Implementasi IPTables untuk Packet Filtering Firewall pada Raspberry Pi

Desi Andriani Rahman[1], L.A.Syamsul Irfan A[2], I Made Budi Suksmadana[3]
[1,2,3] Jurusan Teknik elektro, Fakultas Teknik , Universitas Mataram, Nusa Tenggara Barat, Indonesia
Email : laluirfan@gmail.com[2]; mdbudi@gmail.com[3]

ABSTRAK

Keamanan jaringan komputer menjadi begitu penting untuk diperhatikan saat ini. Firewall berfungsi sebagai sistem keamanan jaringan yang dapat mengatur dan mengontrol lalu lintas data yang diizinkan untuk mengakses data pada server. Aplikasi firewall yang dapat digunakan untuk melakukan filtering yaitu IPTables yang merupakan bawaan dari linux. Snort yang bertindak sebagai IDS digunakan untuk pendeteksian serangan yang dilakukan oleh client terhadap server. Hasil dari penelitian yang telah dilakukan memperlihatkan bahwa Raspberry Pi sebagai firewall dapat mengimplementasikan penggunaan IPTables dengan memblok IP ping secara terus-menerus dengan ukuran paket besar, memblok IP scanning dan memblok scanning port yang terbuka.

Kata kunci : Firewall, IPTables, Snort, Raspberry Pi, Server, Client

ABSTRACT

Computer network security becomes so important to note at this time. Firewall serves as a network security systemcan manage and control the data traffic to server. IPTables is one of firewall on linux that can be used to filter traffic. Firewall that can be used to perform filtering that is IPTables which is the default of linux. Snort acting as IDS use for detection of attacks performed by the client against the server. The results of the research have shown that Raspberry Pi as a firewall can implement the use of IPTables by blocking IP ping continuously with large packet size, blocking IP scanning and blocking open port scanning.

Keywords: *Firewall, IPTables, Snort, Raspberry Pi, Server, Client.*

INTRODUCTION

Kebutuhan suatu universitas dengan ruang lingkup yang luas memerlukan suatu koneksi antar gedung atau fakultas. Disinilah pentingnya peran komputer dalam membuat jaringan antar fakultas. Dengan penerapan teknologi ini, sangatlah mudah untuk mengirim *file* dan dokumen-dokumen penting dari tempat satu ke tempat yang lain. Namun teknologi ini pun memiliki kelemahan, yaitu sangat rentan terhadap pencurian, perusakan, dan kerahasiaan dokumen. Hal ini terjadi karena komputer berada dalam suatu jaringan umum, sehingga file dan dokumen pada suatu universitas dapat dilihat oleh banyak orang dalam jaringan. Oleh sebab itu, mutlak bagi suatu universitas memiliki sistem pengamanan (*Computer Security*) dalam jaringannya.

Firewall merupakan salah satu pelindung yang dibutuhkan untuk mendapatkan akses yang aman ketika berhubungan dengan jaringan komputer, baik dari luar (internet) maupun dari dalam (intranet) dengan cara membuat aturan tertentu. Salah satu cara *firewall* mengamankan sistem jaringan komputer adalah dengan menerapkan penyaringan paket data. Salah satu aplikasi *firewall* yang memiliki *fitur* untuk dapat melakukannya yaitu aplikasi *IPTables* pada linux. Aplikasi *IPTables* merupakan fasilitas *firewall* bawaan yang tersedia pada sistem operasi linux yang mampu melakukan penyaringan terhadap lalu lintas data. *IPTables* yang akan digunakan masih dalam keadaan normal dan *firewall* masih kosong, sehingga perlu dilakukan pengaturan *rule-rulefirewall* terlebih dahulu.

Dalam hal ini dibutuhkan *firewall* yang dapat mengatur lalu lintas jaringan agar tetap aman, sehingga penulis meneliti tentang "Implementasi *IPTables* untuk *packet filtering firewall* pada *raspberry pi*".

Jaringan Komputer. Jaringan Komputer adalah kumpulan"interkoneksi" antara 2 komputer autonomous atau lebih yang

terhubung dengan media transmisi kabel atau tanpa kabel (*wireless*). Bila sebuah komputer dapat membuat komputer lainnya *restart*, *shutdown*, atau melakukan kontrol lainnya, maka komputer – komputer lainnya tersebut bukan autonomous (Syafrizal, 2005).

IDS. IDS (Intrusion Detection System) adalah sebuah sistem yang melakukan pengawasan terhadap lalu lintas jaringan dan pengawasan terhadap kegiatan – kegiatan yang mencurigakan didalam sebuah sistem jaringan. Jika ditemukan kegiatan yang mencurigakan maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan. Dalam banyak kasus, IDS juga merespon terhadap lalu lintas data yang tidak normal melalui aksi pemblokiran *user* ataupun alamat IP. Pada umumnya, terdapat dua jenis IDS, yaitu Network IDS (NIDS) dan Host IDS (HIDS) (Taufikurrahman, 2014).

Snort. Snort IDS merupakan IDS *open source* yang secara defacto menjadi standar IDS di industri. Snort dapat diimplementasikan dalam jaringan yang *multiplatform*, salah satu kelebihannya adalah mampu mengirimkan *alert* dari mesin Unix atupun Linux ke platform Microsoft Windows dengan melalui *Server Message Block* (SMB). Snort diciptakan untuk menjadi IDS berbasiskan *open source* yang berkualitas tinggi (Taufikurrahman, 2014).

Firewall. *Firewall* adalah sebuah sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman. Umumnya, sebuah *firewall* diimplementasikan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang *(gateway)* antara jaringan lokal dan jaringan lainnya (jaringan eksternal). *Firewall* umumnya juga digunakan untuk mengontrol akses terhadap siapa saja yang memiliki akses terhadapjaringan pribadi dari pihak luar (Ariefati, 2010).

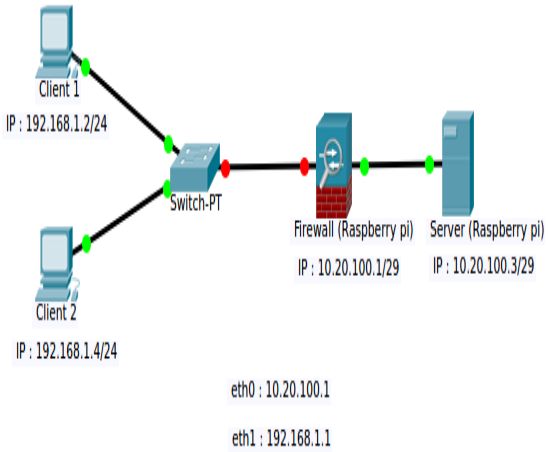
IP Tables. *IPTables* adalah modul di *Linux* yang memberikan dukungan langsung untuk keamanan sistem serta beberapa keperluan jaringan lainnya. Sebuah kebijakan atau *Policy* dapat dibuat dengan *IPTables* sebuah *policy* pada IPTables dibuat berdasarkan sekumpulan peraturan yang diberikan pada kernel untuk mengatur setiap paket yang datang. Pada *IPTables* ada istilah yang disebut dengan IP *Chain* yang merupakan daftar aturan bawaan dalam IPTables. Ketiga chain tersebut adalah *INPUT, OUTPUT* dan *FORWARD* (Muhar Syarif, 2008).

Raspberry Pi. Raspberry pi adalah komputer papan tunggal (Single Board Circuit /SBC)yang memiliki ukuran sebesar kartu kredit. *Raspberry Pi* bersifat *open source* (berbasis Linux). Cara mengakses *Raspberry Pi* jarak jauh menggunakan perintah ssh. *Raspberry Pi* telah dikonfigurasi untuk secara otomatis memulai *Shell Server* ketika *boot*. Untuk mengakses *Raspberry Pi* jarak jauh menggunakan *Shell client*, ssh (Rick Golden, 2013).

METHODOLOGY

Design Topologi Jaringan

Pengalamatan IP Address merupakan suatu identitas penomoran suatu interface seperti yang dilihat pada gambar 1.



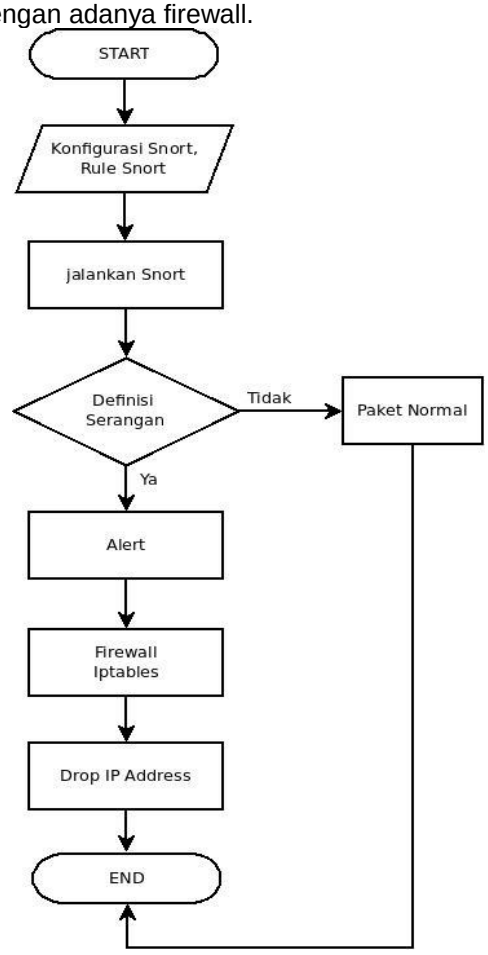
Gambar 1. Topologi Jaringan

Fungsi dari masing-masing komputer pada topologi jaringan sebagai berikut :

a. *Client* melakukan akses terhadap infomasi yang dimiliki oleh *server*. Disini *client* melakukan pengujian terhadap *server*.
b. *client* 1akan melakukan serangan *ping* secara terus menerus dengan ukuran paket melebihi batas, melakukan *ping sweep* dan melakukan *scanning port* yang terbuka. Sedangkan client 2 akan mengirimkan ping dengan ukuran normal sehingga tidak dianggap sebagai serangan
c. *Firewall* bertugas untuk mengatur, mengontrol lalu lintas data yang diizinkan antara *client* dengan *server*.

d. *Server* merupakan jaringan komputer penyedia informasi dan data. *Server* inilah yang dilindungi oleh *firewall* agar *client* yang diizinkan saja yang dapat mengakses informasi dan data yang ada pada *server.*

Diagram Alir Sistem. Gambar 2 menunjukkan diagram alir proses penggunaan IPTables. Dimulai dengan menjalankan snort, dimana snort berfungsi untuk melakukan pengawasan terhadap lalu lintas jaringan dan sebagai pendeteksi serangan. Apabila tidak terdapat serangan maka paket akan diloloskan dan proses selesai. Apabila terdapat serangan maka snort akan mengirimkan pesan berupa alert kepada komputer firewall, setelah itu firewall IPTables akan melakukan drop terhadap IP Address dari komputer client yang melakukan serangan. Sehingga server tetap aman dengan adanya firewall.

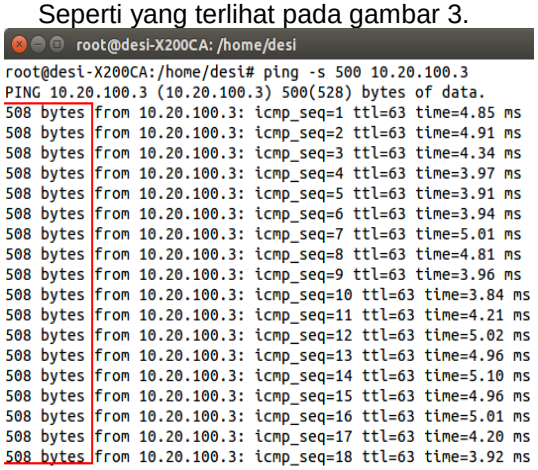


Gambar 2. Diagram alir sistem

HASIL DAN PEMBAHASAN

Serangan yang dilakukan client terhadap server

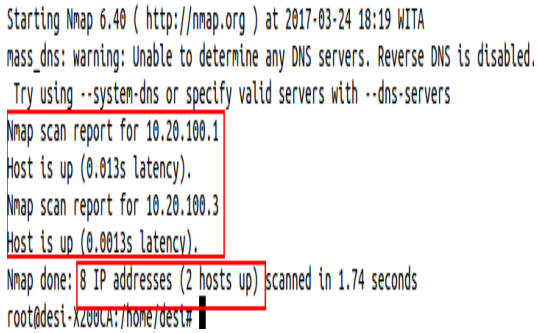
1. Melakukan ping terus menerus dengan ukuran paket yang besar yaitu 500 byte. Seperti yang terlihat pada gambar 3.



Gambar 3. Serangan Ping terus menerus

Ping dapat menjadi indikasi awal gangguan. Penyerang dapat mengirimkan paket ping untuk kemudian mengirimkan gangguan berupa denial of service. Gangguan denial of service adalah gangguan berupa paket ping dalam jumlah banyak yang menyebabkan resource pada server terganggu sehingga akses terhadap server oleh pengguna lain tidak dapat dilayani.

2. Melakukan Scanning IP (Ping Sweep). Nmap digunakan untuk melakukan scanning IP dengan perintah sebagai berikut : `nmap -sP 10.20.100.0/29`



Gambar 4. Serangan Scanning IP

Gambar 4 menunjukkan pengguna jaringan melakukan ping scanning terhadap server untuk mencari host yang sedang aktif agar dapat dijadikan sebagai target scanning. Dari 8 host yang tersedia dalam jaringan tersebut, setelah dilakukan scanning ip di ditemukan 2 host yang sedang aktif.

3. Melakukan Scanning Port yang terbuka (port 22, port 21 dan port 80). Nmap digunakan untuk melakukan scanning port dengan perintah sebagai berikut : `nmap -Pn -sN -n -p21,22,80,3306 10.20.100.3`

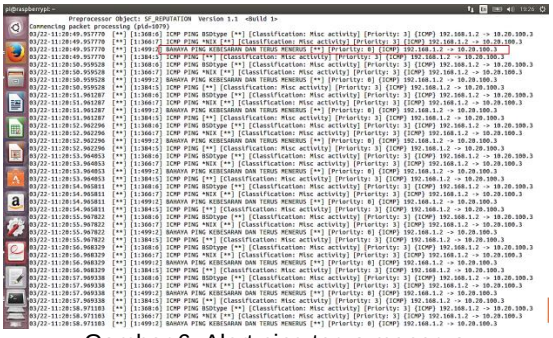
```
root@desi-X200CA:/home/desi# nmap -Pn -sN -n -p21,22,80,3306 10.20.100.3

Starting Nmap 6.40 ( http://nmap.org ) at 2017-03-22 19:13 WITA
Nmap scan report for 10.20.100.3
Host is up (0.0019s latency).
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
80/tcp   open|filtered http
3306/tcp closed        mysql
```

Gambar 5. Serangan scanning port

Gambar 5 menunjukkan pengguna jaringan melakukan scanning port terhadap server untuk menentukan status port apakah open atau close. Dari gambar 6 dapat dilihat port yang terbuka yaitu port 21 ftp , port 22 ssh , port 80 http. Apabila terdapat port yang terbukamaka client akan dengan mudah masuk dan mengolah data pada server.

Pendeteksian Serangan Menggunakan Snort

1. Alert pada snort untuk ping terus menerus dengan ukuran paket besar yaitu 500 byte, pada gambar 6. Snort mengirimkan alert dengan pesan "BAHAYA PING KEBESARAN DAN TERUS MENERUS" dengan IP client sebagai penyerang 192.168.1.2 melakukan ping terhadap server dengan ip 10.20.100.3.



Gambar 6. Alert ping terus menerus

2. Alert pada snort untuk Scanning IP. Snort mengirimkan alert dengan pesan "IP Scanning" dengan IP client 192.168.1.2 melakukan IP Scanning terhadap server dengan IP 10.20.100.3. Dari gambar 8 juga dapat dilihat hasil dari ip scanning yaitu IP 10.20.100.0, 10.20.100.2, 10.20.100.3, 10.20.100.4, 10.20.100.5, 10.20.100.6.

```
] IP Scanning [**] [Priority: 0] {TCP} 192.168.1.2:47395 -> 10.20.100.2:443
] IP Scanning [**] [Priority: 0] {TCP} 192.168.1.2:47394 -> 10.20.100.5:443
] IP Scanning [**] [Priority: 0] {TCP} 192.168.1.2:47395 -> 10.20.100.0:443
] IP Scanning [**] [Priority: 0] {TCP} 192.168.1.2:47395 -> 10.20.100.5:443
] IP Scanning [**] [Priority: 0] {TCP} 192.168.1.2:47395 -> 10.20.100.6:443
] IP Scanning [**] [Priority: 0] {TCP} 192.168.1.2:47395 -> 10.20.100.3:443
] IP Scanning [**] [Priority: 0] {TCP} 192.168.1.2:47395 -> 10.20.100.4:443
```

Gambar 7. Alert scanning IP

3. Alert pada snort untuk Scanning Port yang terbuka. Pada gambar 8, snort mengirimkan alert dengan pesan "Peringatan Scanning Port". dengan IP penyerang 192.168.1.2, melakukan Scanning port terhadap server dengan IP 10.20.100.3. Sehingga client telah menemukan beberapa port dari aplikasi yang ada pada server, seperti yang di tunjukan pada gambar 9 terlihat ip server dengan nomor port yang berbeda-beda yaitu port 80 http, port 22 ssh, port 3306 mysql, port 21 ftp.

```
Peringatan Scanning Port [**] [Priority: 0] {TCP} 192.168.1.2:63763 -> 10.20.100.3:80
Peringatan Scanning Port [**] [Priority: 0] {TCP} 192.168.1.2:63763 -> 10.20.100.3:22
Peringatan Scanning Port [**] [Priority: 0] {TCP} 192.168.1.2:63764 -> 10.20.100.3:3306
Peringatan Scanning Port [**] [Priority: 0] {TCP} 192.168.1.2:63764 -> 10.20.100.3:21
Peringatan Scanning Port [**] [Priority: 0] {TCP} 192.168.1.2:63765 -> 10.20.100.3:80
Peringatan Scanning Port [**] [Priority: 0] {TCP} 192.168.1.2:63765 -> 10.20.100.3:22
Peringatan Scanning Port [**] [Priority: 0] {TCP} 192.168.1.2:63774 -> 10.20.100.3:3306
Peringatan Scanning Port [**] [Priority: 0] {TCP} 192.168.1.2:63765 -> 10.20.100.3:21
```

Gambar 8. Alert scanning port

Mencegah serangan dengan Firewall IPTables

Kondisi IPTables yang masih kosong sebelum dibuat rules untuk melakukan drop, dapat dilihat pada gambar 9 :

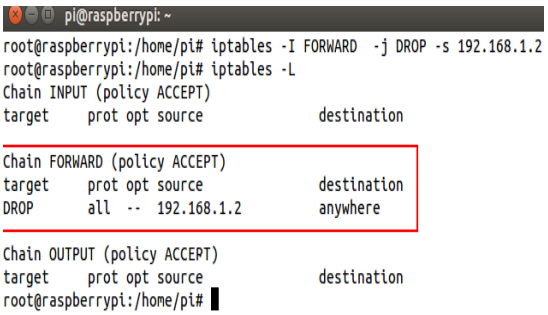
```
pi@raspberrypi: ~
root@raspberrypi:/home/pi# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@raspberrypi:/home/pi#
```

Gambar 9. IPTables non configure

IPTables setelah dibuatkan rules untuk melakukan drop, yaitu : Perintah untuk melakukan drop IP Address yang telah melakukan serangan terhadap server :

`IPTables -I FORWARD -j DROP -s 192.168.1.2.`

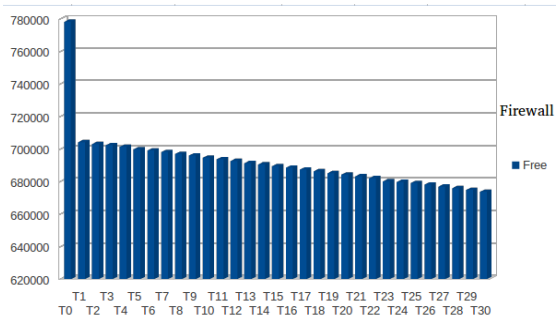
Setiap paket yang melewati firewall dengan ip sumber 192.168.1.2 akan di drop dan tidak diizinkan untuk melakukan akses terhadap server. Setiap paket yang masuk di arahkan melalui sistem dengan perintah FORWARD, Kemudian akan melakukan jump -j DROP dan DROP terhadap IP yang bersumber dari 192.168.1.2. Seperti yang ditunjukkan pada gambar 10.



Gambar 10. IPTables setelah drop

Kondisi RAM pada Firewall dan Server Saat Firewall ON

1. Kondisi RAM pada Firewall. Kondisi RAM pada Raspberry Pi yang digunakan sebagai firewall sebelum dan setelah melakukan serangan dengan mengirimkan paket ping terus menerus selama 30 menit dengan ukuran paket 4000 byte dapat dilihat pada grafik berikut :

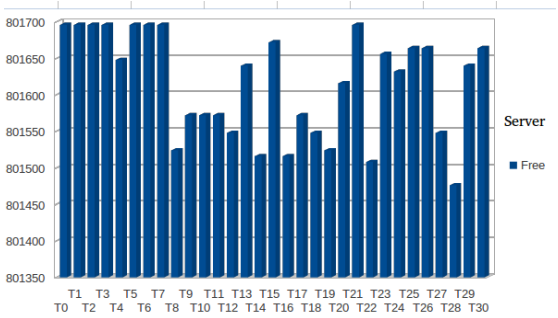


Gambar 11. Kondisi RAM Firewall

Dari grafik pada gambar 11 dapat dilihat kondisi RAM pada raspberry pi untuk free memori pada waktu sebelum serangan (T0) yaitu 778120 KB. Kemudian setelah 1 menit serangan (T1) jumlah free memori berkurang cukup signifikan menjadi 704112 KB. Untuk 2 menit sampai 30 menit berikutnya nilai free memori semakin berkurang.

2. Kondisi RAM pada Server

Kondisi RAM pada Raspberry Pi yang digunakan sebagai server sebelum dan setelah melakukan serangan dengan mengirimkan paket ping terus menerus selama 30 menit dengan ukuran paket 4000 byte, dapat dilihat pada grafik berikut :



Gambar 12. Kondisi RAM Server

Dari grafik pada gambar 12 dapat dilihat kondisi RAM pada raspberry pi yang bertugas sebagai server. Dimana kondisi normal sebelum serangan hingga 3 menit setelah serangan (T0-T3) jumlah free memori tetap yaitu 801696 KB. Kemudian pada 4 menit (T4) setelah serangan jumlah memori sedikit berkurang menjadi 801648 KB. Pada 5 menit (T5) jumlah free memori bertambah dan di menit berikutnya jumlah free memori berkurang dan bertambah. Sehingga memori cenderung tidak berkurang.

KESIMPULAN

1. Dengan menggunakan Raspbian Jessie Lite pada Raspberry Pi dapat mengimplementasi penggunaan IPTables sebagai firewall untuk melindungi server.
2. Snort yang bertindak sebagaiIDS (Intrusion Detection System) berhasilmelakukan pengawasan terhadap lalu lintas jaringan dan serangan yang dilakukan oleh client seperti melakukan ping secara terus menerus dengan ukuran paket besar, scanning IP (ping sweep), dan scanning port yang terbuka. Dengan mengaktifkan icmp rules dan scan rules yang ada pada konfigurasi snort.
3. RAM pada Raspberry Pi yang digunakan sebagai firewall cenderung berkurang, dimana kondisi normal yaitu 778120KB, kemudian setelah 30 menit serangan memori semakin berkurang menjadi 678318,4KB. Sedangkan RAM pada Raspberry Pi yang digunakan sebagai server cenderug tidak berkurang, dimana pada kondisi normal jumlah memori yaitu

801696KB, kemudian setelah 30 menit serangan memori bertambah menjadi 801624KB. Sehingga memori yang ada pada server cenderung tidak berkurang.

SARAN

1. Sistem yang dirancang memiliki keterbatasan dari segi rules yang ada. Semakin lengkap rules yang dimiliki, sistem akan semakin terlindungi dari gangguan.
2. Sistem ini juga dapat digunakan untuk sistem keamanan pada satu host.
3. Raspberry Pi dapat dijadikan sebagai firewall, dengan menggunakan Raspberry Pi dapat mempermudah penggunaan dan dapat menghemat tempat karena ukurannya yang kecil dibandingkan dengan PC.

DAFTAR PUSTAKA

Wiratama, Ariefati. 2010. Penerapan Statefull Firewall Pada Arsitektur Dual Homed Host (Studi Kasus : PT.PLN (Persero) APL Mampang). Program Studi Teknik Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Syarif Hidayatullah.

Golden, Rick. 2013. Raspberry Pi Networking Cookbook. Birmingham :Packt Publishing.

Rafiudin, Rahmat. 2010. Menggayang Hacker dengan Snort. Yogyakarta : Andi.

Syarif, Muhar. 2008. Implementasi IPTables sebagai Filtering Firewall. Jurnal Universitas Sriwijaya.

Syafrizal dan Melwin. 2006. Pengantar Jaringan Komputer. Yogyakarta : Andi.

Tufikurrahman, Arief. 2014. Sistem Pendeteksi dan Pencegah Serangan pada Server. Jurnal Teknik Elektro Universitas Mataram.