Abstrak

Forensik Router untuk Mendeteksi *Flooding Attack* Menggunakan Metode *Live Forensic*

Teknologi informasi di era saat ini menunjukkan perkembangan yang pesat khususnya dalam bidang komputer berbasis jaringan sehingga dapat membuat para penggunanya terlena. Beberapa oknum-oknum tertentu masih banyak yang menyalahgunakan teknologi tersebut salah satunya dengan melakukan serangan pada jaringan komputer. Router merupakan perangkat jaringan yang dapat membuat jaringan local bisa terhubung ke jaringan public. Router seringkali menjadi target serangan, disebabkan router suatu perangkat yang berfungsi sebagai jalur lalu lintas pengiriman data. *Flooding Attack* merupakan salah satu serangan pada jaringan komputer. Serangan yang dilakukan bertujuan membanjiri lalu lintas data pada jaringan sehingga dapat menyebabkan jaringan menjadi down (lumpuh) diakibatkan kelebihan beban. Beberapa tools yang dapat digunakan untuk mendeteksi *Flooding Attack* seperti Winbox serta Wireshark. Kedua alat tersebut dapat membantu dalam mendeteksi adanya serangan pada router. Disisi lain, dapat digunakan untuk mencari informasi yang dapat digunakan sebagai bukti digital dengan menggunakan metode *Live Forensics*. Informasi yang akan digali adalah Log Activity, Log Traffics dan IP Address. Untuk memperoleh informasi tersebut, maka dilakukan beberapa simulasi serangan pada router. Berdasarkan simulasi yang dilakukan, ditemukan adanya peningkatan signifikan pada lalu lintas jaringan router serta penggunaan sumber daya yang juga meningkat. Serangan yang dilakukan menggunakan Metasploit yang merupakan suatu alat yang digunakan untuk melakukan serangan pada jaringan. Penggunaan metode *Live Forensics* dalam mendeteksi serangan flooding pada router diketahui mampu mendeteksi adanya serangan pada router. Serangan tersebut berhasil terdeteksi setelah mengakuisisi router serta mendapatkan informasi dari Log Activity dan Log Traffics yang berhasil ditarik. Informasi yang diperoleh pada file log tersebut yaitu ditemukan adanya IP Address yang terdeteksi melakukan serangan yaitu IP Address 192.168.2.252. Beberapa informasi yang terdapat pada log file yang telah ditarik juga dapat dijadikan sebagai barang bukti dalam persidangan.

Kata kunci:
Flooding Attack; *Live Forensics;* Router;

Abstract

Router Forensics To Detect Flooding Attack Using Live Forensics Method

Information technology in the current era shows rapid development, especially in the field of network-based computers so as to make users complacent. Some certain elements are still many who misuse the technology, one of them by carrying out attacks on computer networks. A router is a network device that can make a local network connected to a public network. Routers are often the target of attacks, due to the router of a device that functions as a traffic for sending data. Flooding Attack is an attack on a computer network. The attack carried out aimed at flooding data traffic on the network so that it can cause the network to be down (paralyzed) due to overload. Some tools that can be used to detect Flooding Attack such as Winbox and Wireshark. Both of these tools can help in detecting attacks on the router. On the other hand, it can be used to find information that can be used as digital evidence using the Live Forensics method. The information to be extracted is the Activity Log, Log Traffics and IP Address. To obtain this information, several simulation attacks are carried out on the router. Based on the simulations carried out, it was found that there was a significant increase in router network traffic and resource usage which also increased. The attack carried out using Metasploit which is a tool used to carry out attacks on the network. The use of Live Forensics method in detecting flooding attacks on routers is known to be able to detect attacks on routers. The attack was detected after acquiring the router and getting information from the Activity Log and Log Traffics that were successfully pulled. The information obtained in the log file is found the presence of an IP Address that was detected to attack the IP Address 192.168.2.252. Some information contained in the log file that has been withdrawn can also be used as evidence in court.

Keywords:
Flooding Attack; Live Forensics; Routers;