Veetarag Vardhaman Patil

Bangalore, India — +91 7417437513 — veetaragpatil333@gmail.com — github.com/veetaragpatil — linkedin.com/in/veetarag-patil

SUMMARY

Results-driven Computer Science graduate with hands-on expertise in network engineering, TCP/IP architecture, routing protocols (OSPF, BGP fundamentals), LAN/WAN administration, and network security. Proven ability to conduct vulnerability assessments, monitor and analyze network traffic, and harden enterprise infrastructure. Seeking a Network Engineer role to design, deploy, and secure scalable network environments.

EDUCATION

B.Tech in Computer Science & Engineering — Sanjay Ghodawat University, Kolhapur *Sep 2022 – Jun 2026 — GPA: 7.65/10*
Coursework: Computer Networks, Network Security, Network Administration, Operating Systems, Data Structures

CERTIFICATIONS & TRAINING

Cisco CCNA (in progress – actively studying) — **CompTIA Network+** (in progress – actively studying)
Cyber Security 101 – TryHackMe — **Ethical Hacking & Web Penetration Testing** – Udemy

TECHNICAL SKILLS

Routing & Switching	OSPF, BGP (fundamentals), EIGRP (fundamentals), STP, VLANs, Inter-VLAN Routing, Trunking, EtherChannel
Protocols	TCP/IP, OSI Model, DNS, DHCP, HTTP/S, FTP, SSH, ICMP, ARP, NAT, IPSec, VPN, MPLS (concepts), Subnetting
Network Security	Firewall Configuration, ACLs, IDS/IPS, Network Traffic Analysis, Vulnerability Assessment, CVSS
Monitoring & Tools	Wireshark, Nmap, Nessus, Snort, Cisco Packet Tracer, SNMP (concepts), Metasploit, Kali Linux, VirtualBox, Git
Languages & OS	Python (network automation), Bash scripting, HTML/CSS — Linux (Kali, Ubuntu), Windows Server

EXPERIENCE

Network Security Intern (CyberSecurity) — Theta Dynamics Pvt. Ltd., Belagavi, Karnataka *Jan 2026 – Jun 2026*

- Conducted network reconnaissance with Nmap across 200+ hosts, mapping live hosts, open ports, and running services to define the full network attack surface.
- Deployed Nessus vulnerability scanner to audit 50+ network-facing services; correlated scan results with manual testing and prioritized 5+ critical findings by CVSS score.
- Engineered and delivered a comprehensive VAPT report documenting network topology, 15+ exposed endpoints, and remediation recommendations aligned to NIST/CIS security standards.
- Remediated identified vulnerabilities by reconfiguring firewall rules (iptables/ACLs) and tightening access controls, reducing the network attack surface by an estimated 40%.

PROJECTS

Home Network Lab – Routing, Switching & Monitoring — *Kali Linux, VirtualBox, Cisco Packet Tracer, Wireshark*

- Designed and deployed a virtualized multi-segment enterprise network across 4 VLANs with inter-VLAN routing, simulating LAN/WAN topology using VirtualBox and Cisco Packet Tracer.
- Configured OSPF-style static routing between segments; practiced STP, trunking, and EtherChannel concepts in Packet Tracer simulations.
- Performed continuous network monitoring with Wireshark, capturing and analyzing 500+ ARP, DNS, ICMP, and TCP packets; configured iptables ACLs to block unauthorized traffic.

Network Traffic Analysis & Intrusion Detection Lab — *Wireshark, Snort, Kali Linux, Python*

- Simulated 5+ real-world network attacks (port scanning, ARP spoofing, brute-force SSH) and deployed Snort IDS rules to detect and alert on malicious traffic in real time.
- Performed deep packet inspection on 10+ .pcap files using Wireshark; identified attack signatures, anomalies, and lateral movement indicators.
- Automated threat log parsing with Python scripts; produced structured SOC-style incident reports aligned to real-world network operations workflows.

ACHIEVEMENTS

- Completed 10+ hands-on labs on TryHackMe and VulnHub (Top 10% ranking) covering network enumeration, traffic analysis, privilege escalation, and web exploitation.
- Built and actively maintain a personal home lab replicating enterprise network topology with routers, switches, firewalls, IDS, and multi-VLAN segmentation.