BAB I

PENDAHULUAN

1.1 Latar Belakang

Tahun 2022 hingga 2023 merupakan tahun dengan kejadian kebocoran data terbesar di Indonesia. Pakar Keamanan Siber, Teguh Aprianto memberikan informasi bahwa telah terjadi kebocoran data 34 juta *passports* Indonesia pada 05 Juli 2023. Hal ini dikonfirmasi langsung melalui media ANTARA kepada Direktur Jendral Imigrasi Kementerian Hukum dan Hak Asasi Manusia, Silmy Karim bahwa kejadian tersebut sedang dilakukan identifikasi untuk menemukan *root cause analysis* sesuai dengan prosedur yang berlaku [1]. Kasus kebocoran data lainnya juga terjadi pada 08 Mei 2023, Bank Syariah Indonesia (BSI) mengalami gangguan layanan perbankan dikarenakan serangan Ransomware dengan jenis Lockbit 3.0. Serangan ini mengakibatkan keluhan yang cukup tinggi oleh para nasabah. Menurut Pakar Keamanan Siber dan Forensik Digital, Alfons Tanujaya, Ransomware akan berusaha semaksimal mungkin untuk mengenkripsi data penting, *backup*, dan sistem yang bertujuan mengganggu jalannya perusahaan [2]. Pada 03 Juli 2023 Teguh Aprianto kembali memberikan informasi bahwa telah terjadi kebocoran 35 juta data dari program MyIndiHome [3]. Hal ini terjadi bukan tanpa sebab, namun berasal dari kelemahan *people* dan kurangnya *security* yang mendukung pada *endpoint device* seperti Laptop atau *smartphone.*

Berdasarkan StatCounter pada tahun 2018 hingga 2022 tercatat sebanyak 74,95% pengguna *smartphone* menggunakan Android sebagai sistem operasi yang digunakan [4]. Sistem Operasi ini didukung dengan aplikasi-aplikasi yang memudahkan aktivitas manusia. Namun, kemudahan yang ditawarkan tentunya beriringan dengan bahaya yang ditimbulkan karena aplikasi yang ada akan menjadi target utama oleh *Hacker* untuk melakukan serangan.

Aplikasi yang tersedia di *smartphone* harus melalui pengujian keamanan dengan baik sesuai dengan ISO/IEC 27001 [5]. Dalam hal ini salah satu organisasi yang memberikan metode pengujian keamanan pada aplikasi adalah. *Open Sources Foundation for Application Security* (OWASP). OWASP merupakan salah satu organisasi yang berfokus pada pengujian keamanan aplikasi dengan merilis *Top* 10

Mobile Risks berupa *Insecure Data Storage, Improper Platform Usage, Insecure Authentication, Insufficient Cyptography,* dan lain sebagainya pada celah keamanan aplikasi Android [6].

Dalam melakukan aksinya, *Hacker* menggunakan beberapa media untuk mengirimkan *malware* kepada korban. *Malware* merupakan perangkat lunak yang diciptakan untuk menyusup atau merusak sistem komputer dari pemilik sehingga memungkinkan untuk melakukan pencurian data / informasi. Menurut Badan Siber dan Sandi Negara (BSSN), serangan melalui *malware* merupakan salah satu dari *Top* 10 jenis serangan siber yang paling sering dilaporkan di Indonesia. Media yang digunakan oleh *Hacker* dapat berupa *social media* seperti: *WhatsApp Messenger* atau Telegram, *email attachment,* dan URL palsu yang mengarahkan *user* untuk mengunduh aplikasi berbahaya dengan mengatasnamakan instansi atau pihak tertentu seperti: Undangan Pernikahan.apk dan Cek Resi J&T.apk.

Tingginya korban yang mengalami kerugian secara *financial* akibat menginstal aplikasi Undangan Pernikahan.apk dan Cek Resi J&T.apk, tentu hal ini dirasa perlu untuk dilakukan pengujian pada aplikasi tersebut dengan *Static and Dynamic Application Security Testing*. Untuk menciptakan sebuah simulasi yang *end-to-end* diperlukan pembuatan sebuah aplikasi tambahan dengan memanfaatkan Metasploit untuk dapat melakukan *command and control attack.*

Melalui permasalahan di atas penulis mengambil topik untuk dijadikan judul "Analisis Pengaruh *Virtual Private Network* Pada Aplikasi Berbasis Android Terinfeksi *Malware* Dengan *Static and Dynamic Application Security Testing*". Diharapkan dengan adanya penelitian ini dapat menganalisis *risk rating, vulnerability, threat actor, threat intelligence platform, TLS/SSL security test, speedtest* dan *command and control attack* dengan atau tanpa *Virtual Private Network.*

1.2 Rumusan Masalah

1. Bagaimana cara melakukan analisis *Static and Dynamic Application Security Testing* pada aplikasi *Creator*.apk, Undangan Pernikahan.apk dan Cek Resi J&T.apk?
2. Bagaimana risiko dan kerentanan yang dihasilkan pada aplikasi *Creator*.apk, Undangan Pernikahan.apk dan Cek Resi J&T.apk?

3. Bagaimana cara untuk mengetahui *URL Malicious* yang terdapat pada aplikasi Undangan Pernikahan.apk dan Cek Resi J&T.apk?
4. Bagaimana pengaruh VPN pada serangan *command and control*?
5. Bagaimana kualitas layanan internet ketika menggunakan VPN dan *non*-VPN?

1.3 Batasan Masalah

1. Simulasi *Static and Dynamic Application Security Testing* ini menggunakan aplikasi yang bersifat *open source;*
2. Keluaran dari simulasi ini adalah berupa hasil analisis dan rekomendasi untuk melakukan mitigasi dari sisi *user* dan tidak sampai ke dalam tahap perbaikan aplikasi.

1.4 Tujuan

1. Melakukan pengujian keamanan pada aplikasi Android menggunakan metode SAST dan DAST;
2. Menganalisis *risk rating* dan *vulnerability* dari aplikasi Android;
3. Menganalisis *threat actor, threat intelligence platform,* dan TLS/SSL *security*;
4. Menganalisis kemampuan VPN dan *non*-VPN terhadap serangan *command and control*;
5. Menganalisis kualitas layanan internet ketika menggunakan VPN dan *non*-VPN.

1.5 Manfaat

1. Untuk mencegah terjadinya *lateral movement* yang dapat merugikan individu maupun instansi*;*
2. Memberikan informasi secara *detail* tentang *vulnerability* apa saja yang terdapat pada aplikasi Android;
3. Memberikan klasifikasi *vulnerability* yang ditemukan berdasarkan dampak yang dihasilkan kepada *user*;
4. Mengetahui manfaat VPN pada aplikasi android terhadap serangan *command and control*;
5. Mengetahui pengaruh VPN dan *non*-VPN terhadap kualitas layanan internet.

1.6 Sistematika Penulisan

1. **BAB 1: PENDAHULUAN**

   Pada bagian ini membahas mengenai latar belakang, rumusan masalah, yang diangkat, batasan masalah, tujuan dan manfaat penelitian.

2. **BAB 2: DASAR TEORI**

   Pada bagian ini membahas mengenai referensi penelitian sebelumnya, landasan teori mengenai *Static and Dynamic Application Security Testing.*

3. **BAB 3: METODE PENELITIAN**

   Pada bagian ini membahas mengenai perangkat keras dan perangkat lunak yang digunakan, rancangan blok diagram, alur penelitian, penjelasan *script* atau *command* yang digunakan serta skenario pengujian aplikasi.

4. **BAB 4: HASIL DAN PEMBAHASAN**

   Pada bagian ini membahas mengenai *risk rating analysis, vulnerability analysis, threat actor analysis, threat intelligence platform analysis, TLS/SSL security test*, *speedtest analysis* dan *C&C attack analysis*.

5. **BAB 5: PENUTUP**

   Pada bagian ini membahas mengenai kesimpulan dan saran.