Rancang bangun dan implementasi sistem monitoring jaringan berbasis web untuk menetukan tingkat resiko ancaman keamanan secara dinamis = Design and implementation of web based network monitoring system for dynamic risk level calculation

Reza Hadi Saputra, author

Abstrak

IT Risk Management merupakan suatu metodologi yang digunakan suatu perusahaan/ organisasi untuk dapat membantu mengatur resiko dari semua divais dan infrastruktur IT yang dimilikinya. Dengan IT Risk Management yang baik, maka perusahaan/ organisasi dapat mengatur seluruh aset IT yang dimiliki sehingga dapat membantu meningkatkan produktifitas perusahaan/ organisasi tersebut. IT Risk Management terdiri atas tiga tahapan, yaitu risk assessment, risk mitigation serta evaluation dan assessment. Pada setiap tahapan tersebut akan diperoleh output tertentu yang berupa report mengenai perusahaan/ organisasi. Untuk membantu dalam implementasi IT Risk Management, dibutuhkan Intrusion Detection System (IDS) yang akan memberikan report mengenai kondisi jaringan suatu perusahaan/ organisasi, meliputi pelaporan apabila terjadi gangguan serta tindakan yang akan dilakukan terhadap gangguan tersebut.
Pada skripsi ini dibuat suatu perancangan aplikasi berbasis web yang digunakan untuk perhitungan risk level (tingkat resiko) dalam suatu LAN pada tahapan risk assessment. Aplikasi tersebut digunakan untuk menghitung nilai risk level untuk setiap ancaman (threat) yang terdeteksi oleh IDS untuk suatu pilihan waktu yang dimasukkan oleh user. Aspek keamanan jaringan untuk suatu LAN merupakan hal yang sangat penting, terutama apabila di dalam LAN tersebut terdapat komputer yang didalamnya terdapat data yang sangat penting dan pada jaringan yang sama dengan komputer tersebut, terdapat komputer-komputer lain yang dipakai oleh banyak orang. Ancaman terhadap data pada komputer tersebut tidak hanya dapat berasal dari internet, tetapi juga dapat berasal dari computer-komputer dalam LAN. Oleh karena itu, dengan adanya aplikasi ini diharapkan apabila muncul suatu serangan terhadap suatu komputer yang berasal dari komputer lain pada LAN yang sama, serangan tersebut dapat terdeteksi sehingga tindakan perlindungan data dapat dilakukan.
Pada bagian akhir dari skripsi ini, sistem tersebut diujicoba pada LAN suatu perusahaan, untuk selanjutnya dilakukan suatu ujicoba serangan. Ada tiga tahapan ujicoba dengan setiap tahapan dilihat nilai Risk Level yang dihasilkan sistem. Pada tahap pertama, yaitu pencarian IP Address pada suatu LAN, menghasilkan nilai kuantitatif Risk Level sebesar 4 (Low Risk Level). Pada skenario ujicoba tahap 2, yaitu pencarian informasi meliputi port dan nama komputer untuk suatu komputer, menghasilkan nilai kuantitatif Risk Level sebesar 232 (High Risk Level). Pada skenario ujicoba tahap 3, yaitu pengambilalihan suatu computer target, menghasilkan nilai kuantitatif Risk Level sebesar 232 (High Risk Level).
<hr><i>IT Risk Management is a methodology used by a company / organization that can help them to manage risk from all devices and IT infrastructure assets. With the good IT Risk Management, the company / organization can manage all IT assets owned so can help them to increase the productivity of the company / organization. IT Risk Management consists of three phases, namely risk assessment, risk mitigation and the evaluation and assessment. At each stage, there are an output in the form of a report to the company / organization. To assist in the implementation of IT Risk Management, Intrusion Detection System (IDS) is

required, to provide a report on the condition of the network of a company / organization, including reporting of when an interruption occurs and the action will be taken.
In this thesis, a web-based application is designed, that is used to calculate the risk level in a LAN on the risk assessment stage. That application is used to calculate the value of the risk level for each threat detected by the IDS for a selection entered by the user. Aspects of network security for a LAN is very important, especially where in the LAN there are computers that contains a very important data and at the same with computers, there are computers that are used by many people. Threats to the data on the computers not only can come from the internet, but can also come from computers in the LAN. Therefore, this application is expected to appear when an attack against a computer that came from another computer on the same LAN, the attack can be detected so that the data protection act can be done.
At the end of this thesis, the system is tested on a corporate LAN, to be a trial of attacks. There are three stages of testing with each of the stages seen the value of the resulting Risk Level system. In the first stage, the IP Address is searched on a LAN, the quantitative value of Risk Level is 4 (Low Risk Level). In the phase 2 trial scenario, the search information includes the port and the name of the computer to a computer, the quantitative value of Risk Level is 232 (High Risk Level). In the phase 3 trial scenario, the takeovers process of a target computer, the quantitative value of Risk Level is 232(High Risk Level).</i>