Penerapan Intrusion Detection System (IDS) dengan metode Deteksi Port Scanning pada Jaringan Komputer di Politeknik Negeri Semarang

Muhammad Anif[1], Sindung HWS, Mokhamad Daman Huri[1]

[1]*Jurusan Teknik Elektro, Politeknik Negeri Semarang, Indonesia*
Email: muhammad.anif@gmail.com, ssindung@gmail.com, daemontool12@gmail.com

Abstrak — Keamanan jaringan komputer merupakan isu yang sangat penting, seiring dengan pentingnya informasi yang terkandung pada jaringan. *Port scanning* merupakan langkah awal serangan terhadap jaringan komputer. Dari keberhasilan melakukan *port scanning*, penyerang dapat melanjutkan serangan lanjutan ke jaringan komputer. Penelitian ini bertujuan menciptakan sistem keamanan jaringan komputer yang ringan, berbasis *open source*, mudah diatur dan dianalisis oleh administrator jaringan. Sistem dirancang menggunakan *portsentry* sebagai *Intrusion Detection System* (IDS) yang diintegrasikan dengan *syslog-notify* sebagai *alert*. Sistem akan memblokir alamat *Internet Protocol* (IP) yang diketahui melakukan aktivitas *port scanning*. Dari penelitian ini diketahui bahwa *portsentry* efektif dalam menangkal serangan *port scanning* namun tidak mampu memblokir serangan jenis *sniffer*, IP *spoofing* dan *Denial of Service* (DoS) karena bersifat tersembunyi dan tidak dianggap sebagai tindakan berbahaya. Untuk mengantisipasi serangan jenis ini, *portsentry* perlu dikombinasikan dengan *tool* pengaman lain misalnya *firewall* dan antivirus.

Kata kunci — *Intrusion Detection System*, port scanning, portsentry, syslog-notify, keamanan jaringan

Abstract *— Network security is a very important issue, along with the importance of the information contained on the network. Port scanning is the first step attacks against computer networks. From the success of doing port scanning, the attacker can proceed further attacks to a computer network. This study aims to create a system that is lightweight computer network security, based on open source, easy to set up and analyzed by the network administrator. The system is designed to use portsentry as Intrusion Detection System (IDS) which is integrated with syslog-notify as alerts. The system will block Internet Protocol (IP) that is known to conduct port scanning activity. From this research note that portsentry effective in repelling port scanning but are not able to block the attack type of sniffer, IP spoofing, and Denial of Service (DoS) because it is hidden and not seen as dangerous. To anticipate this type of attack, portsentry need to be combined with other security tools such as a firewall and antivirus.*

Keywords — Intrusion Detection System, port scanning, portsentry, syslog-notify, network security

I. PENDAHULUAN

Internet (*Interconnected Network*) adalah sebutan untuk sistem komunikasi global yang menghubungkan komputer-komputer dan jaringan-jaringan komputer di seluruh dunia. Setiap komputer dan jaringan komputer terhubung – baik secara langsung maupun tidak langsung – ke beberapa jalur utama yang disebut jalur tulang punggung (*backbone*) dan dibedakan satu dengan yang lainnya menggunakan nama unik yang biasa disebut dengan alamat IP.

Internet kemudian menjadi media yang sangat pesat perkembangannya dalam sepuluh tahun terakhir ini bukan hanya di dunia, tetapi juga di Indonesia. Pesatnya perkembangan Internet juga didukung dengan harga perangkat telekomunikasi sebagai teknologi pendukung yang makin murah dan makin mudah dijangkau oleh masyarakat umum. Bukan hanya perangkat yang berbasis teknologi kabel (*wired technology*), namun juga perangkat yang berbasis teknologi nirkabel (*wireless technology*). Bahkan karena kemudahan instalasi dan fleksibilitas penggunaannya, perangkat berbasis teknologi nirkabel kemudian menjadi lebih disukai.

Penggunaan jaringan Internet yang semakin memasyarakat kurang diimbangi oleh para pengguna dengan upaya menjaga agar jaringan tetap aman. Hal tersebut karena awamnya para pengguna Internet terhadap ancaman maupun serangan keamanan yang ada di jaringan Internet. Padahal, semakin sering pengguna mengakses jaringan Internet, semakin besar potensi terkena ancaman keamanan dari Internet [1]. Hal yang paling ditakuti oleh pengguna awam saat terhubung ke Internet adalah terkena serangan virus dan disusupi oleh peretas jaringan (*hacker*).

Penggunaan perangkat lunak *firewall* maupun anti virus mungkin dapat membantu menahan serangan terhadap suatu host. Namun menahan serangan saja tidak cukup, terlebih bila host yang diserang merupakan suatu sistem atau server yang penting. Teknik umum yang digunakan untuk mendeteksi keamanan sistem adalah *Intrusion Detection System* (IDS). Agar dapat menghindari serangan yang berbahaya, diperlukan suatu sistem yang dapat mendeteksi penyusupan yang

merupakan awal serangan terhadap sistem. Saat ini terdapat beberapa jenis IDS yang digunakan, namun unjuk kerja sistem tersebut umumnya masih menjadi perhatian utama [1].

Sistem IDS memeriksa kejadian, baik pada trafik jaringan maupun pada sistem operasi, dan membangkitkan alarm jika terdapat kejadian yang dipercaya merupakan gejala adanya penyusupan [2]. Ref [3] dan Ref [4] melakukan sejumlah studi yang meneliti IDS dari perspektif teknis. Penelitian yang dilakukan pada umumnya menginvestigasi kualitas teknis sistem terhadap sejumlah variabel, seperti probabilitas sistem dalam mendeteksi serangan, probabilitas membangkitkan alarm yang keliru (*false alarm*), kendala-kendala dalam unjuk kerja maupun cakupan serangan. Meski demikian, IDS bukanlah suatu entitas mandiri yang dapat membuat keputusan, melainkan suatu *tool* yang digunakan oleh administrator jaringan. Administrator memantau keluaran IDS untuk memfilter false alarm dan berupaya memverifikasi jika terjadi kompromi, misalnya dengan menyelidiki sistem yang terkena dampak secara langsung [5]. Dalam lingkungan operasional, keluaran IDS diproses oleh administrator yang mencoba mendeteksi dan merespon serangan.

II. METODE PENELITIAN

A. Alat Penelitian

Perangkat keras dan perangkat lunak yang digunakan pada penelitian ini adalah:

a. Satu unit komputer server sebagai server *Intrusion Detection System* (server IDS)
b. Dua unit komputer (PC atau laptop) sebagai penyerang dan target serangan
c. Satu unit modem *Global System for Mobile communication* (GSM) untuk mengakses Internet
d. Satu unit modem *Asymmetric Digital Subscriber Line* (ADSL) dengan *public Internet Protocol* (IP) sebagai alamat publik bagi server IDS
e. Perangkat lunak Linux Ubuntu 11.04 sebagai sistem operasi bagi server IDS dan target serangan
f. Perangkat lunak Windows sebagai sistem operasi bagi komputer penyerang
g. Perangkat lunak *Portsentry* sebagai paket IDS
h. Perangkat lunak *Syslog-notify* sebagai perangkat lunak informasi *pop-up*.

B. Prosedur Penelitian

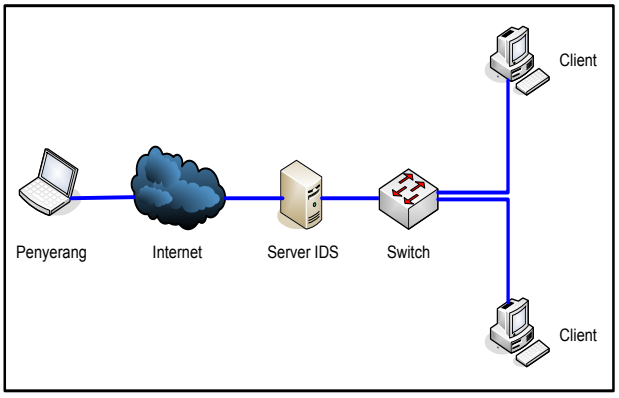
Prosedur penelitian ini disusun sebagai berikut:

a. Perancangan sistem

Sistem yang diperlukan pada penelitian ini dikonfigurasi sebagaimana ditunjukkan pada Gambar 1. Pada gambar tersebut ditunjukkan bahwa server dengan IDS akan dapat mendeteksi seluruh aktivitas *port scanning* yang dilakukan dari Internet menuju ke jaringan dalam (intranet). Jenis IDS yang akan digunakan adalah tipe *Host-based* IDS (HIDS) sehingga dapat mengawasi paket-paket yang masuk ke sistem, baik dari jaringan luar maupun dari jaringan dalam.

Kemampuan IDS dalam mendeteksi seluruh aktivitas *port scanning* adalah karena IDS ditempatkan pada komputer yang menjadi *gateway* dan sekaligus difungsikan sebagai *firewall*. Penempatan IDS pada server *gateway* ini akan melindungi data yang ada di server *gateway* dari serangan hacker. Selain itu, IDS juga dapat ditempatkan pada *host* tertentu yang penting untuk dilindungi, misalnya *web server* atau FTP *server*, agar dapat melindungi data pada host tersebut jika serangan yang dilancarkan lolos dari pengawasan IDS yang ditempatkan pada server *gateway*.

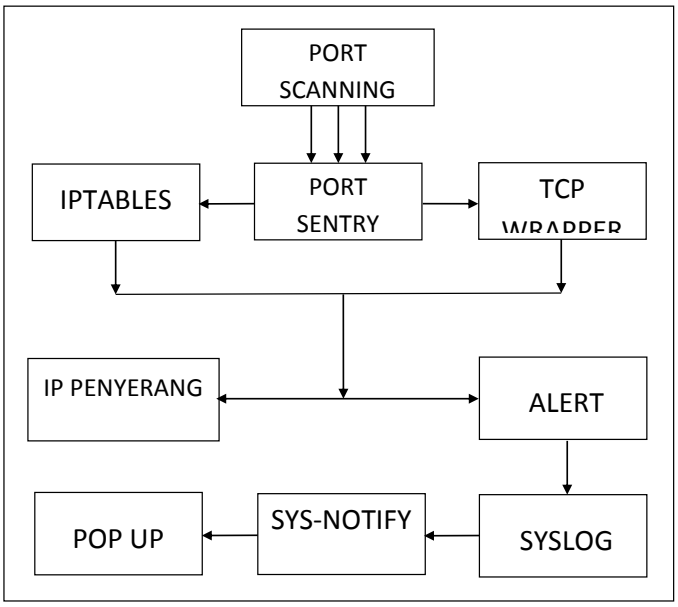
Portsentry didesain untuk mendeteksi dan merespon kegiatan *port scanning* pada sebuah mesin secara *real time*. Ketika IDS dengan *portsentry* mendeteksi *port scanning* pada jaringan, maka *portsentry* akan menjalankan *iptables* dan *TCP wrapper* guna memblokir dengan *rejecting* koneksi dan *filtering* IP penyerang, sehingga serangan *port scanning* dapat digagalkan. Kemudian *portsentry* akan mencatat *log* serangan *port scanning* yang terjadi untuk disimpan ke dalam *file syslog* dan dengan *syslog-notify* data *log* yang tersimpan di *syslog* dapat ditampilkan di layar monitor dalam bentuk *pop up window*. Diagram sistem pendeteksian *port scanning* oleh *portsentry* yang diintegrasikan dengan *syslog-notify* ditunjukkan pada Gambar 2.



Gambar 1 Perancangan sistem IDS secara umum

b. Instalasi dan konfigurasi perangkat lunak

Perangkat lunak yang diperlukan pada penelitian ini, yaitu sistem operasi Linux Ubuntu 11.04 pada server IDS, sistem operasi Windows pada komputer penyerang, paket *portsentry* dan *syslog-notify* pada server IDS, diinstal dan dikonfigurasi pada tiap perangkat keras masing-masing.

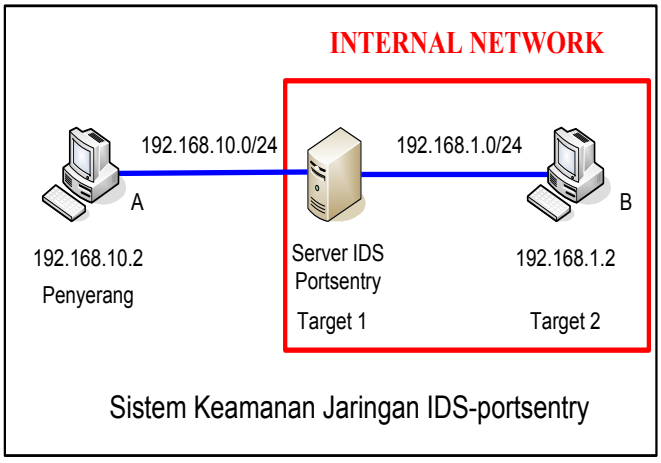


Gambar 2 Diagram sistem kerja *portsentry* dan *syslog-notify*

c. Pengujian sistem

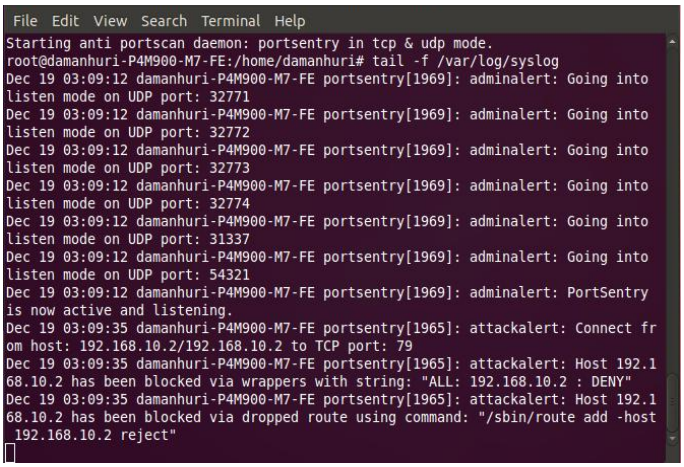
Skema pengujian sistem dilakukan sebagaimana pada Gambar 3. Sebagai penyerang adalah komputer A, sementara target yang diserang adalah server IDS dan host B (klien IDS). Pengujian penyerangan dibedakan dalam dua jenis pengujian, yaitu penyerangan target tanpa penerapan IDS dan penyerangan target dengan penerapan IDS. Terdapat 5 *tool* penyerangan sistem yang digunakan, yaitu *ipscan*, *nmap*, LAN*spy*, *nessus*, *superscan*, *wireshark*, *a-mac address change* dan *ping of death*. Penjelasan masing-masing *tool* adalah sebagai berikut.

1. *IPscan* adalah alat yang digunakan penyerang untuk melakukan *scanning IP* pada suatu jaringan. Dengan menggunakan *IPscan*, penyerang dapat mengetahui alamat IP dari komputer yang menjadi target serangan, *port* yang aktif pada komputer korban, dan nama komputer korban.
2. *Nmap* adalah alat yang digunakan untuk mengetahui *service* yang diberikan oleh suatu komputer melalui *scanning port*. *Nmap* banyak digunakan penyerang untuk mengetahui *port* komputer korban yang aktif, kemudian menggunakan *port* yang aktif tersebut untuk masuk ke sistem komputer korban.
3. *LANspy* adalah sebuah alat *scanner* jaringan yang berguna untuk mendapatkan informasi mengenai komputer-komputer yang koneksi dalam jaringan LAN, *LANspy* mampu mendeteksi *port* TCP dan UDP yang aktif.
4. *Nessus* adalah alat yang mirip dengan *nmap*, namun hasil *scanning* yang dilakukan *nessus* memberikan informasi yang lebih lengkap dari *nmap*. Informasi yang diberikan *nessus* seperti sistem operasi korban, *port* yang terbuka pada komputer korban, jarak dengan komputer korban.
5. *SuperScan* adalah sebuah program *scanning port* dengan menghubungkan pemindai *port* berbasis perangkat lunak yang dirancang untuk mendeteksi *port* TCP dan UDP pada komputer target, menentukan layanan yang berjalan pada *port* tersebut, dan menjalankan *query* seperti *whois, ping, traceroute ICMP,* dan *hostname lookup*.
6. *Wireshark* adalah sebuah aplikasi penyerangan dengan tipe *sniffer*. *Wireshark* mampu mendeteksi paket yang melintas tanpa melakukan tindakan yang mencurigakan. *Wireshark* adalah salah satu peralatan serang yang sulit untuk dideteksi oleh sebuah *Intrusion Detection System* (IDS).
7. *A-Mac Address Change* adalah sebuah alat penyerangan yang digunakan untuk mengetahui *Mac Address* target dan mampu melakukan *port scan* tanpa diketahui oleh IDS. *A-mac Address Change* adalah peralatan serang pada jaringan jenis *spoffing IP*, yaitu dengan memalsukan identitas penyerang agar bisa dikenali oleh target dan agar tidak dianggap sebagai tindakan penyerangan.
8. *Ping of Death* adalah sebuah penyerangan dengan mengirim paket sebesar mungkin secara terus-menerus agar *service-service* atau kinerja sistem pada target mengalami (*hang*) atau berhenti bekerja seperti penyerangan jenis *Denial of Service*. *Ping of Death* biasa dilakukan dengan melakukan pengeriman paket ICMP sebesar mungkin dan secara terus-menerus melalui *command prompt*.

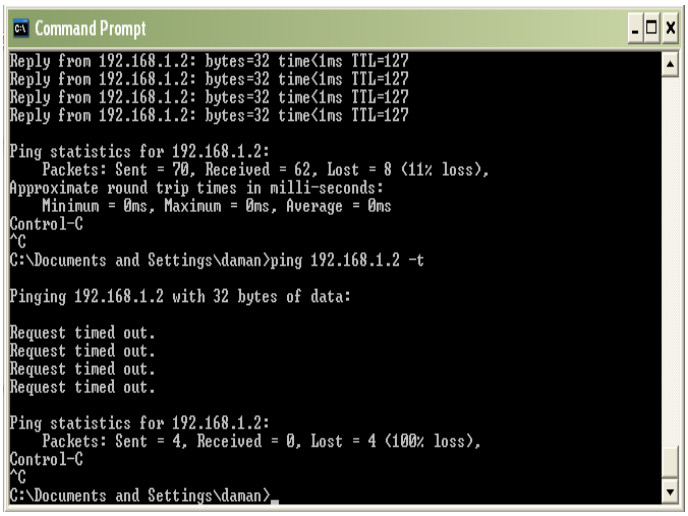


Gambar 3 Skema jaringan pengujian penyerangan

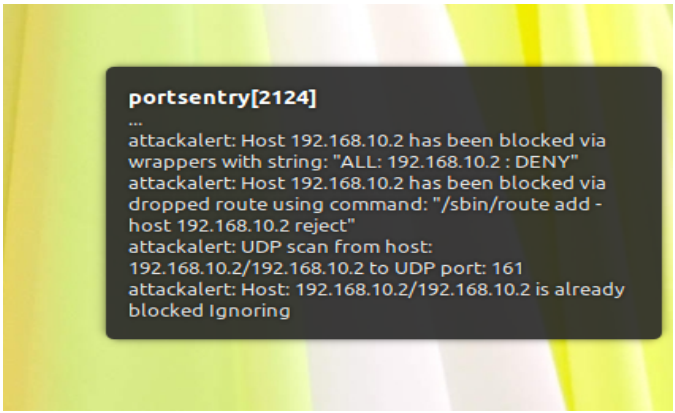
Indikator keberhasilan dari sistem IDS dalam menangkal penyerangan adalah *portsentry* memblokir dengan *rejecting* koneksi dan *filtering* IP *host* penyerang seperti pada Gambar 4, sehingga penyerang tidak bisa terkoneksi lagi seperti pada Gambar 5.



Gambar 4 *Portsentry* memblokir IP penyerang



Gambar 5 Koneksitas komputer penyerang



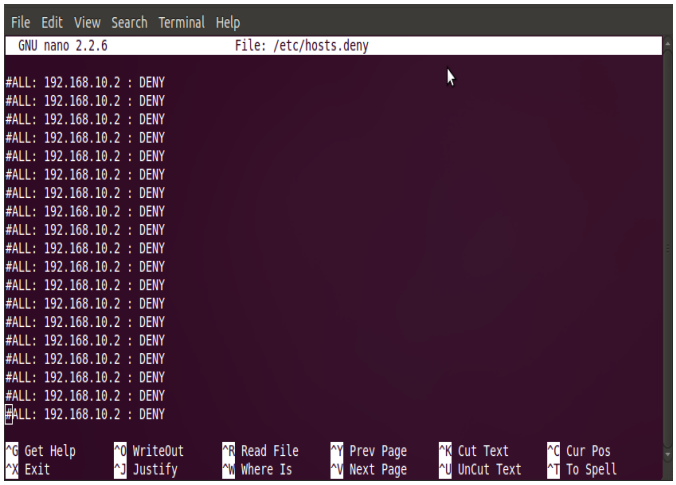
Gambar 6 Informasi *syslog* pada *pop up window*

Informasi serangan juga dapat terlihat di layar monitor dalam bentuk *pop up window* yang keluar secara *real time* ketika terjadi serangan *port scanning* yang terdeteksi oleh *portsentry* seperti pada Gambar 6.

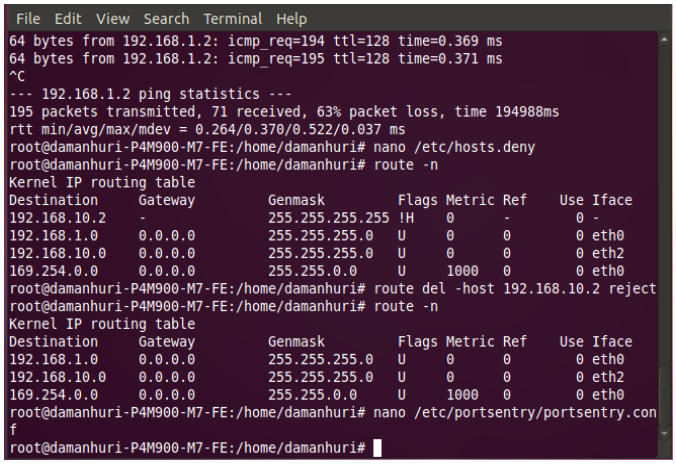
Untuk membuka kembali koneksi komputer penyerang dengan komputer IDS sebagai target yaitu dengan mengedit file */etc/hosts.deny* dan menghapus alamat IP yang terdapat di *kernel* IP pada tabel *routing*. Di dalam file */etc/hosts.deny* terdapat alamat IP penyerang yang dijaga oleh *TCP wrapper*. Jika ingin membuka IP yang terblokir oleh *TCP wrapper* maka harus ditambahkan tanda # di depan

ALL: 192.168.10.2 : DENY

seperti pada Gambar 7 yang berarti bahwa IP 192.168.10.2 telah dijaga oleh *TCP wrapper*. Alamat IP penyerang yang ditolak koneksi oleh *iptables* dalam *kernel IP routing table, IP address* dihapus dengan menjalankan perintah
route del –host 192.168.10.2 reject
seperti pada Gambar 8.



Gambar 7 *IP address* yang dijaga *TCP wrapper*



Gambar 8 *IP address* yang ada di tabel *routing*

III. HASIL DAN PEMBAHASAN

A. Hasil Implementasi Portsentry

Hasil pengujian penyerangan *port scanning* ke target baik yang tidak dilindungi dengan IDS maupun yang dilindungi

IDS disajikan secara ringkas pada Tabel 1. Dari hasil tersebut jika tanpa menggunakan IDS, maka jaringan rawan diserang karena semua port target yang aktif terdeteksi oleh penyerang melalui kegiatan *port scanning*. Serangan berupa *port scanning* merupakan langkah awal terjadi serangan lanjutan. Hal ini dikarenakan *port* merupakan pintu masuk untuk memasuki komputer korban. Dengan menerapkan IDS, maka keberadaan *port* yang aktif tidak terdeteksi oleh penyerang sehingga menghindarkan serangan selanjutnya.

Tabel 1 Hasil pengujian penyerangan menggunakan tiap *tool* serangan

No	Tool serangan	Keberadaan port target yang aktif	
		Tanpa IDS	Dengan IDS
1.	*Ipscan*	Terdeteksi	Tidak terdeteksi
2.	*Nmap*	Terdeteksi	Tidak terdeteksi
3.	*LANspy*	Terdeteksi	Tidak terdeteksi
4.	*Nessus*	Terdeteksi	Tidak terdeteksi
5.	*Superscan*	Terdeteksi	Tidak terdeteksi
6.	*Wireshark*	Terdeteksi	Terdeteksi
7.	*A-Mac Address Change*	Terdeteksi	Terdeteksi
8.	*Ping of Death*	Terdeteksi	Terdeteksi

Dari Tabel 1 juga terlihat bahwa terdapat beberapa penyerangan yang tidak berhasil diblok oleh *portsentry.* Hal tersebut menuntut *administrator* untuk membuat sebuah tindakan pencegahan dari usaha penyerangan atau tindakan mengeksploitasi sistem. Berikut adalah langkah pencegahan yang tepat untuk mengatasi penyerangan tersebut.

1. Komputer server yang menjadi *gateway* antara *intranet* dengan *internet* harus dipasang *firewall* yang mampu menjaga serangan dari luar seperti *comodo firewall, zone alarm firewall* pada sistem operasi *windows* atau menggunakan konfigurasi *iptables* pada sistem operasi *linux.*
2. Komputer pada jaringan *intranet* diharapkan untuk tidak menggunakan *service-service* yang ada di sistem operasi *windows* seperti *internet explorer* karena rawan untuk dieksploitasi.
3. Komputer pada jaringan *intranet* diharapkan untuk menggunakan *antivirus* yang mampu mendeteksi paket-paket berisi *virus* dari luar *internet* seperti *antivirus* yang mempunyai *internet security*.

Penggunaan *portsentry* sebagai sistem keamanan IDS sangat membantu *administrator* melindungi jaringan *intranet* dari usaha penyusupan atau *scanning port* yang dilakukan dari luar *internet*, namun masih sangat rawan ketika terjadi penyerangan jenis lain seperti *sniffer,* IP *spoofing,* dan *Denial of Service* (DoS). IDS dengan *portsentry* mampu membantu menjaga jaringan komputer dari serangan *port scanning*, karena IDS dengan *portsentry* akan segera memblokir jalur akses penyerang sehingga serangan dapat dicegah. Dari hasil analisis penyerangan, ada beberapa kejadian yang menjadi kelemahan dari sistem IDS dengan *portsentry* dalam mendeteksi *scanning port. Portsentry* tidak memblokir serangan yang dilancarkan ke komputer *client* sebagai target uji coba, dikarenakan *portsentry* adalah jenis IDS yang hanya melindungi *host* atau biasa disebut dengan HIDS. *Portsentry* juga tidak mampu memonitoring semua *port* yang ada pada sistem target karena *portsentry* hanya memonitor *port* yang memang berhubungan langsung dengan Internet.

Terdapat beberapa cara yang dapat digunakan untuk mengalokasikan *portsentry* dapat melindungi *client* dalam jaringan yaitu dengan mengkonfigurasi *iptables* seperti menutup semua *port* dan hanya membuka *port* 80 (http) sebagai jalan masuk dari luar maupun menuju ke Internet, atau dapat membuat sebuah *proxy transparant* sebagai penjaga web-web yang dianggap mencurigakan. Konfigurasi *iptables* yang dapat dilakukan adalah dengan membuat semua paket yang mengarah ke *client* sebagai target dan *IP address* target dibelokkan ke server dengan *portsentry* atau *port* seperti *port 3128 (proxy transparant)* sebelum mengalami *routing* agar dapat dimonitor sehingga mengurangi terjadinya usaha penyusupan yang dilakukan untuk mengeksploitasi sistem atau yang biasa disebut dengan DNAT pada aturan *iptables*. *Portsentry* mempunyai kemampuan sebagai berikut:

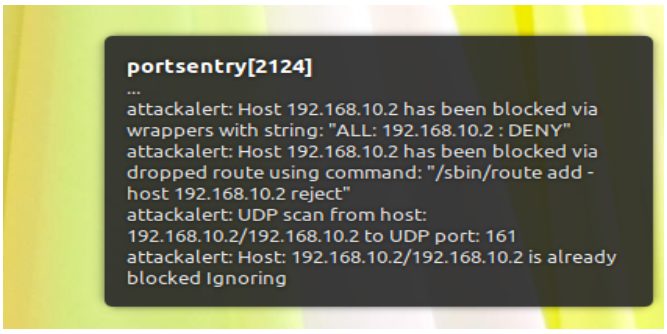
a. Berjalan di atas *soket* TCP & UDP untuk mendeteksi *scanning port* ke sistem.
b. Mendeteksi *stealth scan*, seperti SYN/*half-open*, FIN, NULL, X-MAS.
c. *Portsentry* akan bereaksi secara *real time* (langsung) dengan cara memblokir *IP address* penyerang. Hal ini dilakukan dengan menggunakan *iptables* dan memasukan ke file */etc/host.deny* secara otomatis oleh *TCP Wrapper*.
d. *Portsentry* mempunyai mekanisme untuk mengingat mesin/*host* yang pernah terhubung ke target. Dengan cara itu, hanya mesin/*host* yang terlalu sering melakukan sambungan (karena melakukan *scanning*) yang akan di blokir.
e. *Portsentry* akan melaporkan semua pelanggaran melalui *syslog* dan mengindikasikan nama sistem, waktu serangan,

IP mesin penyerang, TCP / UDP *port* tempat serangan dilakukan.

f. *Portsentry* mampu memonitoring *port* UDP dan *port* TCP, yaitu :
TCP_PORTS="1,7,9,11,15,70,79,80,109,110,111,119,138,139,143,512,513,514,515,540,635,1080,1524,2000,2001,4000,4001,5742,6000,6001,6667,12345,12346,20034,27665,30303,32771,32772,32773,32774,31337,40421,40425,49724,54320"
UDP_PORTS="1,7,9,66,67,68,69,111,137,138,161,162,474,513,517,518,635,640,641,666,700,2049,31335,27444,34555,32770,32771,32772,32773,32774,31337,54321"

B. Hasil Integrasi Portsentry dengan syslog-notify

Hasil pengujian penyerangan yang dilakukan oleh semua *port scanner* yang menjadi *tool* pengujian sistem dan informasi *portsentry* yang diintegrasikan dengan *syslog-notify*, memperlihatkan bahwa *syslog-notify* berhasil menampilkan informasi *portsentry* yang ada di file *syslog* dalam bentuk *pop up windows* yang dapat muncul secara *real time* ketika *portsentry* menangkap aktifitas penyerangan yang dilakukan oleh alat serang dalam pengujian sistem IDS seperti pada Gambar 9. *Syslog-notify* membantu *administrator* dalam memonitoring jaringan dan menganalisa ketika terjadi serangan. *Syslog-notify* dalam menampilkan informasi *pop up window* dilakukan secara bertahap dengan melihat informasi yang ada di file *syslog* yang menjadi tempat informasi sistem komputer saat bekerja terutama *portsentry* dalam melakukan pendeteksian serangan *port scanning*. *Syslog-notify* memerlukan waktu 10 detik untuk dapat menampilkan informasi dari *portsentry*.



Gambar 9 Informasi *pop up* dari *portsentry*

IV. KESIMPULAN

Kesimpulan dari penelitian ini adalah sebagai berikut.

a. Sistem pendeteksi penyusupan (*Intrusion Detection System*, IDS) berbasis Linux Ubuntu dapat dibangun menggunakan *portsentry* yang diintegrasikan dengan *syslog-notify*.
b. IDS menggunakan *portsentry* cukup efektif dalam menangkal serangan *port scanning* (misalnya menggunakan *ipscan*, *nmap*, *LANspy*, *nessus* dan *superscan*) yang merupakan langkah awal dari serangan ke sistem jaringan.
c. Penggunaan *portsentry* yang diintegrasikan dengan *syslog-notify* sangat membantu administrator dalam melindungi jaringan dari usaha penyusupan, karena *syslog-notify* akan memberikan peringatan sehingga administrator dapat mengambil tindakan lebih lanjut.
d. *Portsentry* tidak mampu memblokir serangan jenis *sniffer*, IP *spoofing* dan *Denial of Service* (DoS) karena bersifat tersembunyi dan tidak dianggap sebagai tindakan mencurigakan atau berbahaya. Untuk mengantisipasi serangan jenis ini, perlu dikombinasikan dengan *tool* pengaman lain misalnya berupa *firewall* dan anti virus.

V. SARAN

Saran yang diajukan dari penelitian ini adalah sebagai berikut.

a. Penerapan IDS dalam memantau keamanan jaringan akan lebih efektif jika sistem IDS ditempatkan di belakang *firewall* yang menghubungkan jaringan Internet dengan Intranet.
b. Sistem peringatan (*alert*) pada IDS masih terbatas pada *pop-up window* yang harus selalu dimonitor, sehingga perlu dikembangkan menjadi teknologi *alert* jarak jauh.
c. Kemampuan IDS akan lebih lengkap lagi bila *portsentry* juga mampu mengenali paket berisi virus yang masuk ke jaringan Intranet sebagai serangan.

DAFTAR PUSTAKA

[1] Alhomoud, A., Munir, R., Disso, J. P., Awan, I., & Al-Dhelaan, A. (2011). Performance Evaluation Study of Intrusion Detection Systems. *Procedia Computer Science*.

[2] Sommestad, T. (2012). *Intrusion Detection and the Role of the System Administrator*.

[3] Mell, P., Hu, V., Lippmann, R., Haines, J., & Zissman, M. (2003). *An Overview of Issues in Testing Intrusion Detection Systems*. Available: http://citeseerx.ist.psu.edu. Diunduh pada tanggal 1 Pebruari 2013.

[4] Biermann, E. (2001). A comparison of Intrusion Detection Systems. *Computer & Security* (hal. 676-683).

[5] Werlinger, R., Muldner, K., Hawkey, K., & Beznosov, K. (2010). Preparation, detection, and analysis: the diagnostic work on IT security incident response. *Information Management and Computer Security, 18*, 26-42.