BAB I
PENDAHULUAN

1.1. Latar Belakang

Hadirnya *smartphone* sudah menjadi bagian dari gaya hidup, terlebih dalam perkembangan teknologi *smartphone* sangat berpengaruh. Manusia saling berkomunikasi dengan jaringan internet menggunakan *smartphone*. Dalam perkembangan teknologi yang harus diperhatikan adalah masalah keamanan terhadap jaringan. Keamanan jaringan memerlukan perhatian yang sangat besar. Semakin bertambahnya penggunaan teknologi internet semakin bertambah pula kebutuhan terhadap keamanan jaringan. Jika keamanan jaringan tidak diperhatikan dengan baik, maka hal tersebut mampu mengakibatkan sistem rentan terhadap serangan dari pihak-pihak tidak bertanggung jawab yang dapat menyalahgunakan data. Salah satu serangan keamanan jaringan yang terjadi pada *smartphone* khususnya pada sistem operasi Android adalah serangan *malware*[1].

Berdasarkan *2023 SonicWall Cyber Threat Report*, serangan *malware* secara keseluruhan mengalami peningkatan 11% sebanyak 6.06 milyar serangan pada tahun 2023, dengan mencatat lonjakan yang sangat tinggi pada Amerika Latin dan AS yaitu sekitar 30% dan 15%. Sedangkan, terjadi penurunan sebanyak 2% pada Eropa dan Asia[2]. Tercatat sekitar 74% kebocoran data disebabkan oleh kesalahan manusia *(human error)*[3]. Serangan *malware* termasuk serangan yang berbahaya dan dapat merugikan sebagian besar korbannya karena *malware* dapat menyebar ke dalam sistem dan mengambil data-data sensitive, menyebarkan kerusakan, menguntungkan penyerang secara finansial, dan lain sebagainya. *Malware* dapat masuk ke dalam sistem menggunakan berbagai macam metode seperti *phising*, rekayasa sosial, pengunduhan *software* yang tidak aman, dan masih banyak lagi. Salah satu serangan *malware* adalah dengan memanfaatkan sistem operasi Android menggunakan serangan *backdoor*. *Backdoor* merupakan suatu program yang dirancang untuk memasuki sebuah sistem tanpa melalui proses autentikasi. Jika *backdoor* sudah masuk ke dalam sistem artinya sistem

dapat diambil alih dengan mudah[4]. Serangan *backdoor* dikategorikan sebagai serangan *malware.* Pada mulanya, *backdoor* digunakan pengembang *software* atau *programmer* sebagai hak akses khusus ke dalam sistem untuk memperbaiki masalah seperti *bug* atau *crash*. Namun demikian, seiring berkambangnya teknologi *backdoor* menjadi hal yang perlu diperhatikan karena bisa mengakibatkan serangan keamanan pada sistem. Dengan terjadinya penyisipan *backdoor* pada sebuah sistem dapat mengakibatkan kebocoran data dan bahkan pengambilalihan hak akses sistem[5].

Fenomena serangan *backdoor* yang sering terjadi akhir-akhir ini khususnya di Indonesia adalah menggunakan *social engineering* melalui WhatsApp. Pengguna mendapat sebuah undangan atau surat berbentuk file *.pdf ataupun *.apk yang dikirimkan melalui pesan WhatsApp[6]. Sehingga, dari permasalahan tersebut timbulah penelitian analisis *backdoor*. Penyisipan *backdoor* pada penelitian ini menggunakan *malware* Backdoor-apk. *Malware* Backdoor-apk merupakan sebuah *tool* untuk menginjeksikan *backdoor* ke dalam aplikasi Android yang dibangun dari skrip bahasa Shell. *Malware* Backdoor-apk akan disisipkan masuk ke dalam sistem operasi Android melalui aplikasi Turbo VPN sebagai perantara. Selanjutnya, akan dilakukan analisis menggunakan metode *reverse engineering*. Metode *Reverse engineering* merupakan proses analisis dan pemahaman mengenai desain, struktur, dan fungsi dari sebuah produk atau sistem yang melibatkan pembongkaran objek atau *software* untuk mengetahui informasi dan cara kerja serta memahami cara pembuatannya[7]. Metode *Reverse engineering* ini dipilih karena memungkinkan peneliti untuk mengidentifikasi perilaku *malware* dan mengetahui kerentanan terhadap sebuah aplikasi yang diakibatkan penyisipan *backdoor* pada sistem operasi Android.

Pada penelitian ini akan dilakukan analisis secara otomatis menggunakan MobSF dan analisis manual menggunakan JADX pada aplikasi Turbo VPN sebelum dan sesudah disisipi *malware* Backdoor-apk. Melalui hasil analisis yang didapatkan dari keduanya baik secara otomatis MobSF dan manual JADX akan dilakukan perbandingan. Hal ini, bertujuan untuk mengetahui perubahan dan

anomali yang terjadi sebelum dan sesudah penyisipan *backdoor* secara otomatis MobSF dan manual JADX.

1.2. Rumusan Masalah

Keamanan sistem operasi pada *smartphone* merupakan hal yang sangat penting karena, hal ini dapat menyebabkan terjadinya serangan kepada para pengguna *smartphone* tanpa melihat waktu dan tempat. Maka dari itu, dilakukan sebuah analisis menggunakan teknik *reverse engineering* mengenai *backdoor* yang disisipkan pada aplikasi Turbo VPN di perangkat Android. Kemudian, akan dilakukan perbandingan menggunakan MobSF secara otomatis dan JADX secara manual.

1.3. Pertanyaan penelitian

Berdasarkan rumusan masalah di atas, maka pertanyaan pada penelitian ini adalah:

1. Bagaimana kemampuan *malware* Backdoor-apk setelah terinstal?
2. Bagaimana analisa perubahan kode pada aplikasi Android sebelum dan sesudah dieksploitasi menggunakan *malware* Backdoor-apk?

1.4. Tujuan

Adapun tujuan dari penelitian ini adalah :

1. Mengetahui kemampuan *malware* Backdoor-apk setelah berhasil menyisipi sistem Android.
2. Menganalisa perubahan kode pada aplikasi Android sebelum dan sesudah dilakukan eksploitasi dengan Backdoor-apk menggunakan MobSF dan JADX.

1.5. Batasan masalah

Batasan masalah dari penelitian ini adalah:

1. Pengujian dilakukan dengan *tools* metasploit.
2. Penyisipan *backdoor* dengan menggunakan *malware* Backdoor-apk.
3. Menggunakan sistem operasi Android versi 5.1 untuk pengujian *backdoor* pada *smartphone*.
4. Menggunakan aplikasi Turbo VPN sebagai pengujian exploitasi.
5. Menggunakan JADX untuk membandingkan perubahan sebelum dan sesudah dilakukan eksploitasi.
6. Pengujian secara otomatis dilakukan menggunakan MobSF.
7. Menemukan dan mengidentifikasi anomali yang ada setelah penyisipan menggunakan *malware* Backdoor-apk.

1.6. Manfaat

Dari hasil penelitian yang dilakukan, diharapkan dapat memberi manfaat sebagai berikut:

1. Dapat mengetahui kemampuan dan perilaku *malware* Backdoor-apk setelah dilakukan penyisipan dan instalasi pada sistem Android.
2. Dapat mengetahui perubahan kode dan anomali pada aplikasi Android sebelum dan sesudah dieksploitasi dengan *malware* Backdoor-apk menggunakan JADX dan MobSF.