IMPLEMENTASI PORTSENTRY SEBAGAI KEAMANAN SERVER UBUNTU DARI AKTIFITAS SERANGAN DI SMK NEGERI 2 PEKALONGAN

Makalah Program Studi Teknik Informatika Fakultas Komunikasi dan Informatika



Diajukan Oleh :

Nama	: Meidhita Setyaningtyas
Pembimbing 1	: Fajar Suryawan, S.T.,M.Eng. Sc, Ph.D.
Pembimbing 2	: Muhammad Kusban, S.T., M.T.

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS KOMUNIKASI DAN INFORMATIKA UNIVERSITAS MUHAMMADIYAH SURAKARTA 2013

HALAMAN PENGESAHAN

Publikasi ilmiah dengan judul :

IMPLEMENTASI PORTSENTRY SEBAGAI KEAMANAN SERVER UBUNTU DARI AKTIFITAS SERANGAN

DI SMK NEGERI 2 PEKALONGAN

Yang dipersiapkan dan disusun oleh :

Meidhita Setyaningtyas

L200090170

Telah disetujui pada:

Tanggal :

Pembimbing I

Fajar Suryawan, S.T., M.Eng. Sc, Ph.D. NIK: 924 Pembimbing II

2.02

Muhammad Kusban, S.T.,M.T. NIK: 663

Publikasi ilmiah ini telah diterima sebagai salah satu persyaratan untuk memperoleh gelar sarjana

Tanggal :

Mengetahui, etua Program Studi ikInformatika M.Sc.Ph.D Supriyono, S.T **NIK :98**

IMPLEMENTASI PORTSENTRY SEBAGAI KEAMANAN SERVER UBUNTU DARI AKTIFITAS SERANGAN DI SMK NEGERI 2 PEKALONGAN

Meidhita Setyaningtyas, Fajar Suryawan, Muhammad Kusban

Teknik Informatika, Fakultas Komunikasi dan Informatika Universitas Muhammadiyah Surakarta E-mail : meidhita@gmail.com

ABSTRAKSI

Sistem keamanan jaringan disebuah lingkungan pendidikan khususnya sekolahan merupakan faktor penting untuk menjamin stabilitas, integritas, dan validitas sebuah data. *Implementasi Instrusion Detection System* berbasis *Portsentry* dapat menghemat biaya pengadaan *software* karena bersifat gratis dan cukup handal dalam mendeteksi serangan keamanan *scanning port*.

Portsentry dapat diimplementasikan kedalam sistem operasi Ubuntu yang saat ini sudah banyak digunakan terutama di SMK Negeri 2 Pekalongan. Sebuah serangan *scanning port* dapat terdeteksi dan dilihat jejaknya pada *Syslog*.

Berdasarkan hasil pengujian sistem Porsentry dengan port scan dapat memberikan peringatan adanya serangan keamanan terhadap sistem melalui paket-paket yang melewati jaringan. Hasil tersebut dapat digunakan sebagai acuan untuk menentukan kebijakan keamanan jaringan sekolah.

Kata Kunci: Portsentry, NMAP, Instrusion Detection System, Ubuntu

PENDAHULUAN

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Sementara itu. masalah keamanan ini masih seringkali kurang mendapat perhatian, seringkali masalah keamanan ini berada diurutan kedua, atau bahkan diurutan terakhir dalam daftar halhal yang dianggap kurang penting. Apabila menggangu informasi dari sistem, seringkali keamanan dikurangi atau ditiadakan (Rahardjo, 2002).

Salah satu cara untuk meningkatkan keamanan server dalam jaringan adalah dengan firewall. Implementasi dari sistem firewall ini dapat berupa software ataupun hardware yang bersifat aktif dengan melakukan penyaringan paket data yang lewat berdasarkan pengaturan yang diinginkan. Portsentry merupakan salah program aplikasi *firewall* satu yang digunakan untuk menghalau berbagai macam aktifitas serangan seperti sasaran scanning keamanan maupun virus jaringan.

Dalam hal ini peneliti ingin mencoba mengimplementasikan aplikasi *portsentry* ini kedalam *PC* server di SMK Negeri 2 Pekalongan dengan menggunakan sistem operasi Ubuntu. Dengan *portsentry* ini diharapkan *PC* server bisa terlindungi dari aktifitas serangan seperti percobaan *probe, scanning port.* Karena SMK Negeri 2 Pekalongan juga menjadi *ICT center* di kota Pekalongan, sehingga keamanan data di SMK Negeri 2 Pekalongan perlu terlindungi. *Portsentry* didesain untuk mendeteksi dan merespon kegiatan *scanning port* secara *real time*.

Penelitian ini membahas tentang langkah perlindungan untuk server Ubuntu dari aktifitas *probe* dan *scanninf port* dengan menginstall *portsentry* kedalam sistem, dan juga melihat hasil dari implementasi *portsentry* tersebut. Salah satu pemanfaatan *portsentry* ini juga bisa memblokir port TCP maupun UDP yang dianggap melakukan aktifitas serangan.

Berdasarkan hal tersebut maka peneliti mengangkat judul "Implementasi Portsentry sebagai Keamanan Server Ubuntu Dari Aktifitas Serangan Di SMK Negeri 2 Pekalongan".

TINJAUAN PUSTAKA

Penelitian terdahulu yang berhubungan dengan penelitian yang dilakukan oleh peneliti saat ini adalah penelitian yang berjudul "Implementasi Snort Sebagai Tool Instrusion Detection System Pada Server FreeBsd di PT. Power Telecom". Pada penelitiannya Atiq menggunakan snort sebagai tool Instrusion Detection mendeteksi System untuk serangan pada jaringan. (Atiq, 2012).

Mahardika, Irfan (2003). Secure Remote Login Pada Sistem Operasi Slackware Linux. Dalam skripsinya ini mahardika memanfaatkan perangkat lunak IDS yaitu remote login untuk mendeteksi terhadap adanya serangan keamanan sistem. Remote Login SSH dengan menggunkan kunci publik dan kunci privat vang dibuat oleh klien, memungkinkan *remote login* dapat dilakukan dengan aman tanpa memberikan username dan password digunakan untuk login yang pada komputer.

Alamsyah (2011). Implementasi Instrusion Detection System (IDS) dan Instrusion Prevention System (IPS)Menggunakan Clearos. Pada penelitian ini menyebutkan bahwa dengan adanya Instrusion Detection System (IDS) dan Instrusion Prevention System (IPS, maka serangan-serangan tersebut dapat dicegah ataupun dihilangkan. IDS berguna untuk mendeteksi adanya serangan dari penyusup, sedangkan IPS berguna untuk mendeteksi serangan dan memblokir serangan.

Penelitian-penelitian diatas adalah semua penelitian yang menggunakan tool Instrusion Detection System sebagai objek penelitian. Disini penulis ingin mencoba mengimplementasikan salah satu tool yang termasuk tool Instrusion Detection System yaitu portsentry untuk dipasang di PC server SMK Negeri 2 Pekalongan.

METODE

Metodologi penelitian yang dilakukan yaitu Tahap pertama merupakan tahapan dimana proses penelitian dimulai dengan mengumpulkan bahan dan data yang akan dikerjakan dan dilanjutkan dengan merancang dan mengkonfigurasi. Tahap kedua adalah proses lanjutan dari tahap pertama yang sudah terselesaikan. Tahap kedua terdiri dari evaluasi konfigurasi server dan pengujian simulasi Tahap ketiga Adalah server. tahap penyelesaian penelitian apabila data sudah lengkap dilanjutkan dengan penulisan laporan penelitian.



Gambar 1. Skema Jaringan Penelitian

Langkah pengujian sistem yaitu:

 Instalasi dan Konfigurasi Portsentry Instalasi Portsentry pada ubuntu 12.04 ketik perintah *sudo apt-get install portsentry* pada terminal. Setelah portsentry terisntall, portsentry mulai memonitoring pada berbagai port TCP dan UDP.

igubuntu: -	
ubuntu@ubuntu:-5 grep portsentry /var/log/syslog	
May 28 86:58:12 ubuntu portsentry[1217]: adminalert: Po	ortSentry 1.2 is starting.
May 28 86:58:12 ubuntu portsentry[1218]: adminalert: Go	oing into Listen mode on TCP port: 1
May 28 86:58:12 ubuntu portsentry[1218]: advinalert: Co	oing into Listen mode on TCP port: 11
<pre>Hay 28 86:58:12 ubuntu portsentry[1218]: adminalert: Co</pre>	oing into listen mode on TCP port: 15
May 28 86:58:12 ubuntu portsentry[1218]: adminalert: Go	oing into listen mode on TCP port: 79
May 28 86:58:12 ubuntu portsentry[1218]: adminalert: Ge	oing into Listen mode on TCP port: 111
May 28 86:58:12 ubuntu portsentry[1218]: adminalert: Co	oing into Listen mode on TCP port: 119
May 28 86:58:12 ubuntu portsentry[1218]: adminalert: Go	oing into Listen mode on TCP port: 143
May 28 86:58:12 ubuntu portsentry[1218]: adminalert: Ge	oing into Listen mode on TCP port: 548
May 28 86:58:12 ubuntu portsentry[1218]: adminalert: Ge	oing into Listen mode on TCP port: 635
May 28 86:58:12 ubuntu portsentry[1218]: adminalert: Ge	oing into listen mode on TCP port: 1080
[Hay 28 86:58:12 ubuntu portsentry[1218]: adminalert: Ge	oing into Listen mode on TCP port: 1524
May 28 86:58:12 ubuntu portsentry[1218]: adminalert: Go	oing into listen mode on TCP port: 2080
May 28 86:58:12 ubuntu portsentry[1218]: adminalert: Go	oing into Listen mode on TCP port: 5742
Hay 28 86:58:12 ubuntu portsentry[1218]: adminalert: Co	oing into Listen mode on TCP port: 6667
May 28 86:58:12 ubuntu portsentry[1218]: adminalert: Go	oing into Listen mode on TCP port: 12345
<pre>Hay 28 86:58:12 ubuntu portsentry[1218]: adminalert: Go</pre>	oing into Listen mode on TCP port: 12346
Hay 28 86:58:12 ubuntu portsentry[1218]: advinalert: Go	oing into Listen mode on TCP port: 20834
[Hay 28 86:58:12 ubuntu portsontry[1218]: gdwinalert: Go	oing into listen mode on TCP port: 27665
Hay 28 86:58:12 ubuntu portsentry[1218]: advinalert: Go	oing into Listen mode on TCP port: 31337
May 28 86:58:12 ubuntu portsentry[1218]: adminalert: Ge	oing into Listen mode on TCP port: 32771
Hay 28 86:58:12 ubuntu portsentry[1218]: adminalert: Go	oing into Listen mode on TCP port: 32772
May 28 86:58:12 ubuntu portsentry[1218]: adminalert: Ge	oing into Listen mode on TCP port: 32773
May 28 86:58:12 ubuntu portsentry[1218]: adminalert: Go	oing into Listen mode on TCP port: 32774
May 28 86:58:12 ubuntu portsentry[1218]: adminalert: Go	oing into Listen mode on TCP port: 40421
May 28 86:58:12 ubuntu portsentry[1218]: adminalert: Go	oing into Listen mode on TCP port: 49724
Hay 28 86:58:12 ubuntu portsentry[1218]: advinalert: Go	oing into listen mode on TCP port: 54328
Hay 28 86:58:12 ubuntu portsentry[1218]: adminalert: Po	ortSentry is now active and listening.
May 28 86:58:13 ubuntu portsentry[1221]: adminalert: Personal Providence Person Providence Person	ortSentry 1.2 is starting:

Gambar 2. Indikator keberhasilan

Untuk bisa menjalankan portsentry secara maksimal ada beberapa file pada portsentry yang harus dikonfigurasi yaitu :

a. File /etc/portsentry/portsentry.conf

Merupakan konfigurasi utama portsentry. Disini secara bertahap diset port mana saja yang perlu di monitor, untuk mereject koneksi penyerang dengan *iptables* dan memfilter IP *host* penyerang melalui *TCP wrapper*. Untuk mengedit file /*etc/portsentry/portsentry.conf* dengan cara mengetikkan perintah *sudo gedit* /*etc/portsentry/portsentry.conf*

b. File/etc/portsentry/portsentry.ignore .static

Berisi semua IP address di LAN yang akan diabaikan oleh portsentry. Digunakan jika ingin IP address tertentu agar tidak terblokir secara tidak sengaja.

c. File /etc/default/portsentry

Pada server IDS terdapat file /etc/default/portsentry, untuk memilih mode TCP dan UDP ketika portsentry mendeteksi port TCP/UDP, memilih mode deteksi *port* sesuai dengan yang ditentukan di *portsentry.conf* atau mode *advanced* dan menambah deteksi *stealth scan*.

HASIL DAN PEMBAHASAN

Serangan keamanan yang sering terjadi sebagai bagian untuk melakukan instrusi terhadap suatu sistem dapat berupa *nmap port scan, virus, dan buffer overflow.* Oleh karena itu, langkah pengujian sistem portsentry dalam penelitian ini dilakukan pengujian port scanning.

a. Pengujian 1 : Port scan menggunakan NMAP

Hasil pengujian port scan dengan perintah Nmap -sS -sU -T4 -A -v 192 .168.170.128 dari client dengan IP address 192.168.170.1

7еппир	_	-			-	4 XX
Scan Tools Profile Lle	lp					
Target 192.168.170.128	-	Profile	portsentry	-	Scan	Cance
Command: nmap - s5 -sU	- 14 - A - v - Po -	PU 192150	170128			
Hosts Services	Nmap Qulp	ul Ports/	Hosts Topplogy	Host Details Sri	ans	
OS + Host +	nmap -sS-st	1-TA-A-V	-PS -PU 192.168.170	128	- 1	Detai
M 1921180175129	Granting Complete Upial 100 Complete Oragizet Objectures Discourse	ARP Pin (s) (s) (s) (s) (s) (s) (s) (s) (s) (s)	170-128 [] part 5 ster st 20 20 1 DVs resolution 1 DVs resolution 1 DVs resolution 1 DVs resolution 1 DVs resolution 10/128 [2000 pr 112/128 [2000 pr 1225/129 or 1225/129 or 1215/129 or 12	1 0.445 elappy or of 1 host. r	sed (1 	2 20 213 215, 259 200, 20
Filter Heste	(mage 14)					+

Gambar 3. Hasil scanning port menggunakan NMAP

Maksud dari perintah scan pada pengujian ini adalah memerintahkan nmap untuk melakukan scanning port dengan maksud –sS untuk scanning port yang menggunakan TCP SYN, -sU untuk scanning dengan UDP, -T4 untuk memindah semua perangkat, -A –v untuk scan sistem operasi dan versi yang digunakan

b. Menghapus IP yang tersaring TCP Wrapper

Untuk membuka kembali koneksi komputer penyerang dengan komputer IDS sebagai target yaitu dengan mengedit file /etc/hosts.deny dan hapus IP address yang terdapat di kernel IP routing table. Di dalam file /etc/hosts.deny terdapat no IP address penyerang yang terfilter oleh TCP wrapper.

> #ALL: 10.225.104.227 : DENY #ALL: 192.168.170.1 : DENY

Gambar 4. file /etc/hosts.deny

Jika ingin membuka IP yang terblokir oleh *TCP wrapper* maka harus menambahkan tanda (#) di depan *ALL:* 192.168.170.1 : DENY. Dan selanjutnya menjalankan perintah # route del –host 192.168.170.1 reject.

c. Instalasi dan Konfigurasi *Logcheck*

Logcheck adalah program yang berfungsi mencari pattern/bentuk tertentu (menyaring informasi penting) yang kita inginkan dalam file-file logging lalu mengirimkan laporannya kepada admin, misalnya melalui email.

Ne Carl Andrew Contraction (Contraction Contraction Co
ubuntu@ubuntu:-5_sudo_apt-get_install_logcheck
Reading package lists Done
Building dependency tree
Reading state information Done
Suggested packages: syslog-summary
The following NEW packages will be installed: logcheck
0 upgraded, 1 newly installed, 0 to remove and 272 not upgraded. Need to get 0 8/31.6 kB of archives.
After this operation, 295 kB of additional disk space will be used. Selecting previously unselected package logcheck.
(Reading database 146598 files and directories currently installed. Unpacking logcheck (from/logcheck 1.3.14 all.deb)
Processing triggers for man-db
Setting up logcheck (1.3.14)
ubustukubustu: E

Gambar 5. Instalasi logcheck

Pada gambar diatas server IDS menjalankan *\$ sudo apt-get install logcheck* untuk instalasi melalui terminal yang harus terkoneksi dengan *internet*.

📄 logcheck.conf 🗱
The following variable settings are the initial default values,
which can be uncommented and modified to alter logcheck's behaviour
Controls the format of date-/time-stamps in subject lines:
Alternatively, set the format to suit your locale
#DAIE="\$(date +'%Y-%m-%d %H:%M')"
Controls the presence of boilerplate at the top of each message:
Alternatively, set to "0" to disable the introduction.

IT the files /etc/togcheck/header.ixt and /etc/togcheck/fooler.ixt
footer of any generated mails.
#TNTRO=1
Controls the level of filtering:
Can be Set to "workstation", "server" or "paranoid" for different
levels of filtering. Defaults to server if not set.
REPORTLEVEL="server"
π Controls the address mail goes to:
NOTE the script does not set a default value for this variable!
Should be set to an offsite "emailaddress@some.domain.tld"
SENDMAILTO="logcheck"

Gambar 6. Konfigurasi di logcheck.conf

Pada gambar 4.8 diatas server IDS mensetting alamat email admin yang akan digunakan, beberapa yang harus diubah yaitu

INTRO=1;

REPORTLEVEL="server"; SENDMAILTO="logcheck"; ADDTAG="yes" File kedua yang harus diedit yaitu *logcheck.logfiles* untuk menambahkan beberapa *path* baris untuk melengkapi log saat diperiksa tambahkan baris berikut:

> /var/log/syslog /var/log/auth.log /var/log/sulog



Gambar 7. Instalasi Cron

Gambar diatas memperlihatkan bahwa server menginstall *cron, cron* digunakan untuk mengatur waktu laporan email saat mengirimkan laporan pemeriksaan sistem ke *administrator* dan kita bisa melihat isi dari file *cron* dengan perintah *ls /etc/cron*

Gambar 8. Melihat email di terminal

Perintah *sudo mail* digunakan untuk melihat *email* yang masuk seperti pada gambar diatas



Gambar 9. Melihat isi *email* perintah sudo

gedit /var/mail/root

Melihat isi dari *email* tersebut menggunakan perintah *sudo gedit* /*var/mail/root* seperti pada gambar diatas.

KESIMPULAN

Kesimpulan yang dapat diambil dari penelitian implementasi *Portsentry* sebagai keamanan server ubuntu dari aktifitas serangan di SMK Negeri 2 Pekalongan adalah :

- Berdasarkan hasil pengujian yang dilakukan, *Portsentry* dapat diimplementasikan sebagai *Instrusion Detection System* pada sistem operasi Ubuntu 12.04 untuk mendeteksi scanning port.
- 2. Portsentry dapat memberikan peringatan adanya sebuah aktifitas *scanning port*, sehingga dapat meningkatkan keamanan jaringan melalui paket-paket yang melewati jaringan.

DAFTAR PUSTAKA

- Abdullah, Miftah Faridl,2011.,"Analisis danPerancangan management bandwidth Dengan Menggunakan Mikrotik di Telecenter Kertonegoro Ngawi". Skripsi. Yogyakarta : Fakultas Tekhnik Informatika, AMIKOM.
- Ardi, Sasotya (2012). "Analisa sistem antrian pada RouterBoard 751 dengan multikoneksi". Skripsi Surakarta : Fakultas Teknik Informatika Universitas muhammadiyah Surakarta.
- Basyir, Hafid Abdullah. 2010. "Analisa dan Perancangan Warnet SMART.NET di Bantul dengan Menggunakan Provider Telkom Speedy". Naskah Publikasi.
 Yogyakarta : Sekolah Tinggi Manajemen Informatika dan komputer, Amikom.
- Mujahidin, Tafaul (2011). "OS Mikrotik Sebagai Management Bandwidth Dengan Menerapkan Metode Per Connection Queue". Skripsi: Yogyakarta : Fakultas Teknik Informatika AMIKOM.
- Prabowo, Tito (2010). "Management Bandwidth menggunakan Queue Tree Pada RT/RW Net di Dusun Sulang Kidul Patalan Jetis Bantul Yogyakarta". Skripsi Yogyakarta : Fakultas Teknik Informatika AMIKOM.

Wardhana, Asoka. 2006. "*Modul basic mikrotik Router OS*".Jakarta: Asoka Wardhana. <u>http://digilib.its.ac.id/public/ITS-Undergraudate-11008-2297100037-Chapter1.pdf</u>

diakses tanggal 26 september 2012

http://wiki.mikrotik.com/wiki/Manual:HTB diakses tanggal 26 september 2012 http://repository.usu.ac.id/bitstream/123456789/21077/4/Chapter%2011.pdf diakses

tanggal 25 september 2011

BIODATA PENULIS

Nama	: Meidhita Setyaningtyas
TempatdanTanggalLahir	: Pekalongan, 1 Mei 1991
JenisKelamin	: Perempuan
Agama	: Islam
PerguruanTinggi	: Universitas Muhammadiyah Surakarta
Fakultas	: Fakultas Komunikasi dan Informatika
Jurusan	: Teknik Informatika
Alamat	: Jl. A. YaniTromolPos I Pabelan, Kartasura
Telp./ Fax	: (0271) 717417
AlamatRumah	: Jl. Irian No. 9 Gg.4 Sapuro Pekalongan
No. HP	: 085727979224
Alamat e-mail	: meidhita@gmail.com