YARRAMSETTY VISHNU VARDHAN

vishnuvardhansetty14@gmail.com | +91 9676524560 | www.linkedin.com/in/vishnuvardhan14

PERSONAL STATEMENT:

Strong hands-on experience in IT support and cybersecurity. With a strong foundation in risk assessment, compliance and IT security principles, I am dedicated to safeguarding digital assets and mitigating cyber threats. I have a proven track record of enhancing cybersecurity postures through implementing robust security measures and conducting comprehensive security awareness and data protection training. My strong analytical skills, combined with a passion for problem-solving and continuous learning, equip me to tackle complex cybersecurity challenges.

EDUCATION:

B.Tech in Electronics & communication Engineering, (**6.98 CGPA)** 2021 - 2024

Narasaraopeta Institute of Technology

Diploma in Electronics & communication Engineering, (77%) 2018 - 2021

Loyola Polytechnic College

SKILLS:

- **Web Application Security:** Burp Suite, OWASP Top 10
- **Network Security:** Nmap, Wireshark, Metasploit, Nessus
- **SIEM Tools:** Splunk, Qradar
- **Networking:** TCP/IP, DNS, ARP, ICMP, Firewall, VPN, IDS/IPS, EDR/XDR
- **Operating System:** Linux, Windows, Windows server
- **Programming & Scripting:** Shell Scripting.
- **Security Models:** CIA Triad, Cyber Kill Chain, MITRE ATT&CK
- **Cybersecurity Frameworks**: NIST, ISO 27001

PROJECTS:

Deploying and Managing a Network Firewall:

- Configured and managed a **Pfsense firewall**, achieving a **30% improvement in network traffic efficiency** by implementing optimized rules and policies. Excellent Problem solving under analytical skills like Pcap analytics using wireshark.
- Conducted **detailed monitoring and analysis** of network logs, identifying and mitigating **90% of potential security threats** in the test environment.
- Utilized Wireshark for **deep packet inspection (DPI)** and improved **incident resolution time by 25%** through advanced traffic analysis.
- Generated comprehensive traffic reports, documenting **100% of network usage patterns** to enhance system audits and policy enforcement.
- Implemented and configured a firewall in a virtual environment, reducing unauthorized access attempts by **40%** while monitoring logs and traffic patterns.

SOC Home Lab (Splunk & Qradar) :

- Deployed and configured **Splunk and IBM QRadar** in a Security Operations Center (SOC) environment, ensuring real-time monitoring, log analysis, and incident response.
- Developed custom correlation rules and dashboards to detect anomalies, suspicious login attempts, and potential threats, **enhancing threat visibility by 40%**.
- Aggregated and analyzed security logs from firewalls, endpoint security solutions, and network devices using Splunk's SPL and QRadar's AQL, improving log management efficiency.
- Created security use cases based on the MITRE ATT&CK framework to detect privilege escalation, brute-force attacks, and insider threats, **reducing security breaches by 30%**.
- Generated detailed security reports and compliance dashboards aligned with NIST and ISO 27001, ensuring regulatory compliance and audit readiness.

EXPERIENCE:

Cartel Software September202 - July2024

Cybersecurity Intern:

- Conducted vulnerability scanning of targeted domains, identifying open ports, private directories, and exploitable weaknesses in source code.
- Performed penetration testing, including SQL injection testing, brute force attacks, and application analysis using tools such as Hydra and Burp Suite to identify critical vulnerabilities.
- Prepared detailed technical reports outlining findings and providing actionable recommendations to enhance system security and resilience.
- Developed critical thinking, problem-solving, and analytical skills through structured internship tasks and projects.

Edunet Foundation June 2023 - July 2023

Cybersecurity Internship:

- Conducted comprehensive vulnerability assessments to identify security weaknesses in systems and networks.
- Monitor and analyze security events from various sources including SIEM tools, logs, and alerts.
- Configured and managed firewalls, IDS/IPS, and VPNs to ensure secure network communication.
- Monitor the Network Infrastructure Systems and applications using network monitor tools to ensure optimal performance and availability.
- Developed and enforced security policies and procedures to maintain a secure IT environment.

JOB ROLE IN CYBERSECURITY DOMAIN:

- Vulnerability Management
- Security Specialist
- Incident Responder
- Cybersecurity Engineer
- Network Security Engineer
- IT Security Specialist
- Security Operations Centre Analyst
- Penetration Tester

CERTIFICATIONS:

- **Certified Ethical Hacker CEHv12** - EC-Council – ECC9306457812
- **Google Cybersecurity Professional Certificate** - Coursera
- **Cisco CyberOps Associate** - Cisco
- **Cisco IT Essentials** - Cisco
- **Tata Cybersecurity Analyst Job Simulation Certificate.**
- **Splunk completion of Certificate** - Splunk
- **Ethical Hacking Essentials (EHE)** - EC-Council
- **Completion of the CTF** - Hack the box.

DECLARATION:

I hereby declare that statements made are true and correct to the best of my knowledge and belief**.**

Date: 14/03/2025

Signature
Yarramsetty Vishnu Vardhan