RAJA MUHAMMAD BILAL ARSHAD

FAST National University (NUCES), Chiniot-Faisalabad Campus Pakistan
03218633947 | bilalarshad.code@gmail.com | LinkedIn
Github

SUMMARY

Cyber Security Analyst with handson Purple Team experience, bridging offensive exploitation and defensive architecture. Demonstrated ability to build automated pentesting frameworks and lowcost hardware security tools, recognized as a finalist in the NCCS Idea Cup and securing seed funding. Skilled in MITRE ATT&CK mapping, Splunk SIEM integration, and SOC analysis. Eager to apply expertise to strengthen organizational security posture and reduce risk.

SKILLS

- **Defensive Security**: Linux Operating System, Penetration Testing, IDS/IPS, SIEM, Secure Network Architecture, Vulnerability Assessment, Threat Detection Engineering, SOC Monitoring, Security Automation, Cloud & Virtualization, Protocol Analysis, Exploitation Tools, Firewall Engineering, SOC Analyst L1, SOC Analyst L2, Cybersecurity Analyst, SNORT, Suricata
- **Offensive Security**: Network Penetration Testing, Web App Security (OWASP Top 10), Privilege Escalation, Wi-Fi Auditing, MITRE ATT&CK, x86 NASM Assembly, Active Directory Exploitation, BloodHound Analysis, Reverse Engineering (Ghidra/x64dbg)

PROFESSIONAL EXPERIENCE

CybeCloud **Nov 2025 - Present**
Cyber Security Analyst *Islamabad, Pakistan*
- Conducted vulnerability assessments on client networks using tools such as Nessus and OpenVAS, coordinated remediation of highrisk findings, and reduced exploitable exposure
- Developed Python automation scripts that accelerated MeanTimeToDetect by integrating security findings directly into ServiceNow ticketing workflows
- Tuned Suricata IDS/IPS rules to improve alert fidelity, which reduced false positives in the SOC pipeline

Prodigy InfoTech **Sep 2025 - Nov 2025**
Cyber Security Analyst *Mumbai, Maharashtra, India*
- Executed penetration tests on web applications using Burp Suite and OWASP ZAP, identified Broken Access Control and Injection vulnerabilities, and delivered remediation recommendations that strengthened the organization's security posture
- Assisted in malware analysis and reverse engineering with Ghidra and Cuckoo Sandbox, uncovered attack signatures, and helped update detection rules that enhanced network defense

Hackviser **Sep 2025 - Dec 2025**
Campus Ambassador *Greater London, England, United Kingdom*
- Led technical workshops and Capture The Flag (CTF) training for university students, using virtualization platforms and exploitation tools to simulate realworld attacks, which boosted participants' handson security skills and raised overall cybersecurity awareness on campus
- Organized cybersecurity awareness seminars that demonstrated live socialengineering and phishing scenarios using phishing simulation software, helping students recognize attack tactics and reducing susceptibility to phishing attempts

Redynox **Aug 2025 - Sep 2025**
Cyber Security Analyst *Islmbd, Pakistan*
- Assisted in conducting network security assessments using Nmap and Nessus to identify vulnerabilities and recommended remediation strategies, improving the organization's overall security posture
- Supported penetration testing engagements by analyzing systems with Metasploit and BloodHound, simulating realworld attack scenarios, and documenting findings, which helped prioritize remediation efforts
- Contributed to vulnerability assessment and patch management by scanning environments with Qualys and validating security controls, leading to timely patch deployment across critical systems
- Worked with the cybersecurity team on incident response activities, using SOC monitoring and SNORT for detection, analyzing security events, and reporting findings, which reduced the mean time to detect incidents

KEY PROJECTS & RESEARCH

ARTP & AutoPENT-Bench (Research Paper - Under Review) **Sep 2025 - Dec 2025**
Code and Research Paper Available on Github

FAST NUCES CFD Campus
- Developing a **Responsible Autonomous Red-Team Planner (ARTP)** that leverages LLMs to synthesize multi-stage attack vectors, prioritizing safe and ethical execution in production environments.
- Engineered 'AutoPENT-Bench', a reproducible benchmarking framework for evaluating the performance and safety of autonomous penetration testing agents against standardized vulnerabilities.
- Implemented hallucination-reduction techniques and validation layers, ensuring agents produce actionable and reproducible exploit paths rather than theoretical errors.

Enterprise-Grade Cyber Battlefield: Layered Network Security with Centralized Monitoring **Jun 2025 - Aug 2025**
Github for Verification

FAST NUCES CFD Campus

- Designed and deployed a virtualized datacenter architecture using Proxmox with integrated pfSense, Suricata, pfBlockerNG, and Splunk SIEM, enabling real-time monitoring, intrusion detection, and multi-layered threat defense.
- Implemented VLAN segmentation, ZeroTier remote access, and custom Python-based socket programming tools to simulate attacks, defenses, and live threat response within a controlled enterprise environment.
- Orchestrated automated alerting -> ticketing pipelines (SIEM -> webhook -> remediation workflows) to accelerate SOC response and patch cycles.
- Consolidated logs and alerts into a Splunk-backed SIEM on an Ubuntu server for real-time correlation, threat hunting, and long-term retention.
- Centralized DNS and ad/telemetry filtering with Pi-hole to reduce noise and limit reconnaissance vectors.

ESP32-Based Offensive Security Toolkit for Network Pentesting(Flipper Zero) **Dec 2024 - Feb 2025**
Github for Verification

FAST NUCES CFD Campus

- Engineered a custom ESP32-S3 platform integrating RFID, OLED interface, and SD storage to emulate a lightweight, portable red team device for Wi-Fi auditing and access control testing.
- Developed modules for handshake capture, credential exfiltration, and real-time network reconnaissance, creating a low-cost yet powerful tool for offensive security operations.

CERTIFICATES

- **Certified in CyberSecurity(CC):**By ISC2
- **Certified Cybersecurity Educator Professional (CCEP):**By Red Team Leaders
- **Certifed Ethical Hacker(CEH) (in Progress):**By EC Council
- **SOC Analyst Tier 1 by Blue team:**By Blue Team
- **Certified Associate Penetration tester(CAPT) (in progress):**By Hackviser
- **Google IT Support:**By Coursera

EDUCATION

Rangers Military College
Fsc, pre-Engineering

FAST NUCES
Bachelors, Computer Science