INTISARI

IMPLEMENTASI *HONEYPOT* PADA *SMARTPHONE* DAN ANALISIS PENGUJIAN SERANGAN *MALWARE* MELALUI JARINGAN *WIRELESS*

Saat ini tingkat penggunaan *smartphone* semakin meningkat dapat dilihat dari jumlah pengguna setiap harinya dilihat dari seorang individu selalu sibuk dengan *smartphone* miliknya. Alasan utama menggunakan *smartphone* pastinya tidak sekedar untuk berkomunikasi melalui telepon atau mengirim pesan saja, tetapi penggunaan *smartphone* juga digunakan untuk mengakses informasi yang terhubung dengan *internet*. Agar dapat terhubung ke *internet* harus dihubungkan melalui paket data melalui jaringan seluler maupun *Wireless Local Area Network (WLAN)* pada jaringan *wireless*. Saat terhubung melalui jaringan *wireless* yang secara otomatis terhubung ke *internet* kita tidak tahu apakah jaringan tersebut aman dari ancaman serangan *malware*. Padahal ancaman serangan *malware* tidak hanya menargetkan komputer saja tetapi juga perangkat *mobile* seperti *smartphone*. Banyak pengguna *smartphone* yang tidak menyadari bahwa bahaya serangan yang ada dapat mengancam keamanan *smartphone* itu sendiri baik dari segi perangkat maupun data-data yang tersimpan di dalamnya. Salah satu serangan yang dianggap membahayakan adalah *malware* karena sifatnya yang merusak dan menimbulkan kerugian yang besar. Sebuah tindakan dapat dilakukan untuk mencegah hal tersebut terjadi dengan cara implementasi Honeypot pada *smartphone*. Sensor Honeypot yang akan dipasang yaitu Dionaea yang berfungsi untuk menangkap serangan *malware* yang masuk melalui koneksi jaringan *wireless* yaitu *Wireless Local Area Network (WLAN)* dan jaringan seluler. Ketika serangan *malware* dapat terdeteksi maka terbukti sistem berhasil dijalankan serta didapatkan hasil berupa informasi penyerangan *malware* dalam bentuk *log* serangan yang tersimpan di dalam *database SQLite*.

Kata kunci: *Smartphone*, *Malware*, Honeypot, Dionaea, dan jaringan *wireless*.

ABSTRACT

IMPLEMENTATION OF HONEYPOT *ON SMARTPHONE AND MALWARE ATTACK TESTING ANALYSIS THROUGH WIRELESS NETWORK*

Nowadays, the level of smartphone use is increasing, it can be seen from the number of users every day seen from an individual who is always busy with his smartphone. The main reason for using a smartphone is certainly not just to communicate via telephone or send messages, but also used to access information connected to the internet. In order to be able to connect to the internet, you must be connected via a data packet through a cellular network or a Wireless Local Area Network (WLAN) on a wireless network. When connected to the internet via a wireless network automatically we do not know whether the network is safe from the threat of malware attacks. Though the threat of malware attacks not only target computers but also mobile devices such as smartphones. Many smartphone users do not realize that the dangers of existing attacks can threaten the security of the smartphone itself, both in terms of the device and the data stored on it. One of the attacks that is considered dangerous is malware because it is destructive and causes great losses. An action can be taken to prevent this from happening by implementing Honeypot on smartphones. The Honeypot sensor that will be installed is Dionaea which functions to catch malware attacks that enter through a wireless network connection, namely Wireless Local Area Network (WLAN) and cellular networks. When a malware attack can be detected, it is proven that the system is running successfully and the results are obtained in the form of malware attack information in the form of an attack log stored in the SQLite database.

Keywords: Smartphone, Malware, Honeypot, Dionaea, and wireless network.