Abstract

Denial of Service (DoS) attacks are structured network attacks that originate from multiple sources and converge to form large packet currents. A DoS attack aims to disrupt the services available on the target network by flooding the bandwidth or processing capacity system making the target server network become overloaded. Wireshark is a tool that can be used to detect DoS attacks on a Router network and perform network traffic analysis that has functions that are useful for network professionals, network administrators, researchers, and network software development, requiring the detection of DoS attacks on the Router and multiplying information as well as attracting forensics data as a digital evidence of DoS attacks on the Router through the Live Forensics method. This research succeeded in pulling data information of DoS attack on Router form activity log data and attacker IP address list.

References

1. Fadil A, Riadi I, Aji S. Review of detection DDOS attack detection using naive bayes
doi:10.11591/eei.v6i2.605


Index Terms
Keywords

Analysis of DoS (Denial of Service) Attack, Router, Live Forensics