Shaurya Singh

shhauryasiingh@gmail.com   +1 (201) 582 0024   Bridgeport, CT

linkedin.com/in/shhauryasiingh   github.com/sh1nzer

EDUCATION

Master of Cybersecurity GPA 3.67, *Sacred Heart University* 03/2026
Courses: Network Security, Digital Forensics, Cryptography Fairfield, CT

Bachelor of Science in Computer Science, *University of Wollongong in Dubai, UAE* 01/2022 – 06/2024

SKILLS

Programming Languages
Python, PowerShell, SQL, Java, C, C++

Cybersecurity Skills
Network Security, Cryptography, System Security, Security Management,Digital Forensics

Technologies & Tools
Wireshark, Nmap, Metasploit, Nessus, Kali Linux, Snort,Git, VirtualBox, VMware, Active Directory, Linux/Unix, Windows Server

PROJECTS

Wifi Deauthenticator, *Link- https://github.com/sh1nzer/Wi-Fi-Deauthenticator.git*

- Created a Python-based tool leveraging aircrack-ng suite to scan Wi-Fi networks.
- Enabled selective and broadcast deauthentication of clients to test network security.
- Managed Wi-Fi adapter interface changes and status checks for enhanced control.
- Conducted penetration testing on multiple Wi-Fi networks with 99% success in client deauth.

Keylogger, *Link- https://github.com/sh1nzer/Keylogger.git*

- Developed a Python keylogger to capture keystrokes and log user activity on Windows.
- Achieved over 90% accuracy in key capture and logging for security auditing.
- Implemented encrypted local storage of logs to maintain data confidentiality.
- Enabled real-time monitoring capabilities through periodic log updates.

Network Scanner, *Link- https://github.com/sh1nzer/Network-Scanner.git*

- Developed a Python CLI tool performing ICMP, TCP, and ARP scans to identify live hosts on a network.
- Enabled port scanning for specified ranges, increasing scan flexibility and precision.
- Implemented timeout and configurable scan options for optimized performance.
- Analyzed and reported detailed scan results for over 100 hosts in real-time.

Brute Force Login Bypass, *Link- https://github.com/sh1nzer/brute-force-login-bypass.git*

- Simulated a Flask web app vulnerable to brute force attacks on login credentials.
- Used Burp Suite Intruder to automate username and password brute forcing from lists of 100+ entries.
- Identified admin credentials by analyzing response status codes effectively.
- Demonstrated exploit on admin panel access to highlight login security flaws.