Suyog L

Cyber-Security Engineer

+91 9972340414 suyogln26@gmail.com Bengaluru
linkedin.com/in/suyog-l-856b86304 suyogln.github.io/Portfolio/ suyogln

Profile

Cybersecurity Engineer with professional experience and hands-on internship experience in system engineering. Skilled in Ethical Hacking, Vulnerability Management, Vulnerability Assessments, and Penetration Testing (VAPT), with expertise in simulating cyberattacks, implementing defense strategies, and configuring security infrastructure such as firewalls and IDS. Proven ability to assess risks, automate operations, and contribute to cybersecurity initiatives. Passionate about continuous learning, I aim to become a leader in cybersecurity and contribute to securing digital infrastructures globally.

Areas of Expertise

- **System Engineer:** Proficient in setting up, configuring, and troubleshooting server environments to ensure optimal performance and reliability.
- **Cybersecurity Fundamentals:** Developed a strong foundation in cybersecurity principles, including threat detection, risk assessment, incident response, and providing End-Point security.
- **Network Security:** Familiarity with securing networks, implementing firewalls, and monitoring network traffic for potential vulnerabilities.
- **Vulnerability Assessment and Penetration Testing (VAPT):** Skilled in conducting vulnerability assessments, simulating cyberattacks, performing penetration testing, and applying OWASP Top 10 framework for identifying web application vulnerabilities.
- **Ethical Hacking:** Proficient in performing ethical hacking activities, including network penetration testing, web application security testing, social engineering, and identifying and exploiting system vulnerabilities.
- **Tools Expertise:** Hands-on experience with tools like Metasploit, Burp Suite, Nmap, Nessus, Wireshark, OpenVAS, and Kali Linux for vulnerability scanning, exploitation, and reporting.
- **Operating Systems:** Experience working with various operating systems, including Linux and Unix-based systems.
- **Continuous Learning:** Committed to staying updated with the latest cybersecurity trends, technologies, and best practices.

Professional Experience

DeepByte Technology Private Limited – Sister Company of Repalogic GmbH 01/09/22 - 31/12/22

System Engineer (Intern)

- Configured Intrusion Detection Systems (IDS) using Snort to monitor and analyze network traffic for potential threats.
- Configured firewalls using iptables to control inbound and outbound network traffic, ensuring secure communication.
- Utilized Git for version control to manage and maintain code repositories, ensuring seamless collaboration and deployment.
- Assisted in server automation tasks using Ansible to streamline the configuration and management of server environments.

DeepByte Technology Private Limited – Sister Company of Repalogic GmbH 01/01/23 - 18/06/24

Cyber-Security Engineer

- Conducted comprehensive vulnerability assessments and penetration testing (VAPT) for both web applications and networks, using industry-standard tools such as Nmap, Metasploit, Nessus, and Burp Suite.
- Led vulnerability management efforts by identifying, evaluating, and mitigating security risks in the organization's infrastructure, utilizing tools like Nessus, OpenVAS, and CVE databases to ensure adherence to the latest security protocols.
- Regularly conducted phishing simulations by sending random phishing links to management team members as part of an awareness campaign, aimed at educating them about the risks of clicking on unverified links. This initiative focused on protecting sensitive company information, including financial data and internal communications, by reinforcing the importance of cautious online behavior.
- Developed an automated Python application for network mapping and generating PDF reports using LaTeX, improving efficiency in network security assessments and report generation.
- Used OWASP Top 10, MITRE ATTCK, and NIST Cybersecurity Framework to assess risks and recommend remediation for web and network vulnerabilities. These frameworks guided threat modeling, vulnerability identification, and security controls, enhancing risk mitigation, threat detection, and compliance.
- Participated in ethical hacking activities, including red teaming, exploit development, and post-exploitation techniques, to simulate real-world cyberattacks. Collaborated with my German colleagues experienced in ethical hacking and red teaming to stay current with the latest hacking trends and continuously improve my skills. Focused on understanding human psychology, particularly in social engineering, to develop strategies for influencing individuals to interact with malicious links, both within the organization and client environments.
- Utilized a variety of security tools for vulnerability scanning and remediation, including Nikto, Gobuster, DirBuster, Postman, Wfuzz, and Burp Intruder, to identify and mitigate potential vulnerabilities.
- Ensured compliance with security standards and best practices across the organization's infrastructure and applications.

Freelancer – Vulnerability Management and VAPT *(MINDORIGIN Private Limited)* **Remote** *20/05/24 - 13/11/24*

- Conducted vulnerability assessments and penetration tests based on client requirements, ensuring adherence to OWASP Top 10 and industry standards.
- Delivered customized security solutions, including web application and network penetration testing, tailored to clients' infrastructure.
- Generated comprehensive reports with detailed remediation strategies and presented findings to stakeholders.
- Used tools such as Nessus, OpenVAS, Burp Suite, OWASP ZAP, and Wireshark to identify and mitigate vulnerabilities effectively.
- Collaborated with development teams to remediate security vulnerabilities, ensuring secure coding practices and robust application security.
- Delivered client-specific reports, including risk assessments, technical details, and strategic solutions to enhance cybersecurity resilience.
- Contributing to the secure management of sensitive financial data, focusing on compliance with industry regulations and best practices.

Freelancer – Vulnerability Management *(Fincelerate Private Limited)* **Remote** *08/06/24 - Present*

- Conducted vulnerability assessments and penetration tests based on client requirements, ensuring adherence to OWASP Top 10 and industry standards.
- Delivered customized security solutions, including web application and network penetration testing, tailored to clients' infrastructure.
- Generated comprehensive reports with detailed remediation strategies and presented findings to stakeholders.
- Used tools such as Nessus, OpenVAS, Burp Suite, OWASP ZAP, and Wireshark to identify and mitigate vulnerabilities effectively.
- Collaborated with development teams to remediate security vulnerabilities, ensuring secure coding practices and robust application security.
- Delivered client-specific reports, including risk assessments, technical details, and strategic solutions to enhance cybersecurity resilience.
- Contributing to the secure management of sensitive financial data, focusing on compliance with industry regulations and best practices.

Director and CEO *(Matrica Networks Private Limited)* **On-site** *15/12/2024 - Present*

- Leading the development of a **Cybersecurity Software Platform** tailored for small and medium-scale organizations, focusing on data protection, risk assessment, and threat mitigation.
- Providing comprehensive **cybersecurity services**, including penetration testing, vulnerability assessments, and policy implementation, to strengthen client security frameworks.
- Directing the creation of an **E-Commerce Platform**, ensuring scalability, user-friendliness, and seamless online transaction processes for diverse businesses.
- Overseeing business operations, including strategy development, financial planning, and team management, to ensure consistent growth and operational excellence.
- Building and mentoring a cross-functional team, fostering innovation and collaboration to achieve project milestones and deliverables.
- Expanding the client base by offering tailored **cybersecurity solutions** to small and medium enterprises, enhancing their resilience against cyber threats.
- Enhancing the **Cybersecurity Software Platform** by integrating advanced technologies such as AI-driven threat detection and real-time monitoring.
- Collaborated with stakeholders to refine the **E-Commerce Platform**, focusing on usability and market competitiveness.
- Continuously identifying new growth opportunities and developing strategic partnerships to increase revenue and market presence.

Education

Master of Technology Computer Science specialization in Cyber-Security *PES University* **PES, India** *2022-2024*

Bachelor of Engineering in Computer Science *Visvesvaraya Technological University* **KSSEM, India** *2016-2022*

Skills

- **Network Penetration Testing:** Nmap, Metasploit, Nessus, OpenVAS, Wireshark, TCP/IP, VPN, IDS/IPS, Firewall Testing, Network Traffic Analysis, Netcat, Hydra, Aircrack-ng, Nikto, Netdiscover, John the Ripper, Scapy.
- **Web Application Penetration Testing:** Burp Suite, OWASP ZAP, SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Web Vulnerability Scanning, Authentication Flaws, Data Encryption/Decryption, OWASP Top 10, Nikto, Gobuster, DirBuster, Postman, Wfuzz, Burp Intruder.
- **Vulnerability Assessment & Management:** Nessus, OpenVAS, Maltego, Nikto, CVE databases.
- **Ethical Hacking:** Red Teaming, Exploit Development, Phishing Attacks, Social Engineering Attacks, Post-Exploitation Techniques, Cobalt Strike.
- **Networking:** Nmap, Cisco Packet Tracer, Network Monitoring, Firewall Configuration, IDS/IPS, VPN, TCP/IP, DNS, HTTP/S, FTP, SMB, Tcpdump, Netcat, Wireshark, OpenVPN.
- **Programming & Scripting:** Python, JavaScript, Basics of Bash Scripting.
- **Databases:** MySQL, MongoDB, SQLite.
- **Operating Systems & Tools:** Ubuntu, Parrot OS, macOS, Kali Linux, BlackArch Linux.
- **Cybersecurity Frameworks:** OWASP, OSINT Framework, MITRE ATTCK, NIST Cybersecurity Framework.
- **Others:** Computer Hardware, Wireless Network Attacks, LaTeX, Virtualisation, Docker, Git.

Achievements

- **1st place award** for an IoT-based project at an undergraduate exhibition, demonstrating exceptional problem-solving and technical innovation.

- **Published research papers** in IJERT journal on blockchain technology, advancing knowledge in cybersecurity.
- **Led vulnerability management efforts**, significantly reducing security risks across critical infrastructure.
- **Developed an automated network security reporting tool** using Python, improving efficiency and reducing time spent on vulnerability assessments.
- **Enhanced organizational cybersecurity awareness** through regular phishing simulations, strengthening risk mitigation strategies.
- **Achieved compliance with OWASP Top 10 and NIST Cybersecurity Framework**, reinforcing robust security measures for web and network systems.

Certifications

- **Cisco Cyber-Security Introduction**
- **Kali Linux**
- **Cisco Networking Essentials**
- **Cisco Ethical Hacker Badge**
- **Cisco Python Essentials -1**
- **Cisco Python Essentials -2**
- **Cisco JavaScript**