Ahmad Abdullah

ahmadsomroo3@gmail.com | linkedin.com/in/ahmad-abdullah78/

Professional Summary

Motivated cybersecurity enthusiast with hands-on experience in threat detection, digital forensics, and incident response. Strong foundational knowledge of network security, system analysis, and investigative techniques. Passionate about adversary simulation, capture-the-flag (CTF) development, and designing proactive defence strategies to improve organisational security. Eager to contribute to real-world security challenges and continue growing in a dynamic, team-oriented environment

Projects

CTF Design & Development github.com/CTFsForensics

- Developing Forensics CTFs for Capture the Flag events held at FAST, ISB.

SPLUNK github.com/sem-5/Project

- Utilized Splunk to analyze endpoint machine logs, identifying anomalies and potential threats. Enhanced incident response by generating actionable insights from log data. Using Splunk mobile app to get alerts anywhere.
- Tools Used: Splunk, Search Processing Language

Vulnerability Assessment using AI (VAAI)

- Developed an automated tool to scan a single IP address or entire network for vulnerabilities using Nmap. The tool identifies associated CVEs, retrieves their corresponding CVSS scores, applies linear regression to analyze or predict severity trends, and provides remediation steps based on scan results.
- Tools used: Python, nmap

Firewalls/Intrusion Detection Systems

- Configured Suricata, UFW, PFSense for Network Monitoring in a DMZ environement.
- Configured Snort and Custom Rules to Detect anomalies in the Network.
- Tools Used: SNORT, Suricata, PFSense, Kali Linux

Certifications

Windows Forensics Belkasoft
Certificate ID:1tqxjjg1ev

- **Mastering Cyber Threat Intelligence for SOC Analysts**
  Certificate ID:a0dee7e8-1073-44ef-9eae-80448cd84faa
- **Managing Threat Intelligence with Cortex XSO**
  Certificate ID:ZUON5RR00GX1
- **Ask Questions to Make Data-Driven Decisions(Google)**
  Certificate ID:TAXNSDYARV9R

Education

- **FAST, National University of Emerging and Computer Science**, BS in Cyber Security — Aug 2022 - Present
  - **Coursework:** Artificial Intelligence, Networks and Cyber Sec, Computer Networks, Digital Forensics, Ethical Hacking, Vulnerability Assessment

Technical Skills

Security Operations Center: Splunk, WAZUH, Snort, Suricata

Tools/Platforms: Kali Linux, Autopsy, Volatiltiy, pfsense

Cyber Threat Intelligence:ISO 27001, MITRE ATT&CK Framework, STIX Framework, Threat feed-ingestion

Programming/Scripting: Python, C++, Rust