INTISARI

IMPLEMENTASI SISTEM DETEKSI *MALWARE* DENGAN PENDEKATAN *TOP-DOWN* BERBASIS *HONEYPOT* DAN *YARA*

Serangan siber mengalami peningkatan jumlah pada setiap tahunnya. Termasuk jumlah dan variasi *malware* yang digunakan oleh penyerang untuk melancarkan tujuannya. Tantangan yang dihadapi oleh sistem kemanan siber suatu organisasi untuk melindungi sistem komputer dari serangan *malware* tak dikenal. Sistem *antivirus* pada umumnya menggunakan pendeteksian *malware* dengan pendekatan *signature* untuk mendeteksi *malware*. Kekurangan *antivirus* pendekatan *signature* adalah tidak mampu mendeteksi *malware* yang belum dikenal. Diperlukan sistem deteksi *malware* dengan cara kerja dan pendekatan yang tepat agar dapat mendeteksi *malware* dengan baik. Proyek tugas akhir ini mengembangkan sistem deteksi *malware* dengan pendekatan *Top-Down* berbasis *honeypo*t dan yara. Sistem deteksi *malware top-down* adalah pendeteksian *malware* yang dipicu dari *update malware hash* dari sisi *server* (top) pengolah data *hash malware* yang selanjutnya berproses jika ditemukan persamaan *hash* pada sisi *client* (*bottom*). Dionaea merupakan *honeypot* yang mampu mendapatkan salinan *malware* yang digunakan oleh penyerang, sehingga memungkinkan sistem deteksi *malware* memperoleh data *signature malware (hash)* yang belum dikenal. Yara membantu peneliti *malware* untuk mengenali jenis *malware* pada suatu *file*. Hasil pengujian menunjukkan sistem deteksi *malware* mampu mengumpulkan *hash malware* dan *hash client file* untuk pendeteksian *malware*. Hasil pengujian pendeteksian *malware* mampu mendeteksi dan menghapus *file malware* pada komputer *client*. Sistem deteksi juga mampu mengantisipasi *suspected client file* pada *client* yang sedang *offline*.

Kata kunci: ***Top-Down Malware Detection, Honeypot Dionaea, Yara, false-negative.***

ABSTRACT

IMPLEMENTATION OF TOP-DOWN MALWARE DETECTION SYSTEM BASED ON HONEYPOT AND YARA

Cyber attacks have been increased in numbers every year. Including the quantity and variations of malware used by attacker to accomplish their goals. The challenge faced by an organization's cybersecurity system is to protect computer systems from unknown malware attacks. Antivirus systems generally use signature-based detection approaches to identify malware, but they are still weak in detecting unknown malware. A malware detection system with the appropriate working mechanism and approach is needed to effectively detect malware. In this final project, a malware detection system is developed using a Top-Down approach based on honeypots and Yara. Top-Down malware detection system is malware detection that is triggered by update of hash malware from the server side (top) that processing malware hash data then proceeds if a hash match is found on the client side (bottom). Dionaea honeypot is used with the main objective of obtaining copies of malware used by attackers. Dionaea allowing the malware detection system to obtain signature data for unknown malware. Yara assists malware researchers in identifying the type of malware in a file. Test results show that the malware detection system is able to collect malware hashes and client file hashes for malware detection. In testing malware detection system able to detect and remove malware. The detection system is also able to anticipate suspected client files on offline clients.

Keywords: Top-Down Malware Detection, Honeypot Dionaea, Yara, false-negative.