Abdul Rafay

Passionate about cybersecurity, dedicated to continuous learning and growth in the field.

+923141881703 | rafaymunir330@gmail.com | LinkedIn | GitHub | TryHackMe | Portfolio-Website

Education

FAST NUCES Islamabad Islamabad, Pakistan
Bachelor of Science in Cyber Security *Aug. 2023 – Present*

Bahria College Anchorage Islamabad, Pakistan
FSC Pre Engineering *Sep. 2021 – June. 2023*

Projects

HoneyShield: Virtual Honeypot Lab | pfSense, Snort, OpenCanary, *Kali Linux* Aug 2025

- *Designed and deployed a* ***layered honeynet environment*** *using pfSense as a firewall/IDS gateway, OpenCanary for honeypot services (SSH, HTTP, SMB), and Snort for real-time intrusion detection.*
- *Simulated attacker activity from Kali Linux, including* ***Nmap reconnaissance, SSH brute-force with Hydra, and HTTP probing****, to evaluate detection and logging effectiveness.*
- *Captured and correlated* ***application-level logs (OpenCanary)*** *with* ***network-level alerts (Snort)****, demonstrating attacker behavior patterns and validating security monitoring controls.*
- *Ensured complete* ***isolation of the honeynet*** *with pfSense routing enforcement, enabling safe forensic analysis without risking the production network.*

Vulnerability Assessment Lab (Kioptrix) | *Kali Linux, Nmap, Metasploit, Nikto* Aug 2025

- *Performed full penetration testing on the Kioptrix vulnerable machine, including network discovery, service enumeration, and vulnerability research.*
- *Exploited Apache mod_ssl 2.8.4 via the updated OpenFuck exploit to gain a remote shell; leveraged Samba 2.2.1a trans2open exploit in Metasploit for direct root access.*
- *Conducted post-exploitation by enumerating system users and confirming full administrative privileges, demonstrating risks of outdated and unpatched services.*

M57 Data Exfiltration Investigation |*FTK Imager, Outlook PST Viewer* July 2025

- *Conducted a digital forensic investigation of a data breach involving PII leaked via a spoofed email.*
- *Analyzed disk image (. E01) and Outlook archive (.pst) to trace file origins and communication with the attacker.*
- *Identified metadata proving social engineering and exfiltration path; authored a 13-page forensic report.*

OWASP Juice Shop (Web App Pentest Lab) |*Kali Linux, Nmap, Burp Suite, SQLmap, ffuf, Wireshark* July 2025

- *Performed comprehensive web application penetration testing on OWASP Juice Shop, covering authentication, input validation, access control, and sensitive data exposure.*
- *Exploited SQL injection in login and search functions to bypass authentication and extract sensitive data using SQLmap; successfully conducted brute-force attacks with ffuf.*
- *Demonstrated privilege escalation via JWT tampering and identified session fixation, XSS, and sensitive data leaks through client-side analysis and API testing.*

Skills

Technical Skills

Tools*: WireShark, Burp Suite, Metasploit, Nmap, hydra, Packet Tracer, FTK Imager*

Programming Languages*: C++, JavaScript*

OS*: Windows, Linux*

Developer Tools*: Git, GitHub, VS Code*

Other: *MS Office*

Soft Skills

Problem-Solving

Time Management
Teamwork and Collaboration
Communication

Certifications

Web Fundamentals Path – TryHackMe (July 2025)

Jr Penetration Tester Path – TryHackMe (July 2025)

Foundations of Cybersecurity – Google (July 2025)

Cyber Security 101 Path – TryHackMe (July 2025)

Pre Security Path – TryHackMe (June 2025)

Learn React – SCRIMBA (April 2025)

LANGUAGE SKILLS

URDU*: Native*
ENGLISH*: Fluent*