ISSN 2355-3286

Desain dan Implementasi Honeypot dengan Fwsnort dan PSAD sebagai Intrusion Prevention System

Bosman Tambunan, Willy Sudiarto Raharjo, Joko Purwadi
Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Duta Wacana
22074366@students.ukdw.ac.id, willysr@ti.ukdw.ac.id, jokop@ukdw.ac.id

Diterima 3 Mei 2013
Disetujui 24 Mei 2013

Abstrak—Teknologi Internet saat ini tidak lepas dari banyak masalah ataupun celah keamanan. Banyaknya celah keamanan ini dimanfaatkan oleh orang yang tidak berhak untuk mencuri data-data penting. Kasus serangan terjadi karena pihak yang diserang juga tidak menyadari pentingnya keamanan jaringan untuk diterapkan pada sistem yang dimiliki.

Honeypot yang dipadu dengan IPS menggunakan PSAD dan Fwsnort memberikan solusi untuk masalah tersebut. IPS berfungsi sebagai sistem yang bekerja memantau aktivitas jaringan yang melalui sistem IPS pada mode inline dan memblokir alamat IP yang mencurigakan setelah data stream dicocokan dengan signature yang ada, sedangkan Honeypot bekerja untuk mengetahui aktivitas penyerang dan semua aktivitas yang menuju pada honeypot dianggap mencurigakan.

Hasil penelitian menunjukkan bahwa kemampuan Honeypot yang dipadu dengan IPS PSAD dan Fwsnort dapat saling melengkapi dalam mendeteksi serangan yang tidak diketahui oleh sistem IPS. Sistem ini juga menghasilkan log data yang dapat digunakan oleh administrator dalam menanggulangi serangan yang terjadi.

Kata kunci—intrusion prevention system, honeypot, psad, fwsnort, honeyd

I. Pendahuluan

Berkembangnya jaringan Internet saat ini membantu manusia untuk saling berkomunikasi serta bertukar informasi, tetapi tidak semua informasi bersifat terbuka atau umum. Karena Internet merupakan jaringan publik, maka diperlukan suatu usaha untuk menjamin keamanan informasi tersebut. Di sisi lain, terdapat pihak-pihak dengan maksud tertentu yang berusaha untuk menembus sistem keamanan tersebut. Begitu pula dengan adanya tindakan penyusupan yang belum diketahui atau *zero day exploit*.

Honeypot memungkinkan untuk melakukan hal tersebut dengan cara bertindak sebagai umpan dalam jaringan komputer untuk mengelabui *attacker* dan juga untuk mengumpulkan *malware*. Saat ini ada beberapa jenis honeypot yang ada. Untuk itu akan dilakukan penelitian untuk menggunakan honeypot dengan efisien untuk mengidentifikasi penyusupan atau mengumpulkan malware tersebut. Honeypot adalah sumber daya sistem informasi yang meniru *service* yang ada pada *server* atau *workstation* dan digunakan dalam lingkungan produksi dimana tujuannya adalah untuk dieksploitasi oleh penyerang.

Untuk menghadapi masalah keamanan jaringan juga dapat menggunakan *firewall*. Saat ini *firewall* yang ada dirasa kurang baik dalam melakukan pendeteksian penyusupan oleh karena *firewall* dirancang untuk memblok suatu aktivitas dimana penyusupan dilakukan secara tegas.

Sistem pendeteksian *Intrusion Detection System* (IDS) memegang peranan penting dalam pengamanan jaringan. PSAD (*Port Scan Attack Detector*) dan Fwsnort merupakan produk *Open Source* yang menjadi kombinasi pilihan sebagai pendeteksi intrusion dalam jaringan yang dapat dikembangkan menjadi *Intrusion Prevention System* (IPS). Kombinasi *Intrusion Prevention System* ini akan dikombinasikan dengan kemampuan honeypot untuk melakukan pencegahan maupun melihat aktivitas *attacker*.

Dalam penelitian ini penulis merancang dan membangun sistem IPS dikombinasikan dengan honeypot agar dapat menangani suatu penyerangan berdasarkan pada *alert* yang telah ditampung dalam file *log* dan juga dapat memberikan *log* tentang serangan yang baru dan belum diketahui oleh sistem IPS.

II. Landasan Teori

A. *Intrusion Detection System*

Intrusion Detection System (IDS) merupakan suatu sistem aplikasi yang dapat memonitor lalu lintas jaringan dari aktivitas paket-paket data yang

mencurigakan atau yang melanggar aturan keamanan jaringan dan kemudian membuat laporan dari aktivitas jaringan tersebut (Alder, 2004). Terdapat 3 macam konsep IDS, yaitu :

a. *Network-based Intrusion Detection System* (NIDS), yang bekerja memonitor seluruh *segment* jaringan ataupun *subnet.* Keuntungan dari konsep ini yaitu tidak ada efek yang terjadi pada sistem ataupun jaringan saat dilakukan *monitoring*.

b. *Host-based Intrusion Detection System* (HIDS), tipe ini bekerja untuk melindungi pada sisi *host.* Keuntungan menggunakan konsep ini yaitu kemampuan untuk dapat meletakkan *rules* yang lebih spesifik sesuai kondisi komputer *host*.

c. *Distributed Intrusion Detection System* (DIDS), tipe ini merupakan kombinasi sensor NIDS dan sensor HIDS dalam jaringan yang lebih besar dan kemudian mengirimkan *log* pada sistem yang terpusat.

B. *Intrusion Prevention System*

Intrusion Prevention System (IPS) adalah sebuah aplikasi yang bekerja untuk *monitoring traffic* jaringan, mendeteksi aktivitas yang mencurigakan, dan melakukan pencegahan dini terhadap intrusi atau kejadian yang dapat membuat jaringan menjadi berjalan tidak seperti sebagaimana mestinya (Stiawan, 2011). Produk IPS sendiri dapat berupa perangkat keras (*hardware*) atau perangkat lunak (*software*). Terdapat dua jenis konsep IPS, yaitu:

a. *Network-based Intrusion Prevention System* (NIPS), tipe ini melakukan pemantauan dan proteksi dalam satu jaringan secara keseluruhan.

b. *Host-based Intrusion Prevention System* (HIPS), program *agent* HIPS dipasang secara langsung pada sistem yang diproteksi untuk dipantau aktivitas keluar dan masuk internal sistem tersebut.

C. Honeypot

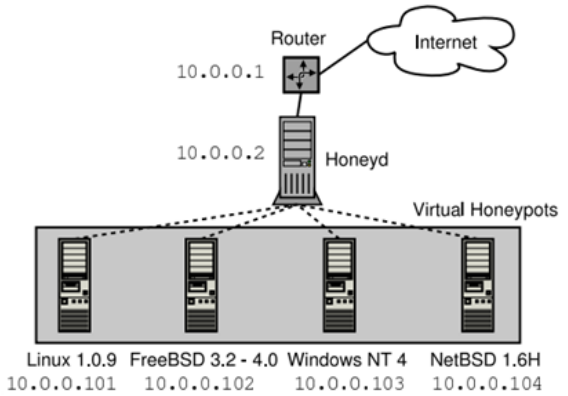
Honeypot adalah sumber sistem informasi yang biasanya didesain bertujuan untuk mendeteksi, menjebak, dalam usaha percobaan penetrasi kedalam sistem (Joshi, 2011). Umumnya honeypot terdiri dari komputer, data, dan segmen jaringan yang terlihat Honeypot juga memiliki fitur *monitoring* untuk memantau aktivitas penyerang ketika masuk ke dalam sistem honeypot. Aktivitas yang bisa diketahui diantaranya *port* yang diserang, *command* yang diketik oleh penyerang, dan perubahan yang dilakukan penyerang di server palsu honeypot. Hal ini dapat dimanfaatkan oleh *Network Administrator* sebagai masukan untuk melakukan *patch* pada sistem yang sesungguhnya, melakukan konfigurasi di segmen jaringan asli untuk dilakukan pencegahan dini (Hoopes, 2009). Honeypot dapat membawa risiko besar pada jaringan vital sehingga harus di perhatikan dengan baik. Jika honeypot tidak diisolasi dengan baik dan sempurna, penyerang dapat menggunakan honeypot untuk menyerang segmen vital dalam jaringan. Honeypot memiliki 2 macam tipe berdasarkan fungsi peletakkannya (Provos, 2007), yaitu:

a. *Production* Honeypot, honeypot tipe ini diletakkan dalam jaringan produksi yang bertujuan untuk mendeteksi serangan dan untuk membantu mengurangi resiko keamanan jaringan sebuah organisasi.

b. *Research* Honeypot, honeypot tipe ini didesain untuk mendapatkan informasi mengenai aktivitas-aktivitas dari komunitas penyerang atau penyusup. Honeypot jenis ini tidak memberikan suatu nilai tambah secara langsung kepada suatu organisasi, melainkan digunakan sebagai alat untuk meneliti ancaman-ancaman keamanan dan bagaimana cara untuk melindungi sistem sendiri dari ancaman tersebut.

Honeypot memiliki klasifikasi berdasarkan kepada tingkat interaksi yang dimilikinya. Tingkat interaksi dapat didefinisikan sebagai tingkat aktivitas penyerang ke dalam sistem yang diperbalahkan oleh honeypot, semakin tinggi tingkat aktivitas yang diperbolehkan maka semakin tinggi pula tingkat interaksi honeypot (Singh, 2009).

a. *Low-Interaction* Honeypot, merupakan honeypot yang didesain untuk mensimulasikan *service* (layanan) seperti pada *server* yang asli dengan *service-service* tertentu (misal SSH, HTTP, FTP) atau dengan kata lain sistem yang bukan merupakan sistem operasi secara keseluruhan, *service* yang berjalan tidak bisa dieksploitasi untuk mendapatkan hak akses penuh terhadap honeypot.



Gambar 1. Honeyd mensimulasikan sistem operasi yang berbeda-beda

b. *High-Interaction H*oneypot, pada honeypot jenis ini terdapat sistem operasi dimana penyerang berinteraksi langsung dan tidak ada batasan yang membatasi interaksi tersebut. Menghilangkan batasan-batasan tersebut menyebabkan tingkat resiko yang dihadapi semakin tinggi karena penyerang

dapat memiliki hak akses *root.* Pada saat yang sama kemungkinan pengumpulan informasi semakin meningkat dikarenakan kemungkinan serangan yang tinggi.

Sebuah honeypot dapat ditempatkan di setiap tempat dimana *server* ditempatkan. Meski demikian, beberapa lokasi penempatan mempunyai nilai yang lebih baik dibandingkan dengan lokasi lain. Biasanya honeypot akan ditempatkan pada lokasi berikut:

a. Penempatan berhadapan langsung dengan Internet, penempatan langsung tanpa adanya *firewall* di depan *gateway* sehingga akan mengurangi resiko terhadap jaringan internal apabila honeypot berhasil disusupi dan diambil alih.

b. Penempatan di belakang *firewall*, penempatan secara tidak langsung, dimana honeypot berada antara sistem *firewall* dan Internet atau di belakang *gateway*. Pada penempatan honeypot ini akan berakibat bertambahnya resiko pada jaringan privat bila honeypot berhasil disusupi dan diambil alih.

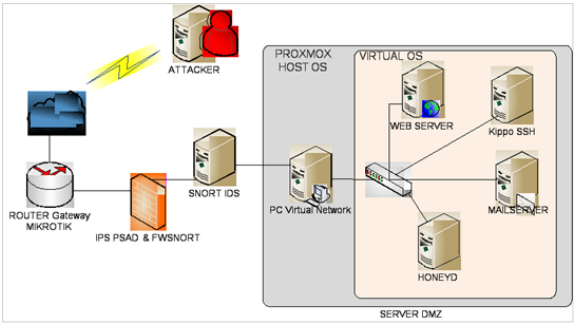
c. Penempatan pada DMZ (*Demiliterized Zone*), karena honeypot berada di belakang *firewall*, maka secara otomatis trafik tidak sah yang biasanya menuju kepada honeypot juga akan melewati *firewall* dan akan tercatat pada *firewall log*. Kekurangan dari lokasi ini adalah sistem lain yang terdapat pada DMZ harus diamankan dari honeypot, karena bila honeypot berhasil disusupi dan diambil alih, maka tidak menutup kemungkinan honeypot tersebut akan digunakan untuk menyerang sistem lain yang terdapat dalam DMZ.

III. Hasil dan Pembahasan

A. Topologi Penelitian

Pada penelitian menggunakan 2 IP publik yang digunakan untuk implementasi beberapa jenis layanan yaitu ssh, *mail server, web server* serta *ftp server* dan akan diujicobakan dengan topologi yang telah penulis rancang. Topologi IPS dan Honeypot pada penelitian ini dirancang supaya memungkinkan penyerangan dapat dilakukan. Pada rancangan topologi penulis menggunakan server DMZ yang pada penelitian ini menggunakan *server virtual* Proxmox.

IPS ini akan dibangun dengan menggunakan tipe NIPS sehingga sistem IPS ini tidak langsung terpasang pada *host*, dalam kasus ini DMZ atau server virtualisasi Proxmox. Pada komputer IPS digunakan 2 *interface* Ethernet untuk mendukung konsep NIPS. *Interface* yang telah dikonfigurasi sebagai *bridge* akan terlihat sebagai 1 *interface*. Hal ini digunakan agar mudah dalam *remote* sistem dan mengurangi penggunaan *routing* pada komputer IPS. Penulis juga menggunakan Snort IDS yang fungsinya *listening* intrusi dan lalu lintas data yang sedang terjadi diantara IPS dan Server DMZ, sebagai pembanding hasil yang terjadi ketika serangan dilakukan pada lingkungan penelitian.



Gambar 2. Topologi Penelitian IPS dan Honeypot

Pada penelitian ini, penulis menggunakan topologi seperti yang telah dijelaskan pada gambar 2. Pengalamatan IP dilakukan terhadap interface pada router dan komputer sesuai dengan tabel 1.

Tabel 1. Rancangan Alamat IP Penelitian IPS dan Honeypot

Hardware dan Aplikasi	Alamat IP
IP Publik Puspindika	124.81.118.213/28, 124.81.118.214/28
Mikrotik	192.168.17.1/24
IPS Fwsnort dan PSAD	192.168.17.85
Snort IDS	192.168.17.67
Server DMZ Proxmox	192.168.17.2
Web Server	192.168.17.20
Mail Server	192.168.17.30
Kippo SSH	192.168.17.56
Honeyd	192.168.17.202

B. *Hardware* dan *SoftwareHardware*

Pada penelitian ini, akan dilakukan uji coba intrusi dengan menggunakan *hardware* sebagai berikut:

a. Router Mikrotik

Mikrotik adalah sebuah router yang menggunakan sistem operasi Linux yaitu Mikrotik RouterOS. Router mikrotik memiliki berbagai macam fitur seperti *bridge*, *port forwarding*, *routing*, dll. Pada penelitian ini menggunakan router sebagai *gateway* dan fungsi *port forwarding* dari ip publik ke alamat ip lokal server yang diujikan.

b. Komputer IPS PSAD dan Fwsnort

Komputer ini dipasang/diinstall dengan *tool* PSAD dan Fwsnort, sehingga fungsi IPS dapat dilakukan oleh komputer ini.

c. Komputer *Server* DMZ atau *Virtual Server*

Komputer ini diinstall dengan Proxmox VE versi 2.3 sehingga dapat mensimulasikan beberapa sistem operasi untuk penelitian. Pada komputer ini juga akan memberikan layanan berupa *mail server* menggunakan Roundcube dan *web server* menggunakan Drupal. Pada server ini juga akan dilakukan instalasi paket honeypot yaitu honeyd dan kippo ssh.

d. Komputer Snort IDS

Komputer ini diinstall dengan Snort IDS dan akan dipantau dengan bantuan *security monitoring* yaitu Snorby.

e. Komputer *Monitoring*

Komputer ini akan melakukan instalasi paket-paket yang dibutuhkan pada penelitian ini dan akan melakukan pemantauan hasil penelitian dengan menggendalikan server dan sistem IPS maupun IDS dari jarak jauh menggunakan *tool* SecureCRT.

f. Komputer *Attacker*

Komputer ini akan melakukan serangan dari luar ip publik ke dalam lingkungan *server* produksi, beberapa *tool* yang akan digunakan pada komputer ini yaitu zenmap untuk melakukan *port scanning* dan metasploit framework untuk melakukan uji intrusi.

Software

Pada penelitian ini, akan dilakukan uji coba intrusi dengan menggunakan *tool*/*software* sebagai berikut:

a. Ubuntu Server

Merupakan salah satu distribusi Linux berbasis Debian, pada penelitian ini menggunakan versi *Server* yang tidak membutuhkan GUI (*Graphical User Interface*). (http://iso.ukdw.ac.id/ubuntu/12.04/ diakses pada 24 April 2013)

b. Proxmox VE 2.3

Proxmox merupakan sistem operasi *server* virtualisasi yang menggunakan distribusi linux Debian dan berbasiskan OpenVZ dan KVM. Untuk mengoperasikannya dapat menggunakan tampilan berupa *Web Interface* ataupun *terminal*. (http://www.proxmox.com/downloads diakses pada tanggal 24 april 2013)

c. PSAD

PSAD adalah *tool* yang memanfaatkan iptables *log messages* untuk mendeteksi, *alert* dan memblokir aktivitas *port scan* serta lalu lintas data yang mencurigakan lainnya. (http://www.cipherdyne.org/psad/download diakses pada tanggal 24 April 2013)

d. Fwsnort

Fwsnort merupakan *tool* untuk menterjemahkan SNORT *rules* ke dalam iptables dan menghasilkan *shell script* yang berguna untuk mengimplementasikan hasil keluaran iptables. (http://www.cipherdyne.org/fwsnort/download diakses pada tanggal 24 April 2013)

e. Snort IDS

Snort adalah *tool open source Intrusion Detection System* yang dikembangkan oleh SourceFire dan dapat digunakan pada berbagai macam *platform* seperti sistem operasi Windows dan Linux. Snort juga merupakan IDS yang berbasis *signature*. (http://www.snort.org/snort-downloads diakses pada tanggal 24 April 2013)

f. Snorby

Snorby adalah aplikasi *open source security monitoring* untuk menampilkan *log* dari kejadian dan *alert* yang terjadi pada Snort IDS. (http://www.snorby.org diakses pada tanggal 24 April 2013)

g. Honeyd

Honeyd adalah honeypot tipe *low interaction* honeypot yang berfungsi melakukan simulasi jaringan secara keseluruhan seperti *service* ftp, ssh, http, router dalam satu mesin/PC dan bisa menambahkan *multiple hops*, *packet losses* dan *latency*. (http://www.honeyd.org/release.php diakses pada tanggal 24 April 2013)

h. Kippo SSH

Kippo SSH adalah honeypot tipe *medium interaction* honeypot yang didesain untuk merekam aktivitas serangan dari *attacker*, seperti *brute force* dan yang paling penting adalah melakukan interaksi pada *attacker* dengan cara meniru *service* ssh. (http://code.google.com/p/kippo/downloads/list diakses pada tanggal 24 April 2013)

i. Roundcube dan iRedmail

Roundcube merupakan *webmail client* yang didesain untuk dapat dijalankan pada *web server* yang menggunakan Apache, Nginx. Roundcube juga mendukung penggunaan *database* seperti MySQL, PostgreSQL. (http://roundcube.net/download diakses pada tanggal 24 April 2013)

j. Drupal

Drupal adalah *open source content management framework* yang menggunakan pemograman PHP, Drupal yang digunakan pada penelitian juga mendukung *database* MySQL. (https://drupal.org/download diakses pada tanggal 24 April 2013)

k. Zenmap

Zenmap merupakan versi GUI dari Nmap. Aplikasi zenmap dapat menggunakan paket IP untuk melihat jaringan, *port* yang terbuka, sistem operasi yang digunakan dan *firewall* yang berjalan dalam suatu sistem. (http://nmap.org/zenmap diakses pada tanggal 24 April 2013)

l. SecureCRT

adalah aplikasi yang digunakan untuk melakukan kendali jarak jauh melalui beberapa macam protokol, diantaranya Raw, Telnet, Rlogin, SSH dan serial.

(http://www.vandyke.com/download/index diakses pada tanggal 24 April 2013)

C. Evaluasi Skema Pengujian

Pengujian penyusupan akan dilakukan melalui berbagai jenis skenario serangan, pembuatan skenario serangan dilakukan untuk menguji sejauh mana kemampuan dari *Intrusion Prevention System* dan Honeypot dalam menghadapi intrusi pada jaringan *server* yang ada. Pengujian menggunakan skenario tersebut bertujuan untuk mengetahui *alert* IPS dan IDS yang telah dipasang dalam *server firewall* dan juga *server* Honeypot. Skenario juga menggunakan 2 IP Publik yaitu 124.81.118.213 yang digunakan untuk *Mail Server* dan 124.81.118.214 yang digunakan untuk *Web Server.* Digunakan 2 IP Publik tersebut mensimulasikan *port* yang umum tetapi tidak dipakai oleh Honeypot. Berikut ini adalah pengujian yang dilakukan dalam penelitian ini:

a. *Port Scan*

Pada pengujian ini akan menggunakan nmap versi GUI yaitu zenmap yang akan diarahkan menuju 2 IP Publik yang digunakan dalam pengujian ini yaitu 124.81.118.213 dan 124.81.118.214. Pengujian ini menggunakan 2 jenis *scan* yaitu *Intense Scan* dan *Slow Comprehensive Scan* agar terlihat perbedaan yang terjadi pada IPS. Penulis juga menggunakan Snort IDS yang menggunakan Snorby untuk dilakukan *monitoring* dan melihat adanya *alert* yang terjadi sesuai dengan *alert* yang tertangkap oleh IPS. Setelah itu digunakan Honeypot jenis Kippo SSH untuk melihat aksi intrusi yang dilakukan oleh *attacker* yang menuju *port* ssh.

- *Intense Scan*

Pada pengujian port scanning jenis Intense Scan, PSAD dapat mendeteksi paket *log* yang yang telah dicocokkan dengan signaturenya setelah melakukan analisa paket *syslog* yang direkam oleh IPTables.

Setelah dilakukan uji coba, pada keterangan PSAD status didapatkan bahwa PSAD telah membuat beberapa email alert serta alamat ip sumber serangan dan alamat ip tujuan serangan. PSAD juga memberikan laporan berupa email alert setelah terjadi Intense Scan. PSAD mampu mendefinisikan serangan yang telah dilakukan nmap dan memberikan informasi berupa TCP flags. Honeypot yang digunakan oleh penulis yaitu Kippo SSH juga menunjukkan *log* aktivitas yang dilakukan oleh IP *attacker*, berupa percobaan dengan *scan port* ssh.

```
2013-05-20 19:44:14+0700 [kippo.core.honeypot.HoneyPotSSHFactory]
New connection: 114.79.28.93:49823 (192.168.17.56:22) [session:
251]

2013-05-20 19:44:15+0700 [HoneyPotTransport,251,114.79.28.93]
connection lost

2013-05-20 19:44:16+0700 [kippo.core.honeypot.HoneyPotSSHFactory]
New connection: 114.79.28.93:49871 (192.168.17.56:22) [session:
252]

2013-05-20 19:44:17+0700 [HoneyPotTransport,252,114.79.28.93]
Remote SSH version: SSH-2.0-Nmap-SSH2-Enum-Algos

2013-05-20 19:44:17+0700 [HoneyPotTransport,252,114.79.28.93] kex
alg, key alg: diffie-hellman-group1-sha1 ssh-rsa

2013-05-20 19:44:17+0700 [HoneyPotTransport,252,114.79.28.93]
outgoing: aes128-cbc hmac-md5 none

2013-05-20 19:44:17+0700 [HoneyPotTransport,252,114.79.28.93]
incoming: aes128-cbc hmac-md5 none

2013-05-20 19:44:17+0700 [HoneyPotTransport,252,114.79.28.93]
connection lost

2013-05-20 19:44:20+0700 [kippo.core.honeypot.HoneyPotSSHFactory]
New connection: 114.79.28.93:50008 (192.168.17.56:22) [session:
253]
```

Gambar 3. Data Log pada Kippo SSH

- *Slow Comprehensive Scan*

Pada pengujian *Slow Comprehensive scan* email alert pada PSAD hanya membaca beberapa paket TCP SYN dan belum membuat triger pada Fwsnort supaya melakukan pemblokiran paket menggunakan IPTables.

Percobaan *Intense* dan *Slow Comprehensive scan* juga memberikan *alert* pada Snort IDS yang ditampilkan melalui Snorby. Pada percobaan ini membuktikan bahwa ketiga sistem yang dipakai penulis yaitu IPS, IDS dan Honeypot mampu memberikan alert dengan baik.

b. Metasploit *Framework*

Skenario ini digunakan untuk menguji kemampuan *Intrusion Prevention System* dalam menghadapi penyusupan yang digunakan oleh *attacker* terhadap *port-port* yang ada. Metasploit *Framework* akan melakukan *scan port* melalui IP Publik 124.81.118.214 yang digunakan untuk *Web Server,* terhadap *port* yang terbuka setelah dilakukan scanning oleh zenmap, yaitu ftp port 21, smtp port 25 dan telnet port 23. Pada Skenario ini akan menguji IPS PSAD dan Fwsnort apakah bekerja dengan baik. Snort IDS juga digunakan dalam penelitian ini untuk memantau terjadinya intrusi dan menghasilkan *alert*. Penulis merancang Honeypot dengan menggunakan honeyd agar melakukan simulasi ftp *port* 21, smtp *port* 25 dan telnet *port* 23. Kemudian akan menggunakan 3 jenis *scan* dengan *payload* berbeda, yang ada pada Metasploit Framework untuk melakukan serangan terhadap *port-port* yang telah disimulasikan dengan honeypot.

Setelah dilakukan proses *scanning* menggunakan Metasploit maka didapatkan bahwa IPS PSAD mendeteksi ketiga serangan tersebut, karena masih dalam batas wajar maka tidak dilakukan pemblokiran alamat ip penyerang oleh PSAD. Pada Snort IDS tidak

menunjukkan adanya aktivitas intrusi, tetapi pada log Honeyd menunjukkan adanya usaha port scanning dari ip *attacker* menuju port 23 yang telah disimulasikan menggunakan honeyd. Begitu juga setelah dilakukan scanning menuju port 25, hasil *log* yang ditunjukkan pada honeyd terdapat aksi *scanning* menggunakan data tcp.

Uji intrusi *port scanning* yang menggunakan payload ftp_login terhadap *port* ftp milik IP publik 124.81.118.214 setelah dilakukan port forwarding menuju alamat ip lokal yang disimulasikan honeyd yaitu 192.168.17.202. Pada status PSAD tidak memberikan *email alert,* hanya saja memberikan informasi bahwa telah terjadi aksi intrusi pada port 21 sampai port 25 yang ditujukan pada alamat ip yang dimulasikan oleh honeyd yaitu 192.168.17.202.

```
SRC:  222.124.22.30, DL: 1, Dsts: 1, Pkts: 7, Total protocols: 1,
Unique sigs: 0, Email alerts: 0

    DST: 192.168.17.202, Local IP

      Scanned ports: TCP 21-25, Pkts: 7, Chain: FORWARD, Intf: br0

      Total scanned IP protocols: 1, Chain: FORWARD, Intf: br0

    Total scan sources: 2

    Total scan destinations: 2
```

Gambar 4. PSAD Status saat uji intrusi Metasploit Framework

Pada Snort IDS tidak mendeteksi adanya aksi intrusi terhadap *port* 23, dan *port* 25 seperti yang dihasilkan saat pengujian port scanning menggunakan nmap. Honeypot yang digunakan pada pengujian ini yaitu honeyd, menghasilkan *log* aksi intrusi terhadap *port* 21.

c. DoS (*Denial of Service*)

Serangan *Denial of Service* pada penelitian ini menggunakan slowloris.pl yang menggunakan bahasa pemograman perl dan menggunakan ping data tcp. Pada percobaan ini *host* akan diserang adalah ip publik 124.81.118.214 yang digunakan untuk *Webserver* Drupal serta menggunakan layanan port 80 yang berada pada *server* DMZ. Serangan berasal dari luar jaringan yang diarahkan menuju IP Publik. Pada penelitian ini akan menggunakan PSAD dan Fwsnort untuk memantau terjadinya intrusi *DoS*, serta Snort IDS digunakan untuk *monitoring* hasil intrusi dalam bentuk *alert*. Honeypot juga digunakan untuk mendeteksi terjadi intrusi berupa *Denial of Service*.

Pada pengujian menggunakan Slowloris.pl, paket data yang masuk ke lingkungan server DMZ tidak terlalu besar dan juga tidak terlalu menghalangi *service* yang ada seperti Web Server dan Mail Server. Bandwidth yang digunakan juga tidak besar hanya 512Kbps, maka tidak terlalu membebani server DMZ dalam memberikan layanan keluar, hanya saja dapat membuat lambat akses Web Server dari luar IP Publik sementara waktu.

Pada saat dilakukan pengujian slowloris, PSAD tidak memberikan reaksi *email alert*, serta Snorby tidak memperlihatkan adanya intrusi. Honeypot juga tidak memberikan reaksi karena serangan slowloris hanya terhadap port 80 yang sedang memberikan *service web* http Drupal. Pada pengujian menggunakan ping juga tidak terjadi hal yang signifikan pada PSAD karena ping hanya membuat sibuk jaringan pada *level* router dan tidak sampai masuk ke lingkungan IPS maupun *server* DMZ, tetapi dapat membuat akses layanan Web Server menjadi lambat.

d. SQL Injection

Penulis menggunakan *tool sql injection* Havij Advanced 1.15 pada sistem operasi Windows. Dalam penelitian ini serangan ditujukan pada *webserver* Drupal yang menggunakan *sql server* yaitu MySQL, dan kemudian akan dilakukan serangan menuju IP publik, untuk mengetahui apakah *tool* dan IP penyerang dapat terdeteksi dan dicegah untuk masuk ke dalam *webserver* yang menggunakan ip publik 124.81.118.214. Penulis menggunakan IPS PSAD dan Fwsnort pada pengujian ini untuk mengenali intrusi tersebut dan memblokir ip yang digunakan untuk melakukan intrusi. Digunakan juga Snort IDS yang memantau hasil *log* berupa *alert* saat terjadi intrusi.

Setelah dilakukan pengujian *Sql Injection*, PSAD tidak mendeteksi adanya serangan dan tidak ada *email alert* yang masuk ke dalam log PSAD. Snort IDS dapat mendeteksi dengan baik serangan yang terjadi dengan memberikan alert dan nomor rules. Kemudian penulis mencoba untuk memasukkan nomor rules tersebut pada fungsi IPS Fwsnort, untuk menguji apakah Fwsnort dapat memblokir alamat ip yang melakukan aktivitas SQL Injection dengan tool Havij. Setelah itu dijalankan untuk *update rules* tersebut ke dalam IPTables supaya paket tcp dari dari penyerangan yang menggunakan tool Havij SQL Injection dapat dibuang oleh IPTables.

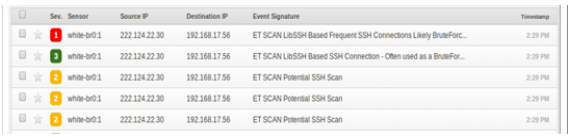
Pengujian telah dilakukan dan paket data yang menggunakan tool Havij masih tetap bisa melewati IPS PSAD tanpa terblokir dan tetap terdeteksi oleh Snort IDS dengan alert yang sama. Pengujian ini tidak terdeteksi pada honeypot sebab honeypot dikonfigurasikan tidak untuk menghadapi serangan ini.

e. Brute Force *Attack*

Serangan ini dilakukan untuk menyerang *port* ssh standar yang terbuka yaitu port 22, memakai *tool* yang sudah ada pada sistem operasi Backtrack R3 yaitu hydra, dan nantinya akan menggunakan *password dictionary* dengan beberapa contoh *username* dan *password* yang telah dibuat penulis. Pada serangan

ini penulis menggunakan *Intrusion Prevention System* yaitu PSAD dan Fwsnort untuk melakukan tugasnya, dan digunakan Honeypot dengan Kippo SSH yang mensimulasikan *port* 22. Dalam implementasinya *port* ssh disimulasikan pada kedua ip publik yang digunakan pada pengujian ini, tetapi dengan melakukan serangan pada salah satu ip publik saja sudah mewakili hasil yang akan dicapai pada pengujian ini.

Pada pengujian Brute Force ini, PSAD tidak menghasilkan *email alert* seperti pada pengujian sebelumnya, tetapi Snort IDS berhasil mendeteksi dan memberikan beberapa *alert*.



Gambar 5. Alert Brute Force pada Snorby

Pada Snort IDS yang menggunakan *tool monitoring* Snorby juga menunjukkan beberapa *alert* yang telah dicocokan dengan *signature* snort dan didalamnya terdapat beberapa *rules*.

Penulis mencoba untuk memasukkan *rules* snort kedalam IPTables dengan bantuan Fwsnort, tetapi snort *rules* untuk Brute Force tidak dapat diterjemahkan dengan baik ke dalam IPTables. Honeypot dengan Kippo SSH yang digunakan pada pengujian serangan Brute Force ini dapat mendeteksi dengan baik dan mencatatkan *log* pada saat Brute Force dilakukan oleh Hydra.

Honeypot dengan *tool* Kippo SSH juga dapat digunakan untuk merekam aktivitas *attacker* yang berhasil masuk ke dalam sistem. Perintah-perintah yang diketikkan akan direkam dengan jelas, serta file yang di*download* ke dalam *server* dapat ditemukan pada direktori *log* kippo yang terletak pada /home/kippo/dl.

IV. Kesimpulan

Dari hasil penelitian yang diuraikan pada bab 4, diperoleh kesimpulan sebagai berikut:

1. Dari hasil penelitian kombinasi IPS dan Honeypot ini memberikan peringatan terjadinya intrusi,walaupun aksi intrusi ke dalam sistem belum optimal untuk dihalangi oleh IPS, tetapi hasil *log* yang diberikan keduanya dapat saling melengkapi dalam memberikan informasi kepada administrator untuk ditindak lanjuti.
2. Dari beberapa jenis serangan yang diuji coba, IPS tidak memberikan *alert* pada beberapa jenis serangan tetapi pada honeyd dapat difungsikan sebagai alat untuk mengecoh *attacker* sebagai target yang diserang dan menghasilkan data *log* yang dapat digunakan administrator untuk di analisa.
3. Setelah diimplementasikan honeypot kippo ssh pada penelitian ini, IPS tidak memberikan alert yang berarti, tetapi kippo berhasil mengecoh *attacker* dan menghasilkan log serta merekam aktivitas *attacker* yang dapat berguna bagi administrator.
4. Pada penelitian ini juga digunakan Snort IDS yang berhasil memberikan alert yang lebih baik dibandingkan yang dihasilkan oleh komputer IPS saat dilakukan beberapa kali teknik intrusi.
5. Honeypot yang digunakan pada penelitian ini adalah jenis low interaction dan digunakan pada server produksi, sehingga log yang dihasilkan sedikit, tetapi tetap mempunyai nilai yang lebih bermanfaat bagi administrator.

Daftar Pustaka

[1] Alder, R., Babbin, J., Beale, J., Doxtater, A., Foster, J., Kohlenberg, T., Rash, M. (2004). *Snort 2.1 Intrusion Detection, Second Edition*. Rockland, MA: Sysngress Publishing, Inc.

[2] Hoopes, J. (2009). *Virtualization for Security*: *Including Sandboxing, Disaster Recovery, High Availability, Forensic Analysis, and Honeypotting.* Burlington, MA: Sysngress Publishing, Inc

[3] Joshi, R.C., Sardana, A. (2011). *Honeypots a New Paradigm to Information Security*. Enfield, New Hampshire:Science Publishers.

[4] Provos,N., Holz,T. (2007). *Virtual Honeypots: From Botnet Tracking to Intrusion Detection.* Massachusetts : Addison Wesley.

[5] Singh, R.K., Ramanujam, T. (2009). *Intrusion Detection System Using Advanced Honeypot*. International Journal of Computer Science and Information Security.Volume 2-No 1.

[6] Stiawan, D., Abdullah, Abdul H., Idris, Mohd.Y. (2011). *Characterizing Network Intrusion Prevention System*. International Journal of Computer Applications.Volume 14-No1.

[7] Trost, R. (2010). *Practical Intrusion Analysis: Prevention and Detection for Twenty-First Century*. Boston, MA: Addison-Wesley.