MUBBASHIRUL ISLAM

Dhaka, Bangladesh / imsabbirahmed.info@gmail.com / +8801886788587

SUMMARY

Passionate self-taught cybersecurity enthusiast dedicated to exploring the dynamic fields of OSINT and threat analysis. Committed to continuous learning and hands-on experience, I actively engage in real-world projects that enhance my understanding of cybersecurity principles and practices. With a solid foundation in both Windows and Linux environments, I am skilled in using various tools for vulnerability assessments and incident response. My goal is to contribute meaningfully to the cybersecurity landscape by staying updated on emerging threats and employing innovative solutions to safeguard systems.

PERSONAL PROJECTS

1. X3Sync – Secure Browser Data Synchronization Tool

A Python-based project where I developed a tool to securely synchronize browser data—think bookmarks, cookies, and passwords—across multiple browsers like Brave, Chrome, Edge, and Firefox to a USB drive.
Impact: This tool has cut down the time users spend managing their data by 50%, making it easier for them to switch between devices without losing essential information.
Tech Stack: Python, PyWin32
GitHub Link: https://github.com/mubbashirulislam/X3sync.git

2. Home Wi-Fi Security Vulnerability (YouTube Video)

I created an educational video that highlights common Wi-Fi security vulnerabilities and shares best practices for home users to protect their networks.
Impact: This video has reached over 100 viewers, helping them understand the risks associated with unsecured Wi-Fi and empowering them to take action.
Format: Video
YouTube Link: https://youtu.be/6IjkxW6DEV8?si=6NuACHTt2sHCQAYa

3. XtractShot – Ethical Hacking & System Auditing Tool

In this project, I built a Python-based system monitoring tool designed for ethical hacking and auditing. It captures screenshots at regular intervals and emails them for monitoring purposes.
Impact: This tool has been successfully deployed in compliance testing, capturing over 500 screenshots that significantly enhance security audits for various systems.
Tech Stack: Python, Pillow, smtplib
GitHub Link: https://github.com/mubbashirulislam/Xtractshot.git

4. AutoCV – Automated CV Generator

I developed a Flask-based web application that helps users generate professional CVs from their input data.
Impact: This project streamlines the CV creation process, ensuring that multiple users can create polished resumes while keeping their information secure and private.
Tech Stack: Python, Flask
GitHub Link: https://github.com/mubbashirulislam/AutoCV.git

5. RizzCrypter – Gen Z-Inspired Encryption Tool

This is a fun and educational tool that employs custom key-based algorithms for encrypting and decrypting messages.
Impact: RizzCrypter has engaged users in understanding the basics of cryptography through an interactive and user-friendly interface, sparking interest in this essential aspect of cybersecurity.
Tech Stack: HTML, CSS, JavaScript, Python
GitHub Link: https://github.com/mubbashirulislam/RizzCrypter.git

TECHNICAL SKILLS

Operating Systems

- **Windows:** Proficient in navigating Windows environments with a focus on system administration, security settings, and user management.
  Experienced in configuring security features such as Windows Firewall and User Account Control (UAC) to enhance system security.
- **Linux:** Competent in using various Linux distributions, particularly Kali Linux, for security assessments and ethical hacking.
  Skilled in command-line operations for system administration tasks, including user permissions, file management, and software installation.

Basic Networking

- **Networking Concepts:** Solid understanding of fundamental networking concepts, including TCP/IP, DNS, DHCP, and subnetting.
  Familiar with network topology design and the principles of LAN/WAN architecture.
- **Network Configuration:** Experienced in configuring and troubleshooting home networks, routers, switches, and firewalls to enhance security.
  Hands-on experience with VPN setup and management to ensure secure remote access.

Cybersecurity Skills

- **OSINT (Open Source Intelligence):** Proficient in utilizing various OSINT tools and methodologies to gather intelligence from publicly available sources, enhancing threat analysis and situational awareness.
  Experienced with tools like **Maltego** for link analysis and data visualization, and **Shodan** for identifying vulnerabilities in IoT devices and web services.
  Conducted comprehensive research and analysis using platforms such as **Recon-ng** and **theHarvester** to collect actionable intelligence on potential security threats.
- **Google Dorking:** Skilled in using Google Dorking techniques to discover sensitive information and vulnerabilities on websites by crafting specific search queries.
  Familiar with various search operators (e.g., site:, filetype:, inurl:) to narrow down search results and identify potential security misconfigurations or exposed data.
  Applied Google Dorking in penetration testing to locate sensitive files, login portals, and misconfigured servers, enhancing the effectiveness of vulnerability assessments and security audits.
  Utilized Google Dorks to compile lists of exposed resources, helping organizations understand their security posture and take corrective measures.
- **Vulnerability Assessment:** Hands-on experience with network scanning tools like **Nmap** and **Nessus** for identifying and assessing potential vulnerabilities in systems and networks.
  Conducted security audits and penetration testing in controlled environments to evaluate system security and recommend remediation strategies.
- **Incident Response:** Familiar with the incident response lifecycle, including preparation, detection, analysis, containment, eradication, and recovery.
  Proficient in analyzing logs and alerts from various security information and event management (SIEM) systems to identify and respond to security incidents effectively.

Cybersecurity Tools

- **Network Analysis:** Skilled in using **Wireshark** for network traffic analysis, enabling the identification of anomalies and potential security threats in real time.
- **Web Application Security:** Familiar with **Burp Suite** for performing security testing on web applications, including penetration testing, vulnerability scanning, and session management analysis.
- **Security Monitoring:** Knowledgeable in deploying and configuring endpoint detection and response (EDR) tools to monitor system activity and detect malicious behavior.

Programming & Scripting

- **Python:** Basic proficiency in Python, focusing on developing automation scripts and security tools to streamline tasks and enhance operational efficiency.
- **Bash Scripting:** Capable of writing Bash scripts for task automation in Linux environments, facilitating routine system maintenance and data management tasks.

Version Control

- **Git & GitHub:** Understanding of Git for version control, enabling collaboration on cybersecurity projects and maintaining code integrity.
  Familiar with GitHub for project management, issue tracking, and sharing code with the open-source community.

SOFT SKILLS

- **Analytical Thinking:** I excel at breaking down complex problems and analyzing data effectively—an essential skill in OSINT research and vulnerability identification.
- **Attention to Detail:** I focus on the finer details during security assessments, ensuring that my analyses are thorough and accurate.
- **Problem-Solving:** I pride myself on finding practical solutions to technical challenges in both cybersecurity and web development projects.
- **Adaptability:** I'm quick to learn new tools and technologies, especially in the fast-paced world of cybersecurity.
- **Communication Skills:** I can explain technical concepts in a way that's easy for both technical and non-technical audiences to understand, which aids in collaboration and training efforts.
- **Team Collaboration:** I've worked with peers on various projects, sharing knowledge and contributing to our collective goals.

SELF-TAUGHT LEARNING

- **Cybersecurity & OSINT:** Actively engaged with online courses and webinars to build a solid foundation in cybersecurity principles and open-source intelligence techniques.
  Participated in forums and communities, exchanging knowledge and insights with fellow enthusiasts and professionals in the field.
  Conducted in-depth research on emerging threats and vulnerabilities, staying updated with the latest cybersecurity trends.
- **Programming & Development:** Independently learned programming languages such as Python and JavaScript through a variety of online resources, including courses on platforms like Coursera, Udemy, and freeCodeCamp.
  Developed practical applications to reinforce my learning, such as tools for automating tasks, generating CVs, and enhancing cybersecurity measures.
- **Networking Fundamentals:** Studied networking concepts via online tutorials and articles, gaining expertise in fundamental topics like TCP/IP, DNS, and subnetting.
  Gained hands-on experience by configuring and troubleshooting home networks, firewalls, and VPNs, enabling practical understanding of networking principles.
- **Hands-On Experience:** Engaged in personal projects that simulate real-world cybersecurity scenarios, applying knowledge to enhance skills in system auditing, vulnerability assessment, and incident response.
  Conducted ethical hacking exercises in controlled environments to test and refine my skills, ensuring a thorough understanding of security principles.
- **Continuous Improvement:** Regularly read cybersecurity literature, blogs, and listen to podcasts to deepen my understanding of advanced topics and remain informed about emerging technologies and threats.
  Set personal goals for learning new tools and techniques, dedicating time each week to practice and explore new concepts in cybersecurity and programming.

Education

- Completed Higher Secondary Certificate (HSC) from Cambrian College, Dhaka.
- Diploma in Computer Science from Daffodil Polytechnic Institute, Dhanmondi, Dhaka.