VISUALISASI MONITORING *PORT* MENGGUNAKAN *SHOREWALL* DAN *LOG ANALIZER*

Imam Riadi[1)] **Eko Brillianto**[2)]
[1)]Program Studi Ilmu Komputer, [2)]Program Studi Teknik Informatika
Universitas Ahmad Dahlan Yogyakarta
Jl. Prof. Soepomo, Janturan, Yogyakarta Telp (0274)-379418
e-mail : imam_riadi@uad.ac.id

Abstrak

Firewall merupakan suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua kegiatan suatu segmen pada jaringan lokal dengan jaringan luar yang bukan merupakan ruang lingkupnya. Dalam penelitian ini akan dilakukan proses memonitor port firewall pada sistem keamanan jaringan komputer menggunakan sebuah interface untuk meningkatkan kinerja jaringan komputer dan memfilter permintaan klien serta dapat mengatur user-user yang ada. Berdasarkan hasil penelitian ini menunjukkan bahwa proses monitoring port TCP dan UDP, logging sebuah server jaringan komputer komputer dapat berjalan dengan baik memberikan proteksi terhadap serangan yang dilakukan oleh pihak yang tidak bertanggung jawab.

Keyword *: Visualisasi, Monitoring, Port, Shorewall, Log Analizer*

1. PENDAHULUAN

Firewall merupakan suatu cara atau mekanisme yang diterapkan baik terhadap *hardware, software* ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua kegiatan suatu segmen pada jaringan lokal dengan jaringan luar yang bukan merupakan ruang lingkupnya. Firewall untuk komputer, pertama kali dilakukan dengan menggunakan prinsip "*non-routing*" pada sebuah Unix host yang menggunakan 2 buah network *interface card, network interface card* yang pertama di hubungkan ke Internet (jaringan lain) sedangkan yang lainnya dihubungkan ke komputer lokal. Untuk dapat terkoneksi dengan Internet maka harus memasuki server *firewall* (bisa secara *remote*, atau langsung), kemudian menggunakan *resource* yang ada pada komputer tersebut untuk berhubungan dengan Internet.

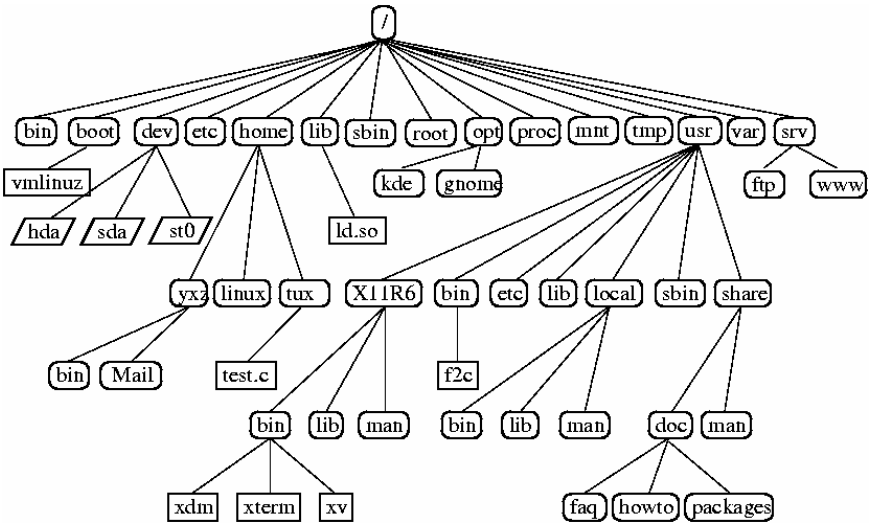
2. TINJAUAN PUSTAKA

1. GNU/LINUX

Platform Linux memiliki kemampuan dikonfigurasikan yang tinggi, stabil dan mudah dipahami serta memiliki banyak produk yang berhubungan dengan keamanan. Namun, hal paling menarik dari Linux, adalah sifat terbukanya. Bahkan, Linux lebih terbuka dari OpenBSD, dan banyak orang di industri keamanan lebih senang kepada prinsip untuk mengungkapkan *source code* kepada siapa pun untuk mencari *error* dan *vulnerability*.

Keuntungan lain dari Linux adalah sebuah fakta financial sederhana: *source code* Linux didistribusikan dengan Cuma-Cuma, Tetapi Linux bukan hanya sekedar menawarkan daya dari *source code* Linux; tetapi juga kebebasan untuk memodifikasi sistem operasi dengan cara-cara yang fundamental untuk memenuhi kebutuhan sebuah organisasi. Hal ini bisa menjadi hal yang kontras dengan meningkatnya sifat pembatasan dan mahalnya lisensi-lisensi *software* lain.

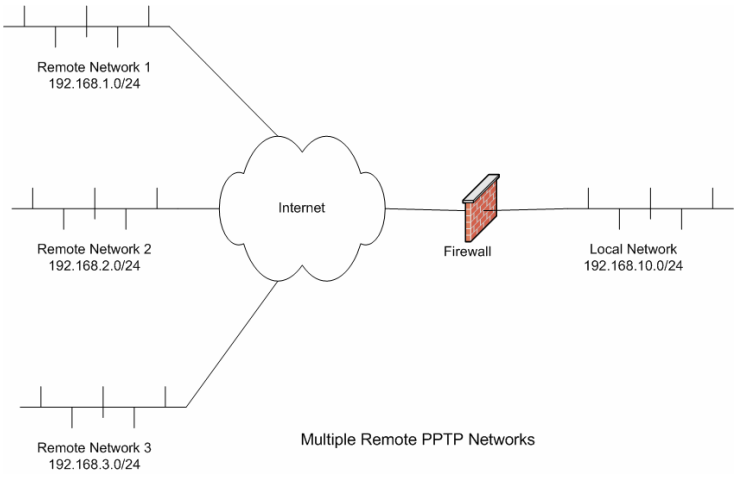
Selama dua tahun terakhir, semua vendor hardware besar telah mengumumkan system yang berjalan pada Linux, bersama dengan dukungan teknis untuk Linux. Bahkan vendor *software* besar telah mengumumkan Linux sebagai sistem operasi pilihan, termasuk Oracle, yang memindahkan semua database Oracle internal-nya ke *platform* tersebut.



Gambar 1. Struktur direktori *filesystem* Linux

2. Shorewall

Shorewall dikenal sebagai aplikasi *firewall* yang populer. *firewall* berlisensi GPL (*GNU Public License)* atau *open source* yang dalam pembuatannya melibatkan banyak orang atau organisasi. Shorewall adalah aplikasi untuk mengkonfigurasi Netfilter di Linux, kita dapat mengkonfigurasi *firewall* dengan menggunakan *interface* yang sudah tersedia di Shorewall, selain itu Shorewall merupakan *Firewall* yang berbasis **`iptables`** yang dapat di gunakan pada suatu sistem *dedicated*, *gateway/router/server* multifungsi atau pada *standalone* linux.
Di Linux terdapat **`iptables`** sebagai salah satu modul dari kernel untuk mengatur koneksi TCP/IP. Terdapat banyak tutorial mengenai **`iptables`** di internet, namun diperlukan pengetahuan yang cukup mendalam mengenai iptables beserta seluruh *syntax* dan kemampuannya untuk bisa menghasilkan *policy* dan *rules* yang *secure* dan cocok dengan yang kita inginkan. Shorewall membantu dalam pengaturan **`iptables`** dengan format *file* konfigurasi yang mudah dipahami.

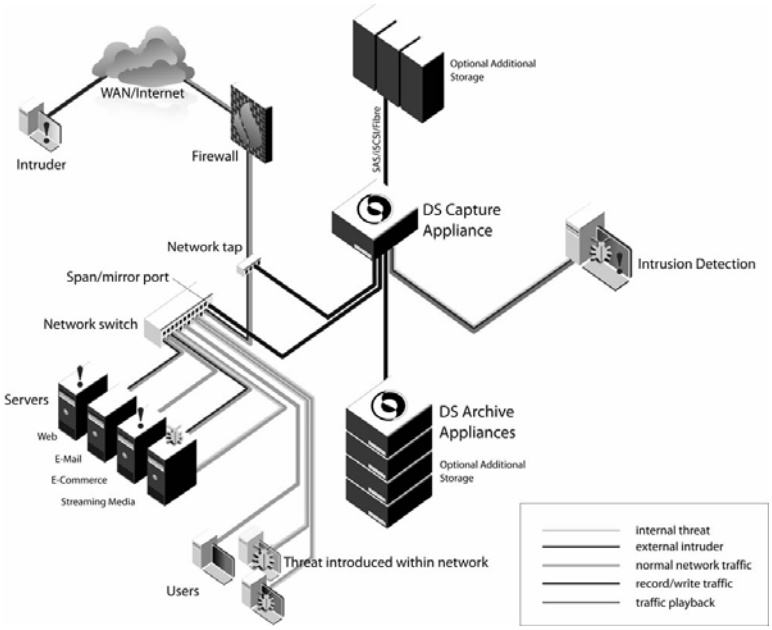


Gambar 2. Cara kerja shorewall dalam jaringan komputer

3. Keamanan Jaringan

Dalam dunia komunikasi data global yang selalu berubah, hubungan internet yang murah, dan cepatnya perkembangan software, keamanan menjadi isu yang semakin penting. Keamanan saat ini menjadi suatu kebutuhan dasar karena komputasi dasar tidak aman. Sebagai contoh, dengan berpindahnya data kita dari titik A ke titik B di Internet, ia mungkin melalui beberapa titik lain selama perjalanan, membuka kesempatan bagi orang lain untuk memotongnya, atau pun merubah data kita ke sesuatu yang tidak kita inginkan. Akses yang tidak diijinkan ke dalam system kita mungkin dapat diperoleh oleh penyusup, juga dikenal sebagai *cracker*. Merupakan tugas dari *Administrator* jaringan yang bersangkutan, untuk menekan resiko tersebut seminimal

mungkin. Pemilihan strategi dan kecakapan *Administrator* jaringan ini, akan sangat membedakan dan menentukan apakah suatu jaringan mudah ditembus atau tidak.
Yang perlu untuk diketahui adalah bahwa kemudahan mengakses informasi berbanding terbalik dengan tingkat keamanan system informasi itu sendiri. Semakin tinggi tingkat keamanan, semakin sulit untuk mengakses informasi. Sebelum memulai segalanya, ada baiknya menentukan terlebih dahulu tingkat ancaman yang harus diatasi dan resiko yang harus diambil maupun resiko yang harus dihindari, sehingga dapat dicapai keseimbangan yang optimal antara keamanan dan kenyamanan



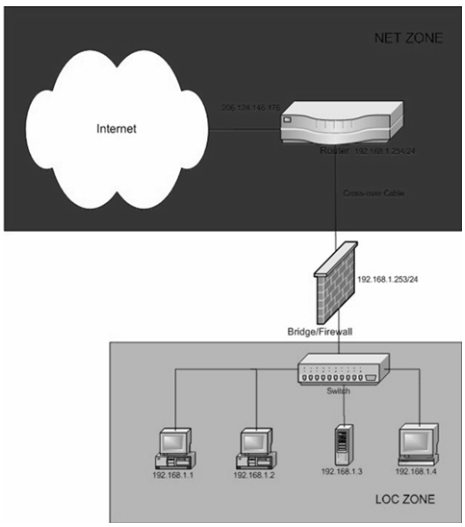
Gambar 3. contoh jaringan komputer yang menerapkan keamanan jaringan komputer.

3. METODE PENELITIAN

Metode yang digunakan dalam penelitian ini menggunakan studi literatur dan eksperimen. Sedangkan kebutuhan perangkat lunak dan perangkat keras yang digunakan antara lain : seperangkat komputer dengan beberapa software pendukung antara lain sistem operasi menggunakan **`openSUSE 10.2`**, **`shorewall`** sebagai *Firewall* dan **`fwlogwatch`** sebagai *Log Analizer.*

4. HASIL DAN PEMBAHASAN

Sebelum membangun Firewall perlu dilakukan perancangan untuk menentukan langkah-langkah yang akan dilakukan dalam membangun Firewall sehingga dapat diimplementasikan dalam jaringan, seperti terlihat pada gambar 4.



Gambar 4. Rancangan jaringan komputer untuk penelitian

A. KONFIGURASI SHOREWALL

Shorewall (Shoreline Firewall) merupakan firewall yang berbasis **iptables** yang dapat digunakan pada suatu sistem dedicated, gateway/router/server multifungsi atau pada standalone linux. File-file yang dibutuhkan untuk melakukan konfigurasi antara lain : **shorewall-1.4.5-1.noarch.rpm, netfilter/iptables, iproute/iproute2**. Berikut ini potongan script konfigurasi file-file shorewall

File **/etc/shorewall/zone** :

```
#       COMMENTS        Comments about the zone
#
# THE ORDER OF THE ENTRIES IN THIS FILE IS IMPORTANT IF YOU HAVE NESTED OR
# OVERLAPPING ZONES DEFINED THROUGH /etc/shorewall/hosts.
#
# See http://www.shorewall.net/Documentation.htm#Nested
#-------------------------------------------------------------------------------
# Example zones:
#
#    You have a three interface firewall with internet, local and DMZ interfaces.
#
#       #ZONE   DISPLAY         COMMENTS
#       net     Internet        The big bad Internet
#       loc     Local           Local Network
#       dmz     DMZ             Demilitarized zone.
#
#ZONE                    DISPLAY         COMMENTS
dmz                     DMZ             Demilitarized zone behind the firewall.
green                   GreenZone       The protected zone, Local Network
red                     RedZone         The Internet zone, unprotected.
#LAST LINE - ADD YOUR ENTRIES ABOVE THIS ONE - DO NOT REMOVE
```

Server tempat shorewall diinstall dikenal sebagai zona yang disebut fw. **/etc/shorewall/policy** File ini berisi aturan untuk semua traffic yang lewat *pada firewall* diatur pada **/etc/shorewall/rules**, jika tidak terdefinisikan pada file tersebut maka akan dicek pada **/etc/shorewall/policy**

```
###############################################################################
#SOURCE          DEST            POLICY          LOG             LIMIT:BURST
#                                                LEVEL
#dmz             fw              REJECT          info
#dmz             green           REJECT          info
#dmz             red             REJECT          info

green           fw              REJECT          info
#green          red             REJECT          info
#green          dmz             REJECT          info

#red            fw              REJECT          info
#red            green           REJECT          info
#red            dmz             REJECT          info

#fw             green           REJECT          info
#fw             red             REJECT          info
#fw             dmz             REJECT          info

all             all             DROP            warning
#LAST LINE -- DO NOT REMOVE
```

File **/etc/shorewall/interface,** File ini untuk menentukan interface yang akan terhubung dengan suatu zona

```
#############################################################################
#ZONE     INTERFACE       BROADCAST       OPTIONS
#
dmz      eth0            detect
green    eth1            detect
red      eth2            detect
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

file diatas berarti **eth0** terhubung dengan jaringan internet dan **eth1** terhubung dengan jaringan lokal.

File **/etc/shorewall/masq.** File ini untuk mendefinikan *masquerade* jaringan lokal dengan jaringan internet Untuk mensetting apakah *traffic* yang melalui **eth1** akan di-*masquerade* dengan dengan IP pada **eth0**

```
#############################################################################
       #INTERFACE SUBNET ADDRESS
         eth0 eth1
       #LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

File **/etc/shorewall/rules,** File ini berisi aturan-aturan dari semua traffic yang melewati firewall

```
#############################################################
  # Rule dari local ke mesin (firewall)
  # Terima koneksi DNS (Port 53)
  ACCEPT     loc     fw     tcp    53
  ACCEPT     loc     fw     udp    53
  # Terima koneksi Proxy (Port 3128/8080)
  ACCEPT     loc    fw     tcp    3128
  ACCEPT     loc    fw     tcp    8080
  # Terima koneksi Web (Port 80)
  ACCEPT     loc    fw     tcp    80
  # Terima koneksi FTP (Port 20, 21)
  ACCEPT     loc    fw     tcp    20
  ACCEPT     loc    fw     tcp    21
  # Terima koneksi SSH (Port 22)
  ACCEPT     loc    fw     tcp    22
  # Terima koneksi Webmin (Port 10000)
  ACCEPT     loc    fw     tcp    10000
  # Rule dari Internet ke mesin (firewall)
  # Terima koneksi DNS
  ACCEPT     net    fw     tcp    53
  ACCEPT     net    fw     udp    53
  # Terima koneksi SSH
  ACCEPT     net    fw     tcp    22
  ACCEPT     fw     loc    tcp    22
  # Terima koneksi Web
  ACCEPT     net    fw     tcp    80
  # Terima koneksi SMTP,POP3,IMAP
  ACCEPT     net    fw     tcp    25,110,143
  ACCEPT     fw     net    tcp    25,110,143
  ACCEPT     loc    fw     tcp    25,110,143
  REJECT     loc    net    tcp    25,110,143
  # Terima koneksi Webmin
  ACCEPT     net    fw     tcp    10000
  # Terima koneksi PING
  ACCEPT     loc    fw     icmp   8
  ACCEPT     net    fw     icmp   8
  ACCEPT     fw     loc    icmp   8
  ACCEPT     fw     net    icmp   8
  # Redirect koneksi local port 80 ke port 3128
  REDIRECT   loc    3128   tcp    80
  #LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

B. Log Analizer

Bagi sebuah server yang terhubung ke Internet, penggunaan *firewall* sangatlah penting. Karena dengan adanya *firewall* dapat mencegah atau setidaknya mengeliminir akses luar yang tidak dikehendaki. Pada umumnya *firewall* akan menghasilkan *log*. *Log* ini adalah catatan / *report* yang berisi informasi tentang paket yang diblokir oleh *firewall* kita seperti asal paket, *port* yang digunakan, waktu dan protokol. Sebagai contoh ada orang luar yang mengakses *port* 80 (**http**) kita, dan port tersebut sudah di set supaya diblokir oleh *firewall*, maka pada saat kejadian firewall otomatis akan merekamnya dan mencatatnya pada log. Sebagai contoh penggunaan shorewall pada distro linux seperti opensuse, redhat dan turunannya secara default akan mencatatkan lognya di **/var/log/messages**

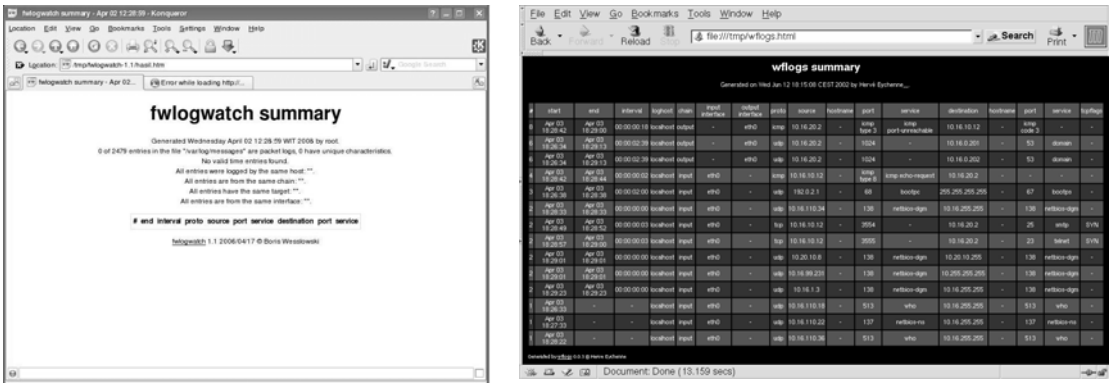
```
Apr  21  19:08:36  pemerintah  kernel:  Shorewall:net2all:DROP:IN=eth0  OUT=
MAC=00:00:00:00:00:21:00:0a:55:33:e4:33:33:00                xsrc=66.123.12.12
DST=72.14.207.99 LEN=40 TOS=0x00 PREC=0x00 TTL=49 ID=22739 PROTO=UDP SPT=5000
DPT=5000 LEN=20
```

Untuk membaca puluhan *log* yang ada, maka dibutuhkan suatu tools untuk membaca log tersebut yaitu **fwlogwatch.**

Berikut ini langkah-langkah instalasi **fwlogwatch:**

```
#tar zxvf fwlogwatch-1.1.tar.gz
# cd fwlogwatch-1.1/
# make
# make install
# make install-config
```

Program akan terinstall di **/usr/local/sbin/fwlogwatch** dan file konfigurasinya di **/etc/fwlogwatch.config**. Secara default apabila dijalankan maka **fwlogwatch** akan menghasilkan output dalam format html. Untuk menyimpannya dalam file html cukup menjalankan program diikuti **opsi -o** dan nama file. Sebagai contoh akan disimpan dalam file **result.htm** maka cukup ketikkan: **/usr/local/sbin/fwlogwatch -o result.htm**



Gambar 5. Hasil tampilan output *Log Analizer*

5. KESIMPULAN

Berdasarkan penelitan yang telah dilakukan dapat disimpulkan bahwa :

a) Telah dihasilkan sebuah modul untuk melakukan monitoring port menggunakan **shorewall** dan **fwlogwatch** untuk menampilkan traffic dalam jaringan komputer sehingga dapat meningkatkan keamanan jaringan tersebut.
b) berdasarkan hasil pengujian membuktikan bahwa fungsionalitas **shorewall** dan **fwlogwatch** dapat bekerja dengan baik.

6. DAFTAR PUSTAKA

Amijaya, Nur, 2004. *Workshop Linux Server With RedHat 8*. Yogyakarta : Bugs Training Center.
Anton, R, Raharja, Afri, Y., dan Wisesa, W., *Open Source Campus Agreement Modul Pelatihan "Administrasi Jaringan Linux*", http://www.pandu.or.id
Hidayat, Risanuri , *proxy*, http://www.te.ugm.ac.id/~risanuri/jarkom/
Indrajit, E.R., Prastowo, B., N., Yuliardi Rofiq., 2002, *Memahami Security Linux***,** PT. Elex Komputindo, Jakarta.
Mansfield, Niall, 2004. *Practical TCP/IPJilid 2*. Yogyakarta : Andi.
Pedyanto, Yudho, 2003. *Modul Pelatihan Internetworking*. Yogyakarta : Linux Learning Center.
Purbo, O.W., 1999, *TCP/IP*, Cetakan Ketiga, PT. Elex Komputindo, Jakarta.
Rudiyanto, Dudy, dkk, 2002. *Administrasi Sistem Linux RedHat***.** Jakarta, PT. Elex Media Komputindo
Rudiyanto, Dudy, dkk, 2003., *Security Open System*, Ketiga, PT. Elex Komputindo, Jakarta
Shorewall, Documentation, http://shorewall.net/Documentation_Index.html
Securing-Optimizing-Linux-The-Ultimate-Solution.pdf, http://www.openna.com
Tanutama, L., dkk, 1992, *Mengenal LAN*, Cetakan Kedua, PT. Elex Komputindo, Jakarta.
Wagito, 2005. Jaringan *Komputer Teori dan Implementasi Berbasis Linux*. Yogyakarta : Gava Media
http://fwlogwatch.inside-security.de/