

KULSUM NAZMEEN . SHAIK

Phone: +91 9347715518

Email: kulsumnazmeen@gmail.com



JOB SUMMARY

Motivated and detail-oriented Cyber Security Analyst with a strong foundation in ethical hacking and information security. Skilled in identifying vulnerabilities, mitigating threats, and implementing robust security measures to safeguard organizational networks and systems. Seeking a dynamic position in a challenging environment to contribute to the enhancement of security frameworks and ensure the protection of critical information assets. Proven ability to stay ahead of emerging threats and deliver innovative security solutions for growth-driven organizations.

RESPONSIBILITIES :

- Knowledge of Cyber Security principles and concepts .
- Worked on multiple Vulnerability Assessment & Penetration Testing Projects related to Network/Infrastructure, Web Applications.
- Hands-on-experience in manual and automated penetration testing.
- Knowledge in Information Security principles including risk assessment, threat and vulnerability management, intrusion detections/prevention.
- Performed Log Analysis, Malware Analysis & Threat Hunting.
- Phishing Detection, Spam Email, and IP Address, Domain Name Reputation Analysis
- Knowledge on Cyber Kill Chain and understanding of MITRE ATT&CK® framework Methodology
- Network Protocol Analysis using with Wireshark
- Knowledge on handling various types of incidents across multiple security solutions such as Firewall, IDS/IPS.
- Basic Knowledge in understanding TTP's detected by EDR solutions.
- Knowledge understanding of OWASP Top 10, IDS, IPS, Threat modelling and Cyber Attacks like DOS, DDOS, MITM, SQL Injection, XSS and CSRF.

CERTIFICATION

CERTIFIED ETHICAL HACKER (CEH) from EC-COUNCIL ECC6042783915

TECHNICAL SKILLS:

<u>OPEN-SOURCE INTELLIGENCE</u>	: OSINT Framework, Spider foot,
<u>NETWORK PENTEST TOOLS</u>	: Nmap, Nessus Professional, Metasploit Framework
<u>WEB APP PENTEST TOOLS</u>	: Burp Suite Professional, SQL Map, Nikto, WPSCAN
<u>SIEM TOOL's</u>	: Splunk Enterprise, Open EDR
<u>MALWARE ANALYSIS</u>	: PEid, CFF Explorer, PESTudio, Regshot, Procmon, Procexp, Sysmon
<u>PHISHING ANALYSIS</u>	: PhishTank, urlscan.io, AbuseIPDB, Virus Total, Mx Toolbox
<u>OPERATING SYSTEM</u>	: Kali / Parrot Security Linux OS, Windows & Virtualization Software
<u>Forensic Tools</u>	: FTK Imager, Autopsy, Ease US Data Recovery, OS Forensic

PROFESSIONAL EXPERIENCE:

INTERNSHIP:

Currently Working in **BERRY9 IT SERVICES PRIVATE LIMITED**, Hyderabad as an Cybersecurity Analyst - Intern from August 2024 to till date.

PROJECT #1

Project Name: Network/Infrastructure Penetration Testing & Web Application Penetration Testing

Duration: 4 months

Description: I participated in 10+ network/infrastructure, web application penetration testing project work activities. As per my role, I did vulnerability assessment scans and penetration testing using Nmap, Tenable Nessus, Metasploit Framework & Burp suite Professional. I reported all issues with proof of concepts and remediations.

PROJECT #2

Project Name: SOC Environment Setup & Improving Threat Detection (DFIR)

Duration: 2 Months

Description:

I participated in implementation of SOC Environment setup using Splunk SIEM, OpenEDR, Sysmon ..etc.

- Configured custom alerts for detecting anomalous behaviour
- Correlated logs from different sources (firewalls, endpoints) to identify potential threats.

ACADEMIC DETAILS:

Degree BCA in - Priyadarshini Degree College , Kothagudem - 2023
Intermediate MPC in - Sri Nalanda Junior College , Kothagudem -2020
10 (CBSE) in - Nava Bharath Public School ,Palvoncha -2018

DECLARATION:

I hereby declare that the above-mentioned information is correct up to my knowledge and I bear the responsibility for the correctness of the above-mentioned particulars