Edu Komputika 10 (1) (2023)

Edu Komputika Journal

http://journal.unnes.ac.id/sju/index.php/edukom

Evaluasi Optimalisasi Alat Forensik Keamanan Jaringan pada Lalu Lintas Virtual Router

Firmansyah[1)]✉, Abdul Fadlil[2)], Rusydi Umar[3]

[1]Program Studi Ilmu Komputer, Fakultas Teknik, Universitas Islam Al-Azhar, Indonesia
[2]Program Studi Teknik Elektro, Universitas Ahmad Dahlan, Indonesia
[3]Program Studi Magister Teknik Informatika, Universitas Ahmad Dahlan, Indonesia

Info Artikel

Sejarah Artikel:
Diterima: tanggal masuk
Direvisi: tanggal revisi
Disetujui: tanggal artikel disetujui

Keywords:
Metarouter, Recording tools, Analysis tools, Forensics, Network traffic.

Abstrak

Penelitian ini bertujuan untuk mengevaluasi optimalisasi alat forensik keamanan jaringan pada lalu lintas virtual router (VR). Metodologi yang digunakan meliputi pemilihan beberapa alat forensik pada sistem operasi *Windows* seperti *Wireshark, Windump*, dan *Network Miner*, dengan pengujian dalam lingkungan jaringan virtual. Pengujian, mencakup simulasi berbagai skenario serangan untuk menilai efektivitas deteksi ancaman, kinerja alat forensik, dan dampak terhadap kinerja jaringan. Hasil utama menunjukkan bahwa alat-alat tersebut memiliki kemampuan deteksi yang beragam dengan variasi penggunaan sumber daya dan dampak pada latensi jaringan. Lalu lintas jaringan telah berhasil di rekam menggunakan alat *Win-dump* pada metode *static* forensik, alat *Wireshark* dan *Network Miner* pada metode *live forensics*. Hasil evaluasi alat rekam forensik jaringan meta-router merekomendasikan Win-dump sebagai alat rekam yang tidak membebani sistem operasi windows dengan penggunaan *Memory* adalah 1696 kb sedangkan aplikasi Wireshark dan Network Miner tercatat lebih dari 20MB. Berdasarkan penelitian ini metode *static forensic* yang telah dibangun dengan objek meta-router dapat digunakan investigator untuk mendeteksi serangan siber. Pemilihan dan konfigurasi yang tepat dari alat forensik sangat penting untuk mencapai keseimbangan antara keamanan dan kinerja jaringan, serta penyesuaian spesifik terhadap kebutuhan jaringan dapat meningkatkan efektivitas deteksi dan mitigasi ancaman.

Abstract

This research aims to evaluate the optimization of network security forensic tools on virtual router (VR) traffic. The methodology used includes the selection of several forensic tools on the Windows operating system such as Wireshark, Windump, and Network Miner, with testing in a virtual network environment. Testing, includes simulating various attack scenarios to assess the effectiveness of threat detection, performance of forensic tools, and impact on network performance. The main results show that the tools have varying detection capabilities with variations in resource usage and impact on network latency. Network traffic has been successfully recorded using the Win-dump tool in the static-forensics method, the Wireshark tool and Network Miner in the live-forensics method. The evaluation results of the meta-router network forensic recording tool recommend Win-dump as a recording tool that does not burden the Windows operating system with memory usage of 1696 kb while the Wireshark and Network Miner applications are recorded at more than 20MB. Based on this research, the static forensic method which have been built with meta-router objects can be used by investigators to detect cyber attacks. Proper selection and configuration of forensic tools is critical to achieving a balance between security and network performance, and specific adjustments to network requirements can increase the effectiveness of threat detection and mitigation.

✉ Alamat korespondensi: (diisi dengan alamat afiliasi penulis utama)
Gedung Lantai 2, Teknik UNIZAR
Sandubaya, Kota Mataram, Nusa Tenggara Bar. 83232
E-mail: firmanyasin@gmail.com

ISSN 2252-6811
E-ISSN 2599-297X