SHAIK NAWAZ AHMED

Hyderabad, Telangana, India | **8125623108** | shaiknawaz3108@gmail.com | linkedin

CAREER OBJECTIVE

Cybersecurity professional with hands-on experience in network, web, and Active Directory penetration testing. Skilled in executing end-to-end attack simulations, identifying high-risk vulnerabilities, and delivering actionable remediation guidance. Seeking to contribute to offensive security engagements by identifying high-impact risks and improving enterprise security posture.

Regulatory Alignment: Experience mapping pentest findings to ISO 27001 Annex A, SAMA Cybersecurity Framework, and NCA ECC for **compliance-aligned risk reporting and enterprise simulations**.

CORE SKILLS & SPECIALIZATIONS

- **Offensive Security & VAPT:** Web, Network, and Active Directory penetration testing; end-to-end attack lifecycle
- **Active Directory Security:** Kerberoasting, AS-REP roasting, delegation abuse, credential dumping, lateral movement, domain compromise
- **Web & Network Testing:** Authentication/authorization flaws, injections, misconfigurations, privilege escalation
- **Reporting & Risk:** Executive and technical reporting; risk impact analysis; remediation guidance
- **Professional Strengths:** Client communication, independent execution under NDA, team coordination for financial and enterprise environments.

CERTIFICATION

Offensive Security Certified Professional (OSCP) – Offensive Security **Dec 2025**

- Demonstrated ability to compromise **multi-host enterprise environments** under strict time constraints.
- Applied structured methodology for enumeration, exploitation, privilege escalation, and reporting.
- Completed while working full-time in a client-facing offensive security role

Offensive Security Experienced Penetration Tester (OSEP) – Offensive Security **In Progress**

- Advanced red-team training focused on **stealthy intrusions, AV/EDR evasion, custom tooling, and advanced AD attacks**.
- Hands-on exposure to **modern enterprise defences and bypass techniques**

Certified Ethical Hacker (CEH) Practical – EC-Council **July 2025**

- Demonstrated expertise in ethical hacking techniques, penetration testing, and vulnerability assessment aligned with industry-standard methodologies

Google Cybersecurity Professional Certificate – Google **Oct 2024**

- Gained hands-on skills in security operations, threat detection, network defense, SIEM tools, and incident response.

WORK EXPERIENCE

Security Analyst – Offensive Security / VAPT **Jan 2025 – Jan 2026**

Cyber Defentech

- Performed **web application and Active Directory penetration testing** under strict NDA, identifying authentication flaws, misconfigurations, and privilege escalation paths.
- Conducted **internal and external network assessments** to uncover exploitable services and insecure configurations.
- Executed **lateral movement and post-exploitation techniques** to validate real-world attack scenarios.
- Identified and validated a **critical Active Directory misconfiguration** that could have enabled full domain compromise, impacting **300+ employees and sensitive financial data**.
- Produced **detailed technical and executive-level documentation** with impact analysis and step-by-step remediation guidance.
- Reduced critical-risk exposure across **20+ enterprise systems and multiple Tier-1 Active Directory services**.
- **Recognized by the CEO** for delivering high-impact security findings and exceptional reporting quality.
- Client-facing cybersecurity services firm supporting enterprise and financial-sector environments.

Security Analyst Intern – VAPT **Aug 2024 – Sept 2024**

Huntmetrics Pvt. Ltd.

- Specialized in information gathering for applications, focusing on comprehensive reconnaissance and vulnerability identification.
- Utilized tools such as Nmap, Nessus, and Metasploit to assess security vulnerabilities in various applications.
- Documented findings and provided actionable mitigation recommendations to enhance security measures.

KEY ENGAGEMENT HIGHLIGHTS & IMPACT

- Led and executed **end-to-end VAPT engagements** across web, network, and Active Directory environments
- Identified and validated **high and critical-risk vulnerabilities**, including credential exposure and privilege escalation paths
- Demonstrated **full attack-chain compromises**, progressing from initial access to domain-level impact
- Delivered **executive and technical reports** with clear risk impact and prioritized remediation guidance
- Communicated findings effectively to **technical and non-technical stakeholders** under NDA

PROJECT

Active Directory Attack Simulation

- Designed a controlled AD lab simulating a corporate environment.
- Executed attack paths from low-privilege user to domain compromise.
- Tested detection gaps and mapped defensive recommendations.

Hands-on Security Research & Simulations

- Completed **50+ enterprise-style lab environments** simulating real-world attack scenarios (web, Linux, Windows, Active Directory).
- Practiced **end-to-end attack chains**: recon → initial access → privilege escalation → lateral movement → domain compromise.
- Specialized in **Active Directory abuse techniques**: Kerberoasting, AS-REP roasting, delegation abuse, credential harvesting, and persistence.
- Documented enterprise-style lab environments using **ISO 27001, SAMA, and NCA ECC control mapping**, simulating regulatory-aligned penetration testing and compliance reporting.

ACHIEVEMENTS & RECOGNITION

- Ranked in the **Top 10% globally** on **TryHackMe** through consistent enterprise-style lab performance.
- CTF by Computer Society of India Achieved a **114th ranking** out of 500 teams at Lords Institute.
- **Delivered a 3-day hands-on cybersecurity workshop** at Lords Institute, Hyderabad, focusing on ethical hacking fundamentals, reconnaissance, and vulnerability assessment.

EDUCATION

Bachelors of Engineering – Information Technology **November 2021-June 2025**

- **Osmania University, Hyderabad** **8.05 CGPA**
  Lords Institute of Engineering and Technology

TOOLS & TECHNOLOGIES

- Nmap, Burp Suite, Metasploit, BloodHound, Mimikatz, Hashcat, SQLmap, ffuf, winPEAS, PowerSploit, Wireshark, Kali Linux, VMware

COMPLIANCE & FRAMEWORKS

- ISO 27001 Annex A • SAMA Cybersecurity Framework • NCA Essential Cybersecurity Controls (ECC) • NIST • OWASP

ADDITIONAL INFORMATION

- **Soft Skills:** Client risk communication, executive security reporting, compliance-driven documentation, stakeholder presentations.
- **Languages:** English, Hindi, Telugu, Urdu.
- Open to **relocation** to KSA | Available for **immediate onboarding** | Passport-ready