INTRUSION PREVENTION SYSTEM BERBASIS SNORT DAN IPTABLES

Tugas Akhir

Oleh:

Yohan Kristianto

22064104

Program Studi Teknik Informatika Fakultas Teknologi Informasi

Universitas Kristen Duta Wacana

2011

INTRUSION PREVENTION SYSTEM BERBASIS SNORT DAN IPTABLES

Tugas Akhir

Diajukan kepada Fakultas Teknologi Informasi Program Studi Teknik Informatika
Universitas Kristen Duta Wacana-Yogyakarta
Sebagai salah satu syarat dalam memperoleh gelar
Sarjana Komputer

Disusun oleh:
Yohan Kristianto
22064104

Program Studi Teknik Informatika
Universitas Kristen Duta Wacana
2011

PERNYATAAN KEASLIAN TUGAS AKHIR

Saya menyatakan dengan sesungguhnya bahwa tugas akhir dengan judul :

Intrusion Prevention System Berbasis Snort dan IPtables

Yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan sarjana Program 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, 17 Desember 2010

(Yohan Kristianto)

22064104

HALAMAN PERSETUJUAN

Judul	:	Intrusion Prevention System Berbasis Snort dan IPTables
Nama	:	Yohan Kristianto
NIM	:	22064104
Mata Kuliah	:	Tugas Akhir
Kode	:	TI2126
`Semester``	:	Genap
Tahun Akademik	:	2010/2011

Telah Diperiksa dan disetujui
Di Yogyakarta,
Pada Tanggal..17..Desember 2010

Dosen Pembimbing I	Dosen Pembimbing II
(Willy Sudiarto Raharjo, S.Kom, M.Cs.)	(Ir. Gani Indriyanta, M.T.)

HALAMAN PENGESAHAN

SKRIPSI

Intrusion Prevention System Berbasis Snort dan IPTables

Oleh : Yohan Kristianto / 22064104

Dipertahankan di depan dewan Penguji Tugas Akhir/Skripsi
Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana – Yogyakarta
Syarat memperoleh gelar
Sarjana Komputer
Pada Tanggal
10 - 1 - 2011

Yogyakarta, 12 - 1 - 2011
Mengesahkan,

Dewan Penguji :

1. Willy Sudiarto Raharjo, S.Kom, M.Cs.
2. Ir. Gani Indriyanta, M.T.
3. Antonius Rachmat, S.Kom, M.Cs.
4. Yuan Lukito, S.Kom

Dekan,

(**Drs. Wimmie Handiwidjojo, MIT**)

Ketua Program Studi,

(**Nugroho Agus. H, S.Si, M.Si.**)

UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa yang telah melimpahkan segala berkat, rahmat dan bimbingan, dan perlindungan-Nya, sehingga penulis dapat menyelesaikan Tugas akhir dengan judul ”Intrusion Prevention System Berbasis Snort dan IPTables” dengan baik dalam semester ini.

Penulisan laporan Tugas Akhir ini merupakan kelengkapan dan pemenuhan dari salah satu syarat untuk 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 analisis penelitian 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 pembimbing 1, yang telah banyak memberikan ide, masukan, kritik dan saran dalam penulisan laporan dan pembuatan program Tugas Akhir ini.
2. Bapak **Ir. Gani Indriyanta., M.T.,** selaku pembimbing 2, yang telah banyak memberikan masukan dan saran selama penulisan laporan Tugas Akhir ini.
3. **PPUKDW UNIVERSITAS KRISTEN DUTA WACANA** yang mengijinkan penulis untuk melakukan implementasi di lab dan peminjaman peralatan yang tidak ternilai harganya sehingga penulis mendapatkan banyak pengalaman baru yang luar biasa.
4. Keluarga tercinta Papa dan Mama, Ko Hendri dan Ko Iwan untuk segala kasih sayang, kesabaran, perhatian serta dukungan doa yang luar biasa yang selalu menjadi motivasi dan semangat penulis sehingga penulis selalu bersemangat dalam menyelesaikan Tugas Akhir ini.

5. Sahabatku Indra, Dimas santoen, Yohan gempil, Widi, Dida, Leo, Ika, Phael, Jenggot, Tyo, Tipi, Gemma, Vita, Anggit, Eko Ahonk, Mas Kris dan Ivan untuk segala bantuan dan kerjasamanya yang terjalin selama ini.
6. Wassy, Abert, Nathan, dan Candra yang telah membagi pengetahuan yang banyak bagi penulis.
7. Rekan-rekan dan pihak-pihak yang tidak dapat penulis sebutkan satu persatu yang secara langsung maupun tidak langsung yang telah mendukung penyelesaian Tugas Akhir ini. Terimakasih atas dukungan dan doanya.

Penulis menyadari bahwa program dan 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 membuat program Tugas Akhir ini. Sekali lagi penulis mohon maaf yang sebesar-besarnya. Dan semoga ini dapat berguna bagi kita semua.

Yogyakarta, Desember 2010

Penulis

INTISARI

Intrusion Prevention System Berbasis Snort dan IPTables

Pesatnya pertumbuhan jaringan internet, membantu manusia untuk berkomunikasi dan bertukar data. Di satu sisi komunikasi dan pertukaran data menjadi lebih mudah, tetapi di sisi lain timbul masalah yang sangat serius, yakni penyerangan terhadap sistem jaringan. Banyak kasus penyerangan jaringan terjadi karena banyak orang yang belum menyadari pentingnya keamanan jaringan untuk diterapkan ke dalam sistem, sehingga menyebabkan sistem mudah untuk disusupi.

Untuk menanggulanginya, IDS Snort dapat digabungkan dengan IPTables *firewall* menjadi IPS (Intrusion Prevention System). IPS diperkaya dengan kemampuan untuk melakukan pencegahan penyusupan. Dalam hal ini, IPS dapat menangani suatu penyusupan secara otomatis. IPS dapat menangani suatu penyerangan berdasarkan pada suatu *signature* atau pola-pola tertentu.

Hasil penelitian menunjukkan bahwa implementasi IPS berbasis Snort dan IPTables pada topologi jaringan PPUKDW UNIVERSITAS KRISTEN DUTA WACANA IPS cocok digunakan untuk melakukan pencegahan *buffer overflow*. Namun, implementasi IPS berbasis Snort dan IPTables tidak cocok digunakan untuk melakukan pencegahan *port scanning* terhadap sistem karena IPS berbasis Snort dan IPTables hanya dapat melakukan pemblokiran terhadap paket data dan bukan alamat IP penyusup.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

Bab 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Pesatnya pertumbuhan jaringan internet, membantu manusia untuk berkomunikasi dan bertukar data. Di satu sisi komunikasi dan pertukaran data menjadi lebih mudah, tetapi di sisi lain timbul masalah yang sangat serius, yakni penyerangan terhadap sistem jaringan. Banyak kasus penyerangan jaringan terjadi karena banyak orang yang belum menyadari pentingnya kemanan jaringan untuk diterapkan ke dalam sistem, sehingga menyebabkan sistem mudah untuk disusupi.

Teknologi *firewall* sebagai tembok penghalang dan *policy* dalam kejahatan internet dirasa tidak selalu efektif terhadap percobaan pernyusupan. Karena biasanya *firewall* dirancang untuk memblokir *traffic* di jaringan yang mencurigakan secara tegas. Begitu juga dengan prosedur untuk mengizinkan paket untuk lewat jika sesuai dengan *policy* dari *firewall*. Masalahnya adalah banyak program *exploit* yang konsentrasi serangannya memanfaatkan *firewall* yang mengijinkan protokol tertentu untuk menembus *firewall*.

Perkembangan keamanan internet menemukan gagasan baru. Dikembangkanlah *Intrusion Detection System* (IDS) sebagai sistem pintar yang bekerja dengan cara memantau lalu lintas jaringan, menangkap dan memeriksa setiap paket yang lewat dalam jaringan, hingga mendeteksi adanya kejanggalan dalam jaringan berdasarkan *database signature* IDS, mungkin karena lalu lintas padat atau karena adanya serangan. Kemudian IDS akan membuat laporan (*report*) yang dapat dengan mudah dimengerti oleh administrator jaringan untuk kemudian dilakukan tindak lanjut atas kejadian yang dilaporkan oleh IDS. IDS hanya memantau jaringan tanpa melakukan *troubleshooting* terhadap masalah yang terjadi, sehingga administrator jaringan harus menanganinya secara manual.

Untuk menanggulanginya, IDS akan dikembangkan menjadi IPS (*Intrusion Prevention System*). IPS diperkaya dengan kemampuan untuk

melakukan pencegahan penyusupan. Dalam hal ini, IPS dapat menangani suatu penyusupan secara otomatis. IPS dapat menangani suatu penyerangan berdasarkan pada suatu *signature* atau pola-pola tertentu.

1.2 Perumusan Masalah

Dalam penelitian ini, rumusan masalah yang akan dibahas oleh penulis yakni bagaimana membangun *Intrusion Prevention System* dengan menggunakan Snort sebagai IDS untuk memblokir paket data yang berbahaya dengan menggunakan IPTables.

1.3 Batasan Masalah

Permasalahan dalam tugas akhir penelitian ini dibatasi oleh beberapa hal sebagai berikut :

a. Penelitian ini hanya diimplementasikan pada topologi jaringan Duta Wacana Training Center.
a. Serangan dapat terdeteksi atau tidak tergantung pola serangan tersebut ada di dalam rule IDS atau tidak. Kerena Snort IDS selalu melakukan perbaharuan terhadap *rule* IDS, dalam penulisan tugas akhir ini tidak dibahas pembuatan *rule* IDS.
b. Serangan yang akan dideteksi adalah serangan yang berasal dari luar jaringan vital, sedangkan serangan yang berasal dari dalam jaringan vital keluar tidak akan dideteksi.
c. Karena keterbatasan ketersediaan alat, performa server tidak akan dibahas dalam penelitian ini.
d. Sistem dibangun pada Sistem Operasi Ubuntu Server LTS 10.4.

1.4 Hipotesis

Snort IDS sebagai pemantau jaringan dan IPTables *firewall* sebagai tembok penghalang dapat dikombinasikan untuk membangun *Intrusion Prevention System* yang dapat melakukan pencegahan penyusupan.

1.5 Tujuan Penelitian

Penelitian ini bertujuan untuk membangun *Intrusion Prevention System* yang bekerja melakukan pencegahan aktifitas penyusupan terhadap server dengan cara membaca *alert* dari Snort IDS dan kemudian menentukan apakah aktifitas pengguna merupakan serangan terhadap server.

1.6 Metodologi Penelitian

Metode yang digunakan dalam melakukan penelitian adalah :

b. Analisis permasalahan
c. Melakukan kajian literatur.
d. Pembuatan prototipe penelitian, dengan pemasangan Snort Server di Duta Wacana Training Center.
e. Pengambilan sampel data.
f. Pengolahan data pengamatan.
g. Penarikan kesimpulan.

1.7 Sistematika Penulisan

Bab 1 PENDAHULUAN, membahas tentang latar belakang masalah dari penelitian, rumusan masalah, batasan – batasan masalah, metode penelitian, hipotesis, tujuan serta sistematika penulisan dari penelitian ini.

Bab 2 TINJAUAN PUSTAKA DAN LANDASAN TEORI, berisi bahasan penelitian dan berbagai referensi mengenai penelitian Snort IDS dan IPTables *firewall* 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 3 ANALISIS DAN PERANCANGAN PENELITIAN, berisi rancangan dari IPS yang mengimplementasikan Snort IDS dan IPTables *firewall*. Alur kerja sistem, serta kebutuhan akan *hardware* maupun *software* untuk mendukung penelitian, serta langkah-langkah penelitian yang akan dilakukan.

Bab 4 IMPLEMENTASI SISTEM DAN ANALISIS SISTEM, berisi uraian detail implementasi sistem serta uraian mengenai hasil analisis yang didapatkan dari hasil ujicoba disetiap tahapan penelitian.

Bab 5 KESIMPULAN DAN SARAN, berisi kesimpulan dari hasil penelitian serta saran – saran berkaitan dengan implementasi Snort IDS dan IPTables *firewall*.

Bab 5
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Setelah penulis melakukan implementasi dan analisis terhadap implementasi IPS berbasis Snort dan IPTables maka diperoleh beberapa hasil penelitian sebagai berikut:

a. Implementasi IPS berbasis Snort dan IPTables dengan menggunakan mode *interface bridge* dapat mempertahankan *throughput* jaringan pada topologi jaringan di DWTC. Penulis meyakini pengaruh implementasi IPS pada *throughput* jaringan akan berbeda dengan implementasi IPS di tempat lain, selain karena faktor penggunaan hardware yang akan berbeda di tempat lain dan juga tingkat kepadatan lalu lintas jaringan yang berbeda.
b. Adaptasi *rule* Snort pada implementasi IPS berbasis Snort dan IPTables di topologi jaringan DWTC dapat dilakukan tanpa adanya halangan sebab pada R.GATEWAY DWTC telah diberi *rule firewall* yang baik sehingga hanya paket yang tidak merupakan *bad traffic* saja yang dapat masuk ke dalam jaringan server *farm*.
c. Pada pengujian *port scanning,* IPS berbasis Snort dan IPTables tidak cocok digunakan untuk memblokir aktivitas *port scanning* karena tidak semua paket *port scanning* dideteksi sebagai *alert* oleh *rule* Snort sehingga hanya beberapa *port* saja yang dapat dilindungi. Selain itu, IPS justru memberikan informasi tambahan berupa *port* yang dilindungi kepada penyusup. Sedangkan pada pengujian *buffer overflow,* IPS berbasis Snort dan IPTables dapat digunakan untuk memblokir aktivitas *buffer overflow* sebab Snort telah memiliki *rule* yang lengkap untuk mendeteksi *exploit* dengan *buffer overflow*.
d. Snort mode *inline* dan IPTables kurang cocok digunakan sebagai IPS karena Snort mode *inline* hanya dapat digunakan untuk memblokir paket bukan alamat IP *address* penyusup.

5.2 Saran

Dalam penelitian ini penulis mendapatkan beberapa hal yang dapat dikembangkan untuk penelitian selanjutnya antara lain :

a. Pengembangan penelitian selanjutnya dapat menggunakan fwsnort yang dikombinasikan dengan psad untuk membangun IPS yang lebih baik. Fwsnort merupakan Snort IDS yang telah dimodifikasi sehingga memiliki fungsi-fungsi IPS. Fwsnort tidak hanya dapat digunakan untuk memblokir paket, tetapi juga dapat digunakan untuk memblokir alamat IP *address*. Walaupun fwsnort dapat digunakan untuk membuat *ruleset* yang dapat memblokiran alamat IP, hal ini tidak sama dengan menulis langsung *rule* pada IPTables *firewall.* Sedangkan psad merupakan aplikasi yang dapat digunakan untuk mendeteksi lalu lintas data yang berbahaya. Bila Fwsnort digabungkan dengan psad maka akan terdapat dua mesin pendeteksi penyusupan yang dapat saling melengkapi.
b. Pengembangan penelitian selanjutnya agar menggunakan *hardware* yang memiliki spesifikasi yang lebih baik sehingga IPS dapat bekerja dengan lebih optimal.
c. Pengembangan penelitian selanjutnya dapat menambahkan tipe serangan yang lakukan pada skenario pengujian sehingga dapat lebih menguji kehandalan IPS.

DAFTAR PUSTAKA

Beale, Jay. (2004). *Snort 2.1 Intrusion Detection, Second Edition.* Syngpress Publishing: Rockland.

Carrera, Blaise. (2008). *http://openmaniak.com/inline.php,* diakses pada tanggal 15 November 2010.

Caswell, Brian, Jay Beale dan Andrew Baker. (2007). *Snort IDS and IPS Toolkit (Jay Beale's Open Source Security).* Syngpress Publishing: Burlington.

Jones, Alan. (2004). *Netfilter and IPTables – A Structural Examination.* SANS institute.

Gullett, David. (2010). *Snort 2.8.6 and Snort Report 1.3.1 on Ubuntu 10.04 LTS Installation Guide*. Symmetrix Technologies.

Mena, Yohanes Benediktus. (2009). *Sistem Keamanan Jaringan Menggunakan Intrusion Prevention System.* Yogyakarta: Universitas Kristen Duta Wacana.

Pappas, Nicholas. (2008). *Network IDS & IPS Deployment Strategies.* SANS institute.

Rehman, Rafeeq Ur. (2003). *Intrusion Detection Systems with Snort Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID.* Parentice Hall, New Jersey

Smith, Mike. (2006). *A Design for Building an IPS Using Open SourceProducts.* SANS institute.