ANALISIS SISTEM KEAMANAN HOTSPOT DENGAN MENGGUNAKAN HONEYPOT DAN IDS DI KAMPUS STMIK PPKIA PRADNYA PARAMITA MALANG

Ahmad Zainuddin, Luqman Affandi, Antonius Duty Susilo
Teknik Informatika, STMIK PPKIA Pradnya Paramita Malang
email: zen@pradnya.ac.id

Abstract

Campus STMIK PPKIA Pradnya Paramita Malang an informatics-based private university in Malang. Security Hotspot used Mikrotik is using a security system. Users who use Hotspot itself is the lecturer and students. Honeypot and IDS is a tool to help security systems that still use Mikrotik Hotspot. Every time there is an attack action using Hotspot then stored into a log of activities each server. Honeypot itself is useful as a shadow Server or Server fake to fool the server where the original moment of the attack. The attack can be done in antaralain Hotspot network using scanning techniques, Arp Spoofing and DDOS. The ultimate goal of this research is to provide a recommendation of Honeypot and IDS analysis results that are tailored to the security system "STMIK PPKIA Pradnya Paramita Malang" and determine the performance of software after testing on Honeypot and IDS. The results of the study indicated that the Snort IDS is able to give a warning on the attack quite well and would be even better if combined with a low interaction and high interaction honeypot honeypot because besides being able to provide better alerting honeypot able to learn what is done by the attacker.

Keywords: *Honeypot - IDS, Snort, Mikrotik, Server,STMIK PPKIA Pradnya Paramita Malang*

PENDAHULUAN

Kampus STMIK PPKIA Pradnya Paramita Malang (STIMATA) adalah salah satu kampus swasta yang berbasiskan informatika yang ada di Kota Malang, Keamanan jaringan Internet yang ada di kampus merupakan suatu hal yang bersifat mutlak diperlukan untuk mendukung aktifitas operasionalnya baik secara *intern* maupun *ekstern* namun saat ini, kampus STIMATA belum menggunakan *Intrusion Detection System (IDS)* dan *Honeypot* untuk keamanan jaringan Internetnya (*Hotspot*) sehingga berefek pada lemahnya pengetahuan administrator dalam menganalisis setiap aktifitas yang dilakukan oleh pengguna Hotspot itu sendiri.

Selama ini keamanan Internet (*Hotspot*) di Kampus STIMATA masih menggunakan *Mikrotik* sebagai akses keamanan *Hotspot*nya. Dalam kemanan *Mikrotik* hanya beberapa yang masuk kedalam *log serve*r setiap kali pengguna *Hotspot* terkoneksi ke Internet. Setiap beberapa menit *log server* mikrotik cepat berganti secara otomatis, hal tersebut membuat *administrator* tidak bisa memantau secara sempurna dalam setiap aktifitas pengguna *Hotspot.*

Beberapa potensi serangan yang bisa dilakukan adalah *Distributed Denial of Service Attack (DDoS)* dan *ARP Spoofing.* Potensi serangan tersebut bisa memberikan beberapa potensi ancaman bagi *client* (Mahasiswa atau Dosen) bahkan *Server* yang menggunakan koneksi internet kampus STMIK PPKIA Pradnya Paramita Malang. Hal ini terjadi karena lemahnya sistem keamanan jaringan komputer dan adanya kesalahan sistem atau kerusakan sistem komputer *client* karena adanya serangan dari hacker. Untuk mengatasi beberapa hal tersebut diatas maka perlu dicari solusi preventif untuk melindungi jaringan internet (*Hotspot*) kampus STMIK PPKIA Pradnya Paramita

Malang sebelum hal tersebut terjadi, salah satu solusi yang dapat digunakan adalah menerapkan suatu sistem deteksi serangan *(Intrusion Detection System)* jaringan internet (*Hotspot*) kampus STMIK PPKIA Pradnya Paramita Malang.

Salah satu solusi yang dapat digunakan sebagai keamanan *Hotspot* adalah pengunaan *Open Source Software* (*OSS)* sebagai alat yang dapat dimanfaatkan dalam kemanan *Hotspot.* OSS adalah software yang dapat diunduh secara gratis di Internet. Software Open Source yang dapat dimanfaatkan dalam keamanan jaringan Internet di Kampus STIMATA adalah *Snort Intrusion Detection*.

Sebagai pelengkap Snort sebagai *Intrusion Detection System (IDS)* di Kampus STIMATA ditawarkan pula suatu solusi untuk mencegah adanya serangan yaitu dengan mengimplementasikan menggunakan *Honeypot*. *Honeypot* adalah sumber daya sistem informasi yang meniru *server* atau workstation yang digunakan dalam lingkungan produksi dimana tujuannya adalah untuk dikompromikan untuk dieksploitasi atau diserang oleh hacker . Kinerja *Network Intrusion Detection System (NIDS)* yang telah ada pada saat ini dianggap belum dapat memenuhi kebutuhan akan kemampuan pendeteksian terhadap sebuah intrusi yang bersifat Zero-Day yang belum pernah diketahui sebelumnya dan tidak tercantum dalam signature NIDS.

Dengan mengimplementasikan dan menganalisis *Honeypot* beserta Snort dalam arsitektur IDS, pola-pola intrusi baru dapat ditangkap dan dipelajari untuk kemudian diintegrasikan dengan NIDS melalui *signature Hotspot* di Kampus STIMATA.

KAJIAN LITERATUR

Linux

Linux adalah nama yang diberikan kepada sistem operasi komputer bertipe Unix. Linux merupakan salah satu contoh hasil pengembangan perangkat lunak bebas dan sumber terbuka utama. Seperti perangkat lunak bebas dan sumber terbuka lainnya pada umumnya, kode sumber Linux dapat dimodifikasi, digunakan dan didistribusikan kembali secara bebas oleh siapa saja (www.linux.org).

Distribusi *linux* yang digunakan pada penelitian ini adalah Backbox Linux turunan dari Ubuntu 12.04 dan Kali Linux turunan dari Debian 7. Ubuntu merupakan salah satu distro *Linux* yang berbasiskan Debian dan didistribusikan sebagai software bebas.

Pengertian Jaringan Komputer

Jaringan komputer adalah sekelompok komputer otonom yang saling berhubungan antara satu dengan lainnya menggunakan protokol komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi, program-program, penggunaan perangkat keras seperti *printer*, *hard disk*, dan sebagainya. Selain itu jaringan komputer bisa diartikan sebagai kumpulan sejumlah terminal komunikasi yang berada di berbagai lokasi yang terdiri dari lebih satu komputer yang saling berhubungan (Wahana, 2003:2) .

Jenis – Jenis Jaringan Komputer

Local Area Network (LAN), jaringan komputer yang dibangun pada area ruangan, rumah, kantor, gedung, kampus. Sebuah LAN dapat terdiri atas puluhan hingga ratusan buah komputer. LAN mendukung kecepatan transfer data cukup tinggi. Ada 4 “bentuk dasar” LAN atau yang disebut *topologi fisik* LAN (Sofana,2011:11).

Metropolitan Area Network (MAN), merupakan jaringan komputer yang meliputi area sebuah kota. Teknologi yang digunakan oleh MAN mrip dengan LAN. Hanya saja areanya lebih besar dan komputer yang dapat dihubungkan pada jaringanpun lebih banyak dibandingkan LAN (Sofana, 20011:27).

Wide Area Network (WAN), merupakan jaringan komputer yang meliputi area geografis sangat besar, seperti antarkota, antarnegara, antarbenua (mungkin saja antarpelanet). WAN dapat menghubungkan LAN atau MAN yang dipisahkan oleh jarak yang sangat jauh. Untuk menghubungkan

kedua jarak yang berjauhan biasanya digunakan saluran telepon atau saluran komunikasi publik (umum) (Sofana, 2011:29).

Pengertian *Intrusion Detection System*

Intrusion Detection System adalah sebuah alarm keamanan yang dikonfigurasi untuk melakukan pengamatan terhadap *access point*. aktifitas *host*. dan kegiatan penyusupan. Cara paling sederhana untuk mendefinisikan IDS mungkin tergantung dari bagaimana mendeskripsikan IDS sehagai *tool* spesial yang dapat membaca dan mengintepretasikan isi dari *file-file* log dari *router*, *firewall server* dan perangkat jaringan lainnya. Secara lebih spesifik, *Intrusion Detection System* adalah sebuah sistem yang dapat mendeteksi adanya penggunaan tak ter-autorisasi (unauthorized use) pada sebuah sistem jaringan (Beale, 2003).

Pengertian Snort

Snort merupakan salah satu contoh program *Network-based Intrusion Detection System*, yaitu sebuah program yang dapat mendeteksi suatu usaha penyusupan pada suatu sistem jaringan komputer. *Snort* bersifat *open source* dengan lisensi GNU General Purpose License sehingga software ini dapat dipergunakan untuk mengamankan sistem server tanpa harus membayar biaya lisensi (Snort, 2009).

Pengertian Honeypot

Honeypot adalah security resource yang yang sengaja dibuat untuk diselidiki, diserang, atau dikompromikan. Pada umumnya Honeypot berupa komputer, data, atau situs jaringan yang terlihat seperti bagian dari jaringan, tapi sebenarnya terisolasi dan dimonitor. Jika dilihat dari kacamata hacker yang akan menyerang, Honeypot terlihat seperti layaknya sistem operasi yang bisa untuk diserang (Firrar,1:2005) .

Pengertian Hotspot

Hotspot (Wifi) adalah satu standar Wireless Netwoking tanpa kabel, hanya dengan komponen yang sesuai dapat terkoneksi ke jaringan (Wireless Local Area Network-WLAN). yang didasari pada spesifikasi IEEE 802.11 (Priyambodo,5:2005)

Tipe Serangan Wifi (*Hotspot)*

Secara umum terdapat beberapa tipe ancaman keamanan yang mungkin terjadi pada jaringan *Hotspot (wifi)* (Gunadi, 2009:54) yaitu :

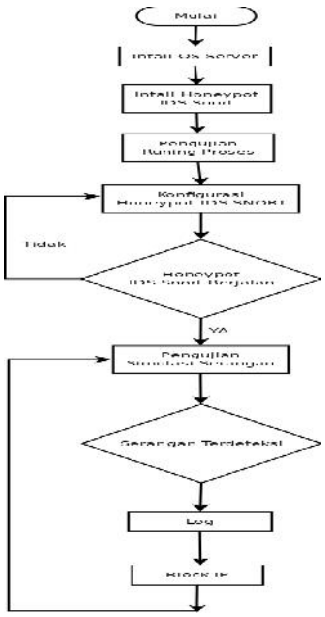
a). Jamming (DDoS)
b). Passive attacks (eavesdropping)
c). Active attacks
d). Man-in-the-middle attacks

METODE PENELITIAN

Analisis Masalah

Sistem keamanan *Hotspot (wifi)* yang menggunakan *Mikrotik* kurang begitu efektif saat adanya proses penyerangan. Dikarenakan saat terjadi penyerangan maka log yang tesimpan hanyalah IP penyerang tanpa adanya keterangan target yang diserang, sehingga bisa membuat *administrator* kesulitan untuk menindak lanjuti adanya serangan. Setiap beberapa menit juga log yang ada disistem *Mikrotik* berganti dengan cepat. Dengan adanya tambahan sistem keamanan dalam jaringan *Hotspot (wifi)* menggunakan *Honeypot* dan IDS Snort maka setiap kali adanya proses penyerangan maka IP penyerang dan target yang diserang langsung masuk kedalam sistem log untuk ditindak lanjuti oleh *administrator* yaitu dengan cara memutus koneksi IP penyerang. Penyerangan dilakukan dengan menggunakan teknik *Spoofing* dan *Distributed Denial of Service* (DDOS)

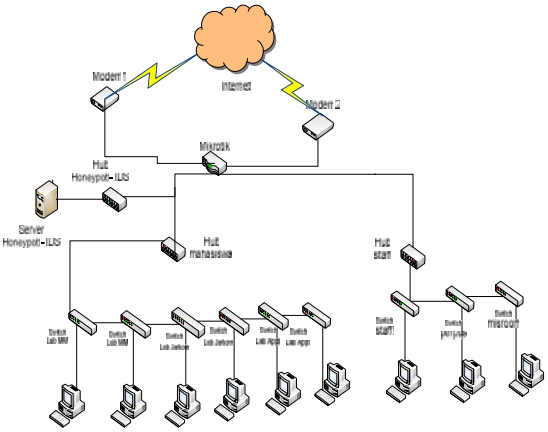
***Flowchart Server Honeypot-IDS Snort* dan Proses Penyerangan**



Gambar 1. Flowchart Server Honeypot-IDS dan Proses Penyerangan

Bagan alir tersebut menentukan langkah-langkah dalam melakukan instalasi *Honeypot* dan IDS Snort sekaligus proses simulasi pengujian serangan.

Topologi Jaringan *Honeypot* dan IDS Snort yang digunakan



Gambar 2. Topologi Jaringan Kampus STIMATA (Honeypot – IDS)

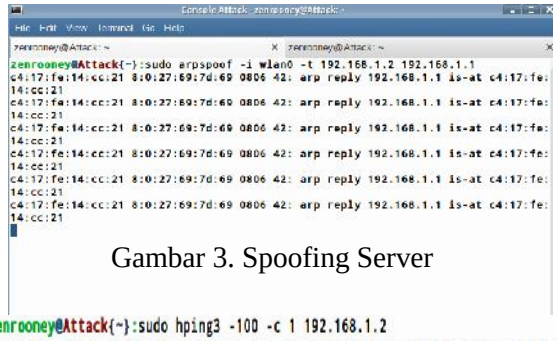
Keamanan Hotspot yang digunakan jika menggunakan Mikrotik dan Honeypot – IDS bisa lebih baik, karena setiap aktifitas pengguna Hotspot bisa terekam lebih lama kedalam *log* Honeypot dan administrator bisa mengetahui serta menanggulangi lebih cepat jika ada salah satu pengguna Hotspot melakukan penyerangan.

HASIL DAN PEMBAHASAN

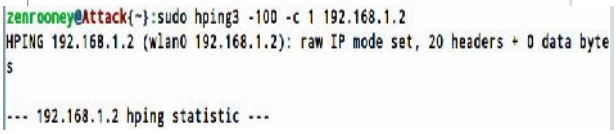
Pengujian Aplikasi

Pengujian aplikasi sistem keamanan menggunakan *Honeypot* dan IDS SNORT ini dengan memakai teknik *Spoofing* dan DDOS.

Tahap awal adalah melakukan proses *scaning* IP target yang kemudian dilanjukan dengan proses penyerangan teknik *Spoofing* dan DDOS.

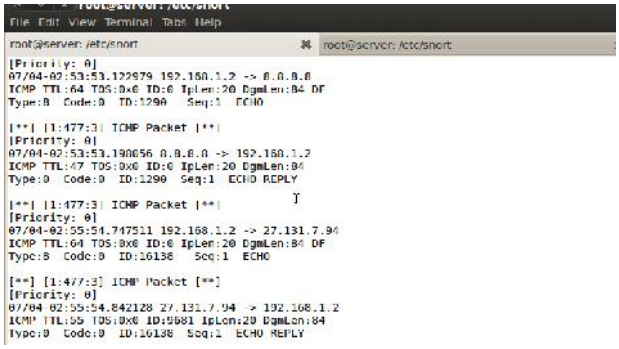


Gambar 3. Spoofing Server

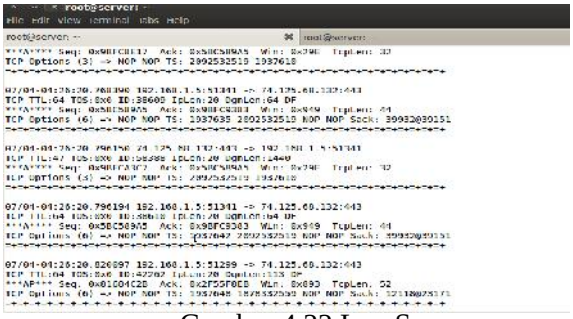


Gambar 4. Attacker Menyerang Dengan DDOS

Setelah proses penyerangan yang dilakukan maka dalam sistem keamanan sudah tersimpan kedalam log *Honeypot* dan IDS.



Gambar 3.13 Log Snort



Gambar 4.22 Log Serangan

Dalam log tersebut memberikan informasi lengkap tentang proses penyerangan, waktu, dan target yang diserang.

KESIMPULAN

Kesimpulan yang dapat diambil berdasarkan hasil penelitian ini adalah sebagai berikut :

1. Berdasarkan hasil pengujian dan analisis yang dilakukan, Honeypot dan Snort dapat diimplementasikan sebagai *Intrusion Detection System* pada sistem keamanan Hotspot untuk mendeteksi serangan berupa *ping*, *nmap port scan*, arp spoof dan DDOS.
2. Honeypot dan Snort bisa memberikan peringatan adanya sebuah serangan yang terjadi dengan menggunakan Hotspot.
3. Mengetahui kelebihan Honeypot dan Snort dalam sistem keamanan Hotspot.

REFERENSI

Beale, Jay. 2003. ***"Snort 2.0 Intrusion Detection"***, Masachusset : Syngress Publishing, Inc.

Fauziah, Lilis. 2009. ***"Pendeteksian Serangan Pada Jaringan Komputer Berbasis IDS Snort Dengan Algoritma Clustering K-Means",*** Surabaya : Institut Teknologi Sepuluh November, Surabaya.

Firrar, Utdirartatmo. 2005. ***"Trik Menjebak Hacker Dengan Honeypot"***. Yogyakarta : ANDI OFFSET.

Gunadi. 2009. **"Wifi - Wireless LAN Jaringan Komputer Tanpa Kabel"**. Bandung: Informatika.

http://www.dvwa.co.uk (online) diakses pada tanggal 19 Mei 2014

http://www.linux.org (online) diakses pada tanggal 19 Mei 2014

http://www.snort.org (online) diakses pada tanggal 19 Mei 2014

http://www.intechopen.com (online) diakses pada tanggal 19 Mei 2014

Priyambodo. 2005. **"Jaringan Hotspot (Wifi)"**. Jogjakarta : ANDI OFFSET

Rafiudin, Rahmat. 2010. ***"Mengganyang Hacker dengan SNORT"***.Surabaya : ANDI OFFSET.

Sofana, Iwan. 2011. ***"Teori dan Modul Praktikum Jaringan Komputer"***. Bandung : Modula.

Snort Teams. Desember 7, 2011. ***"Snort User Manual 2.9.2".*** Columbia: Sourcefire, Inc.

The Ubuntu Manual Team. Juli 30, 2012. ***"Getting Started with Ubuntu 12.04"*** California: Creative Commons.

Wahana, Komputer. 2003. ***"Konsep Jaringan Komputer dan Pengembangannya"***. Jakarta : Salemba Infotek.

Wagoner, Richard. 2007. ***"Performance Testing An Inline Network Intrusion Detection System Snort"***. Master Thesis, Morehead State University.