CURRICULUM VITAE

Asad Muhammad Channar

Cyber Securiy Enthusiast|| Malware Analyst

✉: Contact ☎: +92 333 5177266

:Linkedin

:Github

: Portfolio

Education

Air University, Islamabad Bachelor’s Degree in Cyber Security Aug 2023 – Present…..

Islamabad Model College For Boys G-10/4

F.SC	2021– 2023
Matric	2019-2021

Summary

I'm currently a cybersecurity student at Air University, deeply interested in the world of digital security. My studies have introduced me to the challenges and solutions involved in protecting information and systems from cyber threats.

I'm currently a cybersecurity student at Air University, deeply interested in the world of digital security. My studies have introduced me to the challenges and solutions involved in protecting information and systems from cyber threats.

Skills

Cyber-Security . Malware Analysis . Python . Bash . Networking . Git . Github . Problem Solving . Time Management . C++ . Communication

Experience

Develepor’s Hub Corporation **(Sep 24 – Oct 24) {Cyber Security Interne}**

At Developer's Hub Co-operation, I had the opportunity to work on real-world cybersecurity projects, deepening my understanding of ethical hacking, vulnerability assessment, and digital forensics. Collaborating with industry professionals allowed me to improve my problem-solving skills and stay updated with the latest security trends. This experience significantly shaped my approach to tackling cybersecurity challenges in a professional environment..

CodeAlpha (Mar 24 - April) {Red Team Intern}

As a Red Team Intern at CodeAlpha, I gained hands-on experience in offensive security by simulating real-world cyber attacks to identify vulnerabilities. I worked with penetration testing tools, conducted security assessments, and enhanced my ethical hacking skills to strengthen system defenses. During this internship, I also analyzed exploit techniques, developed custom attack scenarios, and collaborated with security teams to propose mitigation strategies. Additionally, I honed my skills in reconnaissance, privilege escalation, and post-exploitation tactics, further refining my expertise in adversarial cybersecurity operations..

Projects

- ### MailGuard

A robust email filtering system that detects and moves malicious emails to spam, enhancing inbox security.

Key Features:

- **IMAP-Based Email Retrieval** – Connects to email servers using IMAP to fetch incoming messages.
- **Spam Detection** – Analyzes email content, headers, and metadata to identify phishing attempts, malware, and spam.
- **Blacklist & Whitelist Support** – Maintains a list of trusted and blocked email addresses for better filtering.
- **Keyword & Link Analysis** – Scans for suspicious words, links, and attachments that indicate potential threats.
- **Automatic Email Sorting** – Moves flagged emails to the spam folder while keeping legitimate emails in the inbox.
- **GUI Integration** – Provides a user-friendly interface for monitoring filtered emails and adjusting settings.

- ### Pinky Virus

A malware-like program written in Assembly that modifies files in the directory where it runs, altering their extensions and magic bytes.

Key Features:

- **File Extension Manipulation** – Changes all file extensions in the target directory to `.pinky`.
- **Magic Bytes Alteration** – Modifies the magic bytes of files by adding "PINKY" at the beginning, making them unrecognizable by standard applications.

- **Recursive Execution** – Scans and modifies files in subdirectories for widespread impact.
- **Stealth Mode** – Operates discreetly without alerting the user.
- **Minimalistic and Lightweight** – Developed in Assembly for efficient execution and minimal system footprint.
- **Non-Destructive Variant** – Can be configured to reverse changes for controlled testing purposes.
- **Targeted Directory Operation** – Only affects files in the directory where it is executed, preventing system-wide damage unless explicitly configured.
- **Educational & Research Use** – Designed for cybersecurity learning, malware analysis, and red team exercises.

• Wifalyzer

An advanced WiFi analysis tool that provides complete control over nearby wireless networks, allowing users to capture and analyze signal data in real-time.

Key Features:

- **WiFi Signal Scanning** – Detects and lists all available WiFi networks in the area.
- **Signal Strength Analysis** – Measures and displays the strength of detected networks for better insight into coverage.
- **Radio Type Identification** – Identifies the wireless technology used (e.g., 802.11a/b/g/n/ac/ax).
- **Access Point Information** – Extracts details such as SSID, BSSID, frequency, and security protocols.
- **Graphical Data Representation** – Visualizes signal strength trends using interactive graphs.
- **Heat Map Generation** – Creates heat maps to represent WiFi signal distribution in a given area.
- **Real-Time Monitoring** – Continuously updates network information to reflect live changes.
- **User-Friendly Interface** – Designed with an intuitive UI for seamless navigation and analysis.
- **Security Assessment** – Assists in detecting unauthorized access points and weak encryption settings.

• Encryptify

Encryptify is a Python-based encryption tool that ensures secure communication by encrypting and decrypting messages using a randomized key system. It supports both command-line and graphical user interfaces for flexible usage.

Key Features:

- **Random Key Generation** – Generates a unique encryption key each time to enhance security.
- **Encryption & Decryption** – Allows users to securely encode and decode messages.
- **Key Persistence** – Stores encryption keys in a JSON file for retrieval and future use.

- **Dual Interface Support** – Provides both a **CLI** and a **Tkinter-based GUI** for user convenience.

- **Cross-Platform Compatibility** – Runs seamlessly on **Windows, Linux, and macOS**.

- **User-Friendly GUI** – Features an intuitive interface for effortless encryption and decryption.

- **Security-Focused** – Uses a strong encryption mechanism to protect sensitive data.

- **Lightweight & Efficient** – Designed for minimal resource usage while ensuring robust functionality.

- **Customizable Integration** – Can be integrated into other security-related applications.