

Deepak sivan

Cybersecurity Engineer

✉️ sivandepak143@gmail.com ☎️ +91 8848517748 🗺️ Kerala . India 📅 04/06/1999

🔗 deepaksivan.in 💬 LinkedIn 🐾 GitHub 🌐 TryHackMe

👤 Profile

Computer Engineering graduate and Cybersecurity Engineer with expertise in both offensive and defensive security. Skilled in **web penetration testing**, with hands-on experience in identifying and exploiting common web vulnerabilities. Proficient in **SOC operations**, including real-time monitoring, **incident investigation**, and response. Combines a hacker's mindset with a defender's approach to enhance system protection and strengthen overall security posture.

📁 Projects

Intelligent Threat Detection and Response System with Wazuh SIEM, Suricata IPS/IDS, and Shuffle SOAR SOC Project - [Prototype - 2025]

- Built a security automation system with Wazuh SIEM, Suricata (IDS/IPS), and Shuffle SOAR.
- Used Wazuh for log analytics and Suricata for network threat detection.
- Automated incident response with Shuffle SOAR.
- Created custom detection rules and log pipelines for real-time alerting.
- Used a Telegram bot to block IPs, terminate threats, and control endpoints.
- Integrated with Git, Jira, and ticketing workflows.

IoT-Based Smart Security Car Robot with Web-Based Control and Live Sensor Feedback

IoT-Based Smart Security Robot - [Final Year BE Computer Science Engineering - 2021]

- Developed an IoT smart security robot using Arduino UNO and ESP8266, connected via JioFi.
- Built a web interface with HTML, CSS, jQuery for real-time remote control.
- Integrated temperature, ultrasonic, PIR, gas, and light sensors for monitoring.
- Enabled live data streaming to the web dashboard for real-time feedback.

Smart Billing System with Automated Email Reporting using Python

Python Application Development [U.N.I.Q - Technologies -2018]

- Developed a lightweight desktop billing software using Python and Tkinter.
- Designed an intuitive GUI for product entry, total calculation, and transaction storage.
- Scheduled to automatically send billing summaries via email in .txt format.

All-in-One Offensive Security Toolkit: Python-Based Recon, Exploitation, and Response Automation

Offensive Security Toolkit Project - [Prototype - 2024]

- Designed a security automation toolkit using Python and shell scripting.
- Automated web reconnaissance: domain scraping, JS file analysis, and API token detection.
- Included modules for WiFi attacks like deauthentication and handshake capture.
- Built a custom IDS/IPS simulation for behavioral detection testing.
- Linked all tools into a single executable shell script for one-click offensive operations.

Certificates

1 Year Cybersecurity Training Program - [Prototype , Kochi] [11/2024 - 12/2025] – Completed intensive hands-on training in cybersecurity, including penetration testing, Security Operations Center (SOC) practices, web application security, Android and iOS mobile security.

1 Month Cybersecurity Internship Program - [Quovadis Robosofttech , Thiruvananthapuram] [06/2019] – Completed foundational training in Linux fundamentals, networking basics, and CTF (Capture The Flag) methodologies. Gained exposure to structured cybersecurity learning paths and hands-on guidance through beginner-level CTF challenges.

14 day Python Application Development Internship - [U.N.I.Q Technologies , Coimbatore] [11/2018] – Completed a focused internship on Python-based application development. Gained hands-on experience in designing desktop applications using Python and GUI frameworks. Developed mini projects involving user input, data storage, and automation logic.

Cybersecurity Education through Udemy Premium Courses – [Learn Ethical Hacking From Scratch](#)
Instructor: Zaid Sabih (z Security) | [Learn Python & Ethical Hacking From Scratch](#) Instructor: Zaid Sabih (z Security) | [Website Hacking / Penetration Testing](#) Instructor: Zaid Sabih (z Security) | [Learn Bug Bounty Hunting & Web Security Testing From Scratch](#) Instructor: Zaid Sabih (z Security) | [Wireshark: Packet Analysis and Ethical Hacking – Core Skills](#) Instructor: David Bombal | [The Complete Networking Fundamentals Course – Your CCNA Start](#) Instructor: David Bombal | [Bash Beginners Course: Become a Bash Scripting Superhero!](#)
Instructor: Herbert Lindemans | [The Complete Cyber Security Course: Hackers Exposed!](#) Instructor: Nathan House

Education

Bachelor of Computer Science and Engineering 06/2017 – 08/2021
Dhanalakshmi Srinivasan College of Engineering Coimbatore, India

Higher Secondary Education (HSE) 06/2015 – 04/2017
Bio-Maths | Directorate of Higher Secondary Education Kerala, India

Secondary Education 03/2015
Board: Central Board of Secondary Education (CBSE) Kerala, India

Skills

Cybersecurity – Burp Suite | OWASP ZAP | Nmap | Metasploit Framework | Postman | Docker | Network Security Fundamentals | SIEM tools (e.g., Wazuh, Shuffle) | Wireshark | Syslog monitoring | VirtualBox | Web Application Security & Bug Bounty | Mobile Security Testing (Android & iOS)

Programming & Scripting – Python | Bash | HTML | CSS | Bootstrap | JavaScript | SQL | SQLite | Node.js | MongoDB | Arduino (C/C++ based)