Aniket Pagare

Github || Linkedin || Portfolio

Email : aniketpagare1411@gmail.com
Mobile : +919763795323

Education

- **M.S.G College** — Nashik, MH
  Bachelor in Computer Application; CGPA: 8.25 With A+ Grade — *Jan. 2021 – June. 2024*
- **Mankarnika G Patil College** — Shirdi, MH
  Higher Secondary Education — *June. 2018 – July. 2020*

Experience

- **Blue Team Pvt. Ltd** — Baner, Pune
  Vulnerability Assessment And Penetration Tester — *July 2025 - Present*
  - **Vulnerability Assessment**: I conducted vulnerability assessments on web and network infrastructures to identify security weaknesses. I used tools like Nmap, Nessus, OpenVAS, Acunetix, Qualys and Nikto to scan systems, analyze vulnerabilities, and prepare detailed reports with remediation recommendations to enhance overall system security.
  - **Penetration Testing**: As part of my penetration testing tasks, I simulated real-world attacks to exploit identified vulnerabilities using tools such as Metasploit, Burp Suite, and OWASP ZAP. I performed both web and network penetration tests, documented exploitation steps, and proposed mitigation strategies to strengthen system defenses.
- **Sysap Technologies** — Deccan, Pune
  Professional Training & Practical Work — *Jan 2025 - June 2025*
  - **Vulnerability Assessment and Penetration Testing : C**onducted VAPT on web and network systems using tools like Nmap, Nessus, Burp Suite, Metasploit, and OWASP ZAP to identify vulnerabilities, simulate real-world attacks, and provide remediation recommendations to enhance system security.
  - **Digital Forensics**: Practiced evidence acquisition, data recovery, and log analysis during CHFI training using forensic tools to investigate and trace cyber incidents.
  - **Network Security**: Gained hands-on experience in packet analysis and intrusion detection using Wireshark and hping3, analyzing traffic behavior and identifying potential threats..
  - **Web Application Security**: Tested for common OWASP Top 10 vulnerabilities, including SQL Injection, XSS, and CSRF, and documented findings with proof-of-concept exploits and remediation strategies.
  - **Tool Mastery**: Hands-on expertise with tools like Nmap, Burp Suite, Nikto, Nessus, Metasploit, OWASP ZAP, Wireshark, Zenmap, and OpenVAS, Acunetix for scanning, exploitation, and analysis.

Skills

- **Vulnerability Assessment & Penetration Testing (VAPT)**: Nmap, Nessus, OpenVAS, Burp Suite, Nikto, Metasploit, OWASP ZAP
- **Security Information & Event Management (SIEM):** Splunk, Wazuh
- **Web Application Security:** Burp Suite, OWASP ZAP, Acunetix, Nikto, SQLmap
- **Network Security:** Wireshark, hping3, Zenmap, Snort, Cisco Packet Tracer
- **Computer Forensics:** Autopsy, FTK Imager, Volatility, PsTools, Wireshark.

Certification / Achievement

- **EC-Council –** Certified Ethical Hacker (CEHv13) , CCNA (T) , CPENT (T) , CHFI(T) .
- **Cisco –** Introduction to Cyber Security .
- **Mastercard –** Cyber Security Job Simulation .

Projects

- **Internal Network Penetration Testing** : Internal Network Penetration Testing is a security assessment that simulates an attack from inside an organization's network to identify vulnerabilities, misconfigurations, and weaknesses that an insider or a compromised device could exploit.
- **Web Application Penetration Testing** : Tested for OWASP Top 10 vulnerabilities using Burp Suite , OWASP ZAP , Nikto , including SQL Injection and XSS.