Umair Aziz

Cybersecurity Analyst

Mirpur, AJK | +92 3146018728 | umairaziz682@gmail.com | linkedin.com/in/umairaziz001

Summary

Cybersecurity Analyst with hands-on experience in incident response, network security, and vulnerability management. Proficient in using tools like Wireshark, Nessus, and IDS/IPS to analyze threats and secure systems. Skilled in applying NIST, ISO 27001, and CIS frameworks to develop security policies and playbooks. Combines technical expertise in Python and Linux with a proactive approach to safeguarding digital assets and mitigating emerging threats.

Core Competencies

Security Domains	Security Tools & Technologies	Frameworks & Governance
Incident Response & Forensics	Wireshark, Tcpdump, Nmap, Nessus	NIST Cybersecurity Framework (CSF)
Network Security (TCP/IP, VPNs)	IDS/IPS, Firewalls, SIEM (conceptual)	ISO 27001, CIS Controls
Vulnerability Assessment	Malware Analysis & Threat Hunting	Risk Management & Policy Development
Linux/Unix Administration & Hardening	Python (for automation/parsing), SQL	Secure Coding Practices

Professional Experience

Cybersecurity Analyst | Internal Security Team, Mirpur, AJK

Feb 2023 – Present

- Analyzed network traffic with Wireshark and Tcpdump to identify suspicious patterns, leading to the mitigation of potential security threats.
- Developed and implemented incident response playbooks for malware, phishing, and insider threats, standardizing containment and recovery procedures.
- Reduced application-layer vulnerabilities by 30% by collaborating with developers to create and deliver secure coding training.
- Conducted vulnerability scans using Nessus, interpreted CVSS scores, and recommended remediation strategies such as patching and configuration hardening.
- Monitored IDS/IPS alerts and VPN logs, escalating confirmed incidents to senior analysts for timely resolution.
- Delivered quarterly cybersecurity awareness training to employees on topics including phishing, password hygiene, and social engineering.

Technical Projects

- **Incident Response Playbook:** Designed a comprehensive IR playbook for malware/phishing attacks, integrating digital forensics steps (evidence preservation, log collection) and clear escalation paths.

- **Live Network Traffic Analysis:** Configured a virtual lab with Snort IDS; used Wireshark/Tcpdump to analyze traffic, identify anomalies (port scans, DDoS signatures), and map events to the MITRE ATT&CK framework.
- **Vulnerability Assessment & Remediation:** Performed a vulnerability assessment on a simulated SMB network using Nmap and Nessus. Discovered and prioritized critical vulnerabilities, providing a full remediation plan.
- **Log Parsing & IOC Extraction with Python:** Built Python scripts to automate the parsing of large log files, extracting Indicators of Compromise (IOCs) and loading them into an SQLite database for trend analysis.

EDUCATION

Bachelor of Science in Information Technology

MUST University, AJK | Expected Graduation: September 2025

- Relevant Coursework: Ethical Hacking, Computer Network and Security, Operating Systems, Database Administration, Cryptography.

Certifications

- Cybersecurity Professional Certificate | **Google**
- IBM Cybersecurity Analyst Professional Certificate | **IBM**
- CompTIA Network+ (N10-008) | **In Progress**
- Security Analyst Fundamentals | **IBM**
- Cybersecurity Attack and Defense Fundamentals | **EC-Council**
- Applied Cryptography | **University of Colorado System**

LANGUAGES

English | Urdu