ANALISIS KINERJA JARINGAN KOMPUTER BERBASIS *SPANNING TREE PROTOCOL* (STP) TERHADAP SERANGAN *CONFIG BPDU* DAN *TAKE OVER ROOT BRIDGE* MENGGUNAKAN *WIRESHARK*

Oleh

Eviana Yulianti Saputri
16030050

INTISARI

Spanning Tree Protocol (STP) digunakan pada peralatan *switch manageable* yang menerapkan jalur lebih dari satu untuk hubungan antar switch. Penggunaan jalur tersebut dimaksudkan agar kecepatan perpindahan data antar switch mencapai kecepatan diatas 100 mbps. Pada penelitian ini mempunyai tujuan untuk membantu *staff engineer* dalam meningkatkan sebuah keamanan jaringan *Spanning Tree Protocol* (STP). Serta manfaatnya untuk meningkatkan sistem keamanan jaringan *Spanning Tree Protocol* (STP) dengan menggunakan teknik mitigasi *Spanning Tree Protocol* dan VLAN *trunking.* Pada penelitian ini diawali dengan studi pustaka, analisis pemantauan data dan pengambilan data sebelum STP diserang dan setelah diserang menggunakan aplikasi *wireshark*. Kemudian dilakukan pengujian transfer file PC ke PC dengan aplikasi *speed out* versi *5.0*. Hasil pengujian ini terdapat data sebelum STP diserang, setelah STP diserang dan data antisipasi. Kemudian, dilakukan analisis regresi linier sederhana dengan hasil tidak terdapat hubungan yang signifikan antara *time* dengan size pada serangan DoS terdapat 48,6% variable *time* dipengaruhi oleh variabel *size*, sisanya sebesar 51,4% oleh variabel lainnya, sedangkan serangan root 43,8% variable *time* dipengaruhi oleh variabel *size*, sisanya sebesar 56,2% oleh variabel lainnya. *Korelasi Karl Pearson* DoS dan *root* terdapat hubungan yang signifikan antara *time* dan *size* dengan koefisien korelasi DoS adalah (-0,697) sedangkan *root* (-0,662), dan uji T dua sampel berpasangan (*paired sample t-test*) dapat disimpulkan bahwa terdapat perbedaan sebelum STP diserang dan setelah STP diserang. Dapat dilihat dari perbandingan rata-rata sebelum STP diserang dan setelah STP diserang mengalami penurunan rata-rata yang signifikan. Setelah diambil kesimpulan uji T dua sampel berpasangan (*paired sample t-test*) dilakukan antisipasi mitigasi BPDU *guard* dan *root guard* tetapi masih masih bisa diserang, sehingga perlu tahap selanjutnya yaitu VLAN *trunking.* Selain itu juga terdapat aplikasi *website* untuk menampilkan data grafik dan tabel.

Kata Kunci : *Spanning Tree Protocol, wireshark, regresi linier sederhana*

SPANNING TREE PROTOCOL (STP) BASED COMPUTER NETWORK PERFORMANCE ANALYSIS ON BPDU CONFIG ATTACK AND TAKE OVER ROOT BRIDGE USING WIRESHARK

by

Eviana Yulianti Saputri
16030050

ABSTRACT

Spanning Tree Protocol (STP) is used in switch manageable devices that apply more than one path to the connection between switches. The use of these lines is intended so that data transfer speeds between switches reach speeds above 100 mbps. This study aims to assist engineer staff in improving a network security spanning tree protocol (STP). And its benefits are to improve the Spanning Tree Protocol (STP) network security system by using Spanning Tree Protocol mitigation techniques and VLAN trunking. This research begins with literature study, analysis of data monitoring and data retrieval before STP is attacked and after being attacked using the Wireshark application. Then the PC to PC file transfer test was carried out with the speed out version 5.0 application. The results of this test contain data before STP is attacked, after STP is attacked and anticipatory data. Then, a simple linear regression analysis was carried out with the result that there was no significant relationship between time and size in the DoS *attack, where 48.6% of the time variable was influenced by the size variable, the remaining 51.4% by other variables while the root attack was 43.8% variable time is influenced by the size variable, the remaining 56.2% by other variables. The correlation between Karl Pearson* DoS *and root, there is a significant relationship between time and size, with the* DoS *correlation coefficient (-0.697) while root (-0.662), and the paired sample t-test (paired sample t-test) can be concluded that there is a difference before STP attacked and after STP was attacked. It can be seen from the comparison of the mean before the STP was attacked and after the STP was attacked there was a significant decrease in the average. After the conclusion of the paired sample t-test, the BPDU guard and root guard mitigation was carried out, but they could still be attacked so that the next step was needed, namely VLAN trunking. In addition, there is also a website application for displaying graphical data and tables.*

Keywords : *Spanning Tree Protocol, wireshark, simple linier regression*