ABSTRAK

ANALISIS KEAMANAN JARINGAN MENGGUNAKAN METODE VULNERABILITY ASSESSMENT DAN PENETRATION TESTING DENGAN MENGIMPLEMENTASIKAN IDS/IPS MENGGUNAKAN SURICATA

Oleh

ABYYU HAFIZH SEPTRIANTO

Dengan pesatnya perkembangan teknologi internet, lanskap ancaman digital telah meningkat berlipat ganda, membuat arsitektur aplikasi web dan basis data semakin rentan terhadap eksploitasi. Penelitian ini mengusulkan kerangka kerja keamanan jaringan yang diperkuat dengan Penilaian Kerentanan dan Pengujian Penetrasi (VAPT) dan implementasi Suricata sebagai solusi IDS/IPS. Melampaui sekadar identifikasi ancaman, penelitian ini melakukan serangkaian simulasi serangan dunia nyata seperti SQL Injection, Brute Force, dan Reverse Shell untuk menilai efektivitas IDS/IPS Suricata. Dengan menggunakan OpenVAS untuk pemindaian kerentanan awal dan Suricata untuk IDS/IPS, lingkungan simulasi ancaman dengan fidelitas tinggi telah dibuat. Analisis forensik dari kerangka kerja awal menunjukkan kerentanan kritis yang memungkinkan serangan tanpa mitigasi untuk meningkat ke hak akses root. Setelah aturan yang disesuaikan diimplementasikan, kerangka kerja keamanan diubah secara signifikan. Kerangka kerja tersebut terbukti tangguh secara operasional dengan Akurasi 90% dan Tingkat Positif Palsu 0%. Meskipun Tingkat Negatif Palsu sebesar 16,67% menunjukkan perlunya kalibrasi ulang lebih lanjut dari kerangka kerja dengan serangan brute force yang tidak jelas, penelitian ini dengan jelas menunjukkan bahwa implementasi Suricata dengan VAPT secara signifikan memperkuat keamanan server. Dengan implementasi peringatan berbasis Telegram, kerangka kerja ini dapat digunakan sebagai solusi presisi tinggi dan kecepatan tinggi untuk mitigasi ancaman modern.

Kata kunci: *Network Security*, *Vulnerability Assessment*, Analisis Jaringan, *Penetration Testing*, IDS/IPS, Suricata, OpenVAS, SQL *Injection, Brute Force*, *Reverse Shell*

ABSTRACT

NETWORK SECURITY ANALYSIS USING VULNERABILITY ASSESSMENT AND PENETRATION TESTING METHODS WITH IDS/IPS IMPLEMENTATION BASED ON SURICATA

By

ABYYU HAFIZH SEPTRIANTO

The digital threat environment has increased manifold with the rapid growth of the internet, making the database and web application architectures even more vulnerable to exploitation. The use of Suricata IDS/Ips and Vulnerability Assessment and Penetration Testing (VAPT) provides a stronger network security framework, according to the study conducted in the current research study. The study not only assesses the threat environment but also tests the efficiency of the Suricata IDS/Ips by simulating several types of attacks, including SQL Injection, Brute Force, and Reverse Shell attacks. By employing OpenVAS for initial vulnerability scanning and Suricata for IDS/IPS, a high-fidelity threat simulation environment was created. Forensic analysis of the initial framework indicated a critical vulnerability that allowed unmitigated attacks to escalate to root privileges. Once the customized rules were implemented, the security framework was significantly altered. The framework was found to be operationally resilient with an Accuracy of 90% and a 0% False Positive Rate. While a False Negative Rate of 16.67% indicates the need for further recalibration of the framework with obscure brute force attacks, the research clearly indicates that the implementation of Suricata with VAPT significantly strengthens the security of the server. With the implementation of Telegram-based alerts, the framework can be employed as a high-precision, high-speed solution for the mitigation of modern threats.

Keyword: Network Security, Vulnerability Assessment, Network Analysis, Penetration Testing, IDS/IPS, Suricata, OpenVAS, SQL Injection, Brute Force, Reverse Shell