

SIDDHARTH NIGAM

CYBERSECURITY VAPT

Gurugram, Haryana ◆ +917289092221 ◆ siddharthnigam002@gmail.com

Aspiring Penetration Tester with Certified Ethical Hacker (CEH) certification and hands-on experience in ethical hacking, threat analysis, and digital forensics. Completed internships at Ernst & Young and SafeYourWeb, where key contributions included solving 170+ security labs and conducting vulnerability assessments that mitigated 80% of critical risks. Strong analytical and problem-solving skills, eager to leverage cybersecurity expertise to enhance organizational security measures.

AREA OF EXPERTISE

- SIEM: Wazuh, Splunk
- EDR/XDR: Palo Alto Cortex, SentinelOne
- IPS/IDS: Snort, Palo Alto Networks
- Firewalls: Palo Alto, Fortinet, Cyberoam
- Network Monitoring: Nmap, Wireshark
- Web Application Testing: OWASP ZAP, BurpSuite
- Operating Systems: Kali Linux, Windows Home, Windows Server 2022
- Programming Languages: Python, C, Java, PHP, Bash

EDUCATION

Bachelor of Technology in Computer and Communication Engineering **Sept 2022 - July 2026**

Manipal University Jaipur, Jaipur, Rajasthan

- GPA (10 point scale): 9.2

PROFESSIONAL EXPERIENCE

VAPT Internship

Ernst & Young - On-site - Gurugram, Haryana

May 2025 - July 2025

- Completed a training-focused internship in the Cybersecurity (VAPT) team, gaining a strong understanding of foundational and advanced concepts in offensive security
- Solved 170+ labs on **PortSwigger Web Security Academy**, covering topics like XSS, SQLi, access control, authentication flaws, and more.
- Completed multiple **Hack The Box (HTB)** rooms, developing skills in enumeration, exploitation, and post-exploitation across Linux and Windows systems.
- Explored real-world attack scenarios using **OWASP Juice Shop**, learning about common vulnerabilities in web applications.
- Studied and practiced the **bug bounty triage** and reporting process, gaining familiarity with tools, writeups, and disclosure practices.
- Enhanced understanding of OWASP Top 10, reconnaissance, and ethical hacking techniques using tools like Kali Linux and Wireshark, leading to improved vulnerability assessment skills

Cyber Security Internship

SafeYourWeb - Remotely

Oct 2024 - Jan 2025

- Conducted vulnerability assessments on 4 projects, identifying and mitigating 80% of critical risks.
- Assisted with security audits, ensuring 100% compliance with industry standards.
- Investigated and Reported security incidents, contributing to a 30% improvement in incident response time.
- Applied security tools like firewalls, IDS/IPS, and encryption in real world environment, reducing unauthorized access attempts by 40%.
- Applied regular security patches and updates, minimizing system vulnerabilities by 90%.
- Researched and analyzed cybersecurity threats, enhancing proactive threat detection by 60%.
- Worked with cross-functional teams, integrating security best practices into 100% of assigned projects.
- Verified security activities and prepared detailed reports, improving risk assessment processes by 25%.

Cyber Security Internship

Wesecure Technologies - On-Site - Rohini, Delhi

May 2024 - July 2024

- Streamlined firewall configurations using Palo Alto Networks, reducing exposure to external threats and enhancing network security
- Assessed and documented performance metrics for 10 cybersecurity tools, creating a comparative analysis that drove the selection of a solution that reduced incident response time by 15%, enhancing overall security efficiency.
- Enforced security policies for mobile devices and remote access, improving data protection and compliance with company standards
- Provided technical support during maintenance using Windows Server 2022, minimizing disruptions and ensuring continuous system availability
- Engaged in cyber-attack simulations using Wazuh and Nmap, enhancing team preparedness and improving incident response strategies

CERTIFICATIONS AND ACHIEVEMENTS

• Certified Ethical Hacker (CEH) – EC Council	• Cisco: Introduction to Cybersecurity
• EC Council Ethical Hacking Essentials (EHE)	• CCNA Training
• NetAcad Ethical Hacker	• ISRO Geo-data Sharing & Cyber Security
• TryHackMe Top 1%	• Oracle DBMS Training

PROJECTS

- **TVR Classifier:** Developed a CNN-based deep learning model to classify network traffic into Tor, VPN, and regular traffic using the CIC-Darknet 2020 dataset. Preprocessed network flow features, applied feature selection using Random Forest, and implemented 1D CNN for classification. Evaluated model performance with accuracy, precision, recall, and confusion matrices. This project enhances network security monitoring and anomaly detection, aiding in threat intelligence and encrypted traffic analysis for cybersecurity and VAPT.
- **AD Security Project:** This project involves setting up and securing a network environment using Active Directory, Splunk, Sysmon, and Atomic Red Team. The goal is to create a simulated network, configure logging and monitoring, and test security measures.
- **SOC Automation Project:** Executed an SOC automation project to streamline incident detection and response. Integrated Splunk for data ingestion, TheHive for case management, Wazuh for host-based IDS, and Sysmon for detailed monitoring. Automated security event correlation, improving real-time monitoring and threat response efficiency.
- **ERP-SYS:** Developed a full-stack monorepo application for Manipal University Jaipur to streamline KPI creation, assignment, submission, and approval workflows across 30+ departments. Implemented role-based access (QC, HoD, Coordinators, Faculty), real-time analytics dashboards, and multi-level approval pipelines. Tech stack: Next.js, NestJS, Prisma, PostgreSQL (Supabase), Docker, Turborepo.

PROFILES

- [Github Profile](#)
- [LinkedIn Profile](#):
- [TryHackMe Ranking](#)