ABSTRAK

ANALISIS *MALWARE* PADA *TRAFFIC* JARINGAN MENGGUNAKAN WIRESHARK

Oleh

Waskito

1202154223

Malware merupakan sebuah perangkat lunak dieksekusi atau tereksekusi secara otomatis yang dirancang untuk melakukan pencurian informasi, mengendalikan sistem, memanipulasi data, mendapatkan akses terhadap *host* dan dapat dikendalikan dari jarak jauh**.** Penyebaran *malware* bervariasi, dapat melalui *hardware* dan melalui jaringan sehingga penyebarannya sangat pesat. Penyerangan *malware* pada jaringan komputer sangat banyak, karena *attacker* hanya perlu berperan di belakang layar. Penggunaan *packet capture* dilakukan untuk mengetahui paket yang berjalan pada jaringan dilakukan agar dapat melihat paket data yang masuk dan keluar. Oleh karena itu perlu adanya analisis pada *packet capture* untuk mengetahui serangan *malware* terhadap aktivitas yang mencurigakan pada jaringan dan mengetahui *anomaly* yang disebabkan oleh *malware* tersebut. Untuk melakukan analisis pada *packet capture* menggunakan *tools* seperti *packet capture analyzer* sehingga paket data *capture* bisa dibaca. Hasil yang didapatkan dari deteksi dengan menggunakan *packet capture analyzer* adalah perilaku dan aktivitas *malware* ketika berada pada jaringan seperti *port* yang digunakan dan layanan yang menjadi sasaran oleh *malware*. Dari hasil penelitian ini akan diapatkan kriteria serangan yang dilakukan oleh *malware*, kategorisasi berdasarkan dampak dan resiko yang dihasilkan oleh malware yang mengacu pada aspek *access control system*, pada tafik jaringan maupun *host* yang berada di jaringan. Sehingga dapat dilakukan *controlling* terhadap dampak yang dihasilkan berdasarkan data yang di dapat dari hasil analisis paket data pada jaringan.

Kata Kunci: ***malware, malware analysis, cybercrime, traffic analysis, packet capture, network analyzer***