HEMANTH YARLAGADDA

▪San Francisco, California ▪ 973 780 4611 ▪hemanthyarlagadda96@gmail.com
▪ https://www.github.com/Hemanth-Yarlagadda

SKILLS

Languages: Java, Python, C, SQL

Network Security and Protocols: TCP, UDP, HTTP/S, S/FTP, BGP, SMB DNS, SNMP, SMTP, POP, IMAP, Firewalls, IPSec, VPN and SSL

Web: HTML, CSS, JS

Virtualization & Cloud: AWS, Azure, GCP, VirtualBox, VMware, Azure, Office 365.

Tools & Frameworks: Docker, Kubernetes, Wireshark, Nmap, Metasploit, BeEF, Armitage, Power BI, Nessus, Tenable, Regular expression, Git, Tableau, MS O365.

Operating Systems: Debian, Security Onion, Mac OS, Windows, Unix, Linux.

WORK EXPERIENCE

Software Developer Fruitstone, Arizona **Sept 2020 – Present**

- Managing the CI pipelines by integrating Jenkins and version control (Git)
- Implementing webhooks to monitor GitHub events with Azure functions.
- Managing containerized web apps through docker built on Java.

Software Developer Aventure Systems- Ada, Michigan **Feb 2020 – Aug 2020**

- Assisting customers through phone by making SQL queries in the database
- Developing web applications using Python through Django framework
- Dealing with data from external sources and making dashboards using Tableau
- Creating custom measures and transforming the data into appropriate visualizations using Tableau as per client needs.

Software Developer Intern MediTechSafe – Cincinnati, Ohio **June 2019 – Aug 2019**

- Developed a monitoring and scanning tool using python and other open sources tools, which can identify vulnerabilities for a client over 200 devices.
- Used CLI and network security tools to perform network security monitoring of an enterprise network.
- Risk and vulnerability tracking, catalogued physical, digital risks and vulnerabilities. Reviewed, scored and tracked those vulnerabilities through risk remediation- NIST 800-53.
- Maintaining all the devices in the network and setting up firewall within the firm.
- Monitoring, analyzing and resolving the network packets, network security event logs
- Developed a machine learning model aimed to detect and alert suspicious network behavior.

Software Developer Fruitstone - India **Dec 2016 – June 2017**

- Conducted manual penetration testing on Web applications based on OWASP like CSRF, security misconfiguration, XSS etc.
- Performed penetration testing based on the vulnerabilities provided by Nessus, Nexpose.
- Highlighted vulnerabilities using pie chart based on the rarity i.e. critical, high, medium, low.

EDUCATION

Master's in **Computer Engineering – Cyber Security 3.67/4** University of Cincinnati **Dec 2019**
Bachelor's in **Electronics and Communication Engineering** **MGIT,** JNTUH **May 2017**

PROJECTS

Preventing Email Phishing Attack – Team Lead

- Worked along with other team members on developing a software which monitors the employees' email and alerts when there is a possible phishing attempt

Forensic Examination of an Attack – Team Lead

- Conducted analysis on PCAP files that were captured at an attack was taking place on the company's network. The steps of the attack were broken down into cyber kill chain phases and documented them.

Network Scanning tool – Team Lead

- Worked along with team members on developing a software which scans the network for devices and their exploits. Going through the network logs to see if there is any suspicious behavior.

Exploiting a windows machine - Team Member

- Performing network attack by deploying malware on the windows machine using msfvenom, metasploit to obtain root privileges.

ACTIVITIES

- Stood 4th in UC Hackathon CTF | Member of the UC-Cyber hacker community | Organized and Coordinated various technical, cultural events in campus during my under-graduation.