ARYA DHAWALE

Cybersecurity
Engineer

+91-8668935524 | Pune,India | https://aryadhawale.me | aryadhawale93@gmail.com

PROFILE

I'm a Cybersecurity Engineer with practical experience across a wide range of areas—including AI,Cloud, Web, Mobile, and IoT security. I've worked on securing different types of infrastructure by following best practices, running vulnerability assessments and penetration tests, and using frameworks like the CIS benchmarks. I enjoy digging into potential threats before they become real issues, managing vulnerabilities, and building secure systems that actually work in the real world. I also have a solid understanding of how security fits into overall operations—from risk mitigation to staying compliant with industry standards.

WORK EXPERIENCE

MosChip Technologies - Cybersecurity Intern **JAN 2025-NOW**

- **Cloud Security Infrastructure:**
  - Implemented Azure Security Center policies.
  - Used Microsoft Defender for Cloud for threat detection.
  - Monitored security events with Microsoft Sentinel.
  - Configured Azure Firewall for network security.
  - Onboard and monitor security logs using Microsoft Sentinel.
- **Web Application VAPT and Reporting:** Conducted security assessments, identified vulnerabilities, and created detailed reports with remediation steps.
- **Android Application VAPT and Reporting:** Performed vulnerability assessments for mobile applications and documented findings for security improvements.
- **Understanding CIS Benchmarks:** Gained proficiency in applying CIS benchmarks to enhance system and network security.
- **IoT Security with Azure Defender:** Secured IoT devices using Azure Defender for IoT, monitoring activity and mitigating risks.
- **Vulnerability Masterlist and Guidelines:** Created a masterlist of vulnerabilities with guidelines for secure coding practices.
- **AI Security:** Performed security assessments of AI Models to detect and mitigate risks including unauthorized access, data manipulation, and potential misuse.

SKILLS

- **Web Application Penetration Testing:**
  BURP SUITE | NESSUS | OWASP-ZAP | WIRESHARK | NMAP | ACUNETIX | SSLYZE | SQLMAP | NUCLIE | NIKTO | HYDRA.
- **Android Application Penetration Testing:**
  APKTOOL | ADB | JADX | OWASP-MASVS | MOBSF | GENNYMOTION | BURP SUITE.
- **Cloud Security:**
  MICROSOFT AZURE | MICROSOFT DEFENDER FOR CLOUD | MICROSOFT SENTINEL | AZURE FIREWALL | SPLUNK (SIEM) | SNORT.
- **Programming Languages:**
  JAVASCRIPT | HTML | CSS | PYTHON.
- **Soft skills:**
  COMMUNICATION | TEAMWORK | ADAPTABILITY | PROBLEM SOLVING | TIME MANAGEMENT.

PROJECTS

Real time air quality prediction and alert system using AI

KEY SKILLS: | PYTHON | TENSORFLOW | KERAS | DASH | PLOTLY | APSCHEDULER | OPENAQ API |

- DEVELOPED AN AI-DRIVEN SYSTEM TO PREDICT AQI LEVELS USING CNN-LSTM MODELS.
- COLLECTED REAL-TIME DATA FROM OPENAQ API.
- CREATED AN INTERACTIVE DASHBOARD USING DASH AND PLOTLY FOR AQI VISUALIZATION.
- IMPLEMENTED AUTOMATED SMS/EMAIL ALERTS WHEN AQI DROPPED TO UNSAFE LEVELS.

IP Discover Tool

KEY SKILLS: | PYTHON | NETWORKING | SCRIPTING | SOCKET PROGRAMMING | AUTOMATION |

- DEVELOPED A PYTHON-BASED COMMAND-LINE TOOL DESIGNED TO EFFICIENTLY DISCOVER ACTIVE DEVICES.
- LEVERAGING SOCKET PROGRAMMING AND ARP REQUESTS, THE TOOL AUTOMATES THE PROCESS OF SCANNING IP RANGES AND IDENTIFYING CONNECTED HOSTS.
- THIS PROJECT SERVES AS A VALUABLE ASSET FOR NETWORK ADMINISTRATORS AND PENETRATION TESTERS.
- THE OPEN-SOURCE NATURE OF THE TOOL MAKES IT EASILY EXTENSIBLE FOR ADDITIONAL NETWORKING UTILITIES AND ADAPTABLE TO VARIOUS ENVIRONMENTS.

Port Scanner Tool

KEY SKILLS: | PYTHON | NETWORKING | SCRIPTING |

- AUTOMATION AND IMPLEMENTED A PYTHON-BASED PORT SCANNER TO IDENTIFY OPEN PORTS ON REMOTE SERVERS, SUPPORTING CUSTOMIZABLE IPS AND PORT RANGES.
- THE TOOL UTILIZES MULTI-THREADING FOR EFFICIENT AND RAPID SCANNING, OUTPUTTING DETAILED REPORTS THAT ASSIST IN VULNERABILITY ASSESSMENT AND NETWORK INVENTORY MANAGEMENT.
- WITH A USER-FRIENDLY COMMAND-LINE INTERFACE AND COMPREHENSIVE ERROR HANDLING, THE PROJECT OFFERS PRACTICAL VALUE TO CYBERSECURITY PROFESSIONALS AND SYSTEM ADMINISTRATORS. THE CODEBASE IS FULLY DOCUMENTED AND ORGANIZED, ENABLING EASY EXTENSION FOR ADDITIONAL SCANNING FEATURES AND INTEGRATION INTO BROADER SECURITY TOOLKITS.

SYN Flood attack script

KEY SKILLS: | PYTHON | NETWORKING |

- CREATED A PYTHON SCRIPT TO SIMULATE SYN FLOOD DENIAL-OF-SERVICE (DOS) ATTACKS, PRIMARILY FOR EDUCATIONAL AND SECURITY TESTING PURPOSES. THIS TOOL DEMONSTRATES HOW TCP/IP VULNERABILITIES CAN BE EXPLOITED TO OVERWHELM TARGET SERVERS, ALLOWING USERS TO CUSTOMIZE PAYLOADS, SOURCE IPS, AND PORTS FOR FLEXIBLE TEST SCENARIOS.
- EMPHASIZING ETHICAL HACKING AND RESPONSIBLE USAGE, THE SCRIPT AIDS IN UNDERSTANDING DOS MITIGATION TECHNIQUES AND SECURITY BEST PRACTICES. IT FEATURES REAL-TIME FEEDBACK AND LOGGING TO MONITOR ATTACK PROGRESS, AND IS INTENDED FOR CONTROLLED, EDUCATIONAL ENVIRONMENTS TO HELP USERS BETTER COMPREHEND NETWORK SECURITY THREATS

EDUCATION

SAVITRIBAI PHULE PUNE UNIVERSITY **2021-2025**

Dr. D.Y. Patil institute of technology, pimpri , pune
B.E. Computer Engineering with honors in Cybersecurity | CGPA : 8.08

CERTIFICATIONS

- Meta (Facebook) data analytics - Coursera
- AI Governance Certification from Securiti
- AI with python - Great Learning
- SQL injection attacks - Eccouncil