Noaman Shaikh

Karachi, Pakistan | +92 311 3595919 | nomanshykh641@gmail.com

LinkedIn: linkedin.com/in/noaman-shaikh-2151a0216

Professional Summary

Motivated and detail-oriented Cybersecurity Analyst with hands-on experience in penetration testing, vulnerability assessments, and network traffic analysis. Skilled in using industry-standard tools like Wireshark, Nmap, JohnTheRipper, and Aircrack-ng. Passionate about offensive security and eager to contribute to dynamic teams. Demonstrates a strong foundation in OWASP methodologies, incident response, cryptography, and Linux systems. Actively seeking an entry-level penetration testing role to apply and expand technical expertise.

Technical Skills

- Pentesting & Security Tools: Nmap, Wireshark, JohnTheRipper, Aircrack-ng, Burp Suite (basic), OWASP ZAP
- Operating Systems: Kali Linux, Ubuntu, Windows
- Languages & Scripting: C++, Bash (basic)
- Virtualization & Networking: VMware, VirtualBox, TCP/IP, DNS, HTTP/HTTPS
- Security Concepts: OWASP Top 10, Incident Response, Vulnerability Assessment, Cryptography, AD basics
- Other Tools: Microsoft Office, Sandbox Environments

Certifications

- Foundations of Cybersecurity - Google (May 2024 - June 2024)
- Introduction to Cybersecurity - Cisco (April 2024 - May 2024)
- Introduction to Computers, Operating Systems & Security (Aug 2024 - Sep 2024)

Work Experience

Cybersecurity Intern - Bytewise Ltd (Remote)

June 2024 - September 2024

- Conducted network vulnerability assessments and scanning using tools like Nmap and Wireshark
- Gained exposure to Active Directory environments and sandbox testing

Noaman Shaikh

Karachi, Pakistan | +92 311 3595919 | nomanshykh641@gmail.com

LinkedIn: linkedin.com/in/noaman-shaikh-2151a0216

- Assisted in monitoring network activity and identifying security anomalies

Education

BS Computer Science - Mehran University of Engineering and Technology

Jamshoro, Sindh | Jan 2021 - Nov 2024

Projects

Web Application Penetration Testing Lab (DVWA & OWASP Juice Shop)

- Performed black-box and white-box testing on vulnerable applications using OWASP Top 10 methodology
- Discovered and exploited XSS, SQL Injection, Broken Authentication, and IDOR vulnerabilities
- Used Burp Suite, OWASP ZAP, and manual testing for vulnerability validation

Bug Bounty Practice on HackerOne & Bugcrowd (Simulated Targets)

- Conducted reconnaissance using tools like Nmap, Sublist3r, and Gobuster
- Reported findings such as open redirects, exposed sensitive information, and subdomain takeovers (simulated)
- Followed responsible disclosure principles and created professional-level reports

Wi-Fi Pentesting Lab using Aircrack-ng

- Captured WPA2 handshakes using monitor mode and deauthentication attacks
- Cracked pre-shared keys using dictionary attacks on captured packets
- Gained deeper understanding of wireless protocol weaknesses

Languages

- English: Limited Working Proficiency
- Sindhi: Full Professional Proficiency
- Urdu: Native or Bilingual Proficiency