BAB I
PENDAHULUAN

1.1 Latar Belakang

Ancaman keamanan siber di era *digital* saat ini berkembang pesat seiring dengan tingginya penggunaan perangkat *mobile* khususnya *Android*, yang terkoneksi dengan internet. Salah satu ancaman yang mendapat perhatian serius adalah *Remote Access Trojan* (RAT). RAT merupakan perangkat lunak berbahaya yang dirancang untuk mengambil kendali jarak jauh atas perangkat korban dengan cara tersembunyi (Kara & Aydos, 2019; Valeros & Garcia, 2020).

Berdasarkan data Badan Siber dan Sandi Negara (BSSN) tahun 2023, tercatat sekitar 203.990.813 *traffic anomaly* di Indonesia, dengan jenis anomali tertinggi berupa *generic trojan* RAT (Lanskap Keamanan Siber Indonesia 2023, 2024). Temuan ini menunjukkan bahwa aktivitas *malware* yang memanfaatkan akses jarak jauh sudah menjadi ancaman signifikan di Indonesia.

Hal tersebut juga diperkuat oleh data terbaru dari *Kaspersky* yang dilaporkan oleh *Securelist* (2025). Pada kuartal pertama tahun 2025, tercatat lebih dari 12 juta serangan terhadap perangkat *mobile* yang melibatkan *malware, adware,* maupun aplikasi tidak diinginkan. Dari total tersebut, *trojan* menjadi kategori ancaman terbesar dengan kontribusi sekitar 39,56% dari seluruh insiden yang terdeteksi. Selain itu sekitar 15,5% pengguna mengalami dampak dari serangan siber yang memanfaatkan metode rekayasa sosial (*social engineering*).

Penyebaran RAT tidak terlepas dari teknik rekayasa sosial (*social engineering*) yang memanfaatkan kelemahan manusia. Pelaku sering kali menggunakan pesan manipulatif, *email phishing*, atau tautan palsu untuk

mengelabui korban agar tanpa sadar mengunduh dan memasang RAT di perangkat *Android* mereka (Ayumu dkk., 2024). Serangan rekayasa sosial melonjak tajam selama pandemi *COVID*-19 karena meningkatnya aktivitas daring dan rendahnya literasi digital (Hijji & Alam, 2021). Adapun teknik *social engineering* seperti *phishing*, *pretexting*, dan *baiting* telah terbukti efektif dalam mengecoh pengguna *Android* untuk mengunduh dan menginstal RAT (Mokoena dkk., 2020). Teknik ini sangat sulit dideteksi karena tidak meninggalkan jejak teknis, melainkan bermain pada aspek psikologis pengguna.

Oleh karena itu, ancaman RAT yang dikombinasikan dengan *social engineering* menjadi masalah keamanan siber yang kompleks dan multidimensi (G. S. Mahendra dkk., 2022) Secara teknis, RAT yang menyerang *Android* dapat melakukan berbagai aktivitas seperti membaca pesan, merekam percakapan, mengambil alih kamera dan mikrofon, hingga mengakses akun keuangan (Dwiananda dkk., 2019). Proses eksploitasi tersebut semakin canggih dengan pemanfaatan *framework* seperti *Metasploit* untuk membangun *payload Reverse_TCP* yang tertanam dalam APK (Somantri & Alhidamkara, 2024).

Penelitian terdahulu membahas pemanfaatan RAT pada Android untuk memperoleh data pribadi melalui pendekatan social engineering. Aplikasi berbahaya didistribusikan dengan cara menyamarkan fungsinya agar pengguna bersedia menginstalnya, sehingga penyerang dapat mengakses informasi seperti kontak, pesan, serta mengontrol fitur perangkat seperti kamera, mikrofon, dan lokasi. Hasilnya menunjukkan bahwa teknik social engineering memiliki tingkat efektivitas tinggi, namun penelitian ini belum mengimplementasikan sistem

otomatisasi dalam pengolahan dan pengiriman data secara real-tim (Satrio Hadikusuma & Rizaludin, 2023)

Berdasarkan kajian penelitian sebelumnya, dapat disimpulkan bahwa pemanfaatan RAT pada perangkat *Android* yang dipadukan dengan teknik *social engineering* terbukti efektif dalam memberikan akses kendali terhadap perangkat korban serta memungkinkan pengambilan informasi pribadi. Meskipun demikian, sebagian besar pendekatan yang ada masih bergantung pada interaksi manual dalam proses ekstraksi maupun distribusi data, sehingga efisiensi serangan menjadi terbatas.

Kondisi tersebut menegaskan pentingnya penerapan *mekanisme auto exploit* dan *automatic reporting* untuk mengurangi ketergantungan pada intervensi manual, meningkatkan efektivitas eksploitasi, sekaligus mempercepat pendokumentasian hasil serangan secara konsisten. Oleh karena itu, penelitian ini dirancang untuk mengembangkan model eksploitasi *Android* berbasis RAT yang diintegrasikan dengan *social engineering* serta dilengkapi fitur otomatisasi, dengan fokus pada pengambilan kontak dan SMS secara otomatis. Dengan demikian, penelitian ini tidak hanya mereplikasi metode terdahulu, tetapi juga menghadirkan pendekatan yang lebih adaptif terhadap kebutuhan analisis serangan siber modern.

Model yang dikembangkan dalam penelitian ini merupakan representasi konseptual eksploitasi *Android* yang mengintegrasikan aspek teknis dan perilaku pengguna dalam satu alur terstruktur. Model ini mencakup tahapan *social engineering* sebagai pemicu, eksekusi *Remote Access Trojan* (RAT) untuk membangun koneksi, *auto exploitation* untuk menjalankan perintah secara

otomatis, serta automatic reporting untuk mengirimkan data secara real-time. Keterhubungan antar tahapan tersebut membentuk proses eksploitasi yang sistematis dan terukur, sehingga dapat digunakan sebagai kerangka analisis efektivitas serangan secara menyeluruh.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, maka rumusan masalah pada penelitian ini yaitu**:**

1. Bagaimana model integrasi RAT dan teknik *social engineering* dalam skenario exploitasi perangkat *Android*?
2. Bagaimana efektivitas penerapan mekanisme *auto exploitation* dalam meningkatkan proses exploitasi pada perangkat *android*?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dibuat, maka tujuan penelitian ini yaitu:

1. Menganalisis dan merancang integrasi antara *Remote Access Trojan (RAT)* dan teknik *social engineering* sebagai metode eksploitasi pada perangkat *Android*.
2. Mengembangkan dan menerapkan mekanisme *auto exploitation* guna mengotomatisasi proses eksploitasi pada perangkat *Android* sehingga dapat berjalan tanpa intervensi manual.

1.4 Manfaat Penelitian

1. Penelitian ini diharapkan dapat memperkaya literatur akademik di bidang keamanan siber, khususnya terkait teknik pembuatan *Remote Access Trojan* (RAT) menggunakan *Metasploit* dan pola penyebarannya melalui *social*

engineering, sehingga dapat mengisi kesenjangan riset terdahulu yang masih terbatas pada aspek deteksi teknis.

2. Hasil penelitian ini diharapkan dapat menjadi acuan praktis bagi praktisi keamanan, penegak hukum, serta masyarakat umum untuk meningkatkan kewaspadaan, menyusun strategi mitigasi, dan menyempurnakan kebijakan edukasi literasi *digital* agar dapat mencegah penyalahgunaan RAT di perangkat *Android*.

1.5 Batasan Penelitian

1. Penelitian hanya membahas RAT pada perangkat *Android*, tidak mencakup sistem operasi lain seperti *Windows, iOS,* atau *Linux*.
2. Pembuatan RAT difokuskan pada penggunaan *Metasploit*, tanpa menganalisis *framework* atau *tool* pembuat RAT lainnya.
3. Teknik penyebaran yang dikaji hanya terbatas pada metode *social engineering* melalui *fake application*, tidak termasuk metode lain seperti *exploit kit, brute force*, atau *physical access.*
4. Penyebaran aplikasi dilakukan secara terbatas melalui platform *WhatsApp* sebagai media distribusi.
5. Pengujian dilakukan pada jumlah perangkat yang terbatas dengan variasi versi *Android* tertentu.
6. Penelitian ini tidak mengembangkan alat deteksi RAT baru, tetapi hanya menganalisis pola distribusi, pembuatan, dan potensi penyalahgunaan.

7. Penelitian tidak membahas aspek forensik *digital* secara mendalam, melainkan menyoroti faktor perilaku pengguna, pola rekayasa sosial, dan risiko praktis yang muncul.
8. Penelitian ini dilakukan dalam lingkungan tertutup (closed environment) yang terkontrol, sehingga seluruh proses pengujian tidak melibatkan pihak luar dan tidak dilakukan pada jaringan publik secara bebas
9. Perangkat yang digunakan dalam penelitian ini terbatas pada sejumlah perangkat uji tertentu yang telah dikendalikan dan dikonfigurasi secara khusus, sehingga hasil penelitian tidak secara langsung merepresentasikan seluruh variasi perangkat Android di dunia nyata