Jurnal Sarjana Teknik Informatika
Volume 1 Nomor 1, Juni 2013
e-ISSN: 2338-5197

PENERAPAN SISTEM KEAMANAN *HONEYPOT* DAN IDS PADA JARINGAN NIRKABEL (*HOTSPOT*)

[1]Muh Masruri Mustofa (06018022), [2]Eko Aribowo (0006027001)

[1,2] Program Studi Teknik Informatika
Universitas Ahmad Dahlan
Prof. Dr. Soepomo, S.H., Janturan, Umbulharjo, Yogyakarta 55164
[1]Email:
[2]Email: ekoab@tif.uad.ac.id

ABSTRAK

Infrastuktur Jaringan Nirkabel memiliki satu masalah besar, terutama yang membuka akses untuk umum, seperti hotspot adalah masalah keamanannya, dimana banyak terjadi penyerangan oleh satu atau beberapa orang penyerang (attacker) baik pada server penyedia hotspot atau pengguna. Dengan demikian dibutuhkan suatu taktik atau teknik pengamanan guna menanggulangi masalah tersebut.

Subyek penelitian ini adalah penerapan sistem keamanan jaringan nirkabel hotspot. Metode yang digunakan dalam penelitian ini adalah Studi Pustaka (Library Research) dan observasi yaitu melakukan pengamatan secara lagsung terhadap jaringan hospot di UAD. Analisis dilakukan untuk mendapatkan hasil serta data yang bisa dijadikan sebagai acuan guna menerapkan suatu sistem keamanan jaringan hotspot berbasis honeypot dan snort. Sistem hasil implementasi diuji dengan dua metode yaitu Alpha Test dan Beta test.

Hasil penelitian ini adalah kombinasi antara Honeypot dan IDS dengan Honeyd dan Snort ini memberikan sebuah sistem keamanan berlapis dengan menipu dan mendeteksi serangan yang ditujukan ke jaringan hotspot.

Kata kunci : Sistem Keamanan, *Honeypot, IDS*, Jaringan Nirkabel, *Hotspot*.

1. PENDAHULUAN

Honeypot merupakan sebuah sistem atau komputer yang sengaja dijadikan umpan untuk menjadi target serangan dari penyerang (*attacker*). Komputer tersebut melayani serangan yang dilakukan oleh *attacker* dalam melakukan penetrasi terhadap server tersebut. *Honeypot* akan memberikan data palsu apabila ada hal aneh yang yang akan masuk ke dalam sistem atau server. Secara teori *Honeypot* tidak akan mencatat trafik yang legal. Sehingga dapat dilihat bahwa yang berinteraksi dengan *Honeypot* adalah *user* yang menggunakan sumber daya sistem yang digunakan secara ilegal. Jadi *Honeypot* seolah-olah menjadi sistem yang berhasil disusupi oleh *attacker*, padahal penyerang tidak masuk ke sistem sebenarnya, tetapi masuk ke sistem yang palsu.

 e-ISSN: 2338-5197

Salah satu *software Honeypot* yang terkenal dan banyak dipakai adalah *Honeyd*. Ia akan menjebak *attacker* dengan membuat server-server palsu dengan bermacam-macam jenis sistem operasi seperti *Windows, Linux, Unix, Mac Os* dan bahkan *cisco router* dengan berbagi layanan seperti FTP, *Web, Server* dan sebagainya. Salah satu kelebihan *Honeyd* adalah mengemulasikan banyak server dan layanan servis palsu hanya pada satu unit komputer atau server sehingga akan menghemat *resource.*

Sistem keamanan *firewall* tidaklah cukup untuk meminimalkan terjadinya serangan terhadap suatu jaringan komputer. Banyak serangan yang terjadi pada jaringan komputer dapat diketahui setelah adanya kejadian-kejadian yang aneh pada jaringan. Para administrator tidak bisa mengetahui dengan pasti apa yang terjadi, sehingga dibutuhkan waktu yang cukup lama untuk mengaudit sistem guna mencari permasalahan yang telah terjadi.

Untuk mengatasi masalah tersebut dibutuhkan suatu *tool* yang mampu mendeteksi lebih awal terjadinya *intruder* atau kegiatan yang merugikan suatu jaringan. *Intrussion Detection System* merupakan suatu solusi yang sangat tepat untuk keperluan tersebut.

Salah satu IDS (*Intrusion Detection System*) yang sangat populer dalam keamanan IT adalah *Snort*. *Snort* dibuat dan dikembangkan pertama kali oleh Martin Roesh pada bulan November 1998, lalu menjadi sebuah *Open Source project*. Bahkan di situs resminya *www.snort.org* mereka berani mengklaim sebagai standar "*intrussion detection/prevention*". *Snort* merupakan IDS yang sangat populer dan cukup ampuh

2. KAJIAN PUSTAKA

Penelitian yang dilakukan ini mengacu pada penelitian terdahulu yang dilakukan oleh Muhammad Rasyid Syahputra yang berjudul " Implementasi dan analisis serangan pada sistem *Honeypot* menggunakan teknologi jaringan saraf tiruan". Ia memanfaatkan teknologi Jaringan Syaraf tiruan untuk memprediksi jenis serangan yang dilakukan terhadap suatu sistem. Implementasi jaringan saraf tiruan pada sistem *Honeypot* akan membantu prediksi serangan baru yang signaturenya belum terdapat pada basis data serangan. Dengan hasil prediksi tersebut maka *Honeypot* dapat memberikan reaksi yang tepat terhadap suatu jenis serangan baru Univ sehingga dapat memberi interaksi yang sesuai dengan penyerang[5].

Sulistiono Julianto dari Universitas Gunadarma yang melakukan penelitian dengan judul "*Honeypot* sebagai alat bantu pendeteksi serangan pada sistem pengolahan keamanan jaringan komputer". Pada penelitian ini dijelaskan proses dan langkah-langkah membangun suatu sistem *Honeypot* yang menyerupa *production system* yang sesungguhnya dan menggunakan *log* sebagai mekanisme pengawasan pada sistem *Honeypot* [6].

Kemudian penelitian oleh Muhammad Rudyanto Arief yang berjudul "Penggunaan Sistem IDS (*Intrution Detection System*) Untuk Pengamanan Jaringan dan Komputer". Penelitian ini membahas tentang IDS sebagai salah satu sistem pengamanan jaringan dan komputer. IDS hanya cocok digunakan sebagai salah satu sistem pengamanan. Akan tetapi tidak dapat dijadikan sebagai satu-satunya sistem tunggal untuk mengamankan jaringan. Karena karakteristik IDS yang hanya berfungsi sebagai pendeteksi dan pemberi peringatan terhadap gangguan yang datang dari luar dan dalam sistem jaringan itu sendiri[7].

 e-ISSN: 2338-5197

Dari ketiga penelitian di atas yang membedakan dengan penelitian ini adalah bahwa dalam penelitian akan dibangun suatu *Honeypot* dan IDS pada jaringan nirkabel yaitu *hotspot*. *Honeypot* jenis *low involment* yaitu metode menyediakan tiruan dari layanan tertentu. Bentuk paling sederhana dari layanan ini dapat diimplementasikan dengan memasang suatu *listener* pada sebuah *port.*

Honeypot yaitu *honeyd* dan IDS bebasis *snort* akan diimplementasikan pada *hotspot* untuk memgemulasikan beberapa *server* palsu beserta layanan-layanannya, seperti FTP, HTTP, *Telnet*, dan sebagainya.

Berdasarkan hasil penelitian yang dipaparkan di atas maka dilakukan penelitian lebih lanjut dengan judul "Penerapan Sistem Keamanan *Honeypot* dan IDS Pada Jaringan Nirkabel *(Hotpsot*)".

2.1 Honeypot

Pada dunia keamanan jaringan informasi banyak professional yang sangat tertarik pada *Honeypot* karena seorang pengamat serangan akan dapat melihat informasi secara nyata tentang suatu serangan. Kita sering mendengar perusakan sebuah situs web atau sebuah sistem keamanan jaringan pada bank yang di *hack*, tetapi kebanyakan dari kita tidak mengetahui bagaimana sipenyerang masuk dan apa yang sesungguhnya terjadi. Salah satu hal yang bisa didapat dengan *Honeypot* adalah informasi bagaimana seorang penyerang dapat menerobos dan apa yang sudah dilakukannya.

2.1.1 Definisi

Berikut adalah definisi dari *Honeypot*[3] dari tiga orang yang memiliki kopetensi pada penelitian tentang *Honeypot*.

Definisi dari L. Spitzner tentang istilah *Honeypot* adalaha sebagai berikut:

> *"A Honeypot is a resource whose value is being in attacked or compromised. This means, that a Honeypot is expected to get probed, attacked and potentially exploited. Honeypots do not fix anything. They provide us with additional, valuable information."*

Definisi lain menurut Retto Baumann dan Cristian Plattner :

> *"A Honeypot is a resource which pretends to be a real target. A Honeypot is expected to be attacked or compromised. The main goals are the distraction of an attacker and the gain of information about an attack and the attacker."*

Pada dasarnya *Honeypot* adalah suatu alat untuk mendapatkan informasi tentang penyerang. Selanjutnya administrator jaringan dapat mempelajari aktifitas-aktifitas yang dapat merugikan dan melihat kecenderungan dari aktifitas tersebut. *Honeypot* adalah sebuah sistem yang dirancang untuk diperiksa dan diserang.

Sistem dengan *Honeypot* akan menipu dan atau memberikan data palsu apabila ada orang yang memiliki maksud yang tidak baik ketika ia masuk ke suatu sistem. Secara teori *Honeypot* tidak akan mencatat trafik yang legal. Sehingga bisa dilihat bahwa yang berinteraksi dengan *Honeypot* rata-rata adalah user yang menggunakan sumber daya sistem secara ilegal. Jadi *Honeypot* menjadi sistem yang seolah-olah berhasil disusupi oleh penyerang. Padahal penyerang tidak masuk kesistem yang sebenarnya, tetapi malah masuk kedalam sistem yang palsu.

2.1.2 Kategori *Honeypot*

Menurut kategorinya *Honeypot* terdiri atas :

1). Production Honeypot
2). Research Honeypot

Production Honeypot digunakan untuk mengurangi resiko serangan pada sistem keamanan jaringan informasi dalam sebuah organisasi. *Research Honeypot* digunakan untuk mendapatkan infrmasi sebanyak mungkin tentang penyerang sehingga seorang adimnistrator dapat mempelajari sebanyak mungkin informasi tersebut.

2.1.3 Jenis Honeypot

Jenis *Honeypot* adalah berdasarkan *level of involvement* (tingkat keterlibatan). *Level of involvement* mengukur derajat interaksi seorang penyerang dengan sistem informasi. Terdiri dari dua jenis yakni *low involvement Honeypot* dan *high involvement Honeypot*.

1). Low Involvement Honeypot

Low Involvement Honeypot biasanya hanya menyediakan tiruan dari layanan tertentu. Bentuk paling sederhana dari layanan ini dapat diimplementasikan dengan memasang suatu listener pada sebuah *port*. Sebagai contoh, *simple netcat* –l –p 80 > */log/Honeypot/port* 80.*log* dapat digunakan untuk mendengarkan port 80 (HTTP) dan mencatat semua *traffic* yang ada pada *log file*. Pada *Low Involvement Honeypot* tidak ada sistem operasi nyata yang dapat dipakai sebagai tempat operasi penyerang. Ini akan dapat mengurangi resiko secara signifikan karena kompleksitas dari suatu sistem operasi telah ditiadakan. Di sisi lain ini adalah juga suatu kelemahan yang berakibat tidak adanya kemungkinan untuk memperhatikan interaksi penyerang dengan sistem operasi yang bisa jadi sangat menarik. *Low Involvement Honeypot* adalah seperti sebuah koneksi satu arah. Kita hanya akan dapat mendengarkan tanpa bisa menanyakan pertanyaan sendiri. Pendekatan cara ini sangat pasif.

2). High Involvement Honeypot

High involvement Honeypot mempunyai sebuah sistem operasi nyata yang mendasarinya. Hal ini menyebabkan resiko yang sangat tinggi karena kompleksitas menjadi semakin bertambah. Pada saat yang sama, kemampuan untuk mengumpulkan 10 informasi, dan kemungkinan untuk serangan yang lebih atraktif juga semakin bertambah banyak. Satu tujuan dari seorang *hacker* adalah menambah sumber dan mendapatkan akses pada satu mesin yang terhubung ke internet selama 24 jam sehari. *High involvement Honeypots* menawarkan kemungkinan itu. Ketika seorang *hacker* mendapatkan akses, bagian yang sangat menarik dimulai. Sayangnya seorang penyerang akan berkompromi dengan sistem untuk mendapatkan level kebebasan seperti ini. Dia akan mempunyai sumber yang sebenarnya pada sistem dan dapat melakukan apa saja pada setiap saat dalam sistem yang berkompromi tersebut. Oleh sebab itu sistem tidak lagi aman. Bahkan seluruh mesin tidak lagi dapat dikatakan aman. Hal ini tidak akan menjadi masalah jika penyerang berada pada sebuah *jail, sandbox,* atau *VMWare box* karena akan ada jalan untuk keluar dari batas-batas *software* ini.

2.1.4 *Honeyd*

Honeyd [2]adalah *Honeypot Open Source* yang ditulis oleh Niel Provos. *Honeyd* meupakan daemon sederhana yang membuat virtual host tetap pada jaringan. Host

tersebut nantinya bisa dikonfigurasi untuk menjalankan berbagai macam layanan. Kepribadian TCPnya Bisa berjalan sebagai suatu sistem operasi tertentu, umtuk mengelabui *scanner fingerprint* semacam *nmap* atau *xprobe*. Sebenarnya honeyd cukup *powerfull* dan menyediakan fitur yang lengkap, akan tetapi konfigurasinya tidak mudah karena tidak memiliki GUI.

2.2 IDS (*Intrussion Detection System*)

Salah satu masalah keamanan yang cukup signifikan pada jaringan adalah masuknya user dan program (misalnya : *worm, trojan horse, virus*) yang tidak sah sehingga dapat merusak sistem. Untuk itu diperlukan cara untuk menjaga sekuriti sistem. Salah satunya dengan membangun peringatan dini yang disebut deteksi intrusi /penyusupan (*intrusion detection).*

2.2.1 Definisi

IDS (*Intrution Detection System*) [8] adalah sebuah sistem yang melakukan pengawasan terhadap *traffic* jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan didalam sebuah sistem jaringan. Jika ditemukan kegiatan-kegiatan yang mencurigakan berhubungan dengan *traffic* jaringan maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan. Dalam banyak kasus IDS juga merespon terhadap *traffic* yang tidak normal/ anomali melalui aksi pemblokiran seorang *user* atau alamat IP (*Internet Protocol*) sumber dari usaha pengaksesan jaringan.

2.2.2 Arsitektur dan Struktur IDS

Sebuah IDS selalu mempunyai sebuah sensor (mesin analis) yang bertanggung jawab untuk mendeteksi intrusi. Sensor ini terdiri dari mesin pembuat keputusan yang berhubungan dengan intrusi. Sensor-sensor menerima baris data dari 3 sumber informasi utama. IDS memiliki *base, syslog and audit trails*. *Syslog* diincludekan dalam sistem, misal konfigurasi pada *sistem file, autorisasi user*, dsb. Informasi ini menciptakan dasar bagi proses pembuatan keputusan.

Sensor bertugas untuk memfilter informasi dan mendiscard data yang tidak relevan dari sekumpulan kejadian yang terhubung dengan sistem terproteksi, misalnya mendeteksi aktivitas-aktivitas yang mencurigakan. Analis menggunakan database yang berisi kebijakan dalam mendeteksi. Di dalamnya terdapat tandatangan penyerang, deskripsi perilaku normal, dan parameter yang penting (misal, nilai ambang batas*). Database* ini mengatur konfigurasi parameter IDS, termasuk mode komunikasi dengan modul tanggap. Sensor juga mempunyai database yang terdiri atas sejarah dinamis dari intrusi yang komplek.

3. METODE PENELITIAN

3.1 Subyek Penelitian

Subyek penelitian yang aka dibahas pada tugas akhir ini adalah “Penerapan Sistem Keamanan *Honeypot* dan IDS Pada Jaringan Nirkabel (*Hotpsot)*” dengan studi kasus di Lab Jaringan UAD Kampus 3 . Diharapkan dengan adanya sistem keaman pada jaringan *hotspot* yang berupa *Honeyd* dan *Snort* ini akan mengurasi resiko penyerangan, baik terhadap *server* maupun *user*.

 e-ISSN: 2338-5197

3.2 Metode Pengumpulan Data

Metode yang dilakukan bertujuan agar hasil dari penelitian dan analisa lebih terarah serta data yang diperoleh lebih akurat. Kelengkapan data yang diperoleh dapat memberikan kontribusi dalam proses penyusunan skripsi ini, dan memberikan waktu yang lebih singkat. Adapun beberapa metode yang dilakukan dalam pengumpulan data terdiri dari:

3.2.1 Studi Pustaka

Metode pengumpulan data dengan cara membaca berdasarkan kepustakaan dari buku, jurnalmaupun makalah yang mana dimaksudkan untuk mendapatkan konsep teori yang mengenai masalah yang ingin diteliti serta mencari sumber data di internet dan perpustakaan.

3.2.2 Metode Observasi

Pengumpulan data dengan pengamatan secara langsung pada objek yang diteliti untuk memperoleh informasi yang tepat dan sistematis. Meliputi *instalasi*, *konfigurasi*, *tool* yang dipakai dan pengujian koneksi terhadap internet.

4. HASIL DAN PEMBAHASAN

Sesuai dengan penelitian yang dibahas di sub bab 4 didepan, maka hasil yang diperoleh adalah berupa *file log* dari aktifitas penyerang yang telah disimpan oleh *Honeyd* pada direktori /var/log/honeyd/. Setiap ada akses menuju virtual mesin(server palsu) pada alamat ip 192.168.1.100 -192.168.1.105 akan langsung tercatat di *file log*. Setiap aktifitas yang melakukan penyerangan terhadap *hotspot* terutama pada server palsu akan terekam oleh *Honeyd* sesuai dengan jenis server palsu tersebut.

Proses *Honeyd* dan *Farpd* dalam mengemulsikan server-server palsu dna jenis layanan yang diberikannya serta isi dari *file log* yang dihasilkan akan diuraikan pada subbab berikut ini. Tidak ketinggalan juga bentuk *service* yang bekerja mirip dengan servis aslinya.

4.1 Akses *Hotspot*

Akses *hotspot* yang dikonfigurasi pada *hotspot* ini bersifat gratis sehingga setiap user atau penyerang dapat terkoneksi langsung dengan *hotspot* tanpa ada otentikasi seperti *username* ataupun *password*. Karena yang menjadi tujuan utama penelitian ini adalah pada *honeypot* dan *ids* sehingga sistem otentikasi tidak digunakan ataupun sistem *mac filtering* tetapi paling baik sistem tersebut dipakai pada *hotspot* demi keamanan *hotspot*.

Bagi *user* ataupun penyerang disediakan alamat ip 192.168.1.10 samapai dengan 192.168.1.29. Karena alokasi alamat ip sudah di buat dhcp pada server yang bersifat dinamis.

4.2 Prinsip kerja *Honeyd*

Honeyd bekerja saat menerima probe atau koneksi untuk sebuah atau beberapa server palsu dimana server tersebut tercover dalam konfigurasi *Honeyd*. Setelah mengidentifikasikan dirinya sebagai server palsu yang bisa menjadi korban bagi penyerang, *Honeyd* mulai berinteraksi dengan penyerang. Setelah penyerang puas

 e-ISSN: 2338-5197

menyerang server palsu dan koneksi terputus, emulasi service dari server palsu tak langsung terhenti. *Honeyd* akan menunggu koneksi yang lain. *Honeyd* mampu berinteraksi dengan banyak penyerang sekaligus mengemulasikan *service* dari server palsu pada saat yang bersamaan.

Untuk dapat mengulasikan alamat ip, *Honeyd* memerlukan bantuan ARP *spoofing* yang biasanya disediakan oleh *service* dari arpd atau farpd pada ubuntu 10.04. ARP *spoofing*(penyamaran) terjadi pada saat alamat ip dari *user* yang tidak ada (alat ip yang nganggur/tidak terpakai) di *bound* (diklaim) ke *mac address* dari server honeypot berada. Hasilnya paket data pun terkirim ke *honeypot.*

5. SIMPULAN

Berdasarkan pengujian dan analisis data yang telah dilakukan terhadap penelitian *Honeypot* dan *Snort* sebagai monitor penyerang terhadap jaringan nirkabel hotpsot maka dapat disimpulkan :

1. *Honeypot* merupakan sebuah sistem atau komputer server yang sengaja dikorbankan untuk menjadi target serangan bagi penyerang, yang melayani setiap penyerangan yang dilakukan oleh penyerang dalam setiap penetrasi terhadap server utama tersebut dengan menipu atau memberikan data palsu apabila ada yang orang dengan maksud tidak baik ketika ia masuk kesuatu sistem atau server utama. Jadi *Honeypot* seolah-olah menjadi system yang berhasil disusupi oleh penyerang tidak masuk ke sistem sebenarnya, tetapi malah masuk kesistem yang palsu.
2. Implementasi *Honeypot Honeyd* pada jaringan nirkabel *hotspot* yang sangat berkembang pesat saat ini akan memberikan tambahan kesulitan kepada penyerang yang mencoba melakukan penyerangan.
3. *Honeypot* akan merekam aktivitas dari penyerang yang melakukan penyerangan terhadap server-server palsu yang memberikan layanan mirip dengan layanan mirip dengan server utama dalam bentuk *file log.*
4. *Snort* memberikan rekaman trafik yang janggal atau mencurigakan ke server dalam bentuk *file log* atau *alert*.
5. Kombinasi antara *Honeypot* dan IDS dengan *Honeyd* dan *Snort* ini memberikan sebuah sistem keamanan berlapis dengan menipu dan mendeteksi serangan yang ditujukan ke jaringan *hotspot*.

6. DAFTAR PUSTAKA

[1] Mulyana, Edi S., SSI. 2005. *Pengenalan Protokol Jaringan Wireless* Komputer. Yogyakarta: Andi.
[2] Pangera, Ali Abbas. 2008. *Menjadi Admin Jaringan Nirkabel*. Yogyakarta: Andi.
[3] Provos, Niels. Holz, Thorsten. 2007. *Virtual Honeypot:From Botner racking to Intrussion Detection*. Boston: Addison Wesley Professional.
[4] Purbo, Onno W. 2006. *Buku Pegangan Internet Wireless dan Hotspot*. Jakarta: PT. Elex Media Komputindo.

 e-ISSN: 2338-5197

[5] Syahputra, Muhammad Rasyid. 2006. *Implementasi dan Analisis serangan pada sistem Honeypot menggunakan teknologi jaringan syaraf tiruan.* Depok: Universitas Gunadarma.
[6] Julianto, Sulistiono. 2006. *Honeypot sebagai alat bantu pendeteksi serangan pada sistem pengolahan keamanan jaringan*. Depok: Universitas Gunadarma.
[7] Arief, Muhammad Rudiyanto. 2005. *Penggunaan sistem IDS untuk pengamanan jaringan dan komputer*. Yogyakarta: STMIK Amikom.
[8] http://ilmuti.com/2011/03/02/jaringan-lokal-nirkabel/, Jumat, 7 Oktober 2011. Jaringan Lokal Nirkabel.
[9] http://netsecurity.about.com/cs/hackertools/a/aa030504p.htm, Jumat, 7 Oktober 2011,introduction to *Intrussion Detection System*.
[10] http://www.webopedia.com/TERM/I/intrusion_detection_system.html, Jumat, 7 Oktober 2011, Intrussion Detection system.
[11] http://css.its.psu.edu/netpeople/May2002/sos501.html Jumat, 7 Oktober 2011, Penggunaan sistem IDS untuk Jaringan Komputer.
[12] http://202.158.68.230/img/product-1/2011/7/19/406226/406226_acdfee6c-b1a2-11e0-8de1-44df30380690.jpg
[13] http://ayumiska.files.wordpress.com/2009/11/pci-card-wifi.jpg
[14] http://www.windowsecurity.com/img/upl/ids_rys31049723735904.gif
[15] http://2.bp.blogspot.com/_809mNXVJd0I/SuiZ8l3RFII/AAAAAAAAACo/4dY_RhkdMwE/s320/ komponen.JPG
[16] http://www.windowsecurity.com/img/upl/ids_rys11049723546982.gif
[17] http://www.windowsecurity.com/img/upl/ids_rys21049723625665.gif