Proof of Concept TCP Spoofing for Data Control on Public Internet with DPDK = Proof of Concept TCP Spoofing untuk Pengendalian Data di Internet Publik dengan DPDK

Hasibuan, Melchior Natthan Victor Hiras Fernando, author

Abstrak

Penelitian ini bertujuan untuk mengimplementasikan sistem injeksi paket forged TCP untuk memanipulasi sesi komunikasi, yang secara umum disebut dengan Policy Server (PS). Salah satu pemanfaatannya adalah untuk memblokir konten negatif pada internet publik, dalam kasus Indonesia diatur pada Permenkominfo No 19 Tahun 2014. Sayangnya, belum ada produk lokal yang tersedia di pasaran. Pada skripsi ini, DPDK diadopsi guna meningkatkan efisiensi komputasi dan meningkatkan throughput pemrosesan. Pengembangan PS ini meliputi beberapa fitur utama yakni fitur ekstraksi domain dari HTTP GET dan TLS Client Hello, pembuatan paket forged TCP untuk pemutusan koneksi, dan kemampuan remote management yang memungkinkan administrator memodifikasi domain yang dilarang dan memonitor statistik PS. Hasil pengujian fungsional dan performa menunjukkan bahwa seluruh fungsi utama telah berjalan dengan seharusnya. Pengukuran kinerja berhasil mengetahui baseline dan limit dari arsitektur yang dibuat.
.....This research aims to implement a forged TCP packet injection system to manipulate communication sessions, commonly referred to as a Policy Server (PS). One of its uses is to block negative content on the public internet, as regulated in Indonesia under Minister of Communication and Informatics Regulation No. 19 of 2014. Unfortunately, there are no local products available on the market yet. In this thesis, DPDK is adopted to enhance computational efficiency and increase processing throughput. The development of this PS includes several key features, namely domain extraction from HTTP GET and TLS Client Hello, the creation of forged TCP packets for connection termination, and remote management capabilities allowing administrators to modify banned domains and monitor PS statistics. Test results indicate that all main functions have operated as intended. Performance measurements successfully identified the baseline and limits of the architecture created.