GADE NAVEEN

naveen.chowdary5568@gmail.com 9347161675 khammam
linkedin.com/in/naveen-gade-3541482a9 github.com/Naveenchowdary55

CARRER OBJECTIVE

Cybersecurity professional with hands-on experience in Vulnerability Assessment and Penetration Testing (VAPT) across web, network, and API environments. Proficient in using industry-standard tools like Burp Suite, OWASP ZAP, Nmap, Nessus, and Metasploit to identify and exploit vulnerabilities. Experienced in preparing detailed security reports with actionable remediation recommendations to strengthen organizational security posture.

SKILLS

Vapt Tools: Burp Suite, OWASP ZAP, Nmap, Nessus, Metasploit, Wireshark
Web security: OWASP TOP 10, XSS, CSRF, SQL Injection, Authentication Bypass
API Testing: Burp Suite, Postman, JWT Authentication Testing
Operating Systems: Windows, Linux (Kali, Ubuntu)
Networking: TCP/IP, DNS, HTTP, VPN, Firewall, IDS/IPS
Scripting: Python

PROJECTS

MAC Flooding Attack on Switch (vapt)
Tools: macof, Wireshark, Security Onion, Cisco Switch, Packet Tracer/GNS3
Performed a controlled MAC flooding attack using macof to test Layer-2 network security.
Generated spoofed MAC addresses to overflow the switch CAM table and observe fail-open behavior.
Captured and analyzed network traffic with Wireshark after CAM table overflow.
Identified risks such as packet leakage and unauthorized traffic exposure during the attack.
Implemented mitigation techniques including Port Security, limiting MAC address count, and enabling DHCP snooping.
Prepared detailed documentation covering attack methodology, impact analysis, and security hardening recommendations.

Wireshark Network Traffic Analysis
Tools Used: Wireshark, tcpdump, Nmap
Performed detailed packet-level analysis using Wireshark to study network protocols such as TCP, UDP, ARP, DHCP, and DNS.
Captured live network traffic from LAN to identify communication patterns and endpoint behavior.
Analyzed TCP three-way handshake, retransmissions, latency issues, and packet loss indicators.
Investigated suspicious traffic, including ARP spoofing attempts, malformed packets, and unusual port activity.
Created custom display filters and applied color coding for easier protocol analysis and troubleshooting.
Documented findings, security risks, and recommendations for improving network visibility and monitoring.

CERTIFICATES

CEH (Certified Ethical Hacker)
Cybersecurity Certified-Tata
Pre security Certified-Tryhackme

EDUCATION

B.TECH in Electronics and Communication Engineering 2021 – 2025
MLR institute of technology CGPA :71.5

INTERMEDIATE (MPC) 2019 – 2021
Sri Chaitanya Junior Collage PERCENTAGE:91.6

MATRICULATION 2018 – 2019
Sri Vivekananda Vidyalayam CGPA:9.5