Srinath Koilakonda

Srinath.koilakonda@gmail.com | +1 (551) 226-3058 | 222 N 2nd street, Harrison, NJ 07029

Summary:

Cloud/Network Security practitioner possesses thorough knowledge and broad expertise in the security and technology spaces. Abilities are automation, penetration testing, security of network devices and computer systems, Expertise with incident response. Will always take proactive role in the architecture, design, implementation, and support of security focused resources to ensure safe operations.

Education:

New Jersey Institute of Technology (NJIT) Newark, NJ
Master of science, Cyber Security and Privacy

National Institute of technology Rourkela, IND
Bachelor of Technology Electronics Eng.

Skills:

Programming: Python, Go, JavaScript, Java, REST API.
Network: CCNA,TCP/IP,TLS/SSL, HTTP, JSON, Docker, Kubernetes, Ansible, Chef, Vagrant.
Security: MITRE ATT&CK ,SEIM, PCAP analysis, Log analysis, Incident response, IDS/IPS, SAST and DAST.
Others: Burp suite, Wireshark, Nmap, Nessus, OpenVAS, DNS security, Security Onion, forensics, REGEX, Operating system security and Data encryption.

Internships Experience:

- "Cloud infrastructure support" for social Justice + Engineering Initiative
- "Security engineer Intern" at SeedStages startup

Certifications & Training:

- Splunk Fundamentals + User behavior analysis (**Splunk** eLearning)
- Certified **Python** Programming (Hacker rank)
- Wireshark-Malware-forensics (LinkedIn) + Hack the Box CTF practitioner.

Academic Projects:

Python-Chat End- End encryption :

- Server – client architecture application, End to End message encryption using Cryptographic solutions
- SSL to exchange the digital Certificates
- Used Dieffie-hellman (ECDH) for the secret key exchange between the end systems.

Cloud Computing on AWS :

- Auditing and log collections and monitoring the API calls and resource access logs.
- EC2 cluster of instances customized AMI to deploy the Ubuntu java/ Hadoop/ MapReduce **e**nvironment along with the application to analyze.
- Implemented the Network and security aspects of the cluster of nodes to analyze and performed the network bandwidth efficiency tests using iperf tool**.**

Network security & Monitoring :

- Setting up and deploying SEIMs *and* perform network monitoring, and threat triaging and detecting.
- Network packet analysis tools Wireshark, Zeek, Tshark, tcpdump.
- Deploy network-based Intrusion detection tool Snort for the detecting anomalies and signature-based detections**.**
  Python scapy / Hping tools to generate custom network packets to test the network devices and firewalls rules.
- Worked on project to generate vulnerabilities and compliances report using various industry and opensource tools. (Nessus**,** Qualys, OpenVAS).

DevSecOps & WEB application Security(Docker +AWS+ Jenkins):

- Integrated Arachni , retirejs, SonarQube security tools into Jenkins to perform the automate the SAST / DAST vulnerability tests and generate the alerts and reports.
- Developed Ansible ,Docker playbooks to deploy the web servers and load balancers, also networking and security groups in AWS and performed the tests.
- Networked with peers to improve understanding of OWASP TOP 10, including cross-site scripting (XSS) attack project,
- SQLi; Implements protection measures and performed security tests against malicious codes.