Rancang Bangun dan Analisa Kinerja Sistem Operasi Untuk Menganalisa Malware Berbasis Android = Design and Performance Analysis of Operating System for Analyzing Android-Based Malware

Wahyu Nuryanto, author

Abstrak

Android merupakan sistem operasi mobile paling banyak digunakan saat ini di seluruh dunia. Sebanyak 80% pangsa pasar sistem operasi telepon pintar dikuasai oleh Android. Berdasarkan laporan yang dirilis oleh Symantec menunjukkan tren malware pada android yang meningkat hampir 8 kali lipat hanya dalam waktu 1 tahun. Diperlukan adanya sebuah sistem yang secara khusus dibuat untuk dapat melakukan analisa terhadap malware berbasis android. Agar analisa dapat dilakukan oleh siapa saja dan dimana saja, maka perlu dibuat sistem yang mudah digunakan, ringan, dan efektif.
Xubuntu yang merupakan kombinasi dari Ubuntu yang stabil dan XFCE yang ringan kemudian dipilih sebagai dasar dari sistem untuk rancang bangun Distro Linux AMOS. Beberapa perangkat lunak opensource ditambahkan kedalam sistem untuk melakukan analisa seperti apktool, apkanalyser, apkinspector, android sdk, droidbox, androguard dan lainnya. Pengujian dilakukan dengan tes perbandingan platform dan fungsionalitas antara AMOS dengan Kali Linux dan Santoku Linux dengan parameter pengukuran berupa waktu respon, cpu usage, dan memory usage.
Dari hasil pengujian didapatkan hasil bahwa AMOS memiliki keunggulan dalam hal efisiensi penggunaan CPU yang lebih baik dengan hanya menggunakan 7,8% saat menjalankan 1 buah Emulator Android.
.....Android mobile operating system has become the most widely used today throughout the world. Almost 80% share of smartphone operating system market dominated by android. With such a high level of distribution make android becomes a new target for malware to evolve and distributed. Based on report by Symantec indicate that in 1 year number of malware samples in android had increasing almost 8 times. Its Necessary to have a system that is specifically made to do an android -based malware analysis. It needs to make the system easy to use , lightweight , and effective so that the analysis can be done by anyone and anywhere.
Xubuntu is a combination of Ubuntu and XFCE then selected as the basis for the design of the AMOS system. Some open-source software is added into the system to perform analysis such as apktool , apkanalyser , apkinspector , android sdk , droidbox , androguard and others. a comparison test between the AMOS platform with Kali Linux and Santoku Linux with measurement parameters such as response time, CPU usage, and memory usage also done in this research.
Based on examination results, AMOS become the best in cpu usage
efficiency with only 7.8% from total cpu when executing an android emulator.