

MUHAMMAD USMAN ALI

DIGITAL FORENSICS & CYBER SECURITY

Lahore Pakistan | +923392009059 | usmanmalik918031@gmail.com

linkedin.com/in/usman-ali-b7a6691b0/

OBJECTIVE

Passionate cybersecurity professional with hands-on experience in network security, digital forensics, and IT support. Seeking competent role to enhance my expertise in threat intelligence, penetration testing, and OSINT. Committed to leveraging advanced cybersecurity knowledge to strengthen digital defenses and contribute to the field.

SKILLS

- **Cybersecurity & Digital Forensics**
 - Cyber Threat Monitoring & Analysis
 - Security Information & Event Management (SIEM)
 - Digital Forensics & Incident Response
 - Network Traffic Analysis & Threat Intelligence
- **Tools and Platforms**
 - Checkpoint Firewalls
 - Imperva WAF
 - Microsoft Intune
 - Microsoft Sentinel (SIEM)
 - Microsoft Admin Center
- **Technical Support**
 - IT Support
 - Desktop Support
 - Windows Troubleshooting
 - Technical Support
- **Operating Systems**
 - Windows 10/11
 - Linux
- **Ticketing and IT Service Management**
 - Jira Ticketing
 - ServiceNow
- **Programming Languages**
 - Python
 - Shell
 - Ruby
 - HTML/CSS
- **Soft Skills**
 - Strong Analytical
 - Problem-Solving Skills
 - Effective communication
- **Tools**
 - Wireshark
 - Nmap
 - Burp Suite
 - Metasploit
 - Nessus
 - Autopsy
 - FTK Imager
 - John the Ripper
 - Hashcat

EXPERIENCE

Junior Infrastructure / IT Security Engineer
Code Practitioners
Lahore, Pakistan

Present

- Providing day-to-day IT support to staff, ensuring smooth operation of systems and networks.
 - Managing servers and deploying Dynamic VM 365 instances for enhanced virtualization and performance.
 - Configuring and maintaining FortiGate Firewall, including policy management, traffic monitoring, and security rule implementation.
 - Implementing security controls by restricting user account privileges and enforcing system access policies.
 - Monitoring employee activity using employee monitoring software to ensure compliance and productivity.
-

Network Security Analyst

Tekboox

Aug 2023 - Aug 2024

Chicago, USA

- Managed Checkpoint Firewalls, specializing in level 1 troubleshooting, log analysis, and rule modifications.
- Worked on the Security Operation team in Microsoft Sentinel, handling and investigating incidents.
- Proficiently administered firewall rules, optimizing network security and traffic flow.
- Collaborated with cross-functional teams to implement rule changes aligned with business needs.
- Generated comprehensive reports using Tenable Vulnerability Scanner, Imperva, and Checkpoint technologies.
- Demonstrated strong analytical and problem-solving skills in addressing firewall-related issues.

Intern

Punjab Police

Oct 2023 - Nov 2023

CPO Office Lahore

- Completed comprehensive internship with Punjab Police, specializing in digital investigation processes and technology implementation for crime-solving.
- Visited departments such as FIA Cyber Crime, CTD, DIG Investigation, CPO Office IT Branch, and Safe City Punjab.
- Collaborated in small groups to explore digital investigation methodologies, gaining practical insights into leveraging technology for solving complex crimes.
- Acquired valuable exposure to the operations of key law enforcement agencies.

EDUCATION

BS (Hons.) Digital Forensics & Cyber Security

2019 - 2023

Lahore Garrison University, DHA Phase 6 Lahore

Relevant Courses: Network Security, Incident Response, Digital Forensics, Intrusion Detection, Mobile Forensics, Hardware Networking

Final Year Project: Developed a Terrorism-Based Crime Rate Analysis Tool using Python and Streamlit to visualize data and generate insights.

Intermediate

2017 - 2019

Garrison College for Boys Lahore Cantt
F.S.C Pre-Engineering

CERTIFICATIONS

- Certified in Cybersecurity by (ISC)2 Dec 2023
- CISA Training (Lahore Chapter) by ISACA Feb 2021
- Certified White Hat Hacking by DFRSC (LGU) Aug 2023
- Advance Networking by Corvit Lahore Jun 2023 - Dec 2023

PROJECTS & RESEARCH

- Conducted network traffic analysis using Wireshark to detect anomalies and potential threats.
- Performed vulnerability assessments on virtual environments to identify and mitigate risks.
- Completed static malware analysis as part of a research project, examining malicious behaviors.

ACTIVITIES & INTERESTS :

- Capture The Flag (CTF) Challenges (TryHackMe, HackTheBox)
 - Ethical Hacking & Penetration Testing
 - Open-Source Intelligence (OSINT) Research
-