ABSTRACT

As a personal device, the smartphone becomes a place to store personal data are always taken everywhere by their owners. Threats to data security can occur on the spread of malware such as viruses and trojans on a network. The operating system that widely used by smartphone is Android. Android is certainly an attractive target for cybercriminals.

Mobile Honeypot is one solution to detect threats that targeting smartphone. This research aims to develop a Mobile Honeypot system that capable of collecting attack log and malware on public WLAN. Dionaea as part of the Mobile honeypot system will record the attack happened to it and download the malware that detected and spread in the public network. Dionaea applications run on Backtrack 5 ARM is also active with the Android operating system.

From the attack test results based on scenario, Mobile Honeypot in this study were able to record the activity that happen and downloading malware targeted it. Mobile Honeypot can be tested in different networks. Log data without attack scenarios collected in three UGM-Hotspot. The Port that frequently targeted is port 2987 with total occurrence of 1101 times. Port 445 experienced the second largest number of attacks with total occurrence of 45 times. The Test without attack scenarios that done on public WLAN, show that Mobile Honeypot can detect attacks that occur not only on a port that has been provided. This may indicate there are other threats are unknown and endanger smartphone when connected to a public network WLAN.

Keywords: *Mobile*, Honeypot, Android, *Security*, *Smartphone*.

INTISARI

Sebagai perangkat personal, *smartphone* merupakan tempat menyimpan data-data pribadi yang selalu dibawa kemana-mana oleh pemiliknya. Ancaman terhadap keamanan data dapat terjadi dari penyebaran *malware* seperti virus dan *trojan* di dalam sebuah jaringan. Sistem operasi yang banyak digunakan oleh *smartphone* adalah Android. Android tentunya menjadi target yang menarik untuk para penjahat dunia maya.

Mobile Honeypot adalah salah satu solusi untuk mendeteksi ancaman yang mengincar *smartphone*. Penelitian ini bertujuan menerapkan sistem Mobile Honeypot yang mampu mengumpulkan *log* serangan dan *malware* di publik WLAN. Dionaea dan Backtrack 5 ARM sebagai bagian dari sistem Mobile Honeypot akan mencatat serangan yang terjadi padanya dan mengunduh *malware-malware* yang tersebar di dalam jaringan publik tersebut.

Dari hasil pengujian serangan berdasarkan skenario, Mobile Honeypot pada penelitian ini mampu merekam aktivitas yang terjadi dan mengunduh *malware*. Mobile Honeypot ini dapat diuji di jaringan yang berbeda. Pengumpulan data log tanpa skenario serangan dilakukan di tiga UGM-Hotspot. Port yang sering diserang adalah port 2987 sebanyak 1101 kali. Jumlah serangan terbesar kedua terjadi pada port 445 sebanyak 45 kali. Pengujian tanpa skenario yang dilakukan pada publik WLAN, menunjukkan bahwa Mobile Honeypot dapat mendeteksi serangan yang terjadi tidak hanya pada port yang telah disediakan. Hal ini dapat menunjukkan terdapat ancaman-ancaman lain yang belum diketahui dan membahayakan *smartphone* ketika terhubung pada jaringan publik WLAN.

Kata kunci: *Mobile*, Honeypot, Android, *Security*, *Smartphone*