Mohsin Mukhtiar Lashari

📞 033-90012342 ✉ lasharimohsin19@gmail.com in Linkedin ⌾ Github Ⓜ Medium Blog 🔗 Portfolio Site

Summary —

– As a Cyber Security student with a robust foundation in both red and blue teaming, I bring practical experience and a strategic approach to security challenges.
– My skills encompass vulnerability identification, simulated attacks, incident response, and defensive strategies, developed through hands-on roles and active participation in Capture The Flag (CTF) competitions.
– I am committed to leveraging my diverse skill set and academic knowledge to contribute effectively to cybersecurity solutions and continuous improvement in cyber defense.
– Proven track record in delivering actionable insights and solutions, enhancing security posture and resilience.

Technical Competencies

Languages	Python, Bash, C++, Rust (learning)	**Testing**	Pytest
OS	Debian, Ubuntu, Windows, Vercel	**Framework**	Burpsuit, Metasploit, Nmap

Job Experience

Intern at National Center of Cyber Security   Jun 2024 – Aug 2024
Network Security

– **Primary Role** Developed a custom Python tool for packet capturing and intrusion detection.
– **Technologies Used** Utilized Python for end-to-end packet capture, analysis, and intrusion detection.
– **Intrusion Detection Methodologies** Implemented various detection algorithms and custom logic for identifying potential intrusions.
– **Logging and Alerting** Created custom functions for real-time intrusion alert generation and logging. Automatically logged alerts in designated files based on protocol.

Intern at Trillium Information Security Systems   Jun 2024 – Aug 2024
Red Teaming

– **Primary Role** Led comprehensive assessments of web applications to identify critical vulnerabilities, including file upload, CSV injection, and security misconfigurations.
– **Technologies Used** Employed advanced tools such as Burp Suite Pro, Metasploit, and custom scripts to conduct thorough vulnerability analysis and penetration testing.
– **Vulnerability Assessment** Crafted and executed sophisticated attack vectors to exploit identified weaknesses, simulating real-world threat scenarios to evaluate application resilience and security posture.
– **Reporting and Documentation** Produced detailed technical reports outlining vulnerabilities, exploit techniques, risk levels, and prioritized remediation recommendations. Provided actionable insights to development teams for enhancing application security.

Projects

Spamy - Email Filter   **Python**

– Developed a Python-based email analysis tool to detect spam and phishing threats using signature- and heuristic-based detection.
– Parsed and validated email headers (SPF, DKIM) and extracted suspicious links and attachments.
– Integrated VirusTotal and Urlscan APIs for real-time threat intelligence and link verification.
– Enabled configurable blacklists and modular architecture for scalability and maintainability.

Mazeli-2.0 - Maze Solver with GUI   **C++**

– Implemented multiple pathfinding algorithms (BFS, DFS, A*, Weighted A*) with visual feedback and real-time step tracing.
– Developed an interactive GUI using SFML; added voice feedback for accessibility and engagement.
– Tuned performance for large maze datasets and ensured responsiveness under various test cases.

Cryptix - Cryptography Library   **Python**

– Published a Python cryptographic toolkit supporting 15+ classical ciphers and 10+ encoding schemes.
– Wrote modular decryption functions for algorithms including Hill, Affine, Playfair, One-Time Pad, and RSA.
– Used extensive unit testing and docstrings to ensure maintainability and PyPI readiness.
– Designed for educational, forensic, and competitive programming applications.

socketSniffer - Network Packet Sniffer   **Python**

– Engineered a network packet sniffer using raw sockets with support for TCP, UDP, ICMP, HTTP/1/2/3, DNS, and NTP.

– Developed protocol parsers and real-time packet visualization for traffic analysis.
– Focused on modular design for ease of protocol extension and debugging.

xNIDDY - Network Intrusion Detection System **Python**
– Built a lightweight NIDS that monitors raw network traffic and flags anomalies using protocol-aware rules.
– Implemented detection logic for TCP floods, malformed DNS requests, and suspicious HTTP payloads.
– Logged detailed packet metadata and integrated alerts with log monitoring systems.

Fluffy-ware - Malware Simulation Tool **Rust**
– Simulated malware behavior for research, including Defender evasion, privilege escalation, and system destabilization.
– Manipulated Windows Registry and User Access Control (UAC) to demonstrate security bypass vectors.
– Used Rust's system-level control and safety features for reliable malware simulation.

Toralizer - Lightweight Tor Proxy Simulator **C**
– Developed a C-based Tor proxy tool to facilitate anonymous routing through custom SOCKS5 tunnels.
– Emulated Tor-like behavior including node chaining and circuit simulation for privacy-aware networking.
– Designed CLI interface and planned hostname resolution for future releases.

Moni-Crypt - Host-Based Intrusion Detection System **Rust**
– Developed a Rust-based HIDS to monitor critical file paths, user sessions, and privilege changes.
– Implemented rule-based alerts for integrity violations and unusual process behavior.
– Logged incidents in structured JSON for SIEM integration and automated parsing.

Pinky-Virus - ELF Infector **Assembly**
– Wrote a low-level ELF virus in x86_64 Assembly using Reverse Text Segment Infection technique.
– Designed for static analysis and educational demonstration of binary infection techniques.
– Maintained stealth by preserving entry points and using precise PAGE_SIZE alignment.

VOLUNTEER EXPERIENCE

AirRange **Feb 2024 – Present**
Cryptography Challenge Creator

– **Role** Played a pivotal role in the organization and execution of Capture the Flag (CTF) competitions targeted at university students and participants from external institutions.

– **Responsibilities**
– Designed, developed, and tested complex cryptography challenges to be used in CTF events, focusing on various encryption and decryption techniques.
– Collaborated with other team members to create a comprehensive and engaging competition environment, including developing scoring systems and integrating challenges into the event platform.
– Conducted workshops and briefings for participants to explain the challenges and provide guidance, enhancing the educational value of the CTF events.
– Coordinated with external experts and sponsors to secure resources and support for the events, ensuring smooth execution and high-quality experiences for all participants.

– **Achievements**
– Successfully designed and implemented over 20 cryptography challenges, contributing to the intellectual stimulation and growth of participants.
– Received positive feedback from participants and stakeholders for the challenging and educational value of the cryptography problems created.
– Played a key role in increasing the event's visibility, fostering a stronger community around cybersecurity and CTF competitions.

– **Skills Utilized**
– Applied advanced knowledge in cryptography and problem-solving to create intricate and thought-provoking challenges.
– Demonstrated exceptional organizational skills by managing multiple aspects of challenge development, from conception to implementation.
– Exhibited strong teamwork and communication skills by working collaboratively with other organizers and engaging with participants.
– Enhanced event quality and participant satisfaction through meticulous planning and responsive support during competitions.

EDUCATION

Air University, Islamabad   **2023 – 2027**
Bachelor of Science in Cyber Security
Thesis: No Yet

Mehran University Higher Secondary Public School, Jamshoro   **2021 – 2023**
Intermediate (Pre-Engineering)

Mehran University Higher Secondary Public School, Jamshoro   **2019 – 2021**
Matriculation (Science)

ACHIEVEMENTS

- Secured **5th position** in Bandits CTF
- Secured **1st Runner-up** in in Mehran Chess Competition organized by MUHSPS, Jamshoro, onsite (2018)
- Secured **2nd position** in MCC organized by MUHSPS, Jamshoro, onsite (2019)

CERTIFICATIONS

Google   **Feb 16, 2024**

- Crash Course on Python
- Developed a solid understanding of Python's core syntax, including data types, loops, and conditionals.
- Applied Python programming skills to solve real-world problems through hands-on projects.
- Explored error handling techniques to write robust and fault-tolerant code.
- Gained experience with Python's standard libraries and tools, enhancing problem-solving capabilities.

Codio   **Nov 23, 2023**

- C++ Basics: Selection and Iteration
- Mastered the use of selection statements (if-else) to control program flow based on conditions.
- Implemented iteration constructs (for, while loops) to perform repetitive tasks efficiently.
- Developed and tested algorithms to solve common programming problems using C++.
- Gained experience with debugging and optimizing C++ code for better performance.

Coursera Project Network   **Nov 21, 2023**

- Use Bash Scripting on Linux to Execute Common Commands
- Learned to write and execute Bash scripts for automating repetitive tasks in Linux environments.
- Gained proficiency in managing files, directories, and system processes using Bash commands.
- Utilized Bash scripting to automate system administration tasks, enhancing efficiency and productivity.
- Developed scripts for data processing and analysis, improving workflow automation.

IBM   **Dec 21, 2023**

- Introduction to Networking and Storage
- Acquired foundational knowledge of networking principles, including protocols and network topologies.
- Studied the mechanics of data transmission and the role of various network devices.
- Explored the basics of storage systems, including file systems and storage architectures.
- Prepared for roles in network and systems administration by understanding network security and data management.