DESAIN DAN IMPLEMENTASI HONEYPOT DENGAN FWSNORT DAN PSAD SEBAGAI INTRUSION PREVENTION SYSTEM

Skripsi

oleh
BOSMAN JULIANTO TAMBUNAN
22074366

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2013

DESAIN DAN IMPLEMENTASI HONEYPOT DENGAN FWSNORT DAN PSAD SEBAGAI INTRUSION PREVENTION SYSTEM

Skripsi

Diajukan kepada Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana
Sebagai Salah Satu Syarat dalam Memperoleh Gelar
Sarjana Komputer

Disusun oleh

BOSMAN JULIANTO TAMBUNAN
22074366

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2013

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

DESAIN DAN IMPLEMENTASI HONEYPOT DENGAN FWSNORT DAN PSAD SEBAGAI INTRUSION PREVENTION SYSTEM

yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan Sarjana Program Studi Teknik Informatika Fakultas Teknologi Informasi Universitas Kristen Duta Wacana, bukan merupakan tiruan atau duplikasi dari skripsi kesarjanaan di lingkungan Universitas Kristen Duta Wacana maupun di Perguruan Tinggi atau instansi manapun, kecuali bagian yang sumber informasinya dicantumkan sebagaimana mestinya.

Jika dikemudian hari didapati bahwa hasil skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia dikenai sanksi yakni pencabutan gelar kesarjanaan saya.

Yogyakarta, 29 Mei 2013

BOSMAN JULIANTO TAMBUNAN
22074366

HALAMAN PERSETUJUAN

Judul Skripsi	:	DESAIN DAN IMPLEMENTASI HONEYPOT DENGAN FWSNORT DAN PSAD SEBAGAI INTRUSION PREVENTION SYSTEM
Nama Mahasiswa	:	BOSMAN JULIANTO TAMBUNAN
N I M	:	22074366
Matakuliah	:	Skripsi (Tugas Akhir)
Kode	:	TIW276
Semester	:	Genap
Tahun Akademik	:	2012/2013

Telah diperiksa dan disetujui di
Yogyakarta,
Pada tanggal 15 Mei 2013

Dosen Pembimbing I	Dosen Pembimbing II
Willy Sudiarto Raharjo, SKom.,M.Cs	Joko Purwadi, M.Kom

HALAMAN PENGESAHAN

DESAIN DAN IMPLEMENTASI HONEYPOT DENGAN FWSNORT DAN PSAD SEBAGAI INTRUSION PREVENTION SYSTEM

Oleh: BOSMAN JULIANTO TAMBUNAN / 22074366

Dipertahankan di depan Dewan Penguji Skripsi
Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana - Yogyakarta
Dan dinyatakan diterima untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Komputer
pada tanggal 24 Mei 2013

Yogyakarta, 29 Mei 2013
Mengesahkan,

Dewan Penguji:

1. Willy Sudiarto Raharjo, SKom.,M.Cs
2. Joko Purwadi, M.Kom
3. Haryo Susanto, S.Si.
4. Yuan Lukito, S.Kom

Dekan

(Drs. Wimmie Handiwidjojo, MIT.)

Ketua Program Studi

(Nugroho Agus Haryono, M.Si)

UCAPAN TERIMA KASIH

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa yang telah melimpahkan rahmat dan anugerah, sehingga penulis dapat menyelesaikan Tugas Akhir dengan judul "Desain dan Implementasi Honeypot dengan Fwsnort dan Psad sebagai Intrusion Prevention System" dengan baik dalam semester ini.

Penulisan laporan Tugas Akhir ini merupakan kelengkapan dan pemenuhan dari salah satu syarat dalam memperoleh gelar Sarjana Komputer. Selain itu bertujuan melatih mahasiswa untuk dapat menghasilkan suatu karya yang dapat dipertanggungjawabkan secara ilmiah, sehingga dapat bermanfaat bagi penggunanya.

Dalam menyelesaikan pembuatan program dan laporan Tugas Akhir ini, penulis telah banyak menerima bimbingan, saran dan masukan dari berbagai pihak, baik secara langsung maupun secara tidak langsung. Untuk itu dengan segala kerendahan hati, pada kesempatan ini penulis menyampaikan ucapan terima kasih kepada:

1. Bapak **Willy Sudiarto Raharjo, S. Kom, M. Cs.** selaku dosen pembimbing I yang telah memberikan ide, masukan kritik dan saran dalam penulisan laporan dan pembuatan Tugas Akhir ini, juga kepada
2. Bapak **Joko Purwadi, M.Kom** selaku dosen pembimbing II atas bimbingan, petunjuk dan masukan yang diberikan selama pengerjaan Tugas Akhir ini sejak awal hingga akhir.
3. **PPUKDW dan PUSPINDIKA UNIVERSITAS KRISTEN DUTA WACANA** yang mengijinkan penulis untuk melakukan implementasi di lab, peminjaman peralatan dan IP publik yang tidak ternilai harganya, sehingga penulis mendapatkan banyak pengalaman baru saat mengerjakan Tugas akhir ini.

4. Keluarga tercinta, Papa dan Mama, Pondang Tambunan dan Dahlia Siagian, Adikku Christian Fredy Halomoan Tambunan dan Abangku Tumpal Alexandre Tambunan yang dengan segala dukungan doa dan semangat kepada penulis, sehingga penulis mampu mengerjakan Tugas Akhir ini.

5. Wini Sesaria Riwu atas segala dukungan, kasih sayang dan doa yang menjadi semangat tersendiri bagi penulis untuk menyelesaikan Tugas Akhir.

6. Orang-orang terdekat, teman seangkatan dan Keluarga PPTPM yang telah memberikan dukungan dan semangat.

7. Teman-teman yang telah memberikan masukan dan semangat, yang juga menemani mengerjakan Tugas Akhir ini.

8. Pihak lain yang tidak dapat penulis sebutkan satu per satu, sehingga Tugas Akhir ini dapat terselesaikan dengan baik.

Penulis menyadari bahwa laporan Tugas Akhir ini masih jauh dari sempurna. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun dari pembaca sekalian. Sehingga suatu saat penulis dapat memberikan karya yang lebih baik lagi.

Akhir kata penulis ingin meminta maaf bila ada kesalahan baik dalam penyusunan laporan maupun yang pernah penulis lakukan sewaktu melakukan penelitian ini. Sekali lagi penulis mohon maaf sebesar-besarnya. Dan semoga ini dapat berguna bagi kita semua.

Yogyakarta, 16 Mei 2013

Penulis

INTISARI

DESAIN DAN IMPLEMENTASI HONEYPOT DENGAN FWSNORT DAN PSAD SEBAGAI INTRUSION PREVENTION SYSTEM

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

Honeypot yang dipadu dengan IPS yang menggunakan PSAD dan Fwsnort memberikan solusi untuk masalah tersebut, Psad dan Fwsnort berfungsi sebagai sistem yang bekerja untuk memantau aktifitas jaringan dan bekerja bersama untuk memantau *log* data yang melalui IPS pada mode *inline* tersebut dan memblokir alamat ip yang mencurigakan setelah data *stream* dicocokan dengan *signature* yang ada, sedangkan Honeypot bekerja untuk mengetahui aktifitas penyerang, apakah merupakan *false positive* atau *false negative* dan semua aktifitas yang menuju pada honeypot dianggap mencurigakan.

Hasil penelitian menunjukkan bahwa kemampuan Honeypot yang dipadu dengan IPS PSAD dan Fwsnort dapat memudahkan dan saling melengkapi dalam mendeteksi serangan yang tidak diketahui oleh sistem IPS. Sistem *alert* yang dihasilkan oleh perpaduan sistem ini cukup baik untuk meminimalkan *false alarm* yang dimunculkan oleh IPS PSAD dan Fwsnort. Sistem ini juga menghasilkan *log* data yang dapat digunakan oleh administrator dalam menanggulangi serangan yang terjadi.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

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, tetap saja ada 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. Honeypot dapat berfungsi sebagai umpan dalam jaringan komputer untuk mengelabui *attacker* dan juga dapat 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 aktifitas dimana penyusupan dilakukan secara tegas.

Sistem pendeteksian *Intrusion Detection System* (IDS) memegang peranan penting dalam pengamanan jaringan. PSAD atau *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). Dimana kombinasi *Intrusion Prevention System* ini juga akan dikombinasikan dengan kemampuan honeypot untuk melakukan pencegahan maupun melihat aktifitas *attacker*.

Dalam hal ini penulis akan 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.

1.2 Perumusan Masalah

Dalam penelitian ini, rumusan masalah yang akan dibahas oleh penulis yakni bagaimana membangun *Intrusion Prevention System* menggunakan PSAD dan Fwsnort untuk mencatat *log* serta memblokir paket data yang berbahaya, dan juga menggunakan Honeypot untuk mencatat *log* serangan yang tidak terdeteksi oleh *Intrusion Prevention System*.

1.3 Batasan Masalah

Pada penelitian ini, batasan masalah yang digunakan dalam pembangunan sistem adalah sebagai berikut :

a. Penelitian disimulasikan menggunakan IP Publik milik PUSPINDIKA serta serangan yang akan dideteksi adalah serangan yang berasal dari luar jaringan *server* DMZ

b. Fitur Honeypot yang digunakan disesuaikan dengan *service* yang umum dilakukan penyerangan menggunakan Honeyd dan Kippo SSH.

c. Performa *hardware server* tidak akan dibahas dalam penelitian ini.

d. Pada penulisan ini tidak membahas tentang *rules* Fwsnort dan juga tentang konfigurasi *server* DMZ.

e. Pada penulisan ini tidak membahas tentang *source code* dan *tool* yang akan digunakan untuk ujicoba serangan pada sistem.

f. Jenis *Intrusion Prevention System* yang akan digunakan yaitu *Network-based Intrusion Prevention System* yang telah dimodifikasi menjadi Fwsnort dan akan dikombinasikan dengan Psad.

g. Peran IPS lebih sebagai sistem verifikasi paket berdasar *ruleset* IPS. Untuk selanjutnya diputuskan paket yang baik akan diteruskan ke jaringan dan *bad packet* ataupun serangan akan dilakukan pemblokiran.

h. Pada penelitian ini tidak semua *service* menggunakan Honeypot.

i. Intrusi pada jaringan terbatas pada *Port Scanning*, *Metasploit Framework*, *Denial of Service*, *SQL Injection* dan *Brute Force Attack*.

1.4 Hipotesis

Intrusion Prevention System (IPS) menggunakan Fwsnort serta Psad dapat dikombinasikan dengan Honeypot untuk melakukan analisa serangan dengan teknik yang tidak diketahui oleh IPS dan dapat membantu *administrator* dalam memantau serta menanggulangi kerusakan yang disebabkan oleh penyusup sehingga serangan tidak dapat dilakukan kembali.

1.5 Tujuan Penelitian

Berdasarkan latar belakang dan permasalahan di atas, tujuan dari penelitian ini adalah untuk membangun *Intrusion Prevention System* yang bekerja untuk mencegah aktifitas intrusi terhadap *server* dengan cara membaca *log* dan memblokir alamat IP penyerang dengan menggunakan PSAD dan

Fwsnort, kemudian menentukan apakah aktifitas tersebut merupakan serangan terhadap server, jika serangan terjadi dan tidak diketahui *signature*-nya oleh IPS maka Honeypot yang akan melakukan tugasnya sesuai layanan yang diberikan dan memberikan rekomendasi berupa data *log* untuk ditindak lanjuti oleh *administrator*.

1.6 Metode Penelitian

Metode penelitian yang akan dilakukan dalam penelitian adalah sebagai berikut:

a. Studi Pustaka

   Metode studi pustaka dilakukan dengan membaca dan memahami referensi literatur yang mendukung dalam penelitian ini, *Intrusion Detection* dan *Prevention System* serta Honeypot.

b. Perancangan dan Implementasi

   Pada tahap ini akan dilakukan perbandingan secara teori berdasarkan sumber yang telah didapat dari studi pustaka untuk menentukan rancangan arsitektur jaringan. Selanjutnya dilakukan implementasi perangkat keras pendukung dan konfigurasi perangkat lunak Honeypot dan *Intrusion Prevention System* (IPS) Fwsnort dan Psad.

c. Pengambilan sampel data

   Metode ini dilakukan dengan cara melakukan uji coba intrusi pada IP publik PUSPINDIKA.

d. Evaluasi kinerja Honeypot dan *Intrusion Prevention System*

   Metode evaluasi akan dilakukan dengan menganalisa hasil dari uji coba intrusi yang telah dilakukan dengan menganalisa data yang didapatkan dari topologi yang telah diimplementasikan.

e. Penarikan kesimpulan

Penarikan kesimpulan akan dilakukan setelah implementasi uji coba dan analisis dilakukan.

1.7 Sistematika Penulisan

Bab I PENDAHULUAN, membahas tentang latar belakang masalah dari penelitian, rumusan masalah, batasan-batasan masalah, metode penelitian, hipotesis, tujuan serta sistematika penulisan dari penelitian ini.

Bab II TINJAUAN PUSTAKA DAN LANDASAN TEORI, berisi bahasan penelitian dan berbagai referensi mengenai penelitian Honeypot, Fwsnort dan PSAD serta landasan teori yang menjadi dasar dari penelitian ini. Pada bab ini akan diterangkan secara detail sesuai informasi serta studi pustaka yang diperoleh peneliti berkaitan dengan analisis keamanan jaringan.

Bab III ANALISIS DAN PERANCANGAN PENELITIAN, berisi rancangan dari Honeypot dan IPS yang menggunakan Fwsnort dan PSAD. Alur kerja sistem, serta kebutuhan akan *hardware* maupun *software* untuk mendukung penelitian, serta langkah-langkah penelitian yang akan dilakukan.

Bab IV IMPLEMENTASI SISTEM DAN ANALISIS SISTEM, berisi uraian detail implementasi sistem serta uraian mengenai hasil analisis yang didapatkan dari hasil ujicoba disetiap tahapan penelitian.

Bab V KESIMPULAN DAN SARAN, berisi kesimpulan dari hasil penelitian serta saran-saran berkaitan dengan implementasi Honeypot, Fwsnort dan Psad.

BAB V

KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan hasil desain, implementasi dan analisis sistem, maka diperoleh kesimpulan sebagai berikut:

a. Penelitian ini mengimplementasikan kombinasi keamanan jaringan yang terdiri dari *Intrusion Prevention System* dan Honeypot yang dijalankan secara virtual dalam lingkungan server produksi. 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.

b. Honeypot honeyd yang merupakan *low interaction* honeypot pada penelitian ini honeyd dapat difungsikan penuh atas pengujian, 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.

c. Setelah diimplementasikan honeypot kippo ssh pada penelitian ini, IPS tidak memberikan alert yang berarti, tetapi kippo berhasil mengecoh *attacker* dan menghasilkan log serta merekam aktifitas *attacker* yang dapat berguna bagi administrator.

d. 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.

e. 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.

5.2. Saran

a. Pengembangan selanjutnya dapat hasil log dari honeyd untuk diterjemahkan menjadi rule snort baru, sehingga administrator dapat membangun IPS sesuai dengan kondisi keamanan yang telah terjadi dan dapat mengantisipasi serangan berikutnya.

b. Snort IDS dapat ditambahkan dalam lingkungan jaringan IPS sehingga memberikan peringatan telah intrusi lebih lengkap.

c. Terdapat banyak jenis honeypot, serta tool IDS/IPS yang dapat digunakan dan dapat disesuaikan dengan kebutuhan administrator.

DAFTAR PUSTAKA

Alder, Raven. Babbin, Jacob. Beale, Jay. Doxtater, Adam. Foster, James. Kohlenberg, Toby. Rash, Michael. Snort 2.1 Intrusion Detection, Second Edition. Rockland, MA: Sysngress Publishing, Inc. 2004

Benekdiktus Mena, Yohanes. *Sistem Keamanan Jaringan Menggunakan Intrusion Prevention System*. Diakses pada 26 Januari 2012 dari <http://sinta.ukdw.ac.id/sinta/ resources/sintasrv/nim/22043646>

Fuertes, W., Zambrano, P., Sanchez, M., Gamboa, P. Alternative Engine to Detect and Block Port Scan Attacks using Virtual Network Environments. International Journal of Computer Science and Network Security. Volume 11-No 11. November 2011

Hoopes, John. Virtualization for Security: *Including Sandboxing, Disaster Recovery, High Availability, Forensic Analysis, and Honeypotting.* Burlington, MA: Sysngress Publishing, Inc. 2009

Joshi, R.C., Sardana, A. Honeypots a New Paradigm to Information Security. Enfield, New Hampshire:Science Publishers. 2011

Kristianto, Yohan. Intrusion *Prevention System Berbasis Snort dan IPTables*. Diakses pada 26 Januari 2012 dari <http://sinta.ukdw.ac.id/sinta/resources/sintasrv/nim/22064104>

Provos,N., dan Holz,T. *Virtual Honeypots: From Botnet Tracking to Intrusion Detection.* Massachusetts : Addison Wesley. 2007

Ramirez, Gilbert. Caswell, Brian. Rathaus, Noam. Beale, Jay. Nessus, Snort & Ethereal Power Tools: *Customizing Open Source Security Application.* Rockland, MA: Sysngress Publishing, Inc.. 2005

Rash, M., Orebaugh, A., Clark, G., Pinkard, B., Babbin, J. *Intrusion Prevention and Active Response: Deploying Network and Host IPS.* Rockland: Syngress Publishing, Inc. 2005

Rash, Michael. *Linux Firewalls: Attack Detection and Response with Iptables, Psad, and Fwsnort.* San Francisco: No Starch Press. 2007

Singh, Ram Kumar. Ramanujam, T. Intrusion Detection System Using Advanced Honeypot, International Journal of Computer Science and Information Security.Volume 2-No 1. 2009

Spivey, Mark D. Practical Hacking Techniques and Countermeasure. Broken Sound Parkway NW: Autbach Publications. 2007

Stiawan, D., Abdullah, Abdul H., Idris, Mohd.Y. Characterizing Network Intrusion Prevention System. International Journal of Computer Applications.Volume 14-No1.Januari 2011

Trost, Ryan. Practical Intrusion Analysis: *Prevention and Detection for Twenty-First Century*. Boston, MA: Addison-Wesley,2010 Pearson Education, Inc.