Idrees Roshan, BSc

idrees.roshan@outlook.com | 07478768892 | LinkedIn | Portfolio Website

Software Engineer transitioning into Cybersecurity, with firsthand experience in full-stack development, network security and secure software design. Secured vulnerable networks using industry best practices. Successfully developed and applied threat detection measures, security hardening techniques, and cryptographic solutions, applying frameworks like NIST, ISO 27001 and OWASP top 10. Now applying software engineering expertise to identify vulnerabilities, strengthen security controls, and protect organisations from cyber threats.

Skills

Technologies: Kali, Ubuntu, Splunk, Wireshark, tcpdump, Hashcat, Metasploit, Nmap, Git, Sliver

Programming Languages: Python, SQL, Java, HTML/CSS, JavaScript, C++, C#, bash, Git bash

Soft Skills: Team Player, Growth Mindset, Critical thinking, Problem Solving, Technical Documentation

Security: Security Frameworks, Vulnerability Management, Incident Response, Security Hardening

Projects

Home SOC Lab — Feb 2025

- Configured and deployed LimaCharlie, a cloud-based Endpoint Detection and Response platform.
- Simulated adversary tactics by deploying and analysing Sliver C2 implants, elevating privileges and dumping lsass.exe credentials.
- Developed YARA scanning and Detection & Response (D&R) rules to identify malware, block credential dumping, and detect ransomware indicators.

Metasploit Ethical Penetration Testing — Feb 2025

- Conducted network reconnaissance using Nmap scans, to identify open ports and outdated services.
- Exploited a VSFTPD 2.3.4 vulnerability using Metasploit, gaining unauthorised access and establishing persistence with a backdoor account.
- Created a penetration testing report, detailing discovered vulnerabilities, exploitation methods, and recommended security improvements

TCPdump and Wireshark Logging Tool — Feb 2025

- Developed an automated tcpdump shell script to log and analyse suspicious network traffic for forensic investigations.
- Captured and decrypted SSL/TLS keys, enabling inspection of encrypted HTTP traffic in Wireshark.
- Implemented log rotation and filtering to efficiently store, manage, and analyse network packets.

Wireshark Packet Capture — Feb 2025

- Captured and analysed network traffic using Wireshark, applying filters to isolate HTTPS and TLS handshake data.
- Identified and extracted destination IPs from encrypted traffic, correlating them with network activity.
- Completed a capstone task by capturing HTTP/HTTPS packets and filtering out a specific IP address.

Network Security Pen Testing and Hardening — Jan 2024

- Conducted a red team security assessment on a Linux server, exploiting vulnerabilities using Metasploit’s ‘ProFTPD ModCopy Exec’ exploit.
- Demonstrated password security risks by cracking hashes with Hashcat and implementing NIST 800-53 security enhancements, including firewall hardening and least privilege access.
- Secured communications by replacing Telnet with SSH and recommending SIEM tools and MFA.

Experience

Cyber Security Student | Full Time — Jan 2025 – Present

- Current certifications completed and in progress:

- **BCS Certificate in Information Security Management Principles**	exp. Mar 2025
- **TryHackMe SOC level 1**	exp. Mar 2025
- **Google Professional Cybersecurity certificate**	Jan 2025
- **Qualys Vulnerability Management**	Jan 2025

Teragence | Software Engineer Internship — Sep 2023 – Oct 2023

- Developed and maintained containerised application using Docker, streamlining deployment, and increasing system scalability.
- Analysed large datasets from over 1 million cell towers in the UK, optimising data processing and providing valuable insights that informed strategic decisions.
- Delivered a software presentation and assisted with a demo to multiple tech companies, effectively displaying the product's capabilities and fostering potential partnerships.
- Actively updated software and tested functionalities, ensuring robust and secure system performance, which minimised downtime and maintained service reliability.

KL2C Nottingham Hospital Charity | Software Engineer — Oct 2022 – May 2023

- Led the development of a paediatric peripheral eye test application using Unity, C#, and Python, ensuring secure and scalable code practices in the healthcare domain.
- Managed a Git repository with over 200 commits as Git leader, establishing seamless version control and collaboration among 7 developers.
- Followed Agile methodologies and used collaboration tools like Slack and Trello to boost project management efficiency and adaptability to changing requirements.
- Coordinated presentations of the software to 100+ industry professionals, effectively communicating technical concepts to non-technical stakeholders.
- Contributed to backend development and integration, resolving complex challenges that improved system performance and strengthened security.

Education

University of Nottingham | *BSc Computer Science* — **Oct 2021 – Dec 2024**
Mill Hill County High School | *A levels and GCSEs* — **Sep 2014 – Jun 2021**

- A-Levels: Mathematics (A*), Further Mathematics (A*), Computer Science (A)
- GCSEs: 9 GCSEs, Mathematics (9), English Language (7)

Activities and Interests

Sports

- Volleyball Captain and MVP at the University of Nottingham, led the team to a division promotion.
- Climbed Mount Snowden and Scafell Pike, highest points in England.
- Interest in football, basketball, rock climbing/scrambling and motorsports.