

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dengan pesatnya kemajuan teknologi informasi, keamanan data menjadi sangat penting karena meningkatnya jumlah perangkat yang saling terhubung. Ketergantungan berbagai sektor pada data digital sensitif menjadikan keamanan sebagai isu krusial untuk mencegah ancaman tak bertanggung jawab. Serangan *zero-click* adalah jenis eksploitasi yang memungkinkan penyerang mengendalikan perangkat korban tanpa memerlukan interaksi pengguna seperti mengklik tautan atau membuka file. Penelitian ini bertujuan mengevaluasi tingkat kerentanan perangkat terhadap serangan Keystroke Injection via Bluetooth menggunakan BlueDucky. Fakta menunjukkan bahwa serangan berbasis Bluetooth terus meningkat, dengan lebih dari 4,2 miliar perangkat digunakan secara global pada tahun 2023 dan lebih dari 100 kerentanan teridentifikasi sejak 2020. Eksploitasi yang memungkinkan eksekusi kode jarak jauh tanpa interaksi pengguna [1].

Kerentanan Bluetooth seperti “BlueBorne” telah memungkinkan eksploitasi yang dapat menginfeksi perangkat dalam hitungan detik tanpa memerlukan pairing sebelumnya. Berdasarkan urgensi permasalahan ini, penelitian ini diharapkan dapat memberikan wawasan mendalam tentang potensi ancaman Bluetooth *zero-click* dan bagaimana BlueDucky dapat digunakan untuk menguji tingkat keamanan perangkat [2]. Bluetooth memang menawarkan kemudahan dalam menghubungkan berbagai perangkat, namun juga membawa risiko keamanan. Teknologi ini bisa dieksploitasi oleh serangan seperti *zero-click*, yang memungkinkan penyerang mengakses perangkat tanpa interaksi pengguna. Serangan *zero-click* tidak menunjukkan tanda-tanda yang jelas, serangan ini bisa terjadi dengan cepat tanpa kita sadari [3]. Risiko ini muncul karena adanya celah pada sistem Bluetooth yang terbuka. Oleh karena itu, penting untuk mengevaluasi dan mengatasi kerentanan yang ada. Semakin luas penggunaan Bluetooth, semakin besar pula potensi ancaman terhadap privasi dan keamanan data [4].

Teknologi nirkabel seperti Bluetooth dan Wi-Fi sering menjadi celah bagi serangan ini. Aplikasi seperti WhatsApp dan iMessage juga bisa dimanfaatkan untuk melakukan serangan *zero-click* [5]. *Zero-click* adalah serangan siber yang

tidak membutuhkan tindakan apa pun dari pengguna, karena tidak terlihat, serangan ini sangat berbahaya dan sulit dideteksi [6]. Seiring berkembangnya teknologi komunikasi nirkabel, ancaman serangan *zero-click* menjadi semakin besar. Oleh karena itu, penting untuk meningkatkan pemahaman tentang ancaman ini dan melakukan pengujian serta perlindungan secara berkala untuk menjaga perangkat dan data tetap aman dari serangan canggih seperti ini [7]. Serangan seperti *zero-click* menimbulkan kekhawatiran besar terhadap keamanan digital, terutama bagi jurnalis dan aktivis. Kelompok ini rentan karena sering menjadi target pihak berkepentingan. Serangan dapat mengancam privasi, kebebasan berbicara, bahkan keselamatan mereka. Celah ini juga bisa digunakan untuk pengawasan ilegal, pencurian data, atau manipulasi informasi. Maka dari itu, penting untuk meningkatkan kesadaran dan menerapkan perlindungan digital yang ketat [8].

Penelitian sebelumnya mencoba mengatasi serangan *zero-click* dengan menggunakan konsep smartphone virtual. Dalam pendekatan ini, aplikasi yang rentan dipindahkan ke lingkungan virtual seperti sandbox atau server cloud. Tujuannya adalah agar serangan tidak langsung berdampak pada perangkat utama. Hal ini membatasi akses penyerang hanya pada aplikasi tertentu dan mencegah serangan menyebar. Konsep ini terbukti cukup efektif dalam mengurangi dampak dan melindungi data pengguna [9]. Namun, penelitian tersebut juga menemukan beberapa kelemahan penting. Pertama, sistem sandbox masih bisa ditembus oleh serangan *zero-click* yang lebih canggih. Kedua, penggunaan server cloud memerlukan biaya besar dan koneksi internet yang stabil. Hal ini bisa menjadi kendala bagi pengguna dengan akses terbatas. Selain itu, solusi ini belum sepenuhnya efektif melawan jenis serangan *zero-click* yang baru dan belum terdeteksi [10]. Terakhir, ketiadaan notifikasi real-time membuat pengguna harus memeriksa aplikasi secara manual untuk mengetahui pesan baru. Hal ini mengurangi kenyamanan dan efisiensi, terutama dalam situasi yang butuh respons cepat [11].

Salah satu serangan yang paling menonjol adalah BlueDucky, yang menyisipkan perintah ke perangkat korban seolah berasal dari pengguna. Serangan ini memanfaatkan celah pada protokol Bluetooth dan dapat dilakukan tanpa interaksi korban (*zero-click*). Penyerang bisa mencuri data, mengubah sistem,

menginstal malware, atau mengambil alih perangkat sepenuhnya. Karena menyerang lewat proses pairing dan otentikasi, serangan ini berjalan diam-diam tanpa jejak yang jelas. Hal ini membuatnya sulit dideteksi oleh pengguna maupun sistem keamanan [12]. Selain itu, serangan ini tidak terbatas pada perangkat tertentu, melainkan dapat menargetkan berbagai perangkat yang mendukung koneksi Bluetooth, termasuk laptop, *smartphone*, tablet, hingga perangkat *IoT*. Hal ini membuat *BlueDucky* menjadi ancaman serius dalam dunia keamanan siber, terutama bagi organisasi yang bergantung pada teknologi nirkabel untuk operasional sehari-hari [13].

Penelitian sebelumnya menunjukkan bahwa banyak pengguna belum menyadari risiko yang muncul setelah proses pairing Bluetooth. Kurangnya pemahaman tentang potensi serangan membuat perangkat yang sudah terhubung menjadi lebih rentan. Hal ini membuka peluang bagi pihak tak bertanggung jawab untuk mengeksploitasi celah keamanan. Salah satu ancaman serius adalah serangan *zero-click*, yang bisa terjadi tanpa interaksi pengguna. Serangan ini berpotensi membahayakan data dan privasi tanpa disadari oleh pemilik perangkat [14]. Dengan semakin banyaknya perangkat yang menggunakan teknologi Bluetooth dalam kehidupan sehari-hari, penting untuk menganalisis dan memahami kerentanan yang ada, terutama yang terkait dengan serangan *zero-click* seperti *Blue Ducky* [15]. Oleh karena itu, penulis tertarik untuk melakukan penelitian berjudul “Evaluasi Kerentanan Bluetooth *Zero-click* Menggunakan Blue Ducky pada Keystroke Injection”. Penelitian ini bertujuan untuk memberikan kontribusi dalam memahami dan mengatasi kerentanan pada teknologi Bluetooth, khususnya serangan *zero-click* yang dapat terjadi tanpa interaksi pengguna. Tantangan utama dalam penelitian ini adalah terbatasnya literatur, karena Blue Ducky masih tergolong baru dan belum banyak dibahas dalam penelitian sebelumnya.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang di atas maka dapat dipaparkan rumusan masalah sebagai berikut :

1.2.1 Permasalahan

Meskipun kita sering menggunakan Bluetooth untuk menyambungkan HP, earphone, dan perangkat lain, ada bahaya tersembunyi yang disebut serangan *zero-*

click. Artinya, peretas bisa membajak perangkat kita tanpa perlu kita sentuh atau klik apa pun. Salah satu alat yang bisa dipakai peretas adalah BlueDucky, yang bisa “mengetik” perintah berbahaya ke HP kita seolah-olah kita sendiri yang mengetik. Ini bisa sangat merugikan, misalnya data kita dicuri atau HP kita diambil alih. Sayangnya, banyak dari kita, bahkan para ahli keamanan siber, belum sepenuhnya paham bagaimana serangan seperti BlueDucky ini bekerja.

1.2.2 Metode Usulan

Dalam penelitian ini, diusulkan penerapan metode analisis kerentanan Bluetooth *zero-click* menggunakan *Blue Ducky*, dengan fokus pada teknik *Keystroke Injection*. Pendekatan ini memanfaatkan *Keystroke Injection* untuk mengeksploitasi kelemahan Bluetooth, memungkinkan penyerang untuk memasukkan perintah injection ke target pengguna. Metode ini dinilai efektif karena mampu mensimulasikan serangan nyata dengan berbagai skenario, sehingga dapat mengevaluasi sejauh mana kelemahan pada protokol Bluetooth dapat dimanfaatkan.

1.2.3 Pertanyaan Penelitian

Berdasarkan permasalahan yang telah disebutkan di atas dapat dirumuskan pertanyaan penelitian sebagai berikut:

1. Berapa waktu yang dibutuhkan BlueDucky untuk berhasil mengeksploitasi kerentanan Bluetooth *zero-click* dalam serangan *Keystroke Injection* pada perangkat target?

1.3 Tujuan dan Manfaat

1.3.1 Tujuan

Berdasarkan permasalahan yang telah disebutkan diatas, dapat dirumuskan pertanyaan penelitian sebagai berikut:

1. Mengetahui efektivitas serangan *Keystroke Injection* menggunakan BlueDucky pada kerentanan Bluetooth *zero-click* terhadap perangkat smartphone samsung dan xiaomi dengan berbagai versi bluetooth dan sistem operasi android.
2. Menganalisis lalu lintas paket Bluetooth pada Wireshark dapat menjelaskan mekanisme keberhasilan atau kegagalan serangan *Keystroke Injection zero-click* dari BlueDucky pada perangkat target.

1.3.2 Manfaat

Penelitian ini diharapkan dapat secara signifikan meningkatkan kesadaran pengguna akan potensi bahaya serangan siber berbasis Bluetooth, terutama *zero-click Keystroke Injection*.

1.3.3 Batasan Masalah

Dengan didasari latar belakang yang telah dipaparkan, maka dapat ditentukan batasan masalah penelitian sebagai berikut:

1. Fokus pada serangan *Zero Click* dan *BlueDucky*.
2. Sistem operasi open source *hacking* dan *pentesting* menggunakan Debian 12, dan perangkat target menggunakan *handphone (smartphone)*.
3. Bluetooth harus aktif jika Bluetooth tidak aktif maka tidak dapat melakukan penyerangan.
4. Pastikan *handphone (smartphone)* dalam posisi aktif (tidak terkunci kata sandi).
5. Pastikan *handphone (smartphone)* terhubung ke internet.
6. Penelitian ini berlaku untuk *handphone (smartphone)* samsung dan xiaomi.
7. Sistem operasi penyerang terbatas pada Debian 12 dikarenakan pertimbangan kompatibilitas dan stabilitas *BlueDucky* dalam melakukan interaksi *low-level* dengan adaptor Bluetooth.
8. Target smartphone menggunakan sistem operasi Android 11 (Xiaomi) dan Android 12 (Samsung).
9. Windows dan macOS tidak digunakan dalam penelitian ini karena keterbatasan akses terhadap fitur eksploitasi Bluetooth.

1.4 Sistematika Penulisan

Skripsi ini ditulis dengan menggunakan sistematika penulisan seperti berikut :

BAB I PENDAHULUAN

Bab ini mencakup latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, metodologi penelitian, serta sistematika penulisan skripsi

BAB II KAJIAN PUSTAKA

Bab ini akan disajikan tinjauan literatur tentang protokol Bluetooth, jenis-jenis serangan nirkabel, khususnya serangan *zero-click* dan *BlueDucky*, serta studi-studi terkait yang relevan dengan topik penelitian ini.

BAB III METODE USULAN

Bab ini menguraikan perancangan sistem yang dirancang untuk mengevaluasi kerentanan Bluetooth *zero-click* menggunakan metode serangan *Blue Ducky* pada *Keystroke Injection*.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menyajikan hasil evaluasi kerentanan Bluetooth *zero-click* pada pengujian serangan *BlueDucky*.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari keseluruhan penelitian yang telah dilakukan, dan memberikan rekomendasi untuk penelitian selanjutnya serta saran untuk meningkatkan keamanan perangkat Bluetooth.