Muhammad Ehtisham

Islamabad, Pakistan
+92 (332) 9979242 – connectsham95@gmail.com— https://www.linkedin.com/in/ehtishamcyber— www.ehtisham.space

PROFILE

Enthusiastic cybersecurity student and Freelancer specializing in network security, Linux, C++ and information technology. Passionate about Wazuh and SIEM technologies, as well as Cloud computing. Seeking an entry-level position to leverage expertise in cybersecurity and IT support, contributing to organizational development while continuously expanding knowledge and skills.

WORK EXPERIENCE

– SOC Analyst Intern- NASTP

During my internship, I gained hands-on experience in SOC operations, including threat monitoring, alert analysis, and incident response. I performed advanced threat hunting using various techniques and contributed to identifying and analyzing suspicious activity patterns. Additionally, I helped develop and optimize a machine learning–based detection system integrated with real-time monitoring and dashboards.

– Project Contract: Troubleshooting and Implementing Wazuh SIEM Solution at Power Plant:

Successfully completed troubleshooting, configuration, and deployment of a new Wazuh SIEM solution. Tasks included resolving a non-functional SIEM setup, restoring communication between the SCADA system server and PFSence firewall, ensuring seamless network integration, and enhancing overall security and monitoring capabilities.

– Experienced in Freelance cybersecurity and IT projects:

I have done several Freelancing Projects related to Cyber Security Tools, Linux OS, Windows Server AD, and Document Labs reports to enhance my Hands-on skills needed to become proficient in IT & Security.

EDUCATION

Air University

Bachelor's in Cyber Security, 2022 – Present

TECHNICAL PROJECTS

– Deployed Cloud Based Wazuh SIEM Solution on Microsoft Azure.
– Troubleshooting and Implementing Wazuh SIEM Solution at Power Plant
– ELK Fleet SIEM Configurations with Ubuntu Server Cloud.
– Honeypot Deployment in Network on DigitalOcean Cloud Envorment.
– Exploiting vulnerabilities in Metasploitable2 using Kali Linux, Nmap, and Metasploit Framework.
– Virus Total Integration in Wazuh-SIEM Solution.
– DVWA Web Server Pen-testing.
– Deployed and Configured Windows Server 2012 AD.
– Network Access Storage Server on Virtual Machines.

SKILLS

– IBM Qradar – Cyber Security Tools – Wazuh Server – Cloud Server VM Monitoring
– Wireshark – NMAP – Metasploit Framework – Intrusion detection

COURSES

– (ISC)² Certified in Cybersecurity (CC)
– Security Assessment & SOC Boot camp (VaporVM Information Technology & Services Company)
– Google Cyber Security Specialization (Coursera)
– SIEM Basics, Installation and Configuration (LetsDefend.io)
– Cybersecurity Operations Fundamentals Specialization(Coursera)

LANGUAGES

– ENGLISH – URDU