

# Gaurav Bidgar

+91-7350351418 | ✉ [gauravbidgar4@gmail.com](mailto:gauravbidgar4@gmail.com) | <https://www.linkedin.com/in/gaurav-bidgar-0019a8251>

## Career objective

Adaptable and motivated cybersecurity professional with hands-on experience and strong attention to detail. Quick learner with solid communication skills, eager to tackle new challenges in a dynamic environment.

## Technical Skills

- **Network Security:** OSI Model, TCP/IP, VPN, Firewalls, Network Protocols
- **Operating Systems:** Windows, Linux, Android
- **Languages:** C, Python, Assembly
- **Log Sources:** Windows Event Logs, Firewall Logs, IDS/IPS Alerts
- **Tools:** Nmap, Wireshark, Nessus, Burp suite, Metasploit, DIE, PEiD, PESTudio, Process Hacker, Regshot, IDA (Basic)

## Cybersecurity

- **Malware Concepts:** PE File Format, Static & Dynamic Analysis, Identifying malicious and clean samples
- **SIEM Tools:** Splunk (dashboard creation, log correlation)
- Vulnerability Assessment, Penetration Testing, Web Application Security
- SOC Monitoring, Incident Response, Log analysis, Threat Intelligence, EDR, Event management, Malware Analysis
- **Security Frameworks:** OWASP Top 10, MITRE ATT&CK, NIST CSF, ISO 27001, Cyber Kill Chain

## Experience

Lumiverse Solution,

Nashik, India

### Jr. Security Analyst Intern

[ Jan 2025 – June 2025 ]

- Performed vulnerability assessments and penetration testing on web applications and networks.
- Identified and reported security weaknesses using tools like Nessus, Nmap, and Burp Suite.
- Analyzed network traffic and suspicious activity using Wireshark.
- Documented findings and recommended remediation steps to improve security posture.
- Collaborated with team to ensure compliance with security best practices and policies.

## Projects

### Port-Scan Analysis

- Performed port scanning on JadeBlue.com using Nmap to identify open ports and potential vulnerabilities.
- Analyzed services running on ports like HTTP, HTTPS, SMTP, and IMAP to assess security risks.
- Used Kali Linux for basic penetration testing and vulnerability assessment.
- Recommended firewall rules, access controls, and regular patching to strengthen security.

### Command Line Anti-virus

- Developed a command-line antivirus scanner for Windows systems.
- Scans a given directory to detect clean and infected files, and deletes virus files.
- Used string-based signatures for detection.
- Reduced false positives by referencing files from Windows and Program Files folders.

## Education

### Bachelor of Engineering (Information Technology)

June-2024

SND College of Engineering Yeola, Nashik (SPPU)

## Certifications

1. Cyber security and Ethical hacking - BIA (Pune)
2. Ultimate ethical hacking - Udemy
3. Google Cyber security - Coursera