FARIS AVULAN

Information Security Consultant

OBJECTIVE

To strive for excellence in Cyber Security with dedication, focus, proactive approach, positive attitude, and passion. I aim to utilize my knowledge and skills in the best possible way for the fulfillment of organizational goals and learning along the journey.

SKILLS:

- **Good knowledge of Vulnerability and Risk Management**
- **In-depth knowledge of network and application vulnerabilities and ability to articulate their impact to business users**
- **Ability to conduct web application and mobile security assessments and handle vulnerability remediation of applications**
- **Ability to recognize, value, and include different perspectives, experiences, approaches, and cultures in achieving organizational goals**
- **Conducted Cybersecurity Workshop in Banglore college (VIT)**
- **Conducted and was a part of cyber security awarest classes to the Indian Navy Officers, Delhi. (Virtual Mode)**
- **Proven track record of identifying and mitigating complex security vulnerabilities.**
- **Investigated a ransomware attack by analyzing compromised systems, identifying the attack vector, and assessing the extent of the damage.**

EDUCATION

BACHELOR OF COMPUTER APPLICATION,
Information Security and Mobile Application
(ISMA), Jain University, Bangalore.

Masters in Science
Cyber security
Amity University, Jaipur

WORK EXPERIENCE

Company: Arridae Infosec Pvt Ltd.
Domain: Information Security.
Designation: Information Security
Consultant. Experience: 2020 - Present

ROLES

- **Vulnerability Assessment of Network and Applications.**
- **Network Penetration Tester.**
- **Web Application Penetration Tester.**
- **API Vulnerability Assessment and Pentesting**
- **Vulnerability Management of Network and Applications.**
- **Penetration testing of Mobile Applications (iOS and Android).**
- **SOC Engineer. (L1)**
- **Source code review .**
- **Cyber forensics.**

RESPONSIBILTIES

- **Planning, Execution and Manage projects or contribute to committee or teamwork.**
- **Understanding of web application security concepts and standards, checking for vulnerabilities in application as per OWASP and SANS guidelines.**
- **Performing Vulnerability Assessment of Servers, Network devices, Access Points and Security devices.**
- **Hands on Experience in IBM Security APPSCAN regarding the Scanning configuration and understanding of predefined policies.**
- **Mobile Application Security: Conducted thorough mobile app security assessments based on OWASP Mobile Top 10, identifying issues such as insecure data storage, improper platform usage, and reverse engineering vulnerabilities.**
- **Identify information security weaknesses and/or gaps in the client operations and work with the stakeholders to bring information security operations up to industry standards and best practices.**

TOOLS

- KALI LINUX
- BURPSUITE
- IBM APPSCAN
- NESSUS
- NMAP
- WIRESHARK
- SQLMAP
- METASPLOIT
- MOBSF
- ADB
- AUTOPSY
- WIFI PINEAPPLE TETRA
- ACCUNETIX
- NETSPARKER
- AIRCRACK-NG
- GENYMOTION
- SONARQUBE
- WAZUH
- HIVE
- CORTEX
- MISP
- SHUFFLER
- OPENVAS
- INVICTI PROFESSIONAL
- QUALYS
- ACCESS FTK MANAGER
- OXYGEN RECOVERY

- Create detailed risk assessment reports which explain identified security weaknesses, describe potential business risks, present prioritized recommendations for remediation, and estimate costs and effort levels for remediation.

- Analyzing findings in investigative matters, and develop fact-based technical reports detailing events over specified periods of time. Prepare reports and documents case details, development and outcome.

- Successfully participated in four rounds of empanelment exams for my organization , demonstrating advanced technical skills. Identified and exploited back door vulnerabilities, compromising four systems effectively.Recognized and appreciated by the team for exceptional problem-solving and technical acumen.

- Knowledge of proper forensic investigation techniques when working with compromised system images or files. Global mind-set for working with different cultures and backgrounds.

- Provide customer consultation involving validation evidence, exposure, remediation, recommendations, and risk posture to both executive management and technical teams

- Created and implemented a complete SOC service by integrating numerous tools into one and was the L1 Engineer under it. (cyberalcon)

- Developed comprehensive threat models and performed risk assessments to identify potential attack vectors and prioritize mitigation strategies.

- Adept at explaining technical security findings to both technical and non-technical stakeholders, ensuring actionable remediation plans are understood and implemented.

DECLARATION

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