Implementasi Firewall Pada Protokol SSH Linux Ubuntu Menggunakan Iptables

Tamsir Ariyadi, M. Rizky Pohan , M. Khairul Hadi, Ahmad Anwar Widodo
Departement of Computer Engineering, Bina Darma University

Correspondence Author: tamsirariyadi@binadarma.ac.id

Abstract
Jaringan *Firewall* merupakan salah satu cara untuk mengamankan sistem komputer dari serangan yang tidak diinginkan. Salah satu metode yang dapat digunakan untuk mengamankan jaringan firewall adalah menggunakan *IPtables*, yaitu sebuah utilitas yang dapat digunakan untuk mengatur paket data yang masuk atau keluar dari jaringan. Implementasi *firewall* pada sistem operasi *Linux Ubuntu* dengan menggunakan *iptables*. Iptables adalah sebuah aplikasi yang digunakan untuk mengatur paket-paket yang masuk dan keluar dari sebuah sistem. Penggunaan *firewall* pada SSH *Linux Ubuntu* akan meningkatkan keamanan sistem dengan menerapkan aturan yang membatasi akses yang tidak diinginkan. Proses implementasi *firewall* menggunakan iptables akan dijelaskan secara detail dan ditunjukkan contohnya. Hasil yang diharapkan dari implementasi *firewall* ini adalah peningkatan keamanan sistem dan pembatasan akses yang tidak diinginkan.

Keyword: *Iptables, SSH, Linux, Firewall, Security*

1. PENDAHULUAN

Keamanan sistem merupakan hal yang sangat penting dalam dunia teknologi saat ini. Salah satu cara untuk meningkatkan keamanan sistem adalah dengan menggunakan firewall [1]. Firewall digunakan untuk membatasi akses yang tidak diinginkan ke sistem, sehingga hanya trafik yang diizinkan yang dapat masuk ke sistem [2]. *Linux Ubuntu* adalah salah satu sistem operasi yang populer digunakan saat ini, dan SSH *Secure Shell* (SSH) adalah protokol jaringan yang digunakan untuk melakukan koneksi aman ke sistem jarak jauh. SSH menyediakan mekanisme enkripsi yang aman untuk melakukan autentikasi dan mengirimkan data melalui jaringan. Protokol ini digunakan untuk mengakses sistem shell pada server atau perangkat jaringan, dan juga digunakan untuk mengirim perintah dan menerima respons dari sistem jarak jauh [3].

Meskipun SSH merupakan solusi yang aman untuk melakukan koneksi jarak jauh ke sistem operasi *Linux Ubuntu*, terdapat beberapa masalah keamanan yang dapat terjadi. Salah satu masalah utama adalah serangan brute force, yaitu jenis serangan yang mencoba untuk menebak kombinasi username dan password yang benar [4]. Jika sistem tidak dilindungi dengan baik, serangan brute force dapat menyebabkan akun yang aman dikompromikan. Masalah lain adalah serangan man-in-the-middle (MitM), di mana attacker akan mencoba untuk menyadap koneksi antara klien dan *server* dengan cara menyamar sebagai server yang dituju. Ini dapat dilakukan dengan menggunakan teknik seperti ARP spoofing atau DNS *spoofing*. Ada juga masalah dengan konfigurasi yang tidak aman, seperti menggunakan port yang tidak standar atau mengaktifkan perintah yang tidak diinginkan, dapat membuat sistem lebih rentan terhadap serangan.

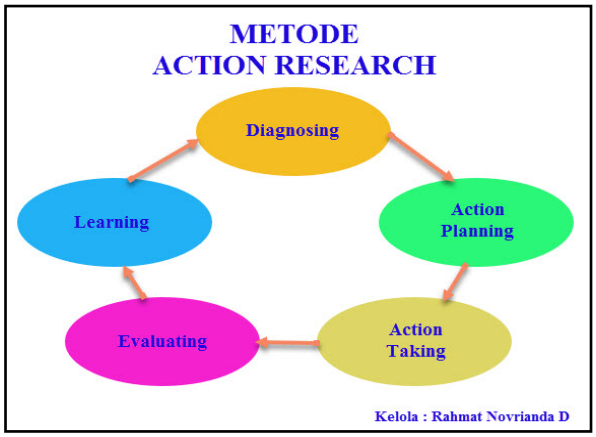
Untuk menunjang topik yang dibahas peneliti menelusuri berbagai literatur dan penelitian terdahulu (*past research*) yang masih berkaitan dengan permasalahan penelitian saat ini, adapun penelitian terdahulu tersebut yaitu SISTEM KEAMANAN OPERASI LINUX UBUNTU IPTABLES SEBAGAI FIREWALL DI DINAS PENDIDIKAN KABUPATEN SERANG. Penelitian ini berfokus dalam perancagan sistem keamanan pada sistem operasi linux menggunakan iptables yang rancangannya di paparkan menggunakan cisco packet tracer [5].

Dari permasalahan yang dijelaskan diatas, akan dibahas tentang implementasi *firewall* pada sistem operasi Linux Ubuntu yang menggunakan SSH, dengan menggunakan iptables sebagai alat untuk mengatur lalu lintas jaringan. *Iptables* adalah sebuah aplikasi yang digunakan untuk mengatur paket-paket yang masuk dan keluar dari sebuah sistem. Penggunaan firewall pada SSH Linux Ubuntu akan meningkatkan keamanan sistem dengan menerapkan aturan yang membatasi akses yang tidak diinginkan [6]. Penelitian ini akan menjelaskan

secara rinci bagaimana cara mengimplementasikan iptables sebagai firewall dan memberikan contoh-contoh dari proses implementasi. Dalam jurnal ini akan dibahas tentang bagaimana mengimplementasikan firewall pada sistem operasi *Linux Ubuntu* dengan menggunakan iptables sebagai alat pengatur lalu lintas jaringan. Implementasi *firewall* ini diharapkan dapat meningkatkan keamanan sistem dan membatasi akses yang tidak diinginkan ke sistem yang digunakan [7].

2. METODE PENELITIAN

Berdasarkan penelitian yang dilakukan oleh peneliti, peneliti menggunakan metode penelitian action research. Metode ini adalah suatu cara yang digunakan untuk menggambarkan, menginterpretasikan, dan menjelaskan suatu keadaan sambil melakukan intervensi yang bertujuan untuk pengembangan yang lebih fokus pada praktik daripada pengetahuan. Metode ini dimulai dari tahap *Diagnosing*, tahap *Action Planning*, tahap *Action Taking*, tahap *Evaluation* dan tahap *Learning* [8].

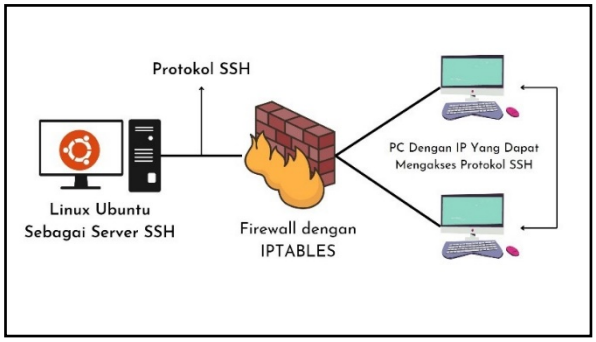


Gambar 1. *Action Research Method.*

2.1. *Diagnosing*

Pada tahap ini akan peneliti melakukan diagnosa terhadap permasalahan dalam keamanan protokol ssh pada sistem operasi *linux ubuntu*. Dimana dalam hal ini peneliti melakukan studi literature untuk mengetahui dan menambah wawasan mengenai permasalahan tersebut dari berbagai sumber seperti jurnal penelitian, paper dan lain sebagainya. Pada tahap ini juga peneliti menemukan solusi apa yang perlu diambil untuk mengatasi permasalahan tersebut.

2.2. *Action Planning*



Gambar 2. Topologi *Firewall Protocol* SSH

Dari diagnosa tersebut peneliti mencoba mencari upaya solusi yang tepat terkait permasalahan dalam keamanan protokol ssh pada sistem operasi *linux ubuntu*. Untuk itu peneliti berencana menggunakan teknologi *firewall* yaitu *iptables* yang nantinya akan dikembangkan menjadi *firewall* dengan menggunakan *iptables* sebagai alat untuk mengatur lalu lintas jaringan. Dengan adanya ini Penggunaan *firewall* pada SSH *Linux Ubuntu* akan meningkatkan keamanan sistem dengan menerapkan aturan yang membatasi akses yang tidak diinginkan. Pada *protocol SSH Linux Ubuntu* diimplementasikan firewall IP tables untuk membatasi komputer yang dapat mengakses *protocol* SSH dari *Linux Ubuntu*.

2.3. *Action Taking*

Setelah perencanaan dibuat peneliti mulai mengeksekusi apa yang telah direncanakan sebelumnya dimana pada bagian ini dibagi menjadi beberapa tahap, yakni :

a) Perancangan sistem
b) Konfigurasi ssh
c) Konfigurasi *iptables*

2.4. *Evaluating*

Pada tahapan ini,peneliti akan melakukan evaluasi terhadap hasil penelitian dimana nantinya peneliti akan mencoba implementasi firewall pada sistem operasi Linux Ubuntu yang menggunakan SSH. Dimana nantinya Penggunaan firewall pada SSH Linux Ubuntu akan meningkatkan keamanan sistem dengan menerapkan aturan yang membatasi akses yang tidak diinginka. Dalam hal ini pula diharapkan dapat meningkatkan keamanan sistem dan membatasi akses yang tidak diinginkan ke sistem yang digunakan.

2.5. *Learning*

Tahapan ini merupakan tahapan akhir dari Metode Penelitian, dimana pada tahapan ini peneliti melakukan uji coba kembali terhadap hasil penelitian dan pemahaman kembali terkait penggunaan dari hasil penelitian agar hasilnya lebih baik.

3. HASIL DAN ANALISA

Terdapat dua prosedur yang penulis gunakan untuk membuat firewall ssh menggunakan iptables. Studi literatur merupakan prosedur pertama untuk mengumpulkan literatur/artikel tentang firewall ssh menggunakan iptables. Prosedur kedua yaitu, perancangan sistem dalam hal ini penulis mulai dari menginstall ssh pada linux ubuntu hingga pembuatan firewall dengan iptables.

3.1. Konfigurasi SSH

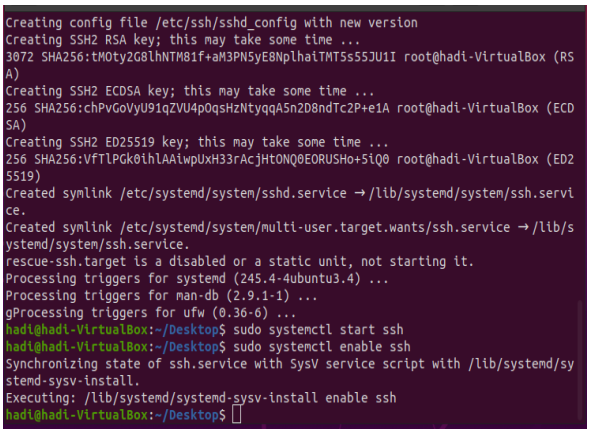
Sebelum konfigurasi dilakukan sebaiknya update list package/aplikasi dari repository server. Setelah selasai instalasi package *openssh-server* [9]. Setelah langkah-langkah tersebut berhasil dilakukan maka langkah selanjutnya yaitu login remote ssh, pada linux ubuntu.

Jalankan terminal pada linux ubuntu, sebelum login ke remote pastikan ssh client bisa terkoneksi ke *server* dengan ping ke ip yang digunakan peda server [10]. Untuk melihat tahapan ini, disajikan pada gambar 3 dan 4.

```
hadi@hadi-VirtualBox:~/Desktop$ sudo apt-get update -y
[sudo] password for hadi:
Hit:1 http://id.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://id.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:3 http://security.ubuntu.com/ubuntu focal-security InRelease
Hit:4 http://id.archive.ubuntu.com/ubuntu focal-backports InRelease
Reading package lists... Done
hadi@hadi-VirtualBox:~/Desktop$ sudo apt-get install openssh-server -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-client openssh-sftp-server ssh-import-id
Suggested packages:
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
The following packages will be upgraded:
  openssh-client
1 upgraded, 4 newly installed, 0 to remove and 518 not upgraded.
Need to get 688 kB/1.359 kB of archives.
After this operation, 6.010 kB of additional disk space will be used.
Get:1 http://id.archive.ubuntu.com/ubuntu focal/main amd64 ncurses-term all 6.2-
0ubuntu2 [249 kB]
```

Gambar 3. *Install package openssh-server*

Konfigurasi dasar ini harus dilakukan pada setiap *Server Linux* setelah instalasi, yang pertama harus dilakukan dengan update terlebih dahulu dengan perintah sudo apt-get update –y. Setelah selesai *update* jalankan *sudo apt-get install openssh-server* –y.

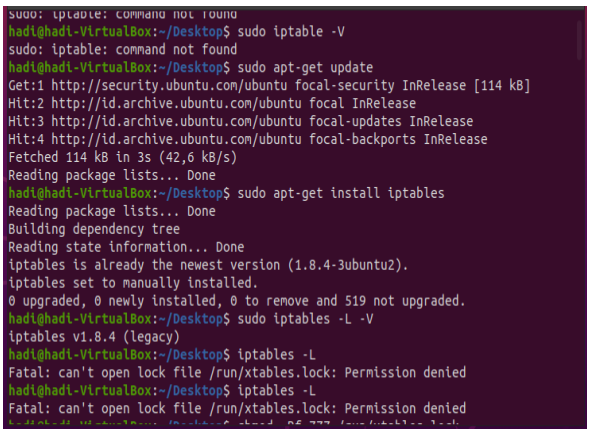


Gambar 4. *Login Remote* SSH

Bertujuan untuk mengakses komputer yang terhubung *internet* agar bisa *login* melakukan konfigurasi. Melalui IP Publik yang sudah dilakukan konfigurasi sesuai dengan yang diinginkan admin.

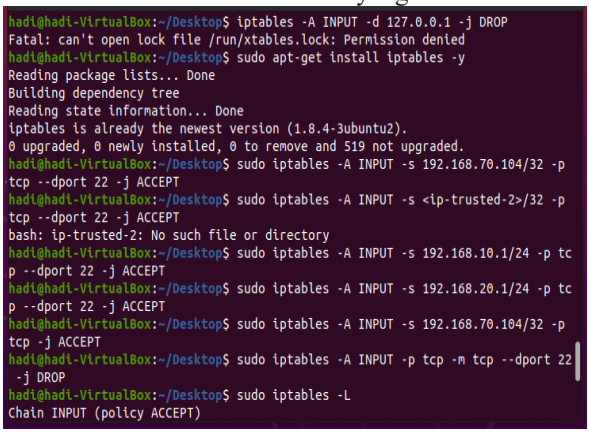
3.2. Konfigurasi *Iptables*

Langkah pertama yaitu, melihat apakah *iptables* sudah terinstal pada *linux ubuntu* dengan cara memasukkan perintah "*sudo iptables* –V". Jika sudah terinstal maka selanjutnya membuat *whitelist* IP *address*. *Whitelist* ini nantinya akan berguna sebagai pembatas apply yang nantinya semua akses ke ssh akan ditolak.Setelah selesai membuat whitelist ip address selanjutnya membuat pembatas akses ssh. Setelah itu login kembali ke *remote ssh*. Untuk melihat tahapan ini, disajikan pada gambar 5, 6 dan 7.



Gambar 5. *Install Iptables*

sudo apt-get install iptables Ini akan mengunduh dan memasang paket iptables beserta dependensi yang dibutuhkan. Perintah *sudo iptables -L -V* pada sistem Linux digunakan untuk menampilkan versi dari iptables yang terpasang pada mesin, serta daftar aturan-aturan firewall yang sudah didefinisikan.



Gambar 6. Membuat *whitelist ip address*

Terlihat pada gambar 6 sudah terbuat *whitelist ip addres* yang bertujuan untuk memudahkan memilih ip yang akan di *accept* atau *drop*.

Gambar 7. *Remote* Login ke SSH.

ssh excelent@192.168.70.115 Ini akan memulai sesi SSH dan meminta untuk memasukkan kata sandi untuk masuk ke mesin tujuan dengan akun "excelent".

3.3. Pembatasan Akses IP Address

Dalam mengamankan sistem terdapat beberapa tahap yang harus di lakukan, mulai dari membuat sistem *accept, rejact* bahkan *drop* [11]. Dengan menggunakan iptables sebagai firewall pada ssh kita bisa drop ip address yang sekiranya membahayakan. Untuk menolak ip address kita harus membuat *whitelist* ip yang akan kita drop atau accept, dengan catatan ip yang akan di whitelist menggunakan format 1 segment IP network [12]. Contoh 192.168.10.1/24 maka semua ip address yang akan di list kisaran (192.168.10.1-192.168.10.254) yg bisa di akses ke ssh. Untuk pembatasan akses ssh dilakukan dengan menjalankan perintah (iptables –A INPUT –p tcp –m tcp –dport 22 –j *DROP*), catatan –dport disesuaikan dengan dport yang di input jika menggunakan dport ssh custom. Untuk remot login ssh sesuaikan dengan ip yang diinput pada remot login ssh pada tahap instalasi package ssh dan ip address yang sudah diwhitelist serta pastikan ip adddress bisa akses ssh server. Contoh perintah (#ssh *excellent*@192.168.10.1) jika testing perintah benar maka akan muncul *(ssh: connect to host 192.168.10.1 port 22: connection time out*) karena ip address sudah di drop dengan sukses. Untuk melihat hasil ini, disajikan pada gambar 8 dan 9.

Tabel 1. Daftar *Whitelist Ip Address*

Ip Address	Destination	Accept	Drop
192.168.70.104	anywhere	√	
192.168.10.1	anywhere	√	
192.168.20.1	anywhere	√	
192.168.70.104	anywhere		√

Tabel 2. Pengujian Implementasi *Firewall* pada Protokol SSH *Linux Ubuntu* menggunakan *Iptables*

Pengujian	Berhasil	Tidak
Konfigurasi SSH	√	
Konfigurasi Ip Tables	√	
Pembatasan Akses Ip Address	√	

4. KESIMPULAN

Firewall digunakan untuk membatasi akses yang tidak diinginkan ke sistem, sehingga hanya trafik yang diizinkan yang dapat masuk ke sistem. *Linux Ubuntu* adalah salah satu sistem operasi yang populer digunakan saat ini, dan *SSH Secure Shell* (SSH) adalah protokol jaringan yang digunakan untuk melakukan koneksi aman ke sistem jarak jauh. Ada juga masalah dengan konfigurasi yang tidak aman, seperti menggunakan port yang tidak standar atau mengaktifkan perintah yang tidak diinginkan, dapat membuat sistem lebih rentan terhadap serangan. Dari permasalahan yang dijelaskan diatas, akan dibahas tentang implementasi *firewall* pada sistem operasi *Linux Ubuntu* yang menggunakan SSH, dengan menggunakan iptables sebagai alat untuk mengatur lalu lintas jaringan. Penggunaan firewall pada *SSH Linux Ubuntu* akan meningkatkan keamanan sistem dengan menerapkan aturan yang membatasi akses yang tidak diinginkan. Penulis menggunakan laptop untuk membuat *firewall* ssh menggunakan iptables yang di instal pada sistem operasi linux ubuntu menggunakan virtual box. Untuk menolak ip address kita harus membuat *whitelist* ip yang akan kita drop atau accept, dengan catatan ip yang akan di whitelist menggunakan format 1 segment IP network. Untuk *remote login* ssh sesuaikan dengan ip

yang diinput pada remot login ssh pada tahap *instalasi package* ssh dan ip address yang sudah diwhitelist serta pastikan ip *adddress* bisa akses *ssh server*.

ACKNOWLEDGEMENTS

Kami ingin mengucapkan terima kasih kepada semua pihak yang telah membantu dalam penelitian ini. Terima kasih kepada program studi teknik komputer. yang telah memberikan dukungan dan masukan yang sangat berguna. Terima kasih juga kepada Universitas Bina Darma Palembang yang telah memberikan sumber daya yang dibutuhkan.

Kami juga ingin mengucapkan terima kasih kepada teman-teman yang telah memberikan dukungan dan semangat selama proses penelitian. Tanpa dukungan dan motivasi dari semua pihak ini, penelitian ini tidak akan mungkin terwujud. Akhir kata, kami ingin mengucapkan terima kasih kepada semua pihak yang tidak dapat kami sebutkan satu per satu.

DAFTAR PUSTAKA

[1] F. Arif, A. Tama, M. Kom, F. Panjaitan, and M. Kom, "Analisis Keamanan Jaringan Pada FasilitasInternet (wifi) Terhadap Serangan PacketSniffing".

[2] M. Iqbal, Arini, and H. Bayu Suseno, "Analysis and Simulation of Ubuntu Server Network Security Using Port Knocking , Honeypot , Iptables , Icmp," *Cyber Secur. dan Forensik Digit.*, vol. 3, no. 1, pp. 27–32, 2020.

[3] R. N. Dasmen, M. Hendra Firmansyah, M. Khadafi, and Tri Yolanda, "Penerapan Keamanan Jaringan Menggunakan Metode Firewall Security Port," *Decod. J. Pendidik. Teknol. Inf.*, vol. 2, no. 1, pp. 1–7, 2022, doi: 10.51454/decode.v2i1.29.

[4] G. Sondakh, M. E. I. Najoan, and A. S. Lumenta, "Perancangan Filtering Firewall Menggunakan Iptables Di Jaringan Pusat Teknologi Informasi Unsrat," *J. Tek. Elektro dan Komput.*, vol. 3, no. 4, pp. 19–27, 2018.

[5] D. Adhi Laksono, "Desain dan Implementasi Firewall dengan Layer 7 Filter Pada Jaringan Teknik Elektro," *Semin. TA*, vol. 2, no. Jaringan Komputer, pp. 1–7, 2012.

[6] R. Ernawati, I. Ruslianto, S. Bahri, J. Rekayasa, and S. Komputer, "Implementasi Metode Port Knocking Pada Sistem Keamanan Server Ubuntu Virtual Berbasis Web Monitoring," *J. Komput. Dan Apl.*, vol. 10, no. 01, pp. 158–169, 2022.

[7] Yuisar, L. Yulianti, and Y. Suzantry, "Analisa Pemanfaatan Proxy Server Sebagai Media Filtering," *J. Media Infotama*, vol. 11, no. 1, pp. 81–90, 2015.

[8] T. Ariyadi, "Mitigasi Distributed Denial of Service (DDoS) Attack Pada Arsitektur Software Defined Network (SDN)," *Techno.Com*, vol. 21, no. 4, pp. 878–886, 2022, doi: 10.33633/tc.v21i4.6879.

[9] T. Ariyadi and M. A. Prabowo, "Perbandingan Kinerja Virtual Private Network Antara Vpn Tunnel Dan Internet Protocols Security," *INOVTEK Polbeng - Seri Inform.*, vol. 6, no. 1, p. 80, 2021, doi: 10.35314/isi.v6i1.1698.

[10] G. Adina and T. Ariyadi, "Perancangan Manajemen Ip Adrress Dan Pembatasan Hak Akses Pada Jaringan Vlan Pt . Bumi Sawindo Permai," *Peranc. Manaj. Ip Adrress Dan Pembatasan Hak Akses Pada Jar. Vlan Pt . Bumi Sawindo Permai*, pp. 82–89, 2021.

[11] M. A. Al Fauzan and T. D. Purwanto, "Perancangan Firewall Router Menggunakan Opnsense Untuk Meningkatkan Keamanan Jaringan Pt. Pertamina Asset 2 Prabumulih," *Pros. Semhavok*, pp. 137–146, 2021.

[12] N. Suryana and D. D. Saputra, "Perancangan Penggunaan Firewall Dan Proxy Server Untuk," *J. Sutet*, vol. 8, no. 1, p. International Research Jurnal of Microbiologi, 2018.