

Sandeep Banothu

7995739465 | sandeepnayak7995@gmail.com | LinkedIn
Hyderabad, India

SUMMARY

Recent MBA(IT) graduate with a passion for IT. Detail-oriented and results-driven cybersecurity enthusiast with a passion for protecting sensitive information.

Well-versed in skills, Networking, Firewalls, Mitree Attack, Kali linux, Splunk, Nessus, Wireshark. Seeking a challenging role to leverage technical expertise and contribute to innovative security solutions.

Education

Osmania University - Holy Mary Institute of Technology & Science
MBA (IT)

Hyderabad (TG)
2022-2024

Experience

Deepija Telecom Pvt Ltd | IT Executive

Hyderabad | Jan 2023 - Sep 2023

- As a dedicated engineer within the organization, I provided technical support to our internal team.
- My responsibilities included troubleshooting and resolving both software and hardware issues, ensuring efficient operations and minimal downtime.
- Utilized Grafana to monitor server performance and health, Tracked key metrics such as CPU usage, memory utilization, Storage.
- Managed Data center operations and maintenance, Troubleshoot and resolved network connectivity and performance issues.
- Deploying network infrastructure components, including cables, racks, and Hardware deployment.
- Configuring basic network settings, such as IP addressing & DHCP.

Ersegement Pvt Ltd| Pentesting - Intern

Hyderabad | Jan 2024 - July 2024

- As an intern, Conducted Vulnerability Assessment on various web application, Generated and presented reports on security vulnerabilities to respective organizations.
- Proficient in understanding application level vulnerabilities like XSS, SQL Injection, LFI & RFI and SSL certificate etc.
- Vulnerability Assessment of various web applications used in the organization using Burp suite.
- Experience in using kali linux to do web application assessments with tools like NMAP, Hydra, Sqlmap and Nikto.
- I collaborate with trainers to assist students in the institute with any questions or any doubts they have regarding the bug bounty program.

Skills

Technologies : Firewalls, Networking, IDS & IPS

Tools : SIEM, Splunk, Wireshark, Nmap, Kali linux, Nessus

Framework : Mitree Attack Framework, Cyber kill Chain

Projects

DOS Detection Using SNORT IDS

- Deployed and configured Snort IDS on a kali Linux environment to monitor network traffic for suspicious activities.
- Created and customized Snort rules to detect various network-based attacks (e.g., port scanning, DoS attempts).