The Implementation Of Virtual Private Network Based On Instruction Detection With Linux Firewalls

Implementasi Virtual Private Network Berbasis Instruction Detection dengan Firewall

Moch. Muslich
amuscan@ums.ac.id
Muhammadiyah University of Surakarta

ABSTRACT

The security of computer network as part from a information system of importance to watch over validity and data integrity with guarantee service availability for the user. System must be protected from all attack kind and infiltration efforts by side not justifiably. many manners is developed to protect network of infrastructure and communication at internet, with wear firewalls, encrypts, and virtual private network. Instruction detection is method relative new. Instruction detection (ids) method, collectable and used offence type information that known and found if try to assault network or host certain.

The network of self defense system maker application Linux this consist of configuration snort and base. in this implementation, data's will pass server will be accepted then be prepared with package decoder. data will pass by preprocessor that functioned there not it data package that has signature and or anomaly (oddity) that make can botch. data's step into detection engine, data's will applied several rules. data's package can sustained, at deliver, at logarithm, and or given alert (warning). if data there signature botch so data package can at deliver.

The research to design and make self defense system a network from attack, apply software open source snort in network and apply application ids integration in computer network

The using of software open source snort that made can be used to detect various attack in server based on Linux fedora core 5, like port scanning and others. Program base that used can simplify in read attack existence in server with web interfaces visualization

Key Word: Instruction Detection, Virtual Privet Network, Linux

ABSTRAK

Keamanan jaringan komputer sebagai bagian dari sebuah sistem informasi adalah sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Sistem harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan oleh pihak yang tidak berhak. Banyak cara dikembangkan untuk mengamankan infrastruktur jaringan dan komunikasi di internet, dengan memakai *firewall*, enkripsi, dan *Virtual Private Network*. *Instruction Detection* adalah metode yang relative baru. Metode *Instruction Detection* (IDS), dapat dikumpulkan dan digunakan informasi tipe penyerangan yang telah diketahui dan ditemukan jika mencoba menyerang jaringan atau host tertentu.

Aplikasi pembuatan sistem pertahanan diri jaringan linux ini terdiri atas konfigurasi Snort dan BASE. Pada implementasi ini, data-data yang lewat melalui *server* akan diterima lalu disiapkan dengan paket decoder. Data akan melewati *preprocessor* yang berfungsi ada tidaknya paket data

yang memiliki *signature* ataupun anomali (keanehan) yang dimungkinkan akan bisa merusak. Data-data tersebut masuk ke *detection engine*, data-data tersebut akan diterapkan beberapa aturan. Paket data-data tersebut bisa diteruskan, di *dro*p, di *log*, ataupun diberikan *alert* (peringatan). Jika data tersebut ada *signature* merusak maka paket data tersebut bisa saja di drop.
Penelitian yang dilakukan untuk merancang dan membuat sistem pertahanan diri suatu jaringan dari serangan, menerapkan *software open source* snort pada jaringan dan menerapkan aplikasi IDS yang terintegrasi dalam jaringan komputer.
Penggunaan *software open sourc*e Snort yang telah dibuat dapat digunakan untuk mendeteksi berbagai serangan pada *server* berbasis linux fedora core 5, seperti port scanning dan lain-lain. Program BASE yang digunakan dapat mempermudah dalam membaca adanya serangan pada server dengan visualisasi *interface web*.

Kata Kunci : Instruction Detection, Virtual Privet Network, Linux