *Raspberry Pi, Kali Linux, Aircrack-ng, Scapy*

- Built a hardware-based wireless lab using Raspberry Pi to simulate Evil Twin attacks and capture WPA2 handshakes for offline cracking.
- Performed deauthentication attacks and packet capture to study 802.11 protocol-level weaknesses and document countermeasures.

Automotive CAN Bus Protocol Exploration | *Raspberry Pi, Linux, can-utils*

- Set up virtual CAN interfaces (vcan0) on Raspberry Pi to simulate, send, and sniff CAN frames; studied arbitration IDs and ECU attack surfaces.

Web Application Penetration Testing Lab | *Burp Suite, OWASP, Python*

- Conducted web pentesting covering OWASP Top 10 (SQLi, XSS, IDOR, SSRF) using Burp Suite on DVWA and HackTheBox platforms.

Browser Data Exfiltration & Keylogging Lab | *Python, Windows*

- Created proof-of-concept malware simulation in an isolated lab to study browser credential theft, persistence techniques, and process obfuscation.
- Captured telemetry logs and documented endpoint hardening and detection strategies (credential protection, least privilege, behavioural monitoring).

Technical Skills

Cybersecurity: Vulnerability Assessment, Threat Modelling, ISO 27001, Wireless Security (802.11/WPA2, Evil Twin, Deauth Attacks), Web Application Pentesting (OWASP Top 10, SQLi, XSS, IDOR, SSRF), Wireshark, TCP/IP & OSI Protocols
Offensive Security & Reverse Engineering: Binary Exploitation, Black-Box Fuzzing, ELF Analysis, pwndbg, Shellcode Development, Burp Suite, Aircrack-ng, Scapy, Capture-The-Flag (CTF) Challenges
Hardware & Embedded: Raspberry Pi, CAN Bus Protocol (vcan0, can-utils), IoT Network Security
Cloud & DevSecOps: Docker, Kubernetes, GitLab CI/CD (SAST, Dependency Scanning)
Programming & Automation: Python, C, C++, Assembly, PowerShell, Bash, REST APIs
Platforms: Kali Linux, MacOS, Windows