J MANASSA SATHVIKA

Email: [manassasathvikajps@gmail.com] | **Phone:** [+91 94892 68239]
LinkedIn: [J.Manassa Sathvika] | **GitHub:** [J.Manassa Sathvika]

Objective:

Aspiring Cybersecurity Engineer with a strong foundation in computer networks, penetration testing, and hands-on experience in solving CTF challenges and conducting web vulnerability assessments. Seeking to leverage my technical skills and problem-solving mindset to contribute to cybersecurity initiatives at Palo Alto Networks.

Area of Interest:

1.Cybersecurity & Ethical Hacking - Vulnerability Assessment, Web Penetration Testing, Ethical Hacking, Steganography
2.Capture the Flag (CTF) & Security Challenges - Web Exploitation, Cryptography, OSINT, picoCTF
3.Computer Networking & Security Tools - Wireshark, Nmap, Burp Suite, Metasploit Framework, Kali Linux
4. Programming & Scripting - Java, Python, C, Bash, Data Structures

Education:

Bachelor of Engineering in Computer Science with Cyber Security | Dr.Mahalingam College of Engineering and Technology, Anna University, Pollachi.
Year of Study : 2023 – 2027 | **CGPA** : 9.522
HSC | Shaanthi School, Jothi Nagar, Pollachi - 642001
June 2023 |**12th Mark** : 512 | **Percentage :** 85.33
SSLC | Shaanthi School, Jothi Nagar, Pollachi - 642001

Skills:

Technical Skills

- **Cybersecurity:** Penetration testing, vulnerability assessment, ethical hacking, CTFs
- **Networking**: Nmap, TCP, UDP, OSI layers, multiplayer logic for game development, server and client scripts for game development
- **Security Tools**: Burp Suite, Wireshark, Nmap, Metasploit Framework, Kali Linux
- **Web Development:** HTML
- **Programming Languages:** Java, Python
- **Database Management:** SQL, Python

Soft Skills

- **Problem-Solving:** Strong analytical thinking and root cause analysis in cybersecurity scenarios
- **Communication**: Excellent verbal and written
- **Team Management:** Experience collaborating during CTFs, workshops and virtual internships
- **Creativity:** Applies creative approaches to solve security challenges and threat simulation

Projects:

Machine Exploitation (Windows & Linux Environments) **[05.04.2025] to [15.04.2025]**
Tools: Metasploit, Searchsploit, Dirbuster, Hydra, LinPEAS, WinPEAS
• Successfully exploited and gained root/system access on CTF machines simulating real-world infrastructure.
• Attacked Windows systems (Windows 7, Windows 10, Windows Server) and Linux-based targets.
• Used EternalBlue exploit (MS17-010) on Windows 7 (HTB Blue)
• Executed post-exploitation tasks including credential dumping, privilege escalation, and persistence.
• Documented attack paths and provided hardening steps for Windows & Linux hosts.

Vulnerability Assessment & Penetration Testing (VAPT) on Web Applications (Live Websites) **[08.05.2025] to [20.05.2025]**
Tools: Burp Suite, OWASP ZAP, Nmap, SQLmap, Nikto
• Performed black-box and gray-box testing on personal and authorized web applications.
• Detected and exploited web vulnerabilities including SQL Injection, XSS, CSRF, and Broken Access Control.
• Used Burp Suite Pro for request manipulation and session hijacking.
• Created detailed technical reports with CVSS scores, PoC screenshots, and mitigation strategies.

Internships:

Cybersecurity Intern – Forage: **[06.08.2024] to [08.09.2024]**
• Participated in a virtual internship focused on cybersecurity theory, tools, and best practices offered by Forage.

• Gained knowledge in network security, threat analysis, vulnerability management, and common attack vectors.
• Completed simulated tasks on identifying phishing attempts and configuring basic firewalls in a virtual lab environment.

AICTE Cybersecurity Virtual Internship: **[15.02.2025] to [14.03.2025]**

• Completed a government-recognized internship through the AICTE Internship Portal focused on practical cybersecurity training.
• Worked on basic cybersecurity tools and applied theoretical knowledge to practical threat scenarios.
• Created sample incident response documentation for simulated breaches and reported vulnerabilities.

Cybersecurity Intern – Prompt Infotech: **[10.06.2025] to [11.07.2025]**

• Completed a hands-on cybersecurity internship at Prompt Infotech with a focus on practical threat detection and mitigation.
• Worked on real-time security assessment tasks including vulnerability scanning, malware analysis, and log monitoring.
• Assisted in configuring SIEM tools and generating daily reports for anomaly detection.

Certifications:

• **Certified in Complete Guide to Ethical Hacking – Udemy** (Instructor: Stone River eLearning, Duration: 42 hours, Certificate ID: UC-0300c4f7-6ffe-42b0-9aee-44f576f7df32).
• **Certified in Networking Essentials – Cisco Networking Academy** (Digital badge earned for completing core networking modules).
• **Certified in Linguaskill – Cambridge English** (Assessed in reading, listening, and writing; demonstrated English proficiency for academic and workplace use).

Achievements:

• Participated in picoCTF *2025*, the world's largest cybersecurity Capture The Flag (CTF) competition;
• Solved diverse challenges across web exploitation, cryptography, forensics, and OSINT.
• Contributed to a team ranking of **133rd out of 10,460 teams worldwide**

Extracurricular Activities:

• Club member at Doodler Fine arts Clubs