Journal of Internet and Software Engineering Vol: 1, No 2, 2024, Page: 1-7

Implementasi *Firewall* menggunakan Fitur dari IPTables pada Sistem Operasi Linux

Divo Wibowo Adi*, Ferdiansyah Irawan, Zaki Rafi Athallah, Shelvie Nidya Neyman

Teknologi Rekayasa Komputer, Sekolah Vokasi, Institut Pertanian Bogor

Abstrak: Implementasi *Firewall* menggunakan fitur dari Iptables pada sistem Operasi Linux dalam penelitian ini, kita akan membahas implementasi *firewall* menggunakan fitur dari iptables pada sistem operasi Linux. Iptables adalah sebuah *tools* yang digunakan untuk melakukan filter (penyaringan) terhadap lalu lintas data. Dengan menggunakan iptables, kita dapat mengatur semua lalu lintas dalam komputer, baik yang masuk ke komputer, keluar dari komputer, ataupun *traffic* yang sekedar melewati komputer. Penelitian ini bertujuan untuk meningkatkan keamanan jaringan dengan menggunakan iptables sebagai *firewall*.

Kata Kunci: IPTables, *Firewall*, Linux, Keamanan Jaringan, Penyaringan Lalu Lintas Data

DOI: https://doi.org/10.47134/pjise.v1i2.2671
*Correspondence: Divo Wibowo Adi
Email: divowibowoadi3@gmail.com

Received: 01-02-2024
Accepted: 15-03-2024
Published: 31-04-2024

Abstract: *Firewall Implementation Using Features of Iptables on Linux Operating Systems In this study, we will discuss firewall implementations using features from iptables on Linux operating systems. Iptables is a tool used to filter data traffic. By using iptables, we can manage all traffic on the computer, both incoming to the computer, leaving the computer, or traffic that just passes through the computer. This research aims to improve network security by using iptables as a firewall.*

Keywords: *IPTables, Firewall, Linux, Network Security, Data Traffic Filtering*

Pendahuluan

Keamanan jaringan komputer adalah proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jaringan komputer (Permana *et al*., 2019). Tujuan keamanan komputer meliputi perlindungan informasi dari pihak yang tidak berkepentingan dengan tetap memudahkan akses dan penggunaan oleh para pengguna (Dali, 2017). Ada banyak faktor yang mengancam keamanan jaringan computer, contohnya spam dan spyware, serangan dan ancaman hacker, implementasi virus, dan kebocoran perangkat lunak komputer. Contoh tersebut menggambarkan faktor-faktor yang mengancam jaringan komputer agar lebih komprehensif (Munawar *et al*., 2020).

Jaringan komputer terus mengalami perkembangan, baik dari skalabilitas, jumlah node, maupun teknologi yang digunakan, oleh sebab itu diperlukan pengelolaan jaringan yang baik, sehingga untuk ketersediaan jaringan selalu ada, namun demikian dalam pengelolaan jaringan memiliki banyak permasalahan diantaranya yang berhubungan dengan keamanan jaringan (Sugiyono, 2016). Untuk Meningkatkan keamanan jaringan komputer beberapa strategi yang dapat dilakukan adalah penggunaan firewall, dan pengelolaan user. Dengan demikian, keamanan jaringan computer sangat penting untuk melindungi sistem komputer dari ancaman serangan dan memastikan ketersediaan jaringan yang terjamin (Pamuji *et al*., 2020).

Firewall adalah sebuah system atau perangkat keamanan khususnya pada jaringan komputer yang bertugas untuk menjaga lalu lintas data di dalam jaringan komputer berjalan dengan aman, dan dalam waktu bersamaan juga mencegah lalu lintas data yang tidak aman untuk masuk di dalam jaringan computer (Doni, 2015). Firewall dapat ditempatkan pada berbagai titik dalam jaringan, seperti di antara router dan internet, di antara server dan jaringan lokal, atau pada komputer pengguna. Untuk membangun sebuah jaringan yang memiliki pengamanan firewall, dibutuhkan hardware yang digunakan sebagai server, serta sistem operasi yang diinstalasikan dalam server tersebut (Hendita & Kusuma, 1997). Dalam dunia nyata, firewall adalah dinding yang bisa memisahkan ruangan, sehingga kebakaran pada suatu ruangan tidak menjalar ke ruangan lainnya. Tapi sebenarnya firewall di Internet lebih seperti pertahanan disekeliling benteng, yakni mempertahankan terhadap serangan dari luar (Adhi Purwaningrum *et al*., 2018).

SSH (secure shell) adalah protokol jaringan yang berada di lapisan aplikasi pada protokol TCP/IP, SSH digunakan untuk mengendalikan komputer jarak jauh (remote), mengirim file, membuat terowongan yang terenkripsi (tunneling/port forwarding) dan lain – lain (Jusuf Heni, 2015). SSH pertama kali diperkenalkan pada tahun 1995 oleh Tatu Ylonen dengan rilis versi 1.0 SSH dan Internet Draft "The SSH Secure Shell Remote Login Protocol". SSH awalnya dibuat untuk menggantikan protokol Telnet yang tidak aman, yang memungkinkan data untuk ditransfer tanpa enkripsi dan rentan terhadap serangan man-in-the-middle (R.Karthikeyan, 2017).

HTTP adalah sebuah protokol meminta atau menjawab antara client dan server. Sebuah client HTTP seperti web browser, biasanya memulai permintaan dengan membuat hubungan TCP/IP ke port tertentu di tuan rumah yang jauh (biasanya port 80) (Zabar & Novianto, 2015). Pada protokol HTTP terdapat 3 jenis hubungan dengan perantara proxy, gateway, dan tunnel. Proxy bertindak sebagai agent penerus, menerima request dalam

bentuk Uniform Resource Identifier (URI) absolut, mengubah format request dan mengirimkan request ke server yang ditunjukan oleh URI. Gateway bertindak sebagai agen penerima dan menterjemahkan request ke protokol server yang dilayaninya. Tunnel bertindak sebagai titik Relay antara dua hubungan HTTP tanpa mengubah request dan response HTTP. Tunnel digunakan jika komunikasi perlu melalui sebuah perantara dan perantara tersebut tidak mengetahui isi pesan dalam hubungan tersebut (Aditya Irfan Puji Handoko, 2017).

Linux adalah sistem operasi berbasis GNU/Linux yang bersifat Open Source dan memiliki banyak varian seperti Debian, Slackware, Open Suse, Archlinux, Redhat dan sebagainya (Harjono, 2016). Satu hal yang membedakan Linux terhadap sistem operasi lainnya adalah harga. Linux ini lebih murah dan dapat diperbanyak serta didistribusikan kembali tanpa harus membayar fee atau royalti kepada seseorang. Tetapi ada hal lain yang lebih utama selain pertimbangan harga yaitu mengenai source code. Source code Linux tersedia bagi semua orang sehingga setiap orang dapat terlibat langsung dalam pengembangannya (Raharja et al., 2001). Kali Linux merupakan pembangunan kembali Back Track Linux Secara sempurna. Jika dulunya Backtrack dibuat berdasarkan sistem operasi ubuntu, kini Kali Linux menggunakan Debian sebagai sistem operasinya (Setyadi, 2017).

IPTables adalah suatu tools dalam sistem operasi linux yang berfungsi sebagai alat untuk melakukan filter (penyaringan) terhadap (traffic) lalu lintas data. Secara sederhana digambarkan sebagai pengatur lalu lintas data. Dengan IPTables inilah akan bisa mengatur semua lalu lintas dalam komputer, baik yang masuk ke komputer, keluar dari komputer, ataupun traffic yang sekedar melewati komputer. IPTables merupakan sistem firewall di sistem open source yang mendukung Layer 3 (Network layer), Layer 4 (Transport layer) dan Layer 7 OSI layer (Hawari, 2017). IPTables dapat digunakan untuk mencegah serangan DDoS dengan cara memblokir akses menuju server sehingga request yang terindikasi sebagai serangan DDoS dapat diredam pergerakannya. Iptables juga dapat digunakan untuk memantau lalu lintas data dan mendeteksi adanya aktivitas yang mencurigakan pada sebuah jaringan (Widianto & Sulistyo, 2021). Ada tiga table di IPTables. Aturan atau rantai khusus yang anda buat akan dimasukkan ke salah satu yang paling banyak digunakan. Tabel filter berisi rantai built-in: INPUT: Proses masuk, MAJU: Proses paket yang dirutekan melalui host, OUTPUT: Proses paket keluar (Al Amien, 2020).

Metode

Metode Penelitian ini menggunakan studi literatur dan studi kasus dalam bentuk simulasi. Studi literatur adalah cara yang dipakai untuk menghimpun data-data atau sumber-sumber yang berhubungan dengan topik yang diangkat dalam suatu penelitian (Habsy, 2017). studi kasusmerupakan salah satu metode penelitian kualitatif yangberbasis pada pemahaman dan perilaku manusiaberdasarkan perbedaan nilai, kepercayaan dan *scientific theory* (Yona, 2014).

Teknik pengumpulan data yang digunakan dalam proyek keamanan siber ini meliputi studi literatur dan studi kasus dengan melakukan simulasi, di mana informasi dikumpulkan melalui tutorial online yang relevan dengan topik penelitian untuk memahami keamanan siber dan cara mengimplementasikannya. Analisis data dilakukan

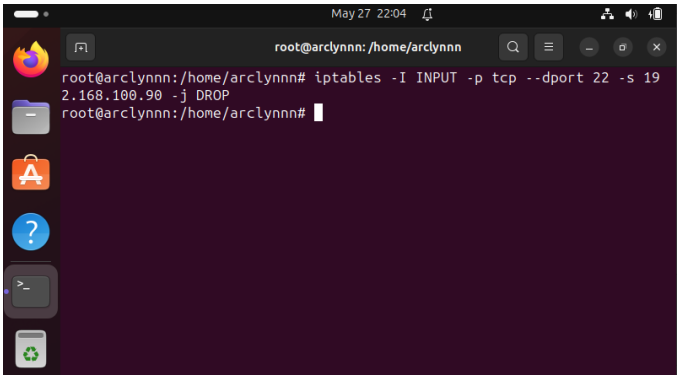
dengan mengumpulkan informasi yang diperoleh saat melakukan simulasi penerapan firewall menggunakan IPTables pada dua Sistem Operasi Linux. Penelitian ini bertujuan untuk memberikan pengalaman tentang penerapan firewall dan dampak dari firewall yang diterapkan.

Hasil dan Pembahasan

1. Membuat Rules Pada Ubuntu Desktop

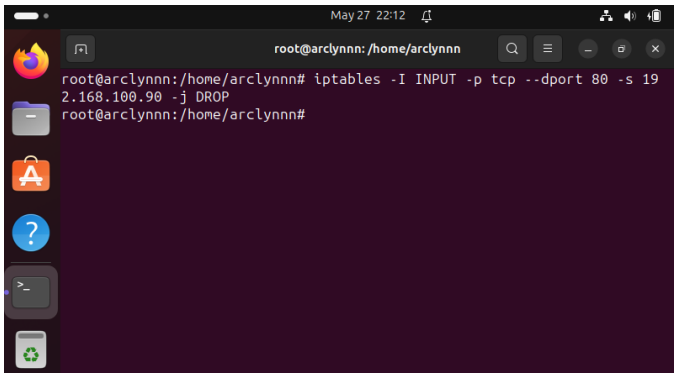
Untuk membuat sebuah rules pada Ubuntu Desktop, jalankan Terminal pada Ubuntu Desktop. Setelah itu pengguna membuat rules seperti dibawah ini :

- Membuat *rules* pada port 22 (SSH):
  Pada port ini untuk command yang dibuat pada terminal yaitu **iptables -I INPUT -p tcp –dport 22 -s 192.168.100.90 -j DROP**, fungsi command pada gambar dibawah tersebut berfungsi untuk memblokir semua koneksi TCP yang masuk ke port 22 dari IP address **192.168.100.90**.



Gambar 1. Rules untuk port SSH

- Membuat *rules* pada port 80 (HTTP):
  Pada port ini untuk command yang dibuat pada terminal yaitu **iptables -I INPUT -p tcp –dport 80 -s 192.168.100.90 -j DROP**, fungsi command pada gambar dibawah tersebut berfungsi untuk memblokir semua koneksi TCP yang masuk ke port 80 atau port HTTP dari IP address 192.168.100.90.

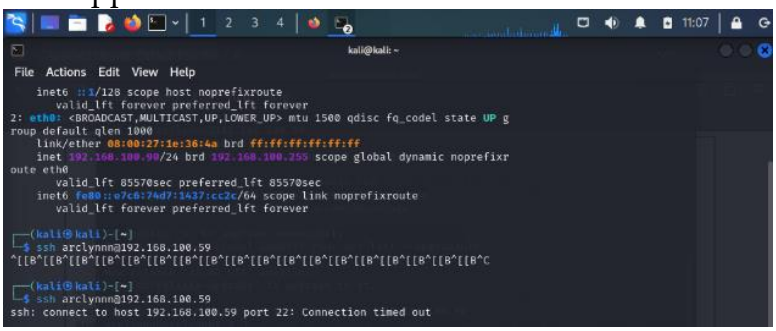


Gambar 2. Rules untuk port HTTP

2. Hasil Apabila Sebuah Rules Telah Dibuat

- Port 22 (SSH)

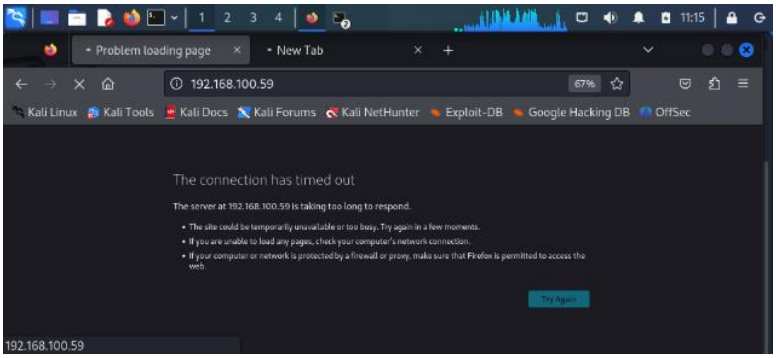
  Ketika client melakukan SSH ke IP Server **192.168.100.59** akan terjadi connection time out dikarenakan komputer tidak bisa menerima dikarenakan sudah dilakukan dropped atau ditolak.



Gambar 3. Hasil Rules pada SSH

- Port 80 (HTTP)

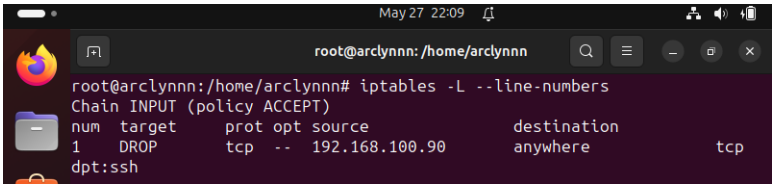
  Dan juga ketika melakukan akses melalui web menggunakan IP **192.168.100.59** akan terjadi juga connection has time out dikarenakan akses dari Server sendiri sudah melakukan dropped atau menolak IP **192.168.100.90** (client) hal ini merupakan cara memblokir dari IP address yang mencurigakan atau tidak sah.



Gambar 4. Hasil Rules pada HTTP

3. Menonaktifkan *rules* yang sudah dibuat

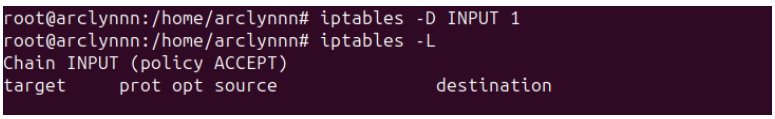
Sebelum menonaktifkan sebuah aturan yang sudah dibuat user melihat numbers pada **chain INPUT** dengan menggunakan command yaitu **iptables -L --line-numbers.**



Gambar 5. Cek Line Numbers Aktif

Setelah melihat daftar semua aturan yang aktif, kemudian user menghapus aturan (rule) pada **chain INPUT** dengan command **iptables -D INPUT 1**, Angka "1" merupakan posisi aturan yang akan dihapus.

Kemudian **iptables -L** berfungsi sebagai menampilkan daftar semua aturan iptables yang aktif. Karena tidak ada aturan yang ditampilkan, berarti aturan aktif pada **chain INPUT** setelah aturan pertama sudah dihapus.



Gambar 6. Delete Rules yang Dibuat

Simpulan

IPTables merupakan tools yang ampuh untuk mengelola traffic network di Linux. Dengan IPTables, kita dapat membuat aturan terutama memblokir berdasarkan berbagai kriteria seperti IP Address, port, protokol, dan lainnya.

Penting untuk berhati-hati saat menggunakan IPTables karena kesalahan dalam mengkonfigurasi dapat menyebabkan masalah konektivitas. Disarankan membuat cadangan konfigurasi IPTables sebelum melakukan perubahan dan uji perubahan tersebut secara menyeluruh sebelum menerapkannya secara permanen.

Daftar Pustaka

Adhi Purwaningrum, F., Purwanto, A., Agus Darmadi, E., Tri Mitra Karya Mandiri Blok Semper Jomin Baru, P., & -Karawang, C. (2018). *Optimalisasi Jaringan Menggunakan Firewall*. *2*(3), 17–23.

Aditya Irfan Puji Handoko. (2017). Prototype Pengendalian Lampu Panggung Menggunakan WEB Broser Melalui Jaringan Lokal Berbasis Arduino. *Repository Universitas Teknologi Digital Indonesia*, 3–8.

Al Amien, J. (2020). Implementasi Keamanan Jaringan Dengan Iptables Sebagai Firewall Menggunakan Metode Port Knocking. *Jurnal Fasilkom*, *10*(2), 159–165.

Dali, F. (2017). Sistem Keamanan Jaringan Menggunakan Cisco AnyConnect Dengan Metode Network Access Manager. *Jurnal Ilmu Teknik Dan Komputer*, *Vol.X*(No. X), 1–7.

Doni, F. . (2015). Optimalisasi Jaringan Wireless Dengan Router Mikrotik Studi Kasus Kampus Bsi Tangerang. *175.45.187.195*, *II*(1), 31124.

Habsy, B. A. (2017). Seni Memehami Penelitian Kuliatatif Dalam Bimbingan Dan Konseling : Studi Literatur. *JURKAM: Jurnal Konseling Andi Matappa*, *1*(2), 90. https://doi.org/10.31100/jurkam.v1i2.56

Harjono, E. B. (2016). Analisa Dan Implementasi Dalam Membangun Sistem Operasi Linux Menggunakan Metode LSF Dan REMASTER. *Jurnal & Penelitian Teknik Informatika*,

1(1), 1–6.

Hawari, M. S. (2017). Penerapan Iptables Firewall Pada Linux Dengan Menggunakan Fedora. *Jurnal Manajemen Informatika*, *6*, 198–207.

Hendita, G., & Kusuma, A. (1997). Perancangan Skema Sistem Keamanan Jaringan Web Server menggunakan Web Application Firewall dan Fortigate untuk Mencegah Kebocoran Data di Masa Pandemi Covid-19. *Journal of Informatics and Advanced Computing*, *92*(1–2), 37–37. https://doi.org/10.1515/zwf-1997-921-220

Jusuf Heni. (2015). Penggunaan Secure Shell (SSH) Sebagai Sistem Komunikasi Aman Pada Web Ujian Online. *Bina Insani Ict Journal*, *2*(2), 75–84.

Munawar, Z., Kom, M., & Putri, N. I. (2020). Keamanan Jaringan Komputer Pada Era Big Data. *Jurnal Sistem Informasi-J-SIKA*, *02*(01), 14–20.

Pamuji, S. A., Iswahyudi, C., & Informatika, T. (2020). Analisis Dan Optimasi Dari Simulasi Keamanan Jaringan Menggunakan Firewall Mikrotik Studi Kasus Di Taman Pintar Yogyakarta. *Jurnal JARKOM*, *7*(1), 65–75.

Permana, R., Ramadhani, D., & Lestari, I. (2019). Proteksi Keamanan Jaringan Komputer di Sekolah Menengah Kejuran Al-Madani Pontianak. *International Journal of Natural Science and Engineering*, *3*(1), 37. https://doi.org/10.23887/ijnse.v3i1.22175

R.Karthikeyan, M. G. ; (2017). A RESEARCH ON SECURE SHELL (SSH) PROTOCOL. *International Journal of Pure and Applied Mathematics*, *116*(16), 559–564.

Raharja, R. A., Yunianto, A., Widyantoro, W., & Wiryana, I. M. (2001). Pengenalan Linux. *Journal Open Source Campus Agreement*, 7.

Setyadi, B. B. H. ; E. B. ; H. J. (2017). *Teknik Hacking Web Server Dengan SQLMAP Di Kali Linux*. https://e-journals.unmul.ac.id/index.php/INF/article/download/642/pdf

Sugiyono. (2016). Sistem keamanan jaringan komputer menggunakan metode watchguard firebox pada pt guna karya indonesia. *Jurnal CKI*, *9*(1), 1–8.

Widianto, T. K., & Sulistyo, W. (2021). Implementasi Iptables Firewall dan Intrusion Detection System Untuk Mencegah Serangan DDoS Pada Linux Server. *MEANS (Media Informasi Analisa Dan Sistem)*, *6*(1), 19–23. https://doi.org/10.54367/means.v6i1.1231

Yona, S. (2014). Penyusunan Studi Kasus. *Jurnal Keperawatan Indonesia*, *10*(2), 76–80. https://doi.org/10.7454/jki.v10i2.177

Zabar, A. A., & Novianto, F. (2015). Keamanan Http Dan Https Berbasis Web Menggunakan Sistem Operasi Kali Linux. *Komputa : Jurnal Ilmiah Komputer Dan Informatika*, *4*(2), 69–74. https://doi.org/10.34010/komputa.v4i2.2427