Naveen Jonnakuti

Cyber Security Analyst

Ph:9391800353 **naveenprabhas070@gmail.com** **LinkedIn** **GitHub** **Portfolio**

SUMMARY

I am a dynamic and results-driven Cyber Security Professional with a solid foundation in information security principles, technologies, and best practices. I am eager to contribute to a forward-thinking organization by leveraging my strong technical expertise, analytical skills, and proactive approach to safeguarding digital assets and minimizing security risks. In addition to cybersecurity, I also have hands-on experience in **Flutter application development**, enabling me to design and secure mobile applications with a strong focus on performance, usability, and data protection.

EXPERIENCE

Cyber Security Analyst

Datavalley.ai

2025 Vijayawada

Cybersecurity Analyst

Datavalley.ai — Vijayawada, India

- Conduct **threat detection, vulnerability assessments, penetration testing, and incident response** to protect enterprise networks and applications.
- Monitor and analyze security events, identifying anomalies using industry tools such as **Nmap, Wireshark, Burp Suite, and Metasploit**.
- Implement and enforce **security policies, firewall rules, and intrusion detection/prevention systems (IDS/IPS)** to safeguard digital infrastructure.
- Research and apply security frameworks (**NIST, OWASP, MITRE ATT&CK**) to strengthen organizational security posture.
- Mentor students and professionals in **ethical hacking, secure coding, malware analysis, and cloud security practices**, guiding over **500+ learners** toward certifications such as **CEH, CompTIA Security+, and OSCP**.
- Conduct workshops and hands-on labs simulating **real-world cyberattacks**, enhancing learner skills in **threat intelligence, phishing detection, and digital forensics**.
- Highlight your accomplishments, using numbers if possible.

Jr. Network Engineer

Negen

2024 Vijayawada

Jr. Network Security Engineer | Negen Diagnostic (2023 – 2024)

- Assisted in the **implementation of network security measures**, including firewall configurations, VPN setups, and access control policies.
- Performed **network traffic monitoring and log analysis** to identify anomalies, unauthorized access attempts, and potential intrusion indicators.
- Supported **server deployment and hardening** by applying security patches, updating firmware, and configuring secure protocols.
- Conducted **application maintenance and vulnerability checks**, ensuring availability and resilience against cyber threats.
- Allocated and managed **IP addressing, VLANs, and subnet configurations** to improve network efficiency and segmentation security.
- Assisted in **incident response activities**, including isolating compromised systems, documenting events, and providing recommendations for mitigation.
- Collaborated with the IT team to enforce **security best practices**, reducing the organization’s attack surface.
- Contributed to **documentation and reporting** of network changes, incidents, and preventive measures for compliance and auditing.
- Highlight your accomplishments, using numbers if possible.

EXPERIENCE

Jr. System Administrator Intern

ITechServ

📅 2023 📍 Mohali

- Assisted in **installing, configuring, and securing** Windows and Linux servers, ensuring optimal performance, uptime, and adherence to security baselines.
- Monitored **network performance and system logs** to detect anomalies and potential security issues, escalating incidents to senior staff.
- Managed **user accounts, access controls, and patch updates**, improving system security posture and reducing vulnerabilities.
- Supported **firewall configurations and endpoint protection measures**, contributing to network defense efforts.
- Conducted routine **backup, recovery, and disaster recovery drills** to maintain business continuity.
- Assisted in **documenting security incidents, system changes, and troubleshooting steps**, creating reusable knowledge for the team.
- Collaborated with senior administrators to learn and apply **cybersecurity best practices (least privilege, patch management, hardening)** across systems.
- Highlight your accomplishments, using numbers if possible.

SKILLS

Programming & Scripting: HTML · CSS · JavaScript · Python Scripting · Bash Scripting · Flutter

- Vulnerability Assessment & Penetration Testing (VAPT)
- Web, Mobile, and API Security Testing
- OWASP Top 10 & SANS Top 25 exploitation techniques
- Vulnerability Scanners (Nessus, Qualys, OpenVAS, Acunetix)
- Manual Testing with Burp Suite, SQL Map, Hydra, and custom scripts
- Application & API Security
- API Penetration Testing (Authentication, Rate Limiting, JWT, OAuth2)
- Phishing Detection & Prevention Techniques
- SSL/TLS, Secure Headers, and Encryption mechanisms
- Network Security
- Firewall Configuration & Access Control
- IDS/IPS (Snort, Suricata) Deployment & Monitoring
- Network Traffic Analysis (Wireshark, Tcpdump)
- VPNs, VLANs, and Secure Network Design
- Security Tools & Frameworks
- Nmap, Metasploit, Go buster, Dir buster, Hydra, Net cat
- C2 Frameworks (Silver, others)
- Threat Analysis & Incident Response
- MITRE ATT&CK, OWASP, and NIST Cybersecurity Framework
- Scripting & Automation
- Python & Bash for Security Automation
- Log Analysis & Threat Hunting scripts
- Linux Security Hardening & Shell Scripting
- Cloud Security
- Information Security
- Network Security
- Application Security
- Linux Security
- Firewall Configurations
- Intrusion Detection Systems
- Security Audits
- Documentation and Reporting

EDUCATION

Bachelor of Technology (Specialization in Cyber Security) - CT University

CT University, Ludhiana, Punjab | 2019 – 2023

- Specialized in **Cybersecurity, Networking, and Information Security** with hands-on labs and projects.

PROJECTS

Phishing Detection Platform (PS-2: AI Grand Challenge) (State-Level Project)

2025 Vijayawada

Short summary of your work

- Designed an AI/ML-based phishing detection framework to identify malicious domains/URLs targeting Critical Sector Entities (CSEs).
- Implemented techniques including domain similarity analysis, DNS/WHOIS metadata evaluation, and web content inspection for phishing classification.
- Developed a continuous monitoring and alerting workflow for new domains, hosted infrastructure (e.g., ngrok), and social media sources.
- Automated reports with domain metadata, phishing indicators, screenshots, and CSE mapping to support real-time threat intelligence.
- **Tools & Tech**: Python, Scikit-learn, NLP, WHOIS, DNS Analysis, Flask/Stream lit

Phish Shield: Simulation & Detection of Phishing Attacks

2025 Vijayawada

Short summary of your work

- Built an AI-driven phishing URL detection system integrating datasets like URL Haus and custom phishing simulation.
- Implemented machine learning-based URL classification and a Flask/stream lit dashboard for real-time phishing analysis.
- Extended features with GeoIP/WHOIS lookups, Chrome Extension integration, and CSV upload scanning for batch detection.
- **Tools & Tech**: Python, Flask, stream lit, ML Models, SQLite/PostgreSQL, Chrome Extension APIs.

Deep Web Intelligence Scraper for Threat Detection

2025 Vijayawada

Short summary of your work

- Designed a dark web and deep web threat intelligence platform to detect phishing, leaks, and brand misuse.
- Leveraged the Tor network, web scraping (Beautiful Soup, Requests), and NLP models (Spacy, NLTK) for real-time intelligence gathering.
- Built an interactive stream lit dashboard for security teams to visualize high-risk domains, keywords, and threat actors.
- Tools & Tech: Python, Beautiful Soup, Tor, Spacy, NLTK, Scikit-learn, stream lit

Intrusion Detection & Prevention System using Snort

2025 Vijayawada

Short summary of your work

- Designed and deployed an Intrusion Detection & Prevention System (IDPS) using Snort to detect and mitigate DNS flood and DDoS attacks.
- Configured custom Snort rules to identify malicious traffic patterns, unauthorized access attempts, and anomalous behaviors.
- Integrated log monitoring and alert generation for real-time incident response and reporting.
- Conducted performance testing and successfully reduced network downtime by mitigating simulated DoS/DDoS threats.
- **Tools & Tech**: Snort, Linux, TCPDump, Wireshark, Python, Shell Scripting

Hybrid Neural Networks for Anomaly Detection in CPS

Date period Vijayawada

Short summary of your work

- Engineered a hybrid deep learning model (CNN + LSTM + Autoencoder) to detect anomalies in Cyber-Physical Systems (CPS).
- Enhanced detection accuracy and reduced false positives by analyzing spatial, temporal, and behavioral patterns.
- Benchmarked performance on CPS datasets, achieving superior results compared to traditional anomaly detection methods.
- **Tools & Tech**: Python, TensorFlow, Kera's, NumPy, Pandas.

INTERNSHIPS

Cyber Security Internship – IBM Skills Build (via Edu-net Foundation)

- Successfully completed
  cybersecurity internship under the **IBM SkillsBuild Program**, gaining
  practical knowledge of **introductory, beginner, and intermediate
  cybersecurity concepts**.
-
- Acquired hands-on
  understanding of **cybersecurity methodologies, tools, and frameworks**,
  focusing on security fundamentals and practical applications.
-
- Strengthened knowledge in **threats,
  vulnerabilities, and defense mechanisms**, applying learning to
  real-world scenarios.

INDUSTRIAL TRAINING

Industrial Training – Palo Alto Networks, Ludhiana

- Completed 45-day industrial training program focused on **Cybersecurity and Networking Fundamentals**.

- Gained practical exposure to **firewalls, malware detection, threat identification, and network traffic monitoring**.

- Learned and applied concepts of **network security, intrusion detection, and malicious content analysis** through guided labs and real-time case studies.

- Enhanced knowledge in **cybersecurity operations, network security policies, and defensive strategies**.

CERTIFICATIONS

Palo Alto Networks : Fundamentals of Network Security

Palo Alto Networks: Fundamental SOC (Security Operations Center)

Cisco: Introduction to Cyber Security

Alison: Computer Networking - Wired and Wireless protocols

Google: Introduction to Cloud Security