








# Safi Ullah Khan

## Cybersecurity Engineer

 20pwcse1943@uetpeshawar.edu.pk  +92 3402661127  LinkedIn  Github  Coursera  Udemy

 Ec-council

### PROFILE

Highly skilled Cybersecurity Engineer with extensive experience in safeguarding systems against cyber threats and vulnerabilities. Expert in designing and implementing robust security architectures, conducting thorough risk assessments, and deploying advanced threat detection and response strategies. Demonstrated proficiency in using a variety of security tools and technologies, including firewalls, SIEM, IDS/IPS, and encryption protocols. Adept at ethical hacking to proactively identify and remediate security weaknesses. Experienced in leading security projects, training teams on best practices, and developing comprehensive security policies to protect sensitive data. Known for strong problem-solving skills, meticulous attention to detail, and a proactive approach to enhancing organizational security posture.

### PROFESSIONAL EXPERIENCE

#### Penetration Tester Internship, National Cyber Security Center UET Peshawar

Sep 2023 – 2024

##### Key Responsibilities

Conducted security assessments using Burp Suite, Metasploit, Nmap, Nessus, Wireshark, OpenVAS, and Astra Pentest. / Performed web application security tests with Burp Suite, uncovering critical security flaws and vulnerabilities. / Simulated cyber attacks to identify weaknesses, enhance defenses, and prepared comprehensive reports. / Used SIEM tools (Splunk) to collaborate on threat detection, containment, and remediation efforts. / Coordinated SIEM development with technical teams to enhance operations and implement response plans. / Protected data and systems, ensured confidentiality, and managed post-incident reporting for optimization. / Collaborated with teams to implement security measures, ensure compliance, and efficiently resolve cases.

##### Key Achievements

Identified and mitigated vulnerabilities like SQL injection, XSS, CSRF, buffer overflows, and privilege escalation. / Improved incident response efficiency by 25% and reduced security incidents by 40% through optimized SIEM tools. Enhanced threat detection and streamlined SIEM development, boosting operational efficiency by 20%. / Implemented robust security measures, ensuring zero data breaches and full compliance with industry standards. / Protected against threats like DDoS, malware, phishing, man-in-the-middle attacks, and zero-day exploits

#### Cybersecurity, Prodigy InfoTech

Jan 2022 – May 2022

Conducted network penetration tests using Nmap, Wireshark, and Metasploit for identifying vulnerabilities. / Utilized Hydra and John the Ripper for password cracking in penetration testing engagements. / Created custom payloads using msfvenom for effective exploitation and security testing. / Performed security assessments of networks and systems, identifying critical vulnerabilities. / Used Python for web scraping to gather data for security analysis and vulnerability assessment. / Automated security testing using Python scripts to identify vulnerabilities in networks.

#### Aspire Leaders Program, 2024, Personal and Professional Development












Nov 2023 – present

Gained valuable insights and skills to enhance leadership capabilities and contribute effectively to future roles

### SKILLS

Malware Analyzer Tools- Reverse Engineering-Wireshark-Tcpdump, Security Testing Tools — Burp Suite, Nmap, Metasploit, Hydra, John the Ripper, msfvenom, Programming Languages — Python, Bash, PowerShell, Java, C/C++, SIEM tools— Snort, Splunk, Threat risks and Vulnerabilities, Operating Systems — Windows, Linux., Vulnerability assessment and penetration testing, Networking — TCP/IP, DNS, DHCP, VPN, Firewall, IDS/IPS, Troubleshooting and problem- solving, Excellent communication and interpersonal skills

### CERTIFICATES

Digital Forensics & Cyber Security [NAVTTTC]  | Google Cybersecurity  | Securing Software, Data and End Points  | Ethical Hacking Essentials (EHE)  | Wireshark for Network Security Analysis  | SQL Injection Attacks | Python for Cybersecurity  | Metasploit for Ethical Penetration Testing  | Web Application Security Testing with OWASP ZAP  | Burp Suite for Penetration Testing  | Introduction to Dark Web Anonymity , And cryptocurrency | Encryption with Python: Encrypt data with key pairs  | JavaScript Security Part 1 

### PROJECTS

#### NCCS-UET TestBeb for Web Applications vulnerabilities : Final Year Project,

Oct 2023

##### Exploit OWASP Top 10 Vulnerabilities 2021

Developed a testbed for identifying and exploiting OWASP Top 10 vulnerabilities using PHP, CSS, HTML, and databases on a localhost XAMPP server , conducted in-depth vulnerability analysis and risk assessments, identifying common attack vectors and proposing mitigation strategies, demonstrated expertise in web application security and collaborated effectively in a team-based environment, executed penetration testing methodologies to identify and report vulnerabilities in web applications, created detailed documentation and presented findings to stakeholders, ensuring clear communication of risks and recommendations.

#### Developed ML models for spam email and malicious link detection.

Jun 2024 – Jul 2024

Developed and implemented machine learning models for detecting spam emails and malicious links. Utilized natural language processing (NLP) techniques to analyze email content and extract features. Applied algorithms such as Random Forest, Support Vector Machine (SVM), and Neural Networks to classify emails and identify suspicious URLs. Evaluated models using precision, recall, F1-score, and ROC-AUC metrics to ensure high accuracy and efficiency. Integrated the solution into an email filtering system, significantly reducing the rate of spam and enhancing cybersecurity measures

- Gathered datasets of spam/ham emails and labeled URLs for training.
- Cleaned and standardized data by stripping unnecessary elements and parsing URLs.
- Extracted features using bag-of-words and specific indicators in emails and URLs.
- Trained models including Random Forest, Support, SVM, and neural networks on preprocessed data.
- Evaluated models using accuracy, precision, recall, and F1 score metrics.
- Deployed the best model for real-time email filtering and malicious link detection.

#### Use Nmap to investigate rogue devices

Jun 2023 – Jul 2023

Utilized Nmap to investigate rogue devices within the network. By leveraging Nmap's advanced scanning capabilities, I conducted thorough network scans to identify unauthorized devices and potential threats. This proactive approach allowed for the timely mitigation of security risks, significantly enhancing the overall security posture of the network. Demonstrated expertise in network security tools and techniques, showcasing my ability to effectively safeguard network infrastructure and maintain a secure environment.

#### Implemented Splunk tools for real-time data analysis from various sources

Jan 2024 – Feb 2024

Responsibilities: Configured SIEM tools to collect and aggregate data. Defined rules for threat detection and alert generation. Optimized SIEM configurations for efficient threat detection. Developed custom dashboards and reports. Conducted audits to ensure compliance with security policies.

#### Wazuh SIEM Deployment for Security Monitoring

Mar 2024 – Apr 2024

Successfully deployed and configured Wazuh SIEM on a Linux server and integrated a Windows agent for real-time security event monitoring. Managed network configurations to ensure seamless communication between virtual machines. Conducted comprehensive testing and documentation of security events. Demonstrated expertise in endpoint management and SIEM operations

## EDUCATION

BS. Computer Systems Engineering,

Nov 2020 – May 2024 | Peshawar, Pakistan

University of Engineering & Technology Peshawar, CGPA : 3.21 