BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam menghadapi perkembangan digitalisasi yang terus berlangsung, tantangan keamanan siber menjadi fokus utama yang perlu diperhatikan. Perkembangan teknologi informasi dan komunikasi telah memberikan kemudahan bagi pengguna dalam mengakses dan menyimpan data. Namun, bersama dengan kemudahan tersebut, muncul pula berbagai risiko keamanan yang perlu diwaspadai.

Salah satu aspek yang menonjol dalam keamanan siber adalah risiko pencurian data melalui perangkat penyimpanan portabel seperti USB. Penggunaan USB sebagai media penyimpanan telah menjadi sangat umum dalam kehidupan sehari-hari. namun keberadaan perangkat USB keylogger menghadirkan ancaman yang serius. Sebuah keylogger merupakan contoh alat yang bersifat menyerang. Memanfaatkan kerentanan ini dalam sistem operasi yang memungkinkan untuk menjalankan serangan keylogger, yang secara diam-diam merekam aktivitas keyboard pada PC korban [1]. USB Keylogger tersebut kita bisa Mengantisipasi ancaman tersebut dengan menghancurkan USB keylogger tersebut agar data kita aman dan tidak disalahgunakan.

Dalam konteks ini, saya membuat alat USB Real time Keylogger pada frekuensi 2,4GHz yang di mana tantangan baru di dunia siber. Alat ini memungkinkan transmisi keystroke tanpa mengandalkan WiFi atau Bluetooth, melainkan memanfaatkan frekuensi radio 2,4GHz yang memiliki kestabilan dan kehandalan dalam pengiriman data. USB Real time Keylogger yang dapat mengirimkan setiap ketikan secara langsung tanpa menyimpannya di dalam USB, sehingga keamanan dan privasi data pengguna tidak aman.

Namun, perlu diingat bahwa tidak semua perangkat USB memiliki dampak negatif yang sama. Beberapa perangkat USB dapat memberikan manfaat yang besar dalam kehidupan sehari-hari, asalkan digunakan dengan bijaksana dan dengan memperhatikan keamanan data. Oleh karena itu, penting bagi pengguna untuk selalu waspada terhadap risiko keamanan yang mungkin timbul dari penggunaan perangkat USB.

1.2 Rumusan Masalah dan Solusi

Rumusan masalah yang dihadapi dalam pengembangan alat USB Real time Keylogger pada frekuensi 2,4GHz mencakup beberapa aspek antara lain:

1. Berapa jarak transmisi yang dapat dicapai oleh USB Real time Keylogger pada frekuensi 2,4GHz?
2. Bagaimana merancang dan membangun perangkat keras keylogger yang memenuhi kriteria ukuran fisik yang praktis dan efisien?
3. Apakah alat tersebut rentan terhadap penyusupan informasi palsu atau manipulasi data oleh pihak yang tidak berwenang?

Solusi yang diusulkan untuk mengatasi masalah ini meliputi:

1. Peningkatan antenna untuk meningkatkan jarak transmisi dan evaluasi kinerja pada berbagai kondisi lingkungan.
2. Penggunaan komponen perangkat keras yang ringkas dan ringan, serta optimalisasi layout untuk mencapai ukuran fisik yang praktis dan efisien.
3. Implementasi teknologi enkripsi untuk melindungi data dari penyusupan atau manipulasi oleh pihak yang tidak berwenang, dan penerapan protokol keamanan yang ketat untuk memastikan keamanan data selama transmisi dan penyimpanan.

Dengan menerapkan solusi-solusi yang telah dijelaskan, diharapkan kinerja dan keamanan alat USB Real time Keylogger pada frekuensi 2,4GHz dapat ditingkatkan secara signifikan, memungkinkan untuk mencapai jarak transmisi yang lebih jauh, meningkatkan kapasitas pengiriman data, serta memastikan desain perangkat keras yang praktis dan efisien. Selain itu, implementasi teknologi enkripsi dan protokol keamanan yang ketat diharapkan dapat melindungi data dari penyusupan atau manipulasi oleh pihak yang tidak berwenang, menjaga integritas dan kerahasiaan informasi yang ditangkap dan ditransmisikan oleh alat ini.

1.3 Tujuan

Berikut tujuan dari rumusan masalah sebagai berikut:

1. Menciptakan alat yang mampu mengirimkan keystroke secara langsung melalui frekuensi radio 2,4GHz.
2. Memastikan keamanan data yang dikirimkan dengan mencegah penyusupan informasi palsu atau manipulasi data oleh pihak yang tidak berwenang.

1.4 Batasan Masalah

1. Fokus Utama pada Pembuatan Alat perekaman data usb keylogger secara real-time melalui gelombang elektromagnetik pada frekuensi 2.4ghz untuk alat peretasan.
2. Implementasi kebijakan keamanan berfokus pada keamanan data pada usb keylogger.
3. Dalam proses pengembangan, tidak ada keterlibatan integrasi alat dengan platform atau sistem operasi tertentu, sehingga alat ini dirancang dengan fleksibilitas untuk dapat beroperasi secara independen tanpa ketergantungan pada lingkungan teknologi khusus.
4. Tidak melibatkan aspek hukum atau regulasi terkait keamanan data yang dapat mempengaruhi kebijakan organisasi ataupun perusahaan.

1.5 Penjadwalan Kerja

Tentu, berikut adalah tabel 1.1 yang memperinci pelaksanaan kerja yang dilakukan selama magang 2 semester dengan posisi sebagai IoT Engineer di Perusahaan CyberArmyID. Tabel ini pelaksanaan kerja, hari pelaksanaan, dan evaluasi pengerjaan tugas yang terkait.

Tabel 1.1 Pelaksanaan Kerja

No	Deskripsi Pekerjaan	Senin	Selasa	Rabu	Kamis	Jumat
1.	Pelaksanaan Kerja	09.00 - 17.00	09.00 - 17.00	09.00 - 17.00	09.00 - 17.00	09.00 - 17.00
2.	Evaluasi pengerjaan tugas	15.00 - 17.00	Opsional	Opsional	Opsional	15.00 - 17.00

Selama 11 minggu, proses pembuatan alat dimulai dari penelitian tentang USB keylogger dan teknologi transmisi radio hingga integrasi perangkat keras dan lunak, dengan setiap minggu memiliki aktivitas harian yang berfokus pada tahapan tertentu dari proses tersebut.

Berikut adalah ringkasan detail pekerjaan yang dijelaskan berdasarkan pembagian mingguan selama proses pembuatan alat yang terbagi menjadi 11 minggu dari mulai penelitian alat usb keylogger yang ditransmisikan melalui gelombang radio sampai dengan dokumentasi alat yang akan dijelaskan pada tabel 1.2 keterangan/aktivitas harian dibawah:

Tabel 1.2 Keterangan/Aktivitas Harian

No	Tanggal	Keterangan/Aktivitas Harian
1.	Minggu 4 (6 November 2023 – 10 November 2023)	Melakukan penelitian dan pembelajaran mandiri untuk mendalami lebih lanjut tentang teknologi USB Keylogger.
2.	Minggu 5 (13 November 2023 – 17 November 2023)	Mengumpulkan bahan dan informasi yang diperlukan untuk implementasi USB Keylogger.
3.	Minggu 6 (20 November 2023 – 24 November 2023)	Menyiapkan langkah-langkah dan sumber daya yang diperlukan untuk mengimplementasikan USB Keylogger.
4.	Minggu 7 (27 November 2023 – 1 Desember 2023)	• Pemahaman sistem kerja USB Keylogger: Memahami cara USB Keylogger bekerja. Tinjau prinsip dasar dan identifikasi potensi skenario penggunaan. • Belajar Mandiri
5.	Minggu 8 (4 Desember 2023 – 8 Desember 2023)	Praktek mengimplementasikan USB Keylogger pada beberapa perangkat. Evaluasi kemampuan dan risiko yang terkait
6.	Minggu 9 (11 Desember 2023 – 15 Desember 2023)	• Dokumentasi Proyek • Pengembangan lanjutan untuk alat USB Keylogger
7.	Minggu 10 (18 Desember 2023 – 22 Desember 2023)	Penyempurnaan Implementasi
8.	Minggu 11 (25 Desember 2023 – 29 desember 2023)	• Dokumentasi Proyek • Pengembangan lanjutan untuk alat USB Keylogger
9.	Minggu 12 (1 Januari 2024 – 5 Januari 2024)	Melakukan evaluasi lanjutan terhadap alat USB Keylogger dan menyiapkan langkah-langkah untuk memperbaiki masalah yang ditemukan.
10.	Minggu 19 (8 Januari 2024 – 12 Januari 2024)	Melakukan evaluasi akhir terhadap produk dan proses pembuatan untuk mengidentifikasi area perbaikan.
11.	Minggu 20 (15 Januari 2024 – 19 Januari 2024)	Membuat Produk dari hasil proyek yang telah dikembangkan dan dibuat