JASH PATEL

+1 (905) 922-2351 | jashdetroj@gmail.com | www.linkedin.com/in/jashdetroj/ | github.com/jash2810

Education

Ontario Tech University, Oshawa, Ontario, Canada — January 2021 - Pursuing
Master of Information Technology Security, GPA – 4.20/4.30

Gujarat Technological University, Ahmedabad, Gujarat, India — March 2015 – April 2019
Bachelor of Information Technology, CGPA – 8.41/10

Coursework

Advanced Communication Networks, Security Policies and Risk Management, Attack & Defence – Metasploitable and Honeypots, Law and Ethics in IT Security, Biometric Access Control and Smart Card Technologies, Cryptography and Secure Communication, Operating System Security, Secure Software System, Information and Network Security, Computer Networks, Data mining and Business Intelligence

Technical Skills

Software Tools: Wireshark, Metasploit, tcpdump, forcepoint, paros proxy, nmap, truecrypt, burp suite, splunk, snort, SEIMs, Netflow, Nessus, Git, MySQL, MongoDB, MS Office
Cloud Technologies: Amazon Web Services (AWS) VPC, EC2 and S3, MIME cast, webroot, solarwind security event manager
Cyber Security Frameworks:, ISO27001, ISO27002, NIST 800-53, NIST CSF
Programming Languages: Python, JavaScript, SQL, C++, C#, R language
Web Frameworks: React JS, Angular JS, DJango, Laravel, React-Native
Operating System: Windows (Windows Server 2003/08/12/16), Linux (Red Hat, Ubuntu, and Kali Linux)

Professional Certifications and Achievements

- CompTIA Security+ by Udemy
- AWS Certified Cloud Practitioner (Pursuing)
- Cisco Certified Network Associate (CCNA) by Udemy
- Python 3 for offensive PenTest by Udemy
- OWASP top 10 by Udemy

Key skills & Competencies

- Web Application Security Assessment
- Secure Code Review Assessment
- Penetration Testing
- Risk and Vulnerability Assessment
- Log Analysis using tools like Splunk
- Python 3.0, Linux Shell Scripting
- Fluent Communication Slills in English
- Problem Solving ability using programming languages.

Professional Experience

The Macrosoft Solutions — Ahmedabad, India
Cyber Security Analyst and JS Developer - Internship: — Sept 2020 – Mar 2021

- Training on analysis of network logs of an organization using Splunk to detect suspicious activities and notifying to the team.
- Training on security assessment tools such as Burp Suite, Wireshark and Nessuss.
- Detecting network intrusions and analysis of network traffic.
- As a JS (JavaScript) developer, I took care of validating the data that has been sent and received through the web to avoid malicious activities such as SQL Injection attack.
- Analyze security test results and presenting it in a graphical manner to the team highlighting the probable vulnerable factors that needs to be improved in the network.
- Training of secure code review of a web application using tools like Burp.

Academic Projects

Implementing Dijikstra's Algorithm in SDN network using Python:

- The objective of this project was to understand the usage of SDN controllers in computer networks. The Dijkstra Algorithm was implemented in a mesh topology along with the SDN controllers. The path and node information was shared with the controller and the shortest path was calculated for each possibility accordingly. The network consisted of 6 switches and 11 hosts in it.

Honeypot Demonstration – Kippo & Pentbox:

- For this project, two machines were used as an attacker and a victim machine. The victim machine had a kippo honeypot installed in it and was vulnerable to SSH attacks. The SSH attack was performed from the attacker machine running on Kali Linux. A deep analysis and report of the attack were created based on the results shown by kippo honeypot. Pentbox - a penetration testing tool has a honeypot in it which was also used to check the web-based attack activities.

Exploiting Metasploitable Box using MSF in kali linux

- this project includes different phases of an attack performed. At first, the victim's IP address is scanned and enumerated, and then some settings are changed using the MSF Console and finally gaining the access to the victim system and using the meterpreter shell to take the screenshots of the victim system to trace what the user is doing on screen.

Buffer Overflow Attack (Server Version)

- understanding and exploiting the buffer-overflow vulnerability on the server which is running the malicious code for buffer overflow. In this project, an exploit code was written in python in which the payload for the badfile is prepared and then this badfile is sent to the vulnerable server to exploit the vulnerability.

Biometric Authentication System using Python (Face Recognition and authentication)

- This is a biometric technology-oriented project developed using python and OpenCV. Other python libraries such as face_recognition and NumPy were also used. It stores the user information along with their images while the process of registration. But, when the user comes back, it opens the camera, scans the face, and provides accurate authentication accordingly.

Research/Survey Papers

- Usability of Authentication Methods and Privacy Concerns in Online Communications
  https://drive.google.com/file/d/1B931UYLbVaSMTC3FD5lMjExTqJCIDbEg/view?usp=sharing
- Survey on 5G Network Softwarization, Slicing and Virtualization
  https://drive.google.com/file/d/1UcuSfMq2qBYoFkeda4aFkCDI9tmIjBQ9/view?usp=sharing