AJIT SINGH

New Delhi, India | P: +91 7898072560 | ✉ ajeetsinghchahar2@gmail.com | **LinkedIn**🔗 | **GitHub**🔗 | **GitLab**🔗

EDUCATION

JAWAHARLAL NEHRU UNIVERSITY   New Delhi, India
(M.tech + B.tech) Dual Degree   Expected May 2024
Major in Computer Science and Engineering
Cumulative GPA: 7.0/9.0;

Relevant Coursework: Computer Networks, Operating Systems, Algorithms, Artificial Intelligence, Database and Management System, Software Engineering;

WORK EXPERIENCE

GOOGLE SUMMER OF CODE 2023
(Organization: GNUTLS)   Jun 2023 – Aug 2023
Project Title: **Add Support for Encrypted ClientHello(ECH)** 🔗
[C] [TLS] [Cryptography] [Security]

- Implemented Encrypted ClientHello(ECH) tls extension support for GNUTLS, which involved implementing different variants of clientHello (Inner and Outer), compressing, encoding and encrypting the ClientHelloInner, and addition of several new APIs. Finally tested the interoperability with other ECH implementations.
- Refactored Hybrid Public Key Encryption implementation exported from the Nettle library as ECH relies on it.
- Preserved privacy of users by encrypting the Server Name Indication, which can be used to censor content and fingerprinting. More Details: [**https://peonix.gitlab.io/gnutls-gsoc-2023/**]

PROJECTS

Adblock AppIndicator
- This blocks unwanted ads by using linux hosts file(/etc/hosts).
- It provides a simple navigation bar app interface created using pyGtk AppIndicator.

A Simple RootKit
- Implemented a rootkit in C that allows the attacker to gain access using a reverse shell.
- Used popular LD_PRELOAD based Jynx rootkits techniques (such as function call hooking) to hide its presence.
- Hosted the rootkit over an Azure cloud server and tested its functionality.

Amsg(Simple Anonymous messaging app)
- A simple messaging app that uses the Tor hidden services to anonymously connect two users without revealing IP addresses.
- Chat Interface could be a simple command line or a simple python flask based web interface (currently: web based only)
- The project is still under development, but it has the potential to be a valuable tool for secure communication.

ACHIEVEMENTS

HULT PRIZE   IIM Calcutta (July-2021)
- Participation in the "Capture the Flag" online contest organized by IIM Calcutta
BEST PAPER AWARD   (RAiSE-2023)
- Combining Forth and Rust: A Robust and Efficient Approach for Low-Level System Programming
LEETCODE 🔗
- 250+ Solved Problems/ 1600+ ratings

ADDITIONAL

Technical Skills: C/C++, Python; Javascript, HTML/CSS, React, Django, MySQL; Git; Linux, Nasm(x86); Flutter; BurpSuite; strace, lsof, docker;
Certifications & Training: Bits & bytes of Computer Networking(Coursera- Google) , SDLC(LinkedIn), Flutter(Udemy)