Muhammad Bilal Badar

Islamabad, Pakistan | +92 320 9683372 | muhammadbilalbadar36@gmail.com
Portfolio: bali-36.github.io | GitHub: github.com/bali-36 | LinkedIn: linkedin.com/in/muhammad-bilal-badar

PROFESSIONAL SUMMARY

Cybersecurity Student and BSc candidate focused on system internals, tool development, and defensive security. Experience in building high-performance security utilities, conducting automated reconnaissance, and analyzing complex threat landscapes. Proven track record in international CTFs and adversary simulation within lab environments.

TECHNICAL SKILLS

Blue Team & SOC: Threat Intelligence (CTI), Log Analysis, Incident Response, Linux Hardening, Access Control Lists.
Forensics & Endpoint: Autopsy, Sysmon monitoring, secure data destruction, malware behavior analysis.
Offensive Knowledge: Vulnerability Assessment (VAPT), Adversary simulation, Kill-chain mapping, Payload generation.
Tools: Wireshark, Nmap, Tenable Nessus, Scapy, Burp Suite, Docker, Git.
Programming: Python, C/C++, Bash Scripting, x86 Assembly.

PROFESSIONAL EXPERIENCE

Cyber Threat Intelligence (CTI) Intern | Resecurity InfoSec *Sept 2025 – Oct 2025*

- **Threat Mapping:** Researched emerging threats and mapped adversary tactics using OSINT and indicator analysis (IoCs) to strengthen defensive postures.
- **Adversary Simulation:** Simulated full kill-chain attacks in isolated lab environments to test and validate detection/response capabilities.

Offensive Security Intern | ITSOLERA PVT. LTD. *June 2025 – August 2025*

- **Vulnerability Assessment:** Conducted manual Web App Pentesting to identify exploit paths, translating findings into actionable remediation steps for defensive teams.
- **Threat Mitigation:** Investigated emerging CVEs to determine impact on client infrastructure and recommended specific patch management strategies.
- **Tool Development:** Built custom Python-based reconnaissance and payload generation tools to automate security auditing phases.

ACADEMIC & SECURITY PROJECTS

Sysmon: Real-time Linux Monitoring *GitHub: /bali-36/Sysmon*

- Developed a monitoring utility tailored for Blue Team operations, providing live alerts on system health and security events.
- Designed log analysis features specifically to flag unauthorized modifications to critical system files.

Digital-Shredder: High-Speed Data Wiping *GitHub: /bali-36/Digital-Shredder*

- Designed a multithreaded C++ utility to securely overwrite files, utilizing forensic-grade wiping patterns to prevent data recovery.

VPN-Client-Server: Secure Tunneling *GitHub: /bali-36/VPN-Client-Server*

- Designed and implemented a secure VPN tunnel using Python to encrypt communication between client and server.
- Focused on understanding tunneling protocols and data encapsulation for secure remote access.

Air Uni CAN: Secure Network Design

- Architected a simulated Campus Area Network that focuses on defense-in-depth, using firewalls, network segmentation, and precise Access Control Lists (ACLs) to isolate sensitive data.

VulnSleuth: Automated Vulnerability Scanner *GitHub: /bali-36/VulnSleuth*

- Built a Python-based auditing tool with a web dashboard to automate the identification of misconfigured services and outdated software across target networks.

CYBER RANGES & CTF ACHIEVEMENTS

TryHackMe (bali36): Top 9% Rank (181,385 pts) with 82 rooms completed. Earned certificates in Pre Security, Industrial Intrusion, HackfinityBattle and Advents of Cyber 2025.
HackTheBox: Participate in Active Directory enumeration and Blue Team Sherlocks to practice real-world incident response.
picoCTF: Solved 100+ challenges, focusing on web exploitation, Cryptography, forensics, and reverse engineering.
CTFtime (Atomic_Pwnz): Active team member. Achieved a global rating of 682 in 2025, competing in 35+ international events including SpookyCTF and EKOPARTY.

EDUCATION

BSc in Cyber Security | Air University, Islamabad *2023 – Present*

- **CGPA:** 3.14
- **Semester:** 6th
- **Focus:** Network Security, Digital Forensics, Cryptography, Penetration Testing, Malware Analysis.

Intermediate in Computer Science (ICS) | Fazaia Inter College, Peshawar *2021 – 2023*

- Completed with 81% marks.

CERTIFICATIONS AND COURSES

- **CSI Certified Linux Investigator** (CSI Linux Academy, 2025)
- **Introduction to OSINT & Forensics** (Security Blue Team, 2025)
- **Certified Ransomware Protection Officer** (ICTTF, 2025)
- **Certified Red Team Operations Management** (Red Team Leaders, 2025)
- **Computer and OS Security** (Microsoft, 2024)