

SISTEM PENGAMANAN JARINGAN ADMIN SERVER DENGAN METODE *INTRUSION DETECTION SYSTEM (IDS) SNORT* MENGGUNAKAN SISTEM OPERASI *CLEAROS*

Suhartono

Pendidikan Teknik Informatika dan Komputer
Universitas Negeri Makassar
Email: suhartonoft@unm.ac.id

Abstract. This type of research is R & D (Research and Development), which aims to build a network monitoring system admin server admin with the base operating system is ClearOS. The method used in monitoring system of network security server admin is with 4D model (four-D model). The 4D model (four-D model) consists of several stages - defining, designing, developing and testing. The results of this research is a server admin server security system that provides convenience to server admin to monitor server performance, monitoring attacks by hackers, attackers, and intruders and able to detect and overcome SSH bruteforce and FTP bruteforce attacks.

Absrak. Jenis penelitian ini adalah penelitian R & D (*Research And Development*), yang bertujuan untuk membangun sistem monitoring keamanan jaringan admin server dengan basis sistem operasi adalah *ClearOS*. Metode yang digunakan dalam sistem monitoring keamanan jaringan admin server ini adalah dengan model 4D (four-D model). Model 4D (four-D model) terdiri dari beberapa tahapan – tahapan yaitu pendefinisian, perancangan, pengembangan dan uji coba. Hasil penelitian ini adalah sebuah sistem pengamanan jaringan admin server yang memberikan kemudahan terhadap admin server untuk memonitor kinerja server, monitoring serangan yang dilakukan oleh *hacker*, *attacker*, dan *intruder* serta mampu mendeteksi dan mengatasi serangan SSH *bruteforce* dan FTP *bruteforce*.

Kata Kunci : ClearOS, 4D, Admin Server, SSH *bruteforce*, FTP *bruteforce*, *Intrusion Detection System Snort* (IDS Snort).

Keamanan teknologi informasi (IT) merupakan sebuah hal mendasar yang penting untuk diperhatikan dalam sebuah lingkaran organisasi maupun individu. Berbagai serangan terhadap server pada organisasi hingga pembajakan akun pada individu, apapun bentuknya tindakan ini hanya mendatangkan kerugian. Menurut ID-SIRTII (*Indonesia Security Incident Response Team On Internet Infrastructure*). Adanya perangkat teknologi yang serba *modern* atau canggih akan tidak ada artinya tanpa diimbangi oleh pengaturan dan penggunaan secara tepat efektif dan efesien. Perangkat yang sederhana namun dikelola secara tepat bias menstabilkan bahkan akan sangat membantu terhadap perkembangan perusahaan, hal tersebut disebabkan keterbatasan *resource* sehingga

harus betul-betul memanfaatkan teknologi yang dimiliki.

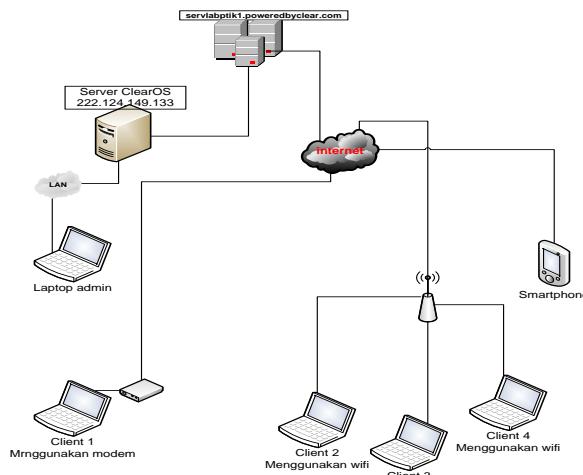
Suatu teknologi jaringan memerlukan yang namanya manajemen jaringan yang fungsinya adalah untuk mengelola seluruh *resource* di jaringan agar bisa memberikan *good services* kepada penggunanya. Mengutip suatu definisi dari Mathews, D.C, bahwa proses suatu manajemen itu adalah “suatu proses yang ditunjukan untuk mempresentasikan pengetahuan suatu organisasi kepada suatu langkah kongkrut yang akan menghasilkan sesuatu yang diharapkan: (Kumar , 2002).

METODE PENELITIAN

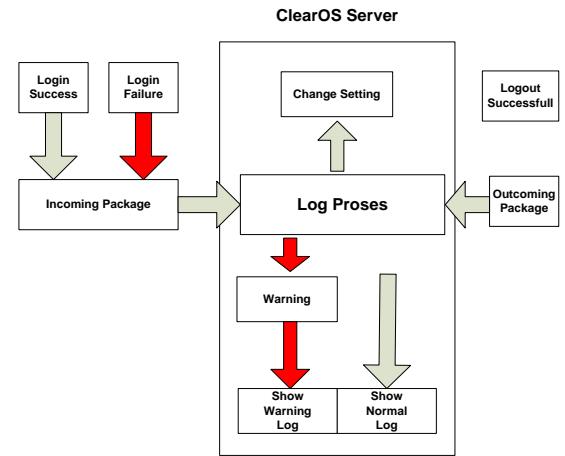
Penelitian ini penulis menggunakan penelitian *Research and Development* (R&D). Menurut Sugiyono (2009:407) metode penelitian

Research and Development yang selanjutnya akan disingkat menjadi R&D adalah metode penelitian yang digunakan untuk menghasilkan produk tertentu, dan menguji keefektifan produk tersebut.

Penelitian ini akan menggunakan metode pengembangan (*development research*) dengan menggunakan pendekatan pengembangan model 4D (four-D model) yang dikemukakan oleh Sivasailam Thiagarajan dkk (1974). Adapun tahapan model pengembangan meliputi tahap pendefinisian (*define*), tahap perancangan (*design*), tahap pengembangan (*develop*) dan tahap ujicoba (*disseminate*). Tahapan yang dilakukan pada penelitian ini baru sampai pada tahap pengembangan (*develop*). Laboratorium PTIK telah memiliki jaringan yang memadai untuk memberikan *service* kepada *client* dalam lingkup besar. Walaupun begitu, keamanan dan kelangsungan jaringan yang ada pada sistem tersebut harus dijaga dan harus dipikirkan strategi penerapan keamanan tersebut. Adapun gambaran umum dari topologinya seperti pada Gambar 1.



Gambar 1
Desain Topologi Jaringan Lab PTIK



Gambar 2.
Alur Kerja ClearOS

Berdasarkan hasil studi literatur diambil simpulan dari berbagai penelitian serupa yang pernah dilakukan untuk menentukan alur sistem terbaik dan sesuai dengan studi kasus penelitian. Desain topologi jaringan yang digunakan tetap dengan model yang sama dengan desain topologi jaringan awal. Perubahan yang dilakukan untuk mengubah Mikrotik menjadi sistem RIDS yaitu penggunaan *firewall* dan mail. Alur kerja *Intrusion Detection System* berawal dari pendektsian paket data yang dianggap berbahaya oleh *firewall*, berikut urutan tindakan yang dilakukan *firewall*.

PEMBAHASAN

Konfigurasi *alert notifications* ini merupakan tahap dimana setiap serangan yang akan masuk ke dalam system server akan terkirim ke *email admin server*.

```

IP=$(echo $SSH_CONNECTION | cut -d " " -f 1)
HOSTNAME=$222.124.149.133/29
NOW=$(date + "%e %b %Y, %a %r")
  
```

```

echo 'SOMEONE from '$IP' logged into '$HOSTNAME'
on '$NOW.' | mail -s 'SSH Login Notification'
servlabptik.unm@gmail.com
echo 'ALERT - SOMEONE Access on:' `date` `who` |
mail -s "Alert: Someone Access from `who | cut -d "(" -f2 |
cut -d ")" -f1`" servlabptik.unm@gmail.com
  
```

```
# JAILS
#
# SSH servers
#
[sshd]
enabled = true
filter = sshd
action = iptables[name=SSH, port=22, protocol=tcp]
    sendmail-whois[name=SSH,
dest=servlabptik.unm@gmail.com,
sender=servlabptik.unm@gmail.com, sendername="ATTACK
DETECTOR"]
maxretry = 5
bantime = 600
logpath = /var/log/secure
port = ssh
logpath = %(sshd_log)s
backend = %(sshd_backend)s
[sshd-ddos]
# This jail corresponds to the standard configuration in Fail2ban.
# The mail-whois action send a notification e-mail with a whois
request
# in the body.
enabled = true
filter = sshd-ddos
action = iptables[name=SSH, port=22, protocol=tcp]
    sendmail-whois[name=SSH,
dest=servlabptik.unm@gmail.com,
sender=servlabptik.unm@gmail.com, sendername=ATTACK
DETECTOR"]
maxretry = 5
bantime = 600
logpath = /var/log/secure
port = ssh
logpath = %(sshd_log)s
backend = %(sshd_backend)s
```

Gambar 3 *Source code* untuk SSH

```
# 
# FTP servers
#
[proftpd]
enabled = true
filter = proftpd
action = iptables[name=ProFTPD, port=21,
protocol=tcp]
    sendmail-whois[name=ProFTPD,
dest=servlabptik.unm@gmail.com,
sender=servlabptik.unm@gmail.com,
sendername="FTP ATTACK DETECTOR"]
logpath = /var/log/secure
maxretry = 5
bantime = 600
port = ftp,ftp-data,ftps,ftps-data
logpath = %(proftpd_log)s
backend = %(proftpd_backend)s
```

Gambar 4 *Source code* untuk FTP

```
[sshd-ddos]
enabled = true
filter = sshd-ddos
action = iptables[name=SSH, port=22,
protocol=tcp]
    sendmail-whois[name=SSH,
dest=labptik.unm@gmail.com,
sender=servlabptik.unm@gmail.com,
sendername="ATTACK DETECTOR"]
maxretry = 5
bantime = 600
```

Gambar 5
Source code untuk SSH

```
[proftpd]
enabled = true
filter = proftpd
action = iptables[name=ProFTPD, port=21,
protocol=tcp]
    sendmail-whois[name=ProFTPD,
dest=servlabptik.unm@gmail.com,
sender=servlabptik.unm@gmail.com,
sendername="FTP ATTACK DETECTOR"]
logpath = /var/log/proftpd.log
maxretry = 5
```

Gambar 6
Source code untuk mendeteksi serangan FTP

Secara umum, penerapan IDS dengan menggunakan data percobaan terhadap IP Public server 1048m2yjx3.poweredbyclear.com secara langsung dilakukan dengan beberapa parameter yang dapat dilihat pada Tabel 1 agar mendapatkan hasil dengan kondisi yang sama.

Tabel 1. Parameter Implementasi IDS terhadap jaringan Server *ClearOS*

No.	Jenis Percobaan	Lama Percobaan	Tool yang digunakan	Objek Percobaan
1.	FTP Attack	15 hari	Login FTP di WinSCP	FTP Server ClearOS
2.	SSH Attack		PuTTY	Port SSH ClearOS

Uji Sistem Terhadap Serangan

Pengujian dilakukan untuk mengetahui keberhasilan sistem. *IDS* ini akan berhasil jika *admin* jaringan server ClearOS yang terdapat di Lab.PTIK UNM bisa dengan mudah melakukan monitoring jaringan, mengetahui jenis serangan yang sedang menyerang sistem yang di monitoringnya, dan menerima laporan serangan dimanapun *admin* jaringan berada dengan syarat *admin* jaringan memiliki *gadget* yang memungkinkan untuk terhubung ke email kapan saja.

Email ClearOS

Pengujian pada *email* merupakan tahapan perencanaan sebelum masuk ke inti sistem. Pengujian ini dilakukan untuk mengetahui bahwa email pengirim pada Server ClearOS telah terkoneksi dengan email penerima. Pengujian dilakukan dengan melakukan pengiriman secara manual tanpa terhubung ke *script* dan *scheduler* manapun. Berikut adalah perintah untuk melakukan pengiriman *email* secara manual.

```
echo "Percobaan dilakukan untuk menguji apakah server telah  
terhubung dengan gmail" | mailx -s "Testing Mail"  
servlabptik.unm@gmail.com
```

Gambar 7
Script untuk mengirim email secara manual

Implementasi Sistem IDS

Pengujian sistem *IDS* ini akan menghasilkan data dan informasi yang dibutuhkan untuk mengambil kesimpulan di akhir penelitian. Berdasarkan batasan masalah yang telah dibahas pada bab sebelumnya, pengujian sistem *IDS* akan dilakukan dengan melakukan serangan-serangan ke IP Publik server Lab PTIK.

Penulis melakukan percobaan melakukan serangan melalui dua port jaringan yaitu, *SSH* dan *FTP*. *SSH* dan *FTP* merupakan port yang paling rentan akan serangan yang dilakukan oleh attacker. Tipe serangan yang dilakukan adalah *SSH Bruteforce* dan *FTP bruteforce*. Serangan *SSH bruteforce* dan *FTP bruteforce* ini bertujuan untuk

mengeksplorasi sistem seseorang dengan mencoba masuk kedalam sistem menggunakan *user* dan *password* yang salah. Penulis merancang dan menkonfigurasi sistem keamanan dengan *IDS* dan menggunakan *ClearOS*. Dalam sistem keamanan ini *IDS* berfungsi untuk mendeteksi penyusupan yang coba dilakukan oleh *attacker*.

KESIMPULAN

Berdasarkan penelitian dan pengujian yang sudah dilakukan mengenai sistem pengamanan jaringan server dengan metode *IDS* (*Intrusion Detection System*) *Snort* berbasis *ClearOS*, penulis dapat menarik beberapa kesimpulan sebagai berikut:

1. Sistem keamanan jaringan server dengan metode *IDS* menggunakan *ClearOS* pada Lab. PTIK dibangun dalam 2 langkah :
 - a. Implementasi *IDS*

Penerapan Sistem *IDS* dengan menggunakan data percobaan terhadap *traffic* jaringan server Lab.PTIK secara langsung dilakukan dengan beberapa parameter yaitu *FTP Bruteforce*, dan *SSH Bruteforce*

- b. Pengujian Sistem

Pengujian dilakukan secara bertahap yang terdiri dari :

- a) Pengujian Email (Email Server)
Pengujian dilakukan dengan melakukan pengiriman secara manual
 - b) Sistem *IDS*
pengujian sistem *RIDS* dilakukan dengan melakukan serangan-serangan ke jaringan server Lab. PTIK dengan parameter implementasi.
2. Untuk menampilkan *report* serangan dalam bentuk *log* dan *mailreport* secara otomatis pada mikrotik dilakukan melalui *FTP Bruteforce* dan *SSH Bruteforce*

DAFTAR PUSTAKA

Andri, Kristanto. 2003. Jaringan Komputer. Graha Ilmu.

Jack Febrian & Farida Andayani. 2012 “Kamus Komputer dan Istilah Teknologi Informasi” Bandung:Informatika

Jogiyanto, Hartono. 2009. Analisis dan Desain Sistem Informasi, Edisi III. Yogyakarta: ANDI.

Kumar, 2002 . Management of Hospital. Hospital Administration In the 21 Century. New Delhi: Deep &Deep Publication. PVT.LTD

Micro, Andi. 2012. Buku Hijau Clear OS 5.2 Edisi Revisi. Banjarbaru. Andi Micro.

O'Brien, James A. dan Marakas, George M. 2011. “Management Information Systems, 10th Edition”. McGraw-Hill/ Irwin, New York

Odon, Wendel, 2005.Computer Network First Step, Penerbit Andi : Yogyakarta

Oskar Pearson. 2003 “ Squid A User's Guide” From <http://www.squid-cache.org> (diakses 00.30 21 Desember 2012)

Setyosari, Punaji. 2010. Metode Penelitian Pendidikan dan Pengembangan, Jakarta : Kencana.

Sofana, Iwan. 2008. Membangun Jaringan Komputer (Membuat Jaringan Komputer (Wire & Wireless) untuk Windows dan Linux. Informatika. Bandung.

Sugiyono. 2009. Metode Penelitian Bisnis (Pendekatan Kuantitatif, Kualitatif, dan R&D). Bandung: Alfabeta.

Sukmaaji, Anjik, S.Kom & R Rianto S.Kom. 2008. “Jaringan Komputer: K'onsep Dasar Pengembangan Jaringan Dan Keamanan Jaringan” Yogyakarta: Andi Offset.

Sutanta, Edhy. 2005. Komunikasi data dan Jaringan Komputer. Yogyakarta: Graha Ilmu.

Wagito. 2007. “Jaringan Komputer (Teori dan Implementasi Berbasis Linux)” Yogyakarta: Gava Media