INTISARI

Serangan keylogger pada server linux semakin meningkat, menghadirkan tantangan signifikan bagi forensik digital. Penelitian ini mengeksplorasi analisis forensik serangan keylogger pada server linux dengan memanfaatkan kerangka kerja National Institute of Standards and Technology (NIST). Penelitian ini bertujuan untuk mengidentifikasi aktivitas mencurigakan terkait serangan keylogger melalui analisis file syslog, mendokumentasikan Chain of Custody menggunakan metode NIST, dan menghasilkan bukti yang valid secara hukum. Menggunakan server CentOS 7 sebagai studi kasus, penelitian ini menerapkan tahap pengumpulan, pemeriksaan, analisis, dan pelaporan dari metode NIST. Penelitian ini memberikan panduan praktis untuk penyelidikan serangan keylogger pada server linux, menekankan pentingnya Chain of Custody yang aman. Dengan mengadopsi kerangka kerja NIST, penelitian ini menawarkan pendekatan terstruktur dan terstandarisasi untuk forensik digital, memastikan integritas dan validitas bukti yang dikumpulkan. Temuan penelitian ini memberikan pemahaman yang komprehensif tentang serangan keylogger pada server linux, penerapan metode NIST, dan pentingnya dokumentasi yang cermat untuk proses hukum. Penelitian ini menyoroti perlunya langkah-langkah keamanan yang kuat untuk mengurangi ancaman serangan spyware yang semakin meningkat. Hasil penelitian menunjukkan bahwa metode NIST dapat diterapkan secara efektif untuk analisis forensik serangan keylogger pada server linux, menghasilkan bukti yang valid dan terstruktur. Penelitian ini merekomendasikan peningkatan kesadaran dan edukasi tentang ancaman keylogger, serta penerapan langkah-langkah keamanan yang lebih ketat untuk melindungi sistem linux dari serangan spyware.

Kata kunci: Keylogger, Linux, Analisis Syslog, Chain of Custody, NIST, CentOS

ABSTRACT

Keylogger attacks on Linux servers are increasing, presenting significant challenges for digital forensics. This research explores the forensic analysis of keylogger attacks on Linux servers by utilizing the National Institute of Standards and Technology (NIST) framework. This research aims to identify suspicious activity related to keylogger attacks through syslog file analysis, document chain of custody using NIST methods, and generate legally valid evidence. Using a CentOS 7 server as a case study, this research applies the collection, examination, analysis, and reporting stages of the NIST method. This research provides practical guidance for the investigation of keylogger attacks on Linux servers, emphasizing the importance of a secure chain of custody. By adopting the NIST framework, this research offers a structured and standardized approach to digital forensics, ensuring the integrity and validity of the evidence collected. The findings of this research provide a comprehensive understanding of keylogger attacks on Linux servers, the applicability of NIST methods, and the importance of careful documentation for legal proceedings. This research highlights the need for robust security measures to mitigate the growing threat of spyware attacks. The results show that the NIST method can be effectively applied for forensic analysis of keylogger attacks on Linux servers, producing valid and structured evidence. This research recommends increased awareness and education about the threat of keyloggers, as well as the implementation of stricter security measures to protect Linux systems from spyware attacks.

Keywords: Keylogger, Linux,Analyis Syslog, Chain of Custody, NIST, CentOS