ABSTRAK

Perkembangan perangkat *Android* yang pesat diiringi dengan meningkatnya ancaman keamanan, khususnya serangan berbasis *Remote Access Trojan* (RAT) yang memanfaatkan kelemahan perilaku pengguna melalui teknik *social engineering*. Penelitian ini bertujuan untuk menganalisis efektivitas eksploitasi perangkat *Android* dengan mengintegrasikan RAT, *social engineering*, serta mekanisme otomatisasi dalam satu model terstruktur. Metode yang digunakan adalah pendekatan eksperimental melalui pengujian pada beberapa perangkat *Android* dengan mengukur tingkat keberhasilan instalasi, pembentukan koneksi, pengambilan data, dan pengiriman data secara kuantitatif. Hasil penelitian menunjukkan bahwa tingkat keberhasilan instalasi mencapai 80%, pembentukan koneksi sebesar 75%, pengambilan data kontak sebesar 100%, serta pengambilan data SMS dan pengiriman data masing-masing sebesar 66,7%. Temuan ini menunjukkan bahwa faktor perilaku pengguna berperan signifikan dalam keberhasilan eksploitasi, sementara mekanisme keamanan sistem *Android*, khususnya kontrol izin akses, menjadi faktor pembatas utama. Penelitian ini berkontribusi dalam pengembangan model eksploitasi yang mengintegrasikan aspek teknis dan perilaku pengguna secara sistematis. Kesimpulan penelitian menunjukkan bahwa efektivitas eksploitasi dipengaruhi oleh interaksi antara pengguna dan kebijakan keamanan sistem. Untuk pengembangan selanjutnya, disarankan memperluas variasi perangkat dan sistem operasi, serta mengintegrasikan mekanisme deteksi dan mitigasi guna meningkatkan keamanan secara komprehensif.

Kata Kunci : Android Exploitation, Auto Exploit, Metasploit, Remote Access Trojan (RAT), Social Engineering

ABSTRACT

The rapid growth of Android devices has been accompanied by increasing security threats, particularly Remote Access Trojan (RAT)-based attacks that exploit user behavior through social engineering techniques. This study aims to analyze the effectiveness of Android device exploitation by integrating RAT, social engineering, and automation mechanisms into a structured model. The research employs an experimental approach by testing several Android devices and quantitatively measuring the success rates of installation, session establishment, data extraction, and data reporting. The results show that the installation success rate reaches 80%, session creation 75%, contact data extraction 100%, and both SMS extraction and data reporting 66.7%. These findings indicate that user behavior plays a significant role in the success of exploitation, while Android security mechanisms, particularly permission control, act as the main limiting factor. This study contributes to the development of an exploitation model that systematically integrates technical and behavioral aspects. The findings suggest that exploitation effectiveness is influenced by the interaction between user behavior and system security policies. For future work, it is recommended to expand device and operating system variations, as well as to incorporate detection and mitigation mechanisms to achieve a more comprehensive approach to improving Android security.

Keywords: *Android Exploitation, Auto Exploit, Metasploit, Remote Access Trojan (RAT), Social Engineering*

MOTTO DAN PERSEMBAHAN