Jurnal Ilmiah ***ESAI Volume 8, No.1, Januari 2014***
ISSN No. 1978-6034

Effectiveness of Instrusion Detection System in Proxy Server XYZ to prevent Port Scanning action by Hacker

Efektivitas *Instrusion Detection System* Pada *Proxy* Server XYZ dalam Mencegah *Scanning Port* oleh *Hacker*

Imam Asrowadi[1)], Eko Subiyantoro[2)]

[1,2)] Dosen pada Program Studi Manajemen Informatika Politeknik Negeri Lampung
Jl. Soekarno – Hatta Bandar Lampung

Abstract

Due to its crucial role, a proxy server needs to be well maintained to ensure its appropriate functions. One of the causes of failure access in proxy server is data manipulation done by irresponsible users that work by scanning, gaining access, maintaining access and covering track. The scanning process appears as an important step as it exposes the types of applications and services utilized in the server. The step is to manipulate four vulnerable points of proxy server related to the operating system, applications, program modules and configurations. In order to prevent the scanning process, it is important to utilize a mechanism which is able to detect and report any indications of intruding access in the proxy server aka intrusion detection system. This research is aimed at producing an application operated in the proxy server to report any indication of access intrusion. The research uses System Development Life Cycle (SDLC) method by applying analyzing, designing, implementing and assessing.

Key words: proxy, server, ids, scanning.

Pendahuluan

*Proxy server*XYZ berfungsi menangani *caching*, *bandwidth management* dan manajemen akses dari jaringan lokal ke jaringan publik (internet). Begitu pentingnya peran *proxy server* tersebut, maka berbagai macam metode digunakan untuk mempertahankan agar *proxy server* dapat terus bekerja sesuai dengan fungsinya. Kegagalan pada *proxy server* ini berdampak pada terganggunya seluruh layanan koneksi internet dari jaringan lokal menuju jaringan publik.

Kegagalan menjalankan fungsi secara umum dapat terjadi karena hilangnya kemampuan pembangkit

listrik memasok sumber daya kepada *proxy server* (pemadaman listrik), kegagalan *hardware*, kegagalan sistem operasi, serta kegagalan konfigurasi pada sistem aplikasi.

Kegagalan konfigurasi pada sistem aplikasi dapat disebabkan oleh kesalahan konfigurasi ketika melakukan proses pembaharuan sistem oleh administrator atau unsur kesengajaan memanipulasi sumber daya yang ada pada *proxyserver* oleh pihak-pihak yang tidak bertanggung jawab (penyusup) dengan menggunakan akses yang tidak sah (Id.Wikipedia, 2011; Ali, dan Heriyanto, 2011).

Penyusup menggunakan akses yang tidak sah tersebut dengan memanfaatkan tahapan *scaning*, *gaining access*, *maintaining acces* dan *covering tracks* (Sto, 2009). Pada tahapan pertama (*reconncaisance)*, digunakan oleh penyusup untuk mendapatkan berbagai informasi mengenai target seperti nama domain, *ip address*, teknologi, kontak dan berbagai macam informasi lain yang bermanfaat oleh penyusup. Tahapan kedua (*scaning)* digunakan oleh penyusup untuk melakukan *probbing* atau penyelidikan terhadap korban untuk mencari lubang keamanan yang dapat dieksploitasi atau sebagai pintu masuk ke sistem target. Jika pada tahapan ke dua berhasil maka penyusup melanjutkan pada tahapan-tahapan berikutnya sehingga *proxy server* dapat dikuasai sepenuhnya.

Berdasarkan tahapan-tahapan tersebut, tahapan pertama memegang peranan penting. Pada tahapan tersebut proses *scanning* berbagai aplikasi servis (*port scanning*) yang dijalankan di *proxy server* dapat diketahui. Tujuannya adalah memanfaatkan empat macam lubang kerawanan yang dimiliki oleh *proxy server* terkait dengan sistem operasi, aplikasi, modul program, dan konfigurasi (Indrajit, 2011). Upaya mencegah terjadinya proses *scanning* yang dilakukan pada tahapan ke dua maka diperlukan sebuah mekanisme yang dapat digunakan untuk mengetahui dan melaporkan adanya indikasi terjadinya pelanggaran akses pada *proxy server*XYZ (*instrusion detection system*). *Intrusion detection system* dibangun dengan memanfaatkan *log* yang tardapat pada *syslog proxy server*. Harapannya, *instrusion detection system* dapat digunakan untuk memonitor dan mencegah terjadinya serangan oleh penyusup (Gandhi dan Srivatsa, 2008; Rebecca, B., dan Petter, M., 2002; Kumar, 2011; Hampton, 2011)

Penelitian ini difokuskan pada pembuatan mekanisme dalam bentuk *service* yang dapat digunakan untuk

mendeteksi adanya indikasi terjadinya pelanggaran akses yang terjadi pada *proxyserver*XYZ (*instrusion detection system*), yaitu dengan cara memotong tahapan-tahapan yang digunakan oleh penyusup untuk menguasai sumber daya yang dimiliki oleh *proxy server.* Penelitian ini sangat penting karena memberikan manfaat *proxy server* bagi seluruh civitas akademika XYZ. Secara khusus penelitian ini bertujuan untuk: 1) Membangun sebuah mekanisme untuk mengingat mesin yang pernah terkoneksi dengan *proxy server*XYZ. 2) Membangun mekanisme pelaporan pelanggaran atau indikasi pelanggaran melalui *syslog*. 3) Memutus tahapan uji coba pengambil alihan *proxy server*XYZ pada tahapan *scaning.*

Metode Pelaksanaan

Penelitian ini dilakukan menggunakan pendekatan konsep SDCL (*System Development Life Cycle)* yang meliputi tahapan:

1. Analisis. Pada tahapan ini yang akan dilakukan adalah menguji kondisi *existing*cara membuat sebuah skenario penyerangan dari sisi internal maupun external *system*. *Output* pada tahapan ini adalah dokumentasi yang berisi kerentanan yang dimiliki oleh *proxy server*terhadap serangan-serangan yang mungkin dilakukan oleh *hacker.*
2. Desain. Pada tahapan ini yang akan dilakukan adalah:
   - Membuat desain arsitetktur IDS dan
   - Membuat desain *flowchatsystem* IDS

   Ouput pada tahapan ini adalah dokumentasi yang berisi desain arsitektur dan desain *flowchat sytem* yang akan digunakan pada tahapan implementasi.
3. Implementasi. Pada tahapan ini yang akan dilakukan adalah mengimplementasikan desain arsitektur dan desain *flowchat* system.

   Output pada tahapan ini adalah *proxy server* yang sudah memiliki pengamanan dari serangan *hacker*.
4. Pengujian dilakukan dengan tahapan:
   a. Percobaan menemukan service yang aktif dalam *proxy server*(s*canning*) dilakukan dari sisi *public area* maupun *local area*.
   b. Memeriksa apakah *proxy server* telah mampu menangkap usaha percobaan penyusupan ke dalam *proxy server* dengan cara melihat *syslog* yang dihasilkan.

c. Memeriksa apakah *proxy server* telah mampu memasukkan *source address*yang digunakan oleh penyusup dan dan waktu percobaan ke dalam *black list address* kemudian menguncinya.

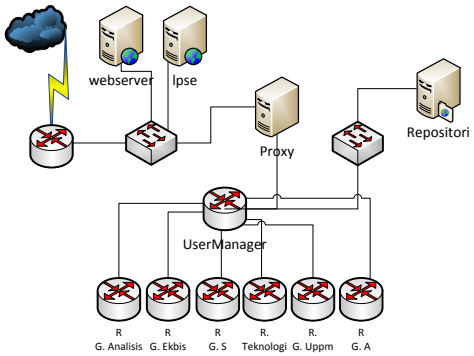
d. Percobaan 1 dilakukan kembali jika penyusup tidak mampu melakukan tindakan *scanning* maka mekanisme IDS telah berjalan dengan baik.

Hasil Dan Pembahasan

Analisis

a. Desain Arsitektur jaringan komputer XYZ

Secara garis besar desain jaringan di XYZ dapat dilihat pada Gambar 1.



Gambar 1. Desain jaringan

Berdasarkan Gambar 1, *Proxy* server memiliki dua *interface*. Satu interface menuju jaringan *local area network* (LAN) dan satu interface menghadap ke jaringan *public.* Ke dua *interface* tersebut merupakan gerbang keluar masuknya data dari jaringan *local area network* menuju ke jaringan *public* begitu juga sebaliknya. Selain berfungsi sebagai media penyimpanan *cache, proxy* server juga berfungsi sebagai *internet gateway*. Melalui ke dua *interface* tersebut, penyusup dapat melakukan proses *scanning* untuk mengetahui *port-port* yang terbuka kemudian berlanjut pada proses serangan berikutnya.

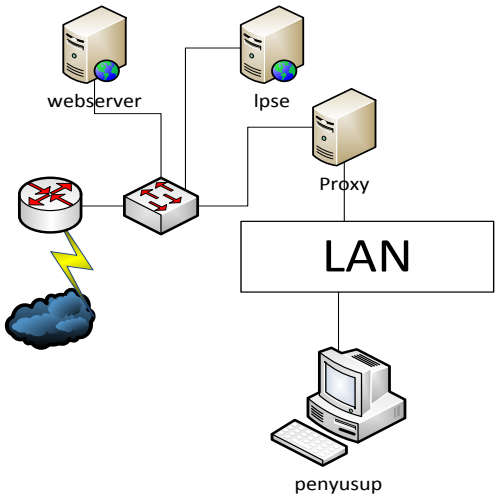
b. Desain Pengujian Tanpa IDS

Pengujian dilakukan dari dua sisi yaitu, sisi internal (*LAN*) dan sisi external (jaringan *public*). Hal ini didasarkan pada pertimbangan bahwa kemungkinan terjadinya penyusupan ke *proxy* server dapat terjadi baik dari sisi jaringan *local*

area network maupun jaringan *public*.

- Desain pengujian dari sisi internal

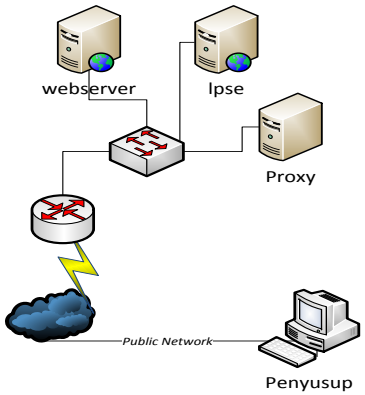
  Desain pengujian dari sisi jaringan LAN ditunjukkan pada Gambar 2. Pada Gambar 2 disimulasikan penyusup yang berasal dari jaringan internal XYZ.



Gambar 2. Desain Pengujian pada Jaringan LAN

- Desain pengujian dari sisi external

  Desain pengujian dari sisi jaringan *public* ditunjukkan pada Gambar 3. Pada Gambar 3 disimulasikan penyusup yang berasal dari jaringan *external*XYZ yang menggunakan koneksi internat yang berasal dari *Internet Service Provider* baik yang berada di Indonesia maupun negara lain.



Gambar 3. Desain Pengujian pada Jaringan *Public*

c. Hasil Pengujian Tanpa IDS

Berdasarkan hasil pengujian menggunakan aplikasi nmap pada sisi internal maupun sisi *external* maka dapat disimpulkan bahwa:

- Penyusup yang berasal dari jaringan internal XYZ mampu melakukan proses *secanningport* dengan baik, tanpa ada proses penolakan pada sisi server.
- Penyusup yang berasal dari jaringan external XYZ juga mampu melakukan proses *secanningport* dengan baik, tanpa ada proses penolakan pada sisi server.

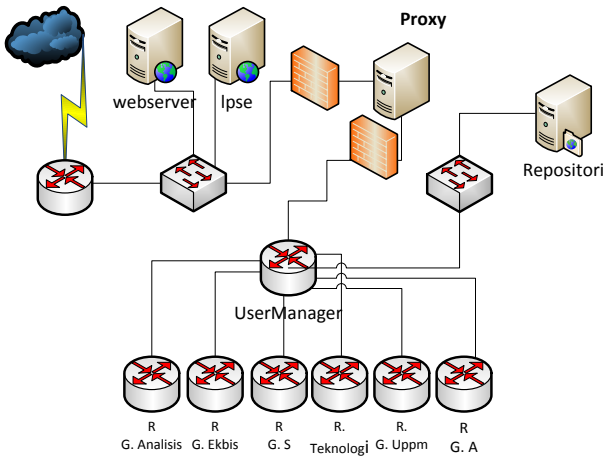
Berdasarkan hasil analisis yang dilakukan maka secara umum *proxy* server XYZ belum memiliki sebuah mekanisme atau aturan yang dapat digunakan untuk menolak proses *scanning port* yang dilakukan oleh penyusup baik yang dilakukan pada sisi internal maupun *external*. Hal tersebut memungkinkan terjadinya tahapan-tahapan berikutnya pada proses *exploitasi* sistem oleh penyusup.

Desain

a. Desain Arsitektur Jaringan XYZ dengan IDS

Desain arsitektur jaringan XYZ dengan IDS ditunjukkan pada Gambar 5. Berdasarkan pada desain arsitektur jaringan XYZ (Gambar 1), maka usulan desain jaringan arsitektur jaringan XYZ dikembangkan dengan menambahkan komponen baru pada arsitektur jaringan tersebut, yaitu IDS. IDS pada arsitektur baru tersebut (Gambar 4) berfungsi untuk menolak *scanning port* yang

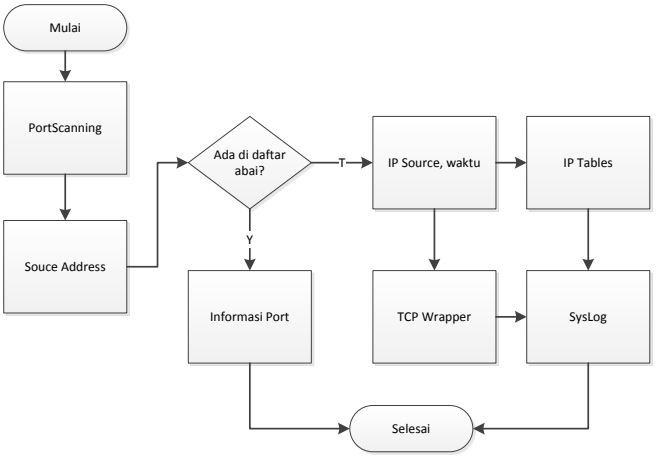
dilakukan oleh penyusup *(hacker)* baik melalui jaringan internal mapun jaringan *public.*



Gambar 4. Desain jaringan dengan IDS

b. Desain *Flowchat* IDS

Desain *flowchat* IDS ditunjukkan pada Gambar 5.



Gambar 5. *Flowchat* IDS

Sebagaimana pada Gambar 5, sistem IDS akan membaca kegiatan *scanning port* yang dilakukan oleh penyusup. Sistem akan memeriksa sumber alamat yang kemudian dibandingkan dengan alamat yang terdapat pada daftar sumber alamat yang diberi hak untuk melakukan kegiatan *scanning port.* Jika sumber alamat tidak terdapat pada

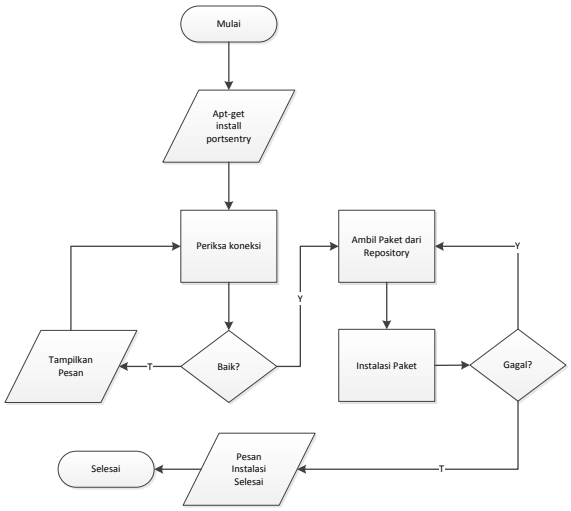
daftar, maka sistem akan mengaktifkan *tcp wrapper* dan *iptables* untuk memblokir serangan yang kemudian mendokumentasikan di dalam syslog sistem. Sistem akan menyimpan sumber alamat yang akan dijadikan sebagai acuan untuk mencegah aktivitas lain yang diinginkan terhadap server.

Implementasi

Implementasi dilakukan dengan memperhatikan pada tahapan sebelumnya (desain). Implementasi dilakukan dengan tahapan:

1. Instalasi

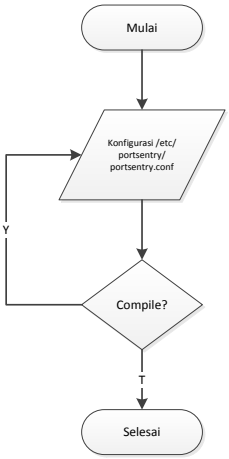
   Instalasi dilakukan dengan tahapan-tahapan sebagaimana ditunjukkan pada Gambar 6.



Gambar 6. *Flowchat* Instalasi IDS

2. Konfigurasi

   Konfigurasi file IDS dilakukan sebagaimana ditunjukkan pada Gambar 7.



Gambar 7. *Flowchat* Konfigurasi File IDS.

Pengujian

Beradasarkan hasil pengujian menggunakan aplikasi *nmap* pada *proxy* server yang telah diimplementasikan IDS baik sisi internal maupun sisi *external* maka dapat disimpulkan bahwa:

- Penyusup yang berasal dari jaringan internal XYZ tidak mampu melakukan proses *scanningport* dengan baik, dengan adanya proses penolakan pada sisi server.
- Penyusup yang berasal dari jaringan *public*XYZ tidak mampu melakukan proses *scanningport* dengan baik, dengan adanya proses penolakan pada sisi server.

Perbandingan hasil pengujian sebelum dan sesudah penerapan IDS dapat di lihat pada Tabel 1.

Tabel 1. Perbadingan hasil pengujian sebelum dan sesudah penerapan IDS

No	Layanan	Sebelum IDS		Sesudah IDS	
		Internal	External	Internal	External
1	PING	V	V	X	X
2	NMAP	V	V	X	X
3	Dictionary Attack	V	V	X	X
4	SSH	V	V	X	X

Simpulan dan Saran

Beradasarkan pada hasil pengujian yang dilakukan maka kesimpulan yang dapat diambil adalah:

a. *Proxy* server XYZ belum memiliki sebuah aturan yang dapat digunakan untuk menolak aktivitas *scanning port* yang dilakukan oleh penyusup baik sisi *internal* maupun *external*.
b. Setelah diimplementasikan sistem IDS maka *proxy* server XYZ telah memiliki sebuah mekanisme atau aturan yang dapat digunakan untuk menolak proses *scanning port* yang dilakukan oleh penyusup baik yang dilakukan pada sisi internal maupun *external*.

1. Implementasi sistem IDS sangat efektif untuk mencegah *scanning port* oleh penyusup. Harapannya, sistem IDS dapat memotong tahapan-tahapan yang digunakan oleh penyusup dalam menguasai sumber daya yang dimiliki oleh *proxy server*.

Penelitian berikutnya dapat dikembangkan pada pembuatan sistem peringatan dini berbasis email, web atau sms. Hal ini penting, karena administrator sistem tidak harus melihat log sistem ketika terjadi proses *scanning port* pada sistem.

Daftar Pustaka

Ali, Shakeel, dan Heriyanto, Tedi. 2011. *BackTrack 4: Assuring Security by Penetration Testing- Master the art of penetration testing with BackTrack.* Packt Publishing. Birmingham – Mumbai

Gandhi, Meera, dan Srivatsa S.K.2008. Detecting and preventing attacks using network intrusion detection systems.International Journal of Computer Science and Security, Volume 2,Issue 1 : Page 49-60. ISSN (Online): 1.985-1.553. CSC Journal (http://www.cscjournals.org). Kuala Lumpur-Malaysia.

Hampton,Tavis J. 2011. *9 Server Security Threats You Should Definitely Know*. http://www.webmasterview.com /2011/03/server-security-threats/akses 9 November2012 .

Indrajit, Eko. 2011. Empat Domain kerawanan system. http://idsirtii.or.id/cyber-6/ diakses tanggal 13 November 2012.

Indrajit, Eko. 2011. Meneropong Isu Keamanan Internet Aspek Teknis, Bisnis, dan Sosial. http://idsirtii.or.id/cyber-6/ diakses tanggal 17 November 2012.

Id.wikipedia. 2011. Serangan brutal. http://id.wikipedia.org/wiki/Serangan_brutal. diakses tanggal 17 November 2012.

Sto. 2009. *CEH Certified Ectical Hacker 100% Illegal*. Penerbit Jasakom. Jakarta.

Kumar, Neeraj. 2011. Investigations in Brute Force Attack on Cellular Security Based on Des and Aes .IJCEM International Journal of Computational Engineering & Management, Vol. 14, October 2011 ISSN (Online): 2230-7893

Rebecca, B., dan Petter, M., 2002, "*Intrusion Detection System*", NIST Special Publication on IDS, USA.