Sistem Pendeteksi Intrusi Menggunakan Metode Honeypot

Iwan Syarif [1)], Ferry Astika S.[2)], Anritsu S. Ch. Polii [3)], Ida Hastuti [4)]
[1,2] Politeknik Elektronika Negeri Surabaya
[3] Teknik Elektro, Politeknik Negeri Manado
[4] Teknik Elektro, Politeknik Negeri Banjarmasin

Abstrak

Salah satu metode yang digunakan dalam pendeteksian intrusi (gangguan) adalah metode Honeypot. Honeypot adalah suatu sumber sistem informasi yang mempunyai nilai kebohongan bagi siapa saja yang secara tidak sah atau tidak mempunyai hak untuk akses sumber sistem informasi. Honeypot mencakup banyak aspek diantaranya bagaimana cara membangun suatu Honeypot dengan sistem decoy (pemikat) yang mempunyai sifat mudah diserang.

Pada paper ini dilakukan pembangunan sistem Honeypot serta pendeteksian intrusi yang disimulasikan menggunakan beberapa tool hacker.

Hasil yang dicapai pada penelitian berupa data statistik keberhasilan sistem melakukan redirect serangan dan waktu yang diperlukan untuk proses switching.

Kata kunci: *Honeypot, IDS (Intrusion Detection System), Network Security*

1. Pendahuluan

Jaringan komputer yang saat ini terhubung ke *Internet* diharapkan peka terhadap berbagai eksploitasi perusakan. Sistem yang andal dapat mencegah atau mengetahui secara dini perusakan dari *hacker* yang bisa saja dapat memperoleh akses ke *Root/Administrator*. Alternatif pengaman pada sebuah *server* yang ada di *Internet* dapat dilakukan dengan *Intrusion Detection System (IDS)* menggunakan metode *Honeypot*.

Pada dasarnya *Honeypot* merupakan sebuah S*erver* dan jaringan palsu yang akan mengelabui penyusup melalui situs-situs palsu, sehingga *Intruder* tak akan pernah mencapai sasaran situs *Web* yang sesungguhnya. Jadi dengan adanya *Honeypot* ini suatu sistem memiliki senjata untuk melindungi dirinya.

Oleh karena itu diharapkan *Honeypot* akan menjadi salah satu aplikasi yang bisa meningkatkan keamanan komputer, baik jaringan maupun pribadi.

2. Intrusion Detection System

Intrusion adalah usaha untuk masuk dan/atau menyalahgunakan sistem yang ada.

Intrusion Detection adalah proses *monitoring event* yang terjadi pada sistem komputer atau jaringan komputer dan melakukan analisa data tersebut untuk mengetahui adanya *Intrusion* ataupun melakukan mekanisme pengamanan.

IDS memiliki karakteristik dan metode yang berbeda-beda dalam melakukan *monitoring* dan analisis terhadap deteksi penyusupan. Metode yang diterapkan dalam *IDS* terbagi atas :

- ✓ *Host-Based*

  Pendeteksian dengan metode *Host-Based* dibagi atas *signature based / misuse detection* dan *anomaly detection.*

- ✓ *Network-Based*

  Sama halnya dengan metode *host-based*, pada metode *network-based* dibagi atas *signature based / misuse detection* dan *anomaly detection*, hanya saja pada metode ini berjalan pada jaringan.

- ✓ *Honeypot*

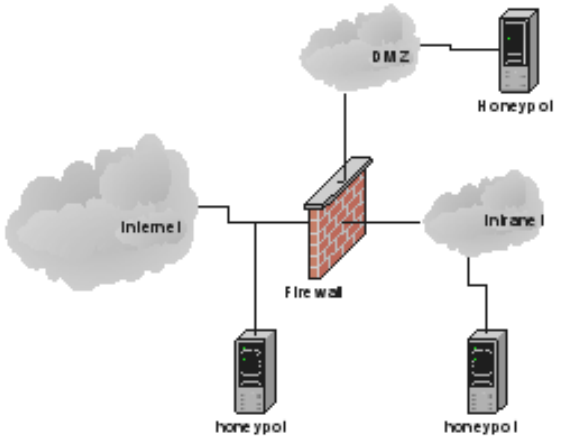
  Data *Source* yang dapat diserang dan dikompromi, berisi data gadungan guna menarik dan mengalihkan *intruder* dari target *real* sehingga diperoleh informasi tentang *intruder* dan teknik serangan.

3 Honeypot

Honeypot adalah suatu sumber sistem informasi yang mempunyai nilai kebohongan bagi siapa saja yang secara tidak sah atau tidak mempunyai hak untuk akses sumber sistem informasi. *Honeypot* merupakan suatu sumber daya keamanan yang mempunyai nilai kebohongan bagi orang yang menyelidiki atau berkompromi dengan sistem tersebut.

Penempatan *Honeypot* dapat dikategorikan dalam 3 (tiga) tempat, yaitu:

- ✓ Sebelum *firewall*
- ✓ Sesudah *firewall* (*intranet*)
- ✓ *DeMilitary Zone (DMZ)*



Gambar 1. Penempatan *Honeypot*

Penggunaan *Honeypot* dibedakan dalam 2 (dua) tipe :

- ✓ *Research Honeypots*

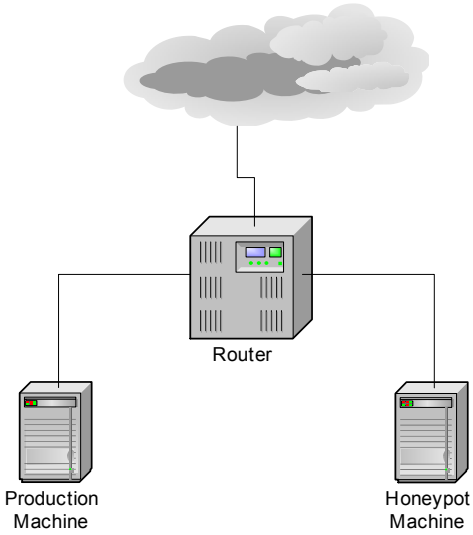
  Kategori tipe ini digunakan untuk keperluan riset dan untuk memperoleh pengetahuan tentang metode intrusi.

- ✓ *Production Honeypots*

  Tipe ini digunakan oleh institusi baik pemerintah maupun swasta sebagai bagian dari pada infrastruktur keamanan untuk mengukur tingkat keamanan suatu institusi.

4. Perancangan Sistem

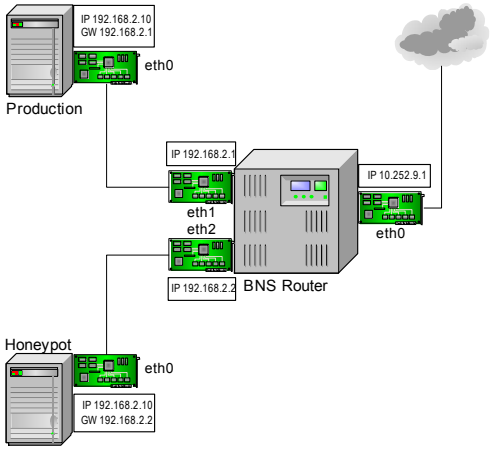
Bentuk sederhana dari perencanaan sistem *Honeypot* yang akan dibangun seperti pada gambar *topologi Honeypot*.



Gambar 2. Topologi Honeypot

Gambar 2 menunjukkan desain ringkas menyangkut wujud *Honeypot*.

Perancangan sistem *Honeypot* terlihat seperti gambar berikut



Gambar 3. Topologi BNS

Honeypot yang dirancang menggunakan perangkat lunak *Bait and Switch (BNS)*. Desain sistem *Honeypot* ini terdiri dari 3 (tiga) komponen utama, yaitu : *BNS Router; Production;* dan *Honeypot.*

Konfigurasi sistem *Honeypot* terdiri dari 2 (dua) perangkat lunak, yaitu *Bait and Switch (BNS)* dan *Snort*. Perangkat lunak ini saling berinteraksi dan tidak dapat lepas satu sama lain untuk menghasilkan suatu sistem *Honeypot* yang terpadu.

5. Simulasi Sistem

Demi kelancaran proses simulasi, dilakukan desain *web page* untuk *Production Server* seperti pada gambar 4.

Gambar 4. Web Page Production

Sedangkan untuk *Honeypot Server* dirancang *web page* seperti pada gambar 5.

Gambar 5. Web Page Honeypot

Sekuensial simulasi secara umum yang dilakukan pada saat pengujian dapat dilihat pada algoritama berikut :

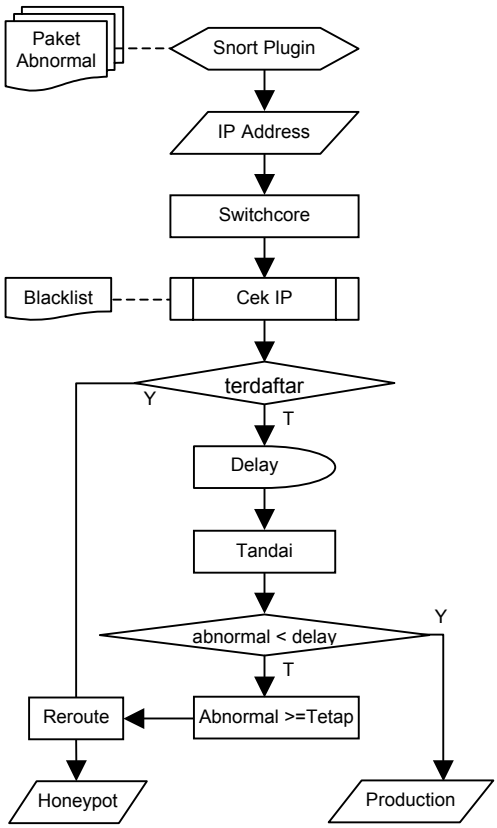
- ✓ Diasumsikan *domain* dari kedua *website* adalah *www.airmadidi.com*.
- ✓ Sebagai awal dari proses simulasi, dilakukan *browsing* dari komputer *hacker* ke situs *www.airmadidi.com*.
- ✓ Hasil dari *browsing* mengarah pada *Production Server* yang dibuktikan dengan tampilan *browser* pada komputer *hacker* sesuai dengan gambar 4.
- ✓ Berdasarkan hasil *browsing*, kemudian dilakukan exploitasi terhadap situs www.*airmadidi.com*.
- ✓ Selanjutnya *browsing* ulang situs *www.airmadidi.com*.
- ✓ *Browsing* ulang yang dilakukan oleh *hacker* menghasilkan tampilan *homepage Honeypot* seperti pada gambar 5.

Simulasi pengujian sistem yang dilakukan menggunakan *Tool Hacker*, yaitu :

- ✓ *Superscan 3.0*
- ✓ *Saint 3.5.1*
- ✓ *Phobia 0.99b*
- ✓ *Imaps*
- ✓ *Script Kiddies*
- ✓ Lainnya (*Fpipe & Fscan*).

6. Analisa Sistem

Analisa hasil pengujian sistem *Honeypot* yang dilakukan dapat dilihat seperti diagram alir sistem *Switchcore*.



Gambar 4. Flowchart Sistem Switchcore

Algoritma dari diagram alir sistem *Switchcore* :

- ✓ Pengiriman paket-paket melalui *traffic* jaringan dapat dideteksi oleh *Snort Plugin*, apabila ada *traffic* yang berpotensi tidak normal dari suatu *IP Address* maka *Snort* akan memberitahu kepada *Switchcore*.
- ✓ *Switchcore* kemudian akan mengecek *IP Address* tersebut.
- ✓ Apabila *IP Address* tersebut belum termasuk daftar *blacklist*, maka akan ditunggu untuk beberapa waktu lamanya tingkat eksploitasi yang dilakukan.
  - o Apabila intensitasnya semakin tinggi, maka *IP Address* tersebut akan di *blacklist*.
  - o Jika paket berpotensi *abnormal* yang diterima untuk beberapa waktu adalah tetap maka *IP Address* tersebut akan ditandai. Dan *IP Address* tersebut akan diarahkan ke *Honeypot Machine*.
  - o Dalam waktu singkat pangiriman paket abnormal terhenti, maka *IP Address* tersebut akan ditandai tetapi tidak akan dikirim ke *Honeypot*.
- ✓ Sedangkan jika *IP Address* tersebut telah berada dalam daftar *blacklist*, maka *IP Address* tersebut akan langsung dikirim ke *Honeypot Machine*.

7. Unjuk Kerja Sistem

Kinerja keberhasilan sistem dapat ditinjau dari statistik hasil serangan dan waktu *redirect* sistem.

Pengujian terhadap 7 (tujuh) *tool hacker* untuk 2 jenis *platform* sistem operasi yang berbeda memberikan informasi berupa statistik keberhasilan *tool* memasuki sistem dan keberhasilan sistem melakukan *redirect* terhadap penyerangan, sebagaimana terlihat pada data berikut :

Tabel 1. Statistik Keberhasilan Sistem

OS	Tool Hacker	Memasuki Sistem		Redirect
		Gagal	Sukses	
Linux	4	0	4	4
Windows	3	2	1	1

Tool hacker Linux yang memasuki *IDS Honeypot* sebanyak 4 (empat), dan semuanya berhasil di *redirect* oleh *IDS Honeypot*.

Tool hacker Windows yang mampu memasuki *IDS Honeypot* hanya 1 (satu) dari 3 (tiga) *tool* yang digunakan dan *IDS Honeypot* berhasil melakukan *redirect* ke *Honeypot Machine*.

Hasil Rekapitulasi jumlah paket yang dideteksi *Snort plugin* seperti tabel berikut :

Tabel 2. Rekapitulasi Jumlah Paket

TOOL	JUMLAH PAKET		
	Out	Drop	Total
Superscan	49	0	49
Saint	79	0	79
Phobia	14209	9254	23463
Imaps	30	0	30
Script Kiddies	262	0	262

Adapun rincian mengenai distribusi paket yang melewati protokol-protokol dapat dilihat pada tabel berikut :

Tabel 3. Rekapitulasi Rincian Paket Setiap Protokol

TOOL	PROTOKOL			
	TCP	UDP	ICMP	ARP
Superscan	0	0	26	23
Saint	52	15	10	2
Phobia	4866	0	0	89
Imaps	24	0	0	6
Script Kiddies	166	0	0	96

Rincian paket yang melalui protokol-protokol didistribusikan oleh *Snort plugin* seperti terlihat pada gambar 3, dimana ada 4 (empat) protokol yang dilewati oleh paket-paket, sedangkan protokol yang lain, yaitu : EAPOL; IPv6; IPX; dan lainnya, tidak ada paket-paket yang melewati protokol tersebut.

Pengiriman paket-paket yang berisi intrusi melalui protokol-protokol yang ada, menghasilkan respon berupa aksi yang dapat dilihat pada tabel 4.

Tabel 4. Rekapitulasi Status Aksi

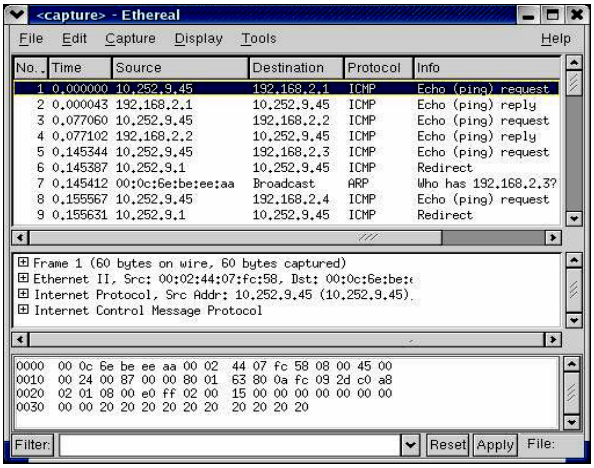
TOOL	STATUS AKSI		
	Alerts	Logged	Passed
Superscan	10	10	0
Saint	17	17	0
Phobia	4	4	0
Imaps	1	1	0
Script Kiddies	1	1	0

Berdasarkan tabel rekapitulasi status aksi, maka sejauh ini pendeteksian terhadap penyerangan dapat dikatakan berhasil dengan pertimbangan :

- ✓ Jumlah *alerts* sama dengan jumlah *log file*
  Alerts = Logged
- ✓ Tidak ada paket-paket yang berisi data *intrusi* yang dilewatkan.
  Passed = 0

Unjuk kerja sistem yang dibangun dapat ditinjau juga dari waktu yang diperlukan oleh sistem untuk melakukan *Switching*.

Parameter yang dijadikan sebagai acuan waktu yang diperlukan untuk *Switching*, yaitu penyerangan menggunakan *tool Superscan*. Hasil rekaman data *Ethereal* mengenai proses *Switching* dengan menggunakan *tool Superscan*, seperti terlihat pada informasi gambar *traffic* jaringan *Superscan*.



Gambar 4. Traffic Jaringan Superscan

Request yang dilakukan oleh komputer *hacker* dengan *IP Address* 10.252.9.45, ditujukan ke situs www.airmadidi.com (192.168.2.10) di *replay* oleh situs ini melalui *gateway Production Machine* pada *BNS Router* dengan *IP Address* 192.168.2.1 yang terjadi pada waktu ke-0.000043 detik. Proses *Switching* ke *Honeypot* terjadi pada waktu ke-0.077102 detik, yang dibuktikan dengan *replay* oleh *IP Address* 192.168.2.2 pada *BNS Router* yang sesungguhnya merupakan *IP Address gateway Honeypot Machine*.

Dengan demikian durasi yang dibutuhkan untuk *Switching* pada penyerangan menggunakan *tool Superscan* $\pm$ 0.077059 detik.

8 Kesimpulan

- ✓ Prinsip kerja dari sistem *Honeypot BNS* adalah seluruh *traffic* normal dari *Client* akan mengakses secara langsung *Production Server*, sedangkan *traffic* yang abnormal akan diarahkan ke *Honeypot Server*.
- ✓ Kinerja *IDS Honeypot* dapat ditinjau melalui keberhasilan *Switching* terhadap serangan, dan waktu yang diperlukan untuk proses *Switching*.
- ✓ Data statistik keberhasilan sistem, menunjukkan bahwa dari 7 (tujuh) penyerangan yang disimulasikan, baik melalui sistem operasi *Windows* maupun *Linux* berhasil di *redirect* ke *Honeypot*.
- ✓ Hasil penyerangan menggunakan *tool hacker* memberikan data *log file Snort* dan *Switchcore*. Berdasarkan data simulasi sistem yang ada, ternyata hanya satu *tool hacker* yang berhasil direkam pada *log file Switchcore*, yaitu *tool Saint*. Hal ini dikarenakan aturan-aturan yang

dikonfigurasikan pada *switch.vars BNS* belum dilanggar. Namun demikian proses *Switching* tetap berlangsung, karena *Plugin* yang dijalankan adalah *Rules Snort* yang terintegrasi dengan *BNS*.

- ✓ Selisih waktu antara *log file Switchcore* dan *log file Snort* tergantung pada jumlah deteksi *alert* dari *Snort* yang banyak dalam waktu yang sangat singkat. Selain itu juga bergantung pada *setting* waktu *switch.vars*.
- ✓ Pada saat pengujian berlangsung ternyata ada selisih waktu *Switching* antara *Production Machine* dengan *Honeypot Machine*. Hal ini dapat dibuktikan dengan hasil analisa traffic jaringan menggunakan *tool Ethereal* untuk penyerangan menggunakan *tool hacker Superscan*. Durasi yang dibutuhkan untuk *Switching* pada penyerangan menggunakan *tool Superscan* $\pm$ 0.077059 detik.
- ✓ Analisa sistem *Switchcore* didasarkan pada informasi yang diberikan *Snort* berupa *IP Address* yang berpotensi sebagai *attacker*, kemudian *Switchcore* mengecek *IP Address*. Jika telah termasuk daftar *blacklist* maka akan langsung diarahkan ke *Honeypot*, apabila tidak termasuk dalam daftar maka *Switchcore* menandai *IP Address* tersebut dan menunggu beberapa saat untuk diambil keputusan mengarahkan *IP Address* tersebut ke *Honeypot*

Daftar Pustaka

[1] Baumann Reto, "***Honeypots"***, *Swiss Federal Institut of Technology*, 2002.

[2] Spitzner Lance, *Paper* ***"Honeypots : Definitions and Value of Honeypots"***, 2003.

[3] Lenkey Gideon J., *Presentation* ***"Hacker Tracking – A Case Study"***, *Ra Security System*, 2002.

[4] Ranum Marcus J., *Presentation* ***"A Whirlwind Introduction to Honeypots"***, *Computer Security Institute(CSI)*, 2002.

[5] Lee Won-Seok, *Presentation* ***"Honeypot"***, *info. Comm. & Security Lab., Ajou University,* 2002.

[6] Rahardjo Budi, ***"Keamanan Sistem Informasi Berbasis Internet"***, PT Insan Infonesia – Bandung & PT Indosic – Jakarta, 2002.

[7] Iwan Syarif, Arif Djunaidy, Febriliyan Samopa, ***Aplikasi Data Mining Untuk Pedeteksian Intrusi Pada Sistem Jaringan Dengan Metode Klasifikasi Dan Clustering***, Surabaya, 2003.

[8] http://www.violating.us

[9] http://baitnswitch.sourceforge.net

[10] http://www.snort.org

[11] http://www.honeypots.net

[12] http://www.honeypots.net/honeypots/links

[13] http://www.honeynet.com

[14] http://www.tracking-hackers.com

[15] http://www.securiteam.com/securitynews