DANIAL ALI NAQVI

Cybersecurity Analyst

Contact Me

danial.official03@gmail.com

+91 9667244457

New Delhi, India

www.danialalinaqvi.com

www.linkedin.com/danial-ali-naqvi

About Me

Dedicated and detail-oriented Cybersecurity Analyst fresher with a strong foundation in security principles and hands-on technical skills. Eager to apply practical cybersecurity knowledge in a dynamic, real-world Security Operations Centre (SOC) environment as part of a collaborative security team. An inquisitive and curious individual, motivated by a desire to learn and grow every day, while staying up to date with the latest trends, tools, and techniques in the cybersecurity field. Committed to contributing to a secure digital future by identifying threats, mitigating risks, and ensuring system integrity.

Education

Bharati Vidyapeeth's College of Engineering
B. Tech in Information Technology : CGPA 8.49
Completed in 2024

Manava Bharati India International School
Primary, Middle and High schooling
Completed in 2019

Professional Experience

SOC Analyst L1 | Media Today Pvt. Ltd. *September 2024 - Present*

- Monitoring and investigating security events and alerts to ensure the security of systems and data using the ELK Stack, osTicket and Wazuh.
- Performing triage, escalating alerts and assisting in Incident Response and reporting on findings.
- Assisting in maintenance of policies, procedures and keeping systems and software up-to-date.

SOC Intern | Cyber & Forensics Security Solutions *November 2024 - December 2024*

- Performing Log Analysis, IDS/IPS configuration, Phishing analysis, EDR investigation, Digital Forensics.
- Challenges - TryHackMe Blue, TryHackMe Wreath, HackTheBox Jerry
- Theoretical training by answering questions and documenting tasks in a report.

Projects

- **Auditing and Compliance -** Documenting a Security Audit and Compliance check (🔗)
- **Linux fundamentals -** file system navigation, content management, Authorization and Access management, user management and hashing (🔗)
- **SQL fundamentals -** basic queries, filtering queries, time, numerical, logical filters, and joins (🔗)
- **Vulnerability Assessment -** Performing a Vulnerability Assessment for a found USB drive (🔗)
- **Investigation and Incident Response -** Performing an investigation on a phishing email and escalating generated alert(🔗)

- **Network Traffic Analysis -** Traffic Analysis using tcpdump and Wireshark (🔗)
- **Intrusion Detection Systems(IDS) -** Configuring IDS signatures in Suricata (🔗)
- **Splunk SIEM -** Identifying Security Issues in a Mail Server using Splunk Cloud (🔗)
- **Chronicle SIEM -** Investigating a phishing attack using Google Chronicle (🔗)
- **Python -** Importing and parsing security logs using Python (🔗)
- **Incident Response -** Performing iterative Incident Response for levels of the Pyramid of Pain(🔗)
- **Intrusion Detection and Prevention (IDS/IPS) -** Using Snort IDS/IPS to stop Brute-Force & Reverse Shell attacks (🔗)
- **Security Operations Centre (SOC) Home Lab - (🔗)**
  - Setting up a Virtual SOC environment using ELK Stack, Fleet Server, osTicket
  - Setting up Sysmon and Windows Defender to forward logs via Elastic Agent
  - Creating Brute Force Alerts and Dashboards visualizing suspicious activity in Kibana
  - Using Kali Linux to perform SSH & RDP Brute Force attacks on Ubuntu & Windows servers respectively, establishing Command & Control(C2) using Mythic Agent and exfiltrating documents.
  - Investigating the recorded attack telemetry and logs.

Certifications

CompTIA Security+ | SY0-701
Expected February 2025
Currently studying key areas like risk management, incident response, and cryptography to secure networks, mitigate threats, and implement security protocols

TryHackMe SOC Level 1
November 2024
Practical knowledge of Security Information and Event Management (SIEM), network security, endpoint monitoring, phishing analysis, and digital forensics using industry tools like Wireshark, Splunk, and Zeek, providing hands-on experience in identifying, analyzing, and responding to security incidents.

Google Cybersecurity Professional
August 2024
Foundational knowledge in cybersecurity, covering topics like threat analysis, risk management, network security, SIEM tools and incident response.

Cisco Networking Basics
July 2024
Foundational networking concepts, including IP addressing, routing, and switching. Practical knowledge on building, securing, and managing networks.

Technical Skills

- Networking and Network Security
- Asset and Risk Management
- Linux OS
- Network Traffic Analysis tools: tcpdump, Wireshark, TShark, Network Miner
- Asset, Threat and Vulnerability Management
- Threat Modeling
- Intrusion Detection & Prevention Systems(IDS/IPS): Suricata, Snort
- Incident Investigation and Response
- SIEM Tools: Splunk, Chronicle, ELK Stack
- ELK Stack: Elasticsearch, Logstash, Kibana

Soft Skills

- Written and verbal communication
- Attention to detail
- Inquisitive nature
- Teamwork and collaboration
- Analytical mindset
- Multi-tasking
- Following instructions
- Documentation and reporting
- Time Management
- Adaptability