Afnan Bin Abbas

+92 3352058647 | afnanbabbas@gmail.com | LinkedIn | MyPortfolioWebsite | GitHub

EDUCATION

Ghulam Ishaq Khan Institute   *June 2022 – July 2026*
Bachelor of Science in Cyber Security - **3.246 CGPA**

Credo College, Karachi
A-levels, Pre-Engineering   *Sep 2019 – Nov 2021*

WORK EXPERIENCE

NEXUS GIK Institute   *March 2024 – Present*
Co-Founder, GIK
- Co-founded GIK's first Cybersecurity Society, scaling student engagement by 90% through strategic leadership and outreach.
- Directed Capture the Flag (CTF) sessions and ethical hacking workshops for 30+ students, reducing skill gaps in penetration testing and offensive hacking by 25% via hands-on training.
- Initiated partnerships with AWS Cloud Club Pakistan, securing 10% stronger student-industry alignment through expert-led sessions (e.g., AWS Generative AI Workshop).

National Foods Limited   *Feb 2025 – Mar 2025*
Web Application Penetration Tester
- Executed a security assessment of nfoods.com, uncovering critical vulnerabilities, including Unauthenticated Stored XSS (CVE-2021-24508, CVE-2022-4477) and Directory Misconfiguration (CWE-200), strengthening web application security posture.
- Performed penetration testing using Burp Suite and WPScan, identifying publicly exposed sensitive directories (robots.txt, sitemap.xml), mitigating information disclosure risks, and enhancing WordPress security measures.
- Delivered a detailed vulnerability report aligned with OWASP and PTES standards, outlining exploitation scenarios, risk impact, and mitigation strategies, leading to proactive security improvements and compliance adherence.

KaiRiz Cyber Technologies (SMC-Private) Ltd   *June 2024 – July 2024*
Web Application and Network Penetration Testing Intern
- Carried out penetration tests across web and network systems, identifying 2 critical vulnerabilities (CVSS 7.0+), boosting remediation efficiency by 40% with a custom prioritization framework.
- Oversaw vulnerability scanning workflows, cutting manual testing time by 30% and enhancing continuous monitoring accuracy by 15%.
- Delivered Penetration Testing Execution Standard (PTES)-aligned reports from weekly training, raising team awareness of emerging threats by 15% and ensuring 100% remediation of high-risk flaws within service-level-agreements (SLA) deadlines.

PROJECTS

Network Auditing | Pakistan Telecommunication Company Ltd (PTCL)   *Cyber Security Principles and Concepts*
Audit, (Groupwork)
- Executed a full-scale cybersecurity audit as a team, mitigating 2 medium vulnerabilities (CVSS 5.0+), reducing exploitation risk by 25% while ensuring confidentiality.
- Enhanced intrusion detection and incident response protocols, cutting vulnerability impact by 20% through policy review and targeted remediation.
- Streamlined audit reporting with Penetration Testing Execution Standards (PTES), achieving 99% compliance with client security requirements.

Cat and Mouse Split-Screen Game | AI-Optimized with Genetic Algorithm   *Artificial Intelligence*
Python, pygame, (Groupwork)
- Engineered an AI-driven game using genetic algorithms, optimizing trap placement by 30% and improving mouse elimination accuracy by 40%.
- Designed a real-time performance tracking system in game simulated environment, enhancing gameplay responsiveness by 25% across 50+ test iterations.
- Integrated adaptive AI logic in a team setting, reducing manual tuning efforts by 35% and delivering a scalable solution.

Android Exploitation | Metasploit   *Cyber Security Principles and Concepts*
Metasploit, Nmap, Kali Linux, CLI
- Developed malicious APKs with a 90% success rate in establishing reverse TCP connections, extracting data (SMS, call logs, contacts) in 85% of test cases.
- Conducted targeted exploits on Android device, securing remote access to features (mic, camera, apps) with 95% attacker IP tracking accuracy via Metasploit.
- Accomplished device fingerprinting workflows, reducing exploitation setup time by 20% and enhancing penetration testing efficiency.

FREELANCE

Network Packet Sniffing   *Freelance Project*
Wireshark,
- Facilitated Senselearner Technologies intern by integrating network packet analyzing tools (Wireshark), reducing project delivery time by 40% and boosting efficiency by 85%.
- Identified 3+ security gaps (e.g., information leakage, open ports), strengthening system resilience by 30% through detailed documentation and remediation plans.
- Leveraged reconnaissance workflows with Wireshark, applying different filters to get specific protocols and ports like (HTTP/80, TCP/443) achieving 95% vulnerability detection accuracy.

SKILLS

- **Languages:** C++, Python, SQL
- **Tools and Technologies:** Burp Suite, Metasploit, OWASP ZAP, Nessus, Nmap, Wireshark, Active Directory, Bug Hunting, Linux (Kali, Ubuntu), Windows, Git, Docker, Jupyter Notebook, PostgreSQL, LaTeX/Overleaf, Public Speaking, Teamwork, Leadership, Content Writing, Singing
- **Libraries:** pandas, NumPy, Matplotlib, tensorflow.

Awards and Achievements

- *Ranked >85% globally in PICOCTF 2025, competed among 10,000+ teams globally.*
- *Semi-finalist in Digital Pakistan Cybersecurity Hackathon 2024, competed among 500+ teams.*
- *Secured James P. Brennan Scholarship among 500 students to join Cyber Security pathway directed by Leading Edge Skills.*
- *3rd place at GIKI HACKWARTS (Microsoft Learn Student Ambassadors Hackathon), March 2023.*