

NEERAJ SIHAG

SOC Intern

+91-83073-17903

neerajsihag@protonmail.com

www.neerajsihag.com

linkedin.com/in/neeraj-sihag

WORK EXPERIENCE

eSec Forte Technologies **SOC Intern**

July, 2025 - Present

Worked on SIEM (QRadar) alert triage, incident detection, and false positive validation. Involved in DLP monitoring and dark web threat intelligence activities.

Gurugram Police

June, 2025

Cyber security Intern

Gained hands-on experience in digital forensics, evidence analysis, and red teaming techniques. Assisted in vulnerability assessment and incident investigation.

PROJECTS

Offensive Security Projects

- External & Internal Penetration Testing Lab (Nessus, Metasploit, manual exploitation)
- Advanced Web Application Testing (Burp Suite, OWASP Top 10 exploitation)
- Active Directory Attack Simulation (Kerberoasting, Pass-the-Hash, lateral movement)
- Password Cracking & Credential Attacks (Hydra, Hashcat, wordlist optimization)
- Social Engineering & Phishing Campaign Design
- Post-Exploitation & Persistence Techniques (C2 setup, data exfiltration)

Defensive Security Projects

- SIEM Implementation & Optimization (QRadar, Wazuh, ELK Stack)
- Dark Web Threat Monitoring & Intelligence Correlation
- DLP Policy Configuration & Data Exfiltration Prevention
- Suricata IDS/IPS Network Threat Detection Lab
- Incident Response Simulation (SOC playbook execution, IOC triage)
- Threat Hunting Engagement (APT behavior detection using MITRE ATT&CK mapping)

EDUCATION

CDLU, Haryana
2022-2025

Bachelor of Technology (B.Tech)

- Course - Computer Science (CSE)
- CGPA - 7.4/10

SKILLS

- Penetration testing
- Vulnerability assessment
- Web app testing (Burp Suite, OWASP Top 10)
- Exploitation techniques
- OSINT
- SIEM (QRadar, Wazuh, Splunk)
- Alert triage & incident response
- Threat hunting
- IDS/IPS (Suricata)
- Log analysis
- Malware analysis
- Threat intelligence

CERTIFICATIONS

- CompTIA A+
- ISC2 Certified in Cybersecurity (CC)
- arcX - Foundation Level Threat Intelligence Analyst