INTISARI

Integrasi Transport Layer Security dalam Implementasi Proksi TDS untuk Honeypot Interaksi Tinggi Microsoft SQL Server

Oleh

Faiz Unisa Jazadi
21/475298/PA/20563

Munculnya ancaman dunia siber yang semakin canggih menimbulkan risiko yang signifikan terhadap infrastruktur penting, terutama sistem basis data yang menyimpan data organisasi yang sensitif dan strategis. Microsoft SQL Server (MSSQL) adalah target umum karena penggunaannya yang luas dan peran sentralnya di banyak lingkungan perusahaan. Untuk mempelajari ancaman tersebut, honeypot dengan interaksi tinggi menawarkan wawasan yang kaya tentang perilaku penyerang. Namun, komunikasi terenkripsi pada protokol *Tabular Data Stream* (TDS) melalui *Transport Layer Security* (TLS) mempersulit pemantauan. Pada TDS versi 7.x, negosiasi TLS terjadi dengan cara yang tidak standar, membuat pilihan metode pemantauan menjadi terbatas. Penelitian ini menyajikan pengembangan proksi terminasi TLS untuk TDS, yang memungkinkan penangkapan dan penerusan paket-paket TDS terenkripsi secara transparan dalam pengaturan honeypot dengan interaksi tinggi. Proksi ini dikembangkan secara bertahap, yang berujung pada implementasi akhir yang mendukung negosiasi TLS, dekripsi, dan penerusan paket menggunakan OpenSSL. Evaluasi fungsional menggunakan klien impacket-mssqlclient dan mssql-cli menunjukkan kompatibilitas yang baik berdasarkan kemampuan pada lima aspek, yaitu koneksi, autentikasi, eksekusi *query*, RPC, dan transaksi. Pengujian non-fungsional terhadap proksi juga menunjukkan durasi *handshake* sebesar 3,312ms (1,7 kali *baseline*) dan latensi sebesar 0,701ms (1,2 kali *baseline*) pada pengaturan enkripsi penuh. Penelitian ini menunjukkan kelayakan dan efektivitas integrasi TLS dalam proksi TDS untuk pemantauan komunikasi pada honeypot MSSQL interaksi tinggi.

ABSTRACT

Integrating Transport Layer Security in TDS Proxy Implementation for High-Interaction Microsoft SQL Server Honeypot

By

Faiz Unisa Jazadi
21/475298/PA/20563

The emergence of increasingly sophisticated cyber threats poses significant risks to critical infrastructure, especially database systems that store sensitive and strategic organizational data. Microsoft SQL Server (MSSQL) is a common target due to its widespread use and central role in many enterprise environments. To study such threats, high-interaction honeypots offer rich insights into attacker behavior. However, encrypted communication over the Tabular Data Stream (TDS) protocol over Transport Layer Security (TLS) makes monitoring difficult. In TDS version 7.x, TLS negotiation occurs in a non-standard manner, limiting the choice of monitoring methods. This paper presents the development of a TLS termination proxy for TDS, which enables transparent capture and forwarding of encrypted TDS packets in a high-interaction honeypot setting. The proxy was developed in stages, culminating in a final implementation that supports TLS negotiation, decryption, and forwarding of packets using OpenSSL. Functional evaluation using impacket-mssqlclient and mssql-cli clients showed good compatibility based on capabilities in five aspects, namely connection, authentication, query execution, RPC, and transaction. Non-functional testing of the proxy also showed a handshake duration of 3.312ms (1.7 times baseline) and a latency of 0.701ms (1.2 times baseline) at full encryption settings. This study demonstrates the feasibility and effectiveness of TLS integration in TDS proxy for communication monitoring on high-interaction MSSQL honeypots.