

AMAN KUMAR

Senior Penetration Tester



Professional Experience

Senior Cybersecurity Engineer – Securado LLC, Muscat, Oman

📅 Sep 2021 – Present

- **LLM & AI Security Testing:** Performed adversarial testing on LLM-based applications to identify vulnerabilities such as prompt injection, jailbreaking, data leakage, and model manipulation using automated fuzzing and AI-driven tools.
- **Cloud Security Assessment:** Conducted advanced penetration testing across AWS, Azure, and GCP environments, identifying misconfigurations, exposed assets, and privilege escalation paths through IAM analysis and attack path enumeration.
- **Penetration Testing (Web, Infrastructure & AD):** Executed Black Box and Grey Box assessments on web applications, infrastructure, and Active Directory environments using tools such as Burp Suite, Nmap, Nessus, and CrackMapExec.
- **Web, Mobile & API Security Testing:** Delivered comprehensive security assessments for web, mobile, API, and thick/thin client applications using industry-standard tools and methodologies aligned with OWASP Top 10.
- **Vulnerability Management & Remediation:** Identified, validated, and re-tested vulnerabilities while collaborating with development and IT teams to ensure effective remediation and risk reduction.
- **Secure Configuration Review:** Performed configuration audits aligned with CIS and NIST benchmarks across operating systems, databases, and Active Directory environments.
- **Secure Code Review:** Conducted manual and automated code reviews using tools such as Fortify, SonarQube, and Semgrep to identify security flaws and improve code quality.
- **Network & Security Device Assessment:** Reviewed firewall and network device configurations using automated tools and manual techniques to strengthen overall security posture.
- **Mobile Application Security (Android):** Performed static and dynamic analysis using tools like Frida, Objection, and MobSF to identify application vulnerabilities.
- **Threat Intelligence & Incident Support:** Collaborated with SOC teams for threat analysis, malware investigation, and proactive risk mitigation.
- **Reporting & Stakeholder Communication:** Delivered detailed technical reports and executive summaries with actionable remediation strategies for both technical and non-technical stakeholders.
- **Proof of Concept (PoC) Development:** **Created detailed exploitation scenarios to demonstrate real-world impact of identified vulnerabilities.**
- **Secure Development Practices:** Worked closely with developers to promote secure coding standards and integrate security into the SDLC.

Major Client Projects

- **Government Sector Engagement:** Led a large-scale VAPT engagement covering 200+ servers and 40+ applications, identifying critical vulnerabilities and driving remediation efforts that reduced overall vulnerability exposure by 40%.
- **Leading Shipping & Logistics Company:** Conducted and led enterprise-wide VAPT across 2000+ servers and 65+ applications, uncovering high-risk security gaps and enabling remediation that reduced organizational risk exposure by 80%.
- **Banking Sector (Oman):** Delivered comprehensive VAPT for 1000+ servers and 100+ applications, identifying high-risk vulnerabilities and enabling effective remediation to strengthen overall cybersecurity posture.

Tools Excellence

- **Vulnerability Assessment Tools:** Rapid7, Nessus, Acunetix
- **Penetration Testing:** Burp Suite (Professional/Community), Metasploit, Postman, Kali Linux
- **Network Penetration Tools:** Nmap, Nuclei, Wireshark, Aircrack-ng
- **Cloud & Enumeration Tools:** ScoutSuite, CloudFox, Steampipe, CloudSploit
- **Active Directory Pentesting Tools:** Mimikatz, Crackmapexec, BloodHound, Smbclient, Impacket suite
- **Configuration review Tools:** Nipper, Rapid7, Nessus, Tripwire, Custom Scripts
- **Source Code Review Tools:** Fortify, SonarQube, Semgrep
- **Mobile Application Pentesting Tools:** APK tool, Frida, Objection, Drozer, MobSF
- **Thick Client & Traffic Analysis Tools:** Eco Mirage, Wireshark, Fiddler, Sysinternals Tools
- **Frameworks:** OWASP Top 10, MITRE ATT&CK, NIST, CIS Benchmarks

+96897477285, +917017467165
✉ aman.kumar.ofc10@gmail.com
🌐 [linkedin.com/in/aman-k0b160a184](https://www.linkedin.com/in/aman-k0b160a184)
📍 Mathura, Uttar Pradesh, India

Summary

Offensive Security Professional with 4+ years of experience in Red Teaming and VAPT, delivering security assessments across 80+ clients. Expertise in identifying critical vulnerabilities across web, mobile, infrastructure, and cloud environments. Skilled in translating technical findings into business risks and driving remediation with development and IT teams.

Technical Skills

- Web Application Penetration Testing
- Mobile Application Security Testing
- API Security Testing
- Infrastructure & Network Penetration Testing
- Active Directory Security Assessment
- Cloud Security Testing (AWS, Azure, GCP)
- Wireless Security Testing
- LLM & AI Security Testing
- Threat Hunting & Threat Intelligence
- Malware Analysis
- Attack Surface Management
- Vulnerability Assessment & Penetration Testing (VAPT)
- Black Box & Grey Box Testing
- Secure Code Review
- Configuration & Compliance Review (CIS, NIST)
- Risk Assessment & Mitigation
- Project Delivery & Stakeholder Management
- Client & Vendor Management
- Team Collaboration & Leadership

Education

- **B. Tech | Anand Engineering College, Agra, Uttar Pradesh | Dr. APJ Abdul Kalam Technical University | 2017 – 2021 | 75%**

Professional Certifications

- **OffSec Certified Professional (OSCP) | 2024**
- **EC-Council Certified Ethical Hacker (C|EHv12) ECC6205318497**