Iftekharul Haque

Cybersecurity | Software Engineer | Web Developer
+88 01886-829707 | Dhaka, Bangladesh | shuvrohawk@gmail.com |linkedin.com/in/iShuvro

Profile Summary

- Security Analyst with experience in **SOC operations**, **web vulnerabilities**, **threat hunting**, and **incident response**, seeking to transition into cybersecurity after 2 years as a full-stack web developer.
- Proficient in building **generative ai**, **machine learning models for malware detection**, **SOC infrastructure automation**, and enhancing **cloud security architectures**.
- Adept at collaborating with cross-functional teams in **cybersecurity, software developers, and cloud architecture**, delivering **proactive threat detection, OSINT** and advanced **digital forensics**.
- Skilled in crafting **AI-driven applications** and integrating cutting-edge monitoring/response tools to safeguard against emerging cyber threats.

Relevant Coursework

- Data Structure & Algorithms
- Software Security
- Network
- Web & Android App Development
- Machine Learning
- Software Quality and Testing
- Operating System
- Artificial Intelligence

Experience

Cybertech Defense — **San Diego, CA (Remote)**
Security Analyst (Intern) — **May 2024 - October 2024**

- Conducted ethical hacking, penetration testing, AI, Python, and Bash with a good understanding of the MITRE ATT&CK Framework
- Built and tested a machine learning model using EMBER dataset for malware detection.
- Implemented a comprehensive security framework for Kaizen Cloud infrastructure by deploying and configuring Wazuh for real-time threat detection, the Hive for incident response management, and Shuffle for orchestrating automated workflows.
- Built and monitored SOC operations within clients cloud infrastructures. Also utilized Elastic and Splunk SIEM stacks, providing AI-assisted cybersecurity testing and event monitoring services, while ensuring compliance with cybersecurity regulations.
- Threat hunting with proactive TTPs to detect threat actors in simulated enterprise environments using Wireshark, VirusTotal, and Splunk.
- Led a comprehensive malware threat-hunting exercise in a simulated lab environment, utilizing advanced packet analysis tools such as Splunk, Wireshark, and RSA NetWitness. Identified and analyzed malicious traffic patterns to mitigate potential risks, while improving network security monitoring protocols.
- Developed an MVP drone detection system using Roboflow CV.
- Completed over 75 modules from OffSec from WEB200, SOC200, TH200 and IR200 courses.

Kaizen Apps — **Remote**
Full-stack Web Developer — **June 2023 - February 2024**

- Developed full stack web applications using React.js, Next.js, Node.js, and other modern Js frameworks.
- Deployed web apps on deployment platforms like Vercel and cloudflare.
- Created AI-powered applications utilizing OpenAI APIs, including chatbot using Llama-3 LLM to summarize medical records.
- Enhanced communication and project management skills through regular interactions with offshore clients and offshore teams.

SKILLS

- **Languages:** Python, C/C++, JavaScript//Node.js, React.js/Next/js
- **Data Management**: NoSQL, MongoDB, MySQL, PostgreSQL, Elastic Search, Firebase
- **Cloud Networking & Cybersecurity**: AWS, GCP, Linux, Ubuntu, Debian, Unix, Mac, FTP / TCP / IP, XML/JSON, ELK, Wazuh, Splunk, Vercel, Cloudflare, Shell Scripting, Bash, PowerShell, Zsh
- **Artificial Intelligence & Machine Learning**: TensorFlow, Keras, PyTorch, OpenAI API, Deep Learning, Natural Language Processing (NLP), Chatbots, Text Analysis, Feature Extraction

- **Software Development**: Backend, Frontend, python, HTML, CSS, Node.js, Express, OpenCV, SQL, API Integration, React.js, Next.js, DevOps, GitHub, Clickup, Slack

EDUCATION

ISLAMIC UNIVERSITY OF TECHNOLOGY (IUT) **2021 - Present**
Bachelor's of Science in Software Engineering **Dhaka, Bangladesh**

PROJECTS

MALWARE DETECTION USING MACHINE LEARNING

Description

Built and tested a machine learning model using EMBER dataset. Here used the EMBER codebase to train and test the model. Built custom malware PE files using encoder and wrapper to test the model extensively as well.

Tools

EMBER dataset, Malware, Jupyter Notebook.

KAIZEN CLOUD SOC AUTOMATION SETUP

Description

Built a SOC automation system integrating Wazuh, theHive, Shuffle, and Sysmon, optimizing IDS/XDR for threat detection. Designed monitoring infrastructure for Kaizen Apps using ELK stack and SOAR EDR in a Proxmox environment with Docker-based deployments.

Tools

Windows 10 VM, Linux Container, Wazuh, Shuffle, theHive, Sysmon, Elasticsearch, Logstash, Kibana, SOAR EDR.

1337SHEETS, A PREMIUM CYBERSECURITY NEWSLETTER

Description

Leet Sheets Premium Cybersecurity Write-ups is a platform associated with Cybertech Defence, delivering in-depth resources that simplify complex cybersecurity concepts into actionable and accessible insights. Designed for both seasoned professionals and cybersecurity enthusiasts, Leet Sheets offers expertly crafted guides on topics like penetration testing, cyber threat hunting, incident response, and advanced security practices.