Jaymeet Patel

(630) 464-4830 *jaymeet5087d@gmail.com* *913 S Western Ave, Chicago, IL* *linkedin.com/in/jaymeet2003*

Professional Summary

Proactive Cybersecurity Professional practitioner with hands-on experience in threat detection, network security, and incident response. Specializes in simulating attacks and fortifying systems using tools like Wireshark, Scapy, Python, and AWS. Developed systems that reduced fraud by 92%, cut DNS spoofing alert time by 40%, and enhanced threat classification pipelines. Passionate about building scalable, secure infrastructures and contributing to teams that value innovation, reliability, and impact.

Education

Depaul University, Chicago, IL *Jun 2027*
Masters of Science in Cybersecurity — **Concentration:** Networking and Infrastructure

University of Illinois Chicago, Chicago, IL *Dec 2024*
Bachelor of Science in Computer Science — **Minor:** Mathematics
Bachelor of Business Administration in Business Administration
Awards: 3× Dean's List Recipient
Relevant Coursework: Network Security, Cryptography, Concurrent Programming, Data Science, Database Systems, Algorithms, Data Structures, Networking

Projects *github.com/jaymeet2003*

ScamurAI (Fraud Detection Firewall) *Apr 2025*

- Engineered a decentralized firewall using ML models to detect fraudulent transactions with 92% accuracy in under 1.5 seconds.
- Integrated P2P alerting via Gun.js and deployed a React-based dashboard for real-time threat visualization.

Honeypot (Intrusion Detection) *Aug 2024 – Dec 2024*

- Simulated SSH/HTTP services using Python to bait attackers, capturing 1,000+ unique intrusion attempts.
- Automated threat categorization, reducing intelligence reporting time from 10 minutes to 5 minutes.

Malicious Proxy Server *Aug 2024 – Dec 2024*

- Developed a transparent proxy server using socket programming to intercept HTTP/HTTPS traffic.
- Reduced unauthorized transmission by 40%, flagging suspicious patterns in real-time.

DNS Poisoning Detection System *Aug 2024 – Dec 2024*

- Designed a hybrid tool integrating Wireshark traffic inspection with Python-based anomaly detection.
- Cut spoofing detection time by 40%, decreasing remediation delays during testing phases.

DNS Injection Simulation *Aug 2024 – Dec 2024*

- SCrafted forged DNS packets using Scapy and dnspython to simulate injection attacks across 3 configurations.
- Strengthened internal testing protocols, improving DNS security validation coverage by 60%.

Skills

Cybersecurity Tools: Wireshark, Scapy, OpenSSL, Honeypots, Squid Proxy, DNS Analysis, Penetration Testing, Incident Response, Vulnerability Assessment.
Languages & Frameworks: Python, C++, Java, C, Golang, R, Node.js, Flask, Django, FastAPI, SQL, MongoDB.
Cloud & DevOps: AWS, Azure, Docker, Kubernetes, Git, REST APIs.
Data & Machine Learning: Pandas, NumPy, Scikit-learn, XGBoost.
Core Competencies: Threat Modeling, Secure System Design, Packet Analysis, Intrusion Detection, Secure Code Review.
Soft Skills: Problem Solving, Analytical Thinking, Team Collaboration, Communication, Leadership.

Certifications

- EC-Council — Applied Data Loss Prevention *Jun 2025*
- EC-Council — Digital Forensics for Pentesters - Hands-on Learning *Jun 2025*
- IBM & ISC2 — Cybersecurity Specialist Certification *Feb 2025*
- Cybrary — PenTest+: Tools and Code Analysis *Jan 2025*