MD TAEF UDDIN NADIM

+1(479)-332-9713 ◇ Fayetteville, AR, United States (Willing to relocate) ◇ nadim@uark.edu

EDUCATION

University of Arkansas, *Fayetteville, AR, United States*
MS in Computer Science, GPA: 4.00/4.00 Aug 2023 - July 2025
Courses: Computer Security, Network Security, Advanced Network Security, Computer Forensics, Cloud Computing and Security, Privacy Enhancing Technologies, Full Stack Deep Learning, Machine Learning

Khulna University of Engineering & Technology, *Khulna, Bangladesh*
Bachelors in Electronics and Communication Engineering, GPA: 3.50/4.00 Jan 2016 - March 2020

PROFESSIONAL EXPERIENCE

Graduate Research Assistant, Security and Privacy Lab Aug 2023 – Present
University of Arkansas *Fayetteville, AR, United States*

- Built an automated vulnerability risk assessment framework with threat intelligence taking into account the organizational context along with CVSS and CVE; capable of ranking associated firewall rules, funded by the Department of Energy.
- Utilized DL models and network traffic (PCAP Analysis) log correlation on MITRE TTPs to detect anomalous connections, entities related to Advanced Persistent Threats (APT) at early stages with explainability ; countermeasure mapping with MITRE D3FEND.
- Built an advanced PoC Security Operations Canter (SOC) with enterprise grade tools: Palo Alto Firewall, Juniper Switches, Splunk Enterprise SIEM (Utilized Splunk Search Processing Language), OpenEDR, Delinea PAM, Forcepoint DLP with a VDI Subnet, Network Analyzer, and a Traffic Monitoring Server.

Cyber Security Specialist Oct 2021 – July 2023
Dhaka Stock Exchange PLC *Dhaka, Bangladesh*

- Conducted regular monitoring, analysis and investigation of incidents using DarkTrace NDR and Logpoint SIEM; tailored threat models, alert rules by Logpoint UEBA, SOAR playbooks based on MITRE ATT&CK, Kill Chain, and organizational requirements.
- Assisted in conducting periodic vulnerability assessments using Qualys and penetration testing using Core Impact and manual scripts to identify breaches of security and mitigate risks of the organization; Assisted in monthly technical reporting of the incidents.
- Assisted in developing policies, procedures and controls required for the protection of information, Datacenter and other IT assets of the organization considering best practices; Assisted in conducting regular cyber-awareness programs within the organization.

PROJECTS

DDoS Attack Detection and Mitigation using SDN: Developed an entropy-based framework for detecting and mitigating DDoS attacks in Software Defined Networks (SDN) by measuring packet entropy at the control plane; (Utilized Mininet emulator, POX Controller, Python, Linux). (Published in IEEE ACMI 2021, **Best Paper Award**)

Network & Side Channel Attacks and Security Countermeasures: Demonstrated SQL injection; Packet Sniffing and Spoofing; ARP cache poisoning ; ICMP redirect and TCP attacks with SYN flood, TCP RST, session hijacking; Spectre Attack. (Utilized Python, C, Scapy, Wireshark, MySQL, Ubuntu VM, Docker, OpenSSL)

ML Model Comparison on Titanic Survival Dataset on Kaggle: Compared Logistic Regression, SVM, Neural Networks, Decision Trees, and ensemble models, with LightGBM achieving 85.47% accuracy. (Utilized Python, Jupyter Notebook, Scikit-Learn)

SKILLS

Programming: Python, C, SQL, JSON.

Framework & Tools: Logpoint SIEM, SOAR & UEBA, Splunk Enterprise, DarkTrace, Powershell, Bash, NIST CSF, MITRE ATT&CK, OWASP top 10, Kill Chain, Qualys, Core Impact, Docker, Kali Linux, SRL, PCAP analysis, Wireshark, Metasploit, Nmap, Burpsuite, Scapy, Active Directory, Vmware, Virtual Box, Oracle, Cisco Routing and Switching, Juniper Switch, Google Colab, Jupyter Notebook, Scikit-Learn, Mininet, POX Controller.

CERTIFICATIONS AND TRAININGS

- Certified Ethical Hacker vii (CEH) (EC-Council)
- Graduate Cybersecurity Certificate (CYBR) (University of Arkansas)
- Certified in Cybersecurity (CC) (ISC)^2
- Cisco Certified Network Associate Routing and Switching Training (CCNA) (Cisco Networking Academy)