Penerapan *Firewall* Pada Sistem Keamanan Jaringan Komputer Di Sekolah SMK Negeri 5 Seluma

Nopri Dwipoyono[1], Khairil[2], Aji Sudarsono[3]

[1]Mahasiswa Prodi Informatika Fakultas Ilmu Komputer Universitas Dehasen Bengkulu.
e-mail : ndpoyono@gmail.com
[2]Dosen Prodi Sistem Informasi Fakultas Ilmu Komputer Universitas Dehasen Bengkulu.
e-mail : khairil@unived.ac.id
[3]Dosen Prodi Informatika Fakultas Ilmu Komputer Universitas Dehasen Bengkulu.
e-mail : sudarsonoaji86@gmail.com
Jalan Meranti Raya Nomor. 32 Sawah Lebar Bengkulu kode Pos.38228 Telp (0736) 22027, Fax.(0736)341139

(Received: Mei 2023, Revised : Agustus 2023, Accepied : Oktober 2023)

Abstract- The Seluma 5 State Vocational High School does not yet have a firewall, so the computer network security at school is still very minimal, both in terms of limiting access to the network. Besides that, internet access at Seluma 5 State Vocational High School is used by teachers and staff to access internet pages by browsing to get information, but there are several teachers and staff who access social media pages and other pages which decreases the effectiveness of the performance of these teachers and staff. Implementation of a Firewall on a computer network security system at the Seluma 5 Vocational High School uses Iptables to monitor packet data traffic processes in the network. With iptables, you can manage network traffic on the server such as allowing, blocking or skipping incoming and outgoing connections, managing ports and so on on the Seluma 5 State Vocational High School Computer Network. Based on the tests that have been carried out, it can be concluded that the implementation of a firewall on the computer network security system at the State Vocational High School 5 Seluma is able to block the ping of death attack and is also able to open and close access to several ports in the network and block the websites facebook.com, instragram .com, and tokopedia.com
Keywords: Firewall, Security System, Computer Network, State Vocational High School 5 Seluma

Intisari-Sekolah Menegah Kejuruan Negeri 5 Seluma tersebut belum memiliki *firewall*, sehingga keamanan jaringan komputer di sekolah masih sangat minim baik dalam pembatasan akses dalam jaringan. Selain itu Akses internet di Sekolah Menegah Kejuruan Negeri 5 Seluma digunakan oleh guru dan staf untuk mengakses laman internet dengan browsing untuk mendapatkan informasi, namun terdapat beberapa guru dan staf yang mengakses laman sosial media dan laman lainnya yang membuat menurunnya efektifitas kinerja dari guru dan staf tersebut Penerapan Firewall pada sistem keamanan jaringan komputer di Sekolah Sekolah Menegah Kejuruan Negeri 5 Seluma menggunakan Iptables untuk memonitoring proses lalu lintas paket data dalam jaringan. Dengan iptables, dapat mengatur lalu lintas jaringan dalam server seperti mengizinkan, memblokir atau melewatkan koneksi masuk dan keluar, mengelola port dan lain sebagainya di Jaringan Komputer Sekolah Sekolah Menegah Kejuruan Negeri 5 Seluma. Berdasarkan pengujian yang telah dilakukan, maka dapat disimpulkan bahwa penerapan firewall pada sistem keamanan jaringan komputer di Sekolah Menegah Kejuruan Negeri 5 Seluma mampu memblokir serangan ping of death dan juga mampu membuka serta menutup akses beberapa port dalam jaringan dan memblokir situs web facebook.com, instragram.com, dan tokopedia.com
Kata Kunci : *Firewall, Sistem Keamanan, Jaringan Komputer,* Sekolah Menegah Kejuruan *Negeri 5 Seluma*

I.PENDAHULUAN

Banyaknya kemudahan yang didapat oleh pengguna internet menyebabkan teknologi tersebut tumbuh dengan sangat cepat. Hampir semua aspek informasi dapat diperoleh melalui internet mulai dari pendidikan, hiburan, olahraga, pemerintahan, sekolah, dan lain-lain. Internet bisa diakses hampir semua kalangan baik anak-anak maupun dewasa untuk mencari informasi. SMK Negeri 5 Seluma merupakan salah satu Sekolah Menengah Kejuruan Negeri yang terdapat di Kabupaten Seluma. Akses internet di SMK Negeri 5 Seluma menggunakan indihome dengan bandwidth 40mbps dimana pengguna internet diperuntukkan untuk guru, staf dan praktek belajar yang berjumlah kurang lebih 30-40 orang. Indihome terkoneksi dengan komputer dan laptop di lingkungan kerja SMK Negeri 5 Seluma melalui akses LAN dan Wifi. SMK Negeri 5 Seluma tersebut belum memiliki *firewall*, sehingga keamanan jaringan komputer di sekolah masih sangat minim baik dalam pembatasan akses dalam jaringan. Selain itu Akses internet di SMK Negeri 5 Seluma digunakan oleh guru dan staf untuk mengakses laman internet dengan browsing untuk mendapatkan informasi, namun terdapat

p-ISSN 1858-2680
e-ISSN 2723-4673

beberapa guru dan staf yang mengakses laman sosial media dan laman lainnya yang membuat menurunnya efektifitas kinerja dari guru dan staf tersebut. Dalam proses praktek belajar mengajar di Laboratorium, baik guru dan siswa dapat mengakses internet pada komputer masing-masing. Namun terkadang, diperlukan pembatasan akses internet pada komputer yang digunakan oleh siswa di Laboratorium untuk membantu siswa agar lebih fokus dalam praktek belajar di Laboratorium, karena terkadang terdapat beberapa siswa yang membuka laman web yang tidak berhubungan dengan pelajaran yang ada di Laboratorium. 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 pada *firewall*. Salah satu cara *firewall* mengamankan sistem jaringan komputer adalah dengan menerapkan penyaringan *port-port web*. Salah satu aplikasi *firewall* yang memiliki fitur untuk dapat melakukannya yaitu aplikasi *iptables* pada *linux*. Dengan adanya *iptables*, pihak sekolah dapat melakukan penyaringan trafik pada server, mengatur lalu lintas jaringan, termasuk mengizinkan atau memblokir koneksi yang masuk, keluar, atau sekedar melewati *server*.

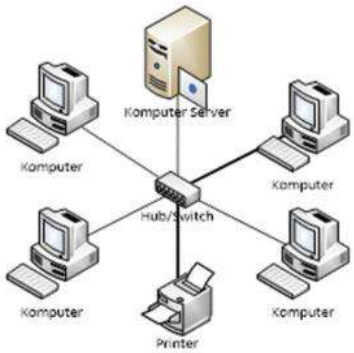
II. TINJAUAN PUSTAKA

A.Jaringan Komputer

Jaringan komputer secara istilah adalah kumpulan komputer yang saling berkaitan dan memiliki hubungan komunikasi antar mereka. Hubungan antara komputer memungkinkan terjadinya operasi yang tidak mungkin dilakukan dalam keadaan *stand alone*. Kata kunci dari jaringan komputer adalah komunikasi (Amien & Mukhtar, 2020). Jaringan komputer merupakan suatu sistem yang terdiri dari komputer-komputer dan perangkat-perangkat jaringan lainnya yang terhubung satu sama lain, bekerja sama untuk mencapai suatu tujuan. Perangkat jaringan sangat penting untuk berlangsungnya hubungan atau komunikasi antar komputer. Informasi berpindah dari komputer ke komputer lainnya dengan menggunakan jaringan daripada melalui perantara manusia, sehingga membuat pertukaran informasi menjadi lebih cepat dan mudah (Simargolang, et al., 2021). Jaringan komputer adalah jaringan telekomunikasi yang memungkinkan antar komputer untuk saling berkomunikasi dengan bertukar data. Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan (service). Pihak yang meminta/menerima layanan disebut klien (client) dan yang memberikan/mengirim layanan disebut peladen (server) (Husen & Surbakti, 2020)

B. Topologi Jaringan

Topologi jaringan adalah hubungan geometris antara unsur-unsur dasar penyusun jaringan, yaitu *node*, *link*, dan *station*. Topologi jaringan dapat dibagi menjadi 5 kategori utama yaitu (Husen & Surbakti, 2020) : Topologi *star* (bintang) merupakan bentuk topologi yang berupa konvergensi dari *node* tengah ke setiap *node* atau pengguna. Topologi jaringan bintang termasuk topologi jaringan dengan biaya menengah.



Gambar 1. Topologi *Star*

C.TCP/IP

TCP/IP (singkatan dari *Transmission Control Protocol/Internet Protocol*) adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan Internet. Protokol ini tidaklah dapat berdiri sendiri, karena memang protokol ini berupa kumpulan protokol (*protocol suite*). Protokol ini juga merupakan protokol yang paling banyak digunakan saat ini. Data tersebut diimplementasikan dalam bentuk perangkat lunak (*software*) di sistem operasi. Protokol ini juga bersifat *routable* yang berarti protokol ini cocok untuk menghubungkan sistem-sistem berbeda (seperti Microsoft Windows dan keluarga *UNIX*) untuk membentuk jaringan yang heterogen Dalam *TCP/IP* terdapat 5 layer yang akan dijelaskan berikut. *Physical Layer* (lapisan fisik) merupakan lapisan terbawah yang mendefinisikan besaran fisik seperti media

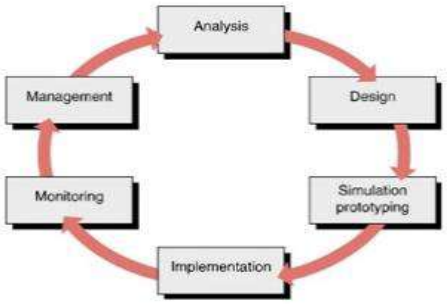
p-ISSN 1858-2680
e-ISSN 2723-4673

komunikasi, tegangan, arus, dan sebagainya. Lapisan ini dapat bervariasi bergantung pada media komunikasi pada jaringan yang bersangkutan. Network Access Layer mempunyai fungsi yang mirip dengan Data Link layer pada OSI. Lapisan ini mengatur penyaluran data *frame-frame* data pada media fisik yang digunakan. Lapisan ini biasanya memberikan servis untuk deteksi dan koreksi kesalahan dari data yang ditransmisikan (Sondakh, et al., 2014).

III. METODOLOGI PENELITIAN

A.Metode Penelitian

Dalam melaksanakan penelitian ini, penulis menggunakan metode *Network Development Life Cycle* (NDLC) yang merupakan sebuah metode yang bergantung pada proses pembangunan sebelumnya seperti perencanaan strategi bisnis, daur hidup pengembangan aplikasi, dan analisis pendistribusian data. Adapun tahapan yang dilakukan dalam NDLC terdiri dari *Analysis*, *Design*, *Simulation Prototyping*, *Implementation*, *Monitoring*, dan *Management*, seperti terlihat pada Gambar 3.1.



Gambar 2. Tahapan Metode *NDLC*

Keterangan :

1. *Analysis*

Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan pengguna, dan analisa topologi jaringan yang sudah ada saat ini.

2. *Design*

Membuat gambaran desain topologi jaringan yang akan dibangun sesuai dengan analisa kebutuhan yang telah dilakukan.

3. *Simulation Prototype*

Tahap dimana dilakukan simulasi dengan bantuan *tools* khusus di bidang jaringan yang digunakan untuk melihat kinerja awal jaringan yang akan dibangun.

4. *Implementation*

Tahap dimana akan dilakukan penerapan rancangan yang telah dibuat agar dapat diuji di lapangan agar dapat menyelesaikan masalah teknik dan non teknis.

5. *Monitoring*

Tahap dimana dilakukan pengamatan terhadap infrastruktur perangkat keras, dan memperhatikan jalannya iptable pada sistem operasi linux ubuntu di dalam jaringan yang telah dibangun

6. *Management*

Tahap dimana menentukan kebijakan untuk membuat/mengatur agar sistem yang telah dibangun dapat berjalan dengan baik dan berlangsung lama.

B. Pengujian Sistem

Pengujian sistem yang dilakukan seperti Tabel

Tabel 1. Pengujian Sistem

Pengujian	Hasil Pengujian	Keterangan
Melakukan serangan ping of deatch dalam jaringan		
Mengakses port 22 SSH pada jaringan		
Mengakses port 80 HTTP pada jaringan		
Mengakses situs web facebook.com		
Mengakses situs web instagram.com		
Mengakses situs web tokopedia.com		

IV.HASIL DAN PEMBAHASAN

A.Hasil

Keamanan jaringan menggunakan iptables terkait terhadap 3 aspek yang diamankan yaitu :

1) Confidentiality yaitu mengharuskan suatau data hanya bisa diakses oleh pengguna sah atau memiliki izin akses.
2) Integrity yaitu mengharuskan suatu data hanya bisa diubah oleh pengguna yang sah atau memiliki izin wewenang
3) Availability yaitu mengharuskan informasi hanya tersedia bagi pengguna yang sah atau memiliki izin akses untuk kebutuhan tersebut

Dari ketiga aspek keamanan jaringan tersebut, telah diterapkan ke dalam iptables dengan membuat rule/aturan dimana user tidak dapat mengakses ping dalam jaringan, hanya mengizinkan IP 192.168.0.100 saja yang dapat mengakses port 22 SHH, mengizinkan semua user untuk mengakses port 80 HTTP, tidak mengizinkan semua user untuk mengakses

p-ISSN 1858-2680
e-ISSN 2723-4673

beberapa situs web (facebook, instagram, dan tokopedia).

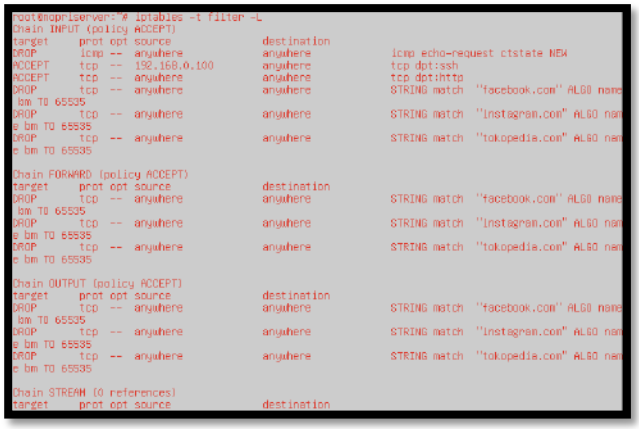
Adapun rule/aturan yang telah diterapkan dengan 3 aspek keamanan tersebut, antara lain :

4) User tidak dapat mengakses ping dalam jaringan
5) Hanya mengizinkan IP 192.168.0.100 saja yang dapat mengakses port 22 SSH
6) Mengizinkan semua user untuk mengakses port 80 HTTP
7) Tidak mengizinkan semua user untuk mengakses beberapa situs web (facebook, instagram, dan tokopedia).

Skema rule/aturan tersebut ditulis dengan membuat perintah iptables dengan memenuhi 3 aspek keamanan *confidentiality*, *integrity*, dan *availability*, dimana pada iptables terdapat chain yang terbagi menjadi 3 bagian yaitu input, forward, dan output yang memiliki fungsi berbeda-beda :

1) Chain INPUT digunakan untuk menangani semua paket yang masuk ke server
2) Chain FORWARD digunakan untuk menangani paket yang diteruskan melalui server
3) Chain OUTPUT digunakan untuk menangani semua paket yang keluar dari server.

Adapun hasil definisi aturan/rule Iptables yang telah dibuat pada server,



Gambar 3. Definisi Aturan/Rule IpTables

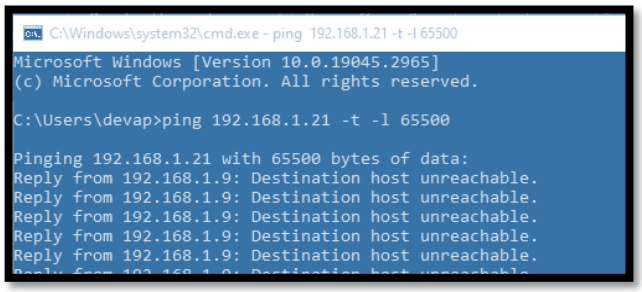
Pada Gambar 3. tersebut terdapat kolom target yang berisi ACCEPT dan DROP, dimana ACCEPT berarti menerima paket yang masuk, sedangkan DROP memutuskan koneksi paket.Setelah aturan/rule iptables didefinisikan seperti Gambar. maka dilakukan pengujian untuk melihat hasil dari penerapan iptables. Adapun hasil penerapan iptables tersebut antara lain :

1) Melakukan serangan ping of death dalam jaringan

Dalam serangan ping of death, dilakukan melalui command prompt melalui client dengan memasukkan perintah :

ping 192.168.1.21 -t -l 65500

dari hasil serangan tersebut, permintaan ping dalam jaringan berhasil diblokir oleh iptables,

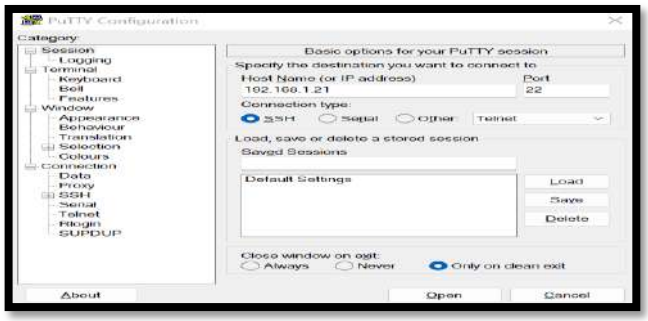


Gambar 4. Blokir Serangan Ping Of Death

Berdasarkan Gambar 4. tersebut, serangan ping of death tersebut di blokir melalui aturan iptables dimana user tidak dapat melakukan ping dengan memberikan informasi destination atau request time out.

2) Mengakses port 22 SSH pada jaringan

Melakukan akses ke port 22 SSH dari client ke server menggunakan aplikasi pihak ketiga yaitu putty. Pada rule/aturan iptable telah didefinisikan bahwa hanya IP Address 192.168.0.100 yang diperbolehkan untuk mengakses port 22 SSH. Adapun pengujian yang dilakukan yaitu dengan membuka aplikasi putty



Gambar 5.. Akses Port 22 SSH Pada Jaringan (1)

Pada Gambar 5. tersebut memasukkan host (sumber) ip address server yaitu 192.168.1.21 dan port 22, kemudian klik open. Jika berhasil maka akan menampilkan hasil.

Gambar 6. Akses Port 22 SSH Pada Jaringan (2)

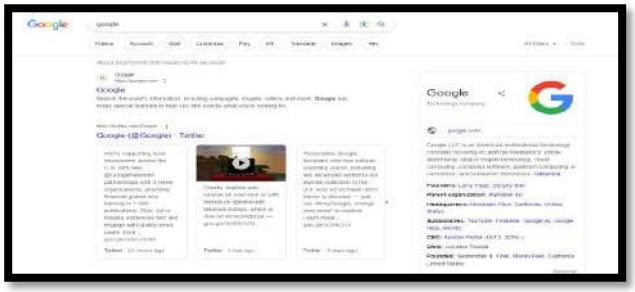
p-ISSN 1858-2680
e-ISSN 2723-4673

Gambar 7. Akses Port 22 SSH Pada Jaringan (3)

Terlihat bahwa IP Address 192.168.0.100 melalui putty berhasil mengakses port 22 SSH sesuai dengan rule/aturan iptables yang telah didefinisikan.

3) Mengakses port 80 HTTP pada jaringan

Melakukan akses ke port 80 HTTP dari client melalui browser web. Pada rule/aturan telah didefinisikan bahwa semua client dapat mengakses port 80 HTTP. Adapun hasil pengujian yang dilakukan yaitu dengan membuka browser dan mengetik url web yang dituju, jika berhasil maka akan menampilkan gambar

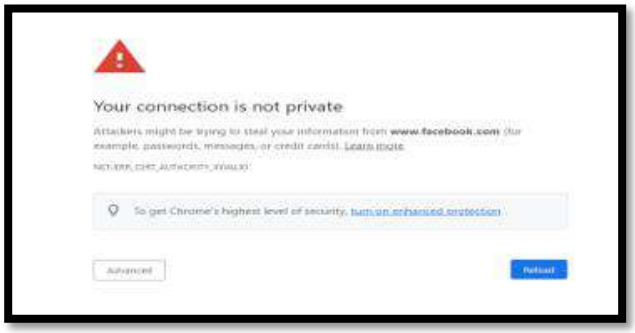


Gambar 8. Akses Port 80 HTTP Pada Jaringan

Berdasarkan Gambar 8. tersebut, terlihat bahwa semua client dapat mengakses port 80 SSH sesuai dengan rule/aturan iptables yang telah didefinisikan.

4) Mengakses situs web facebook.com

Melakukan akses ke situs web facebook.com setelah menerapkan iptable, dan menampilkan halaman web facebook.com yang telah diblokir.

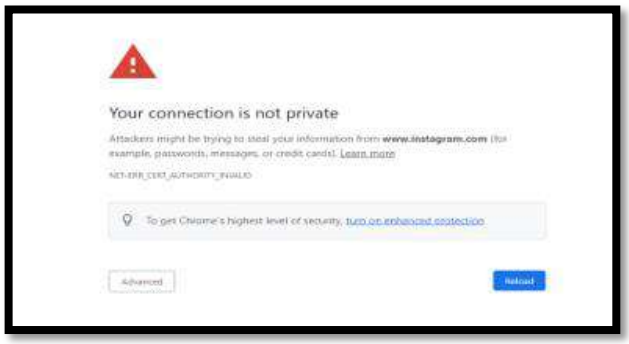


Gambar 9. Akses Situs Web Facebook.com Setelah Menerapkan Iptables

Berdasarkan Gambar 9 tersebut, terlihat bahwa facebook tidak dapat diakses oleh client, sesuai dengan rule/aturan iptables yang telah didefinisikan.

5) Mengakses situs web instagram.com

Melakukan akses ke situs web instagram.com setelah menerapkan iptable, dan menampilkan halaman web instagram.com yang telah diblokir.



Gambar 10. Akses Situs Web instagram.com Setelah Menerapkan Iptables

Berdasarkan Gambar 10 tersebut, terlihat bahwa instagram tidak dapat diakses oleh client, sesuai dengan rule/aturan iptables yang telah didefinisikan

6) Mengakses situs web tokopedia.com

Melakukan akses ke situs web tokopedia.com setelah menerapkan iptable, dan menampilkan halaman web tokopedia.com yang telah diblokir.

Gambar 11. Akses Situs Web tokopedia.com Setelah Menerapkan Iptables

Berdasarkan Gambar 11 tersebut, terlihat bahwa tokopedia tidak dapat diakses oleh client, sesuai dengan rule/aturan iptables yang telah didefinisikan. Dari ke enam hasil penerapan iptables yang telah dilakukan, terlihat bahwa iptables dapat membantu pihak sekolah dalam mengamankan sistem jaringan dan memaksimalkan kinerja staf/guru di sekolah.

B. Pembahasan

Penerapan Firewall pada sistem keamanan jaringan komputer di Sekolah SMK Negeri 5 Seluma dibangun menggunakan sistem operasi

p-ISSN 1858-2680
e-ISSN 2723-4673

Linux Ubuntu Server 20.04.6. dan firewall yang digunakan yaitu Iptables. Sistem operasi Linux Ubuntu Server 20.04.6 diinstal melalui mesin virtual server. Adapun tahapan instalasi tersebut, antara lain :

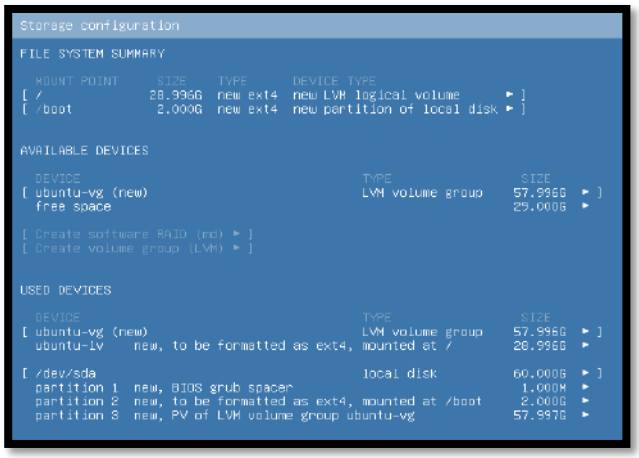
1) Memilih bahasa yang digunakan

Gambar 12. Memilih Bahasa

2) Konfigurasi Keyboard

Gambar 13. Konfigurasi Keyboard

3) Konfigurasi media penyimapan



Gambar 14. Storage Configuration

4) Membuat profile setup.

Gamb 15. Profile Setup

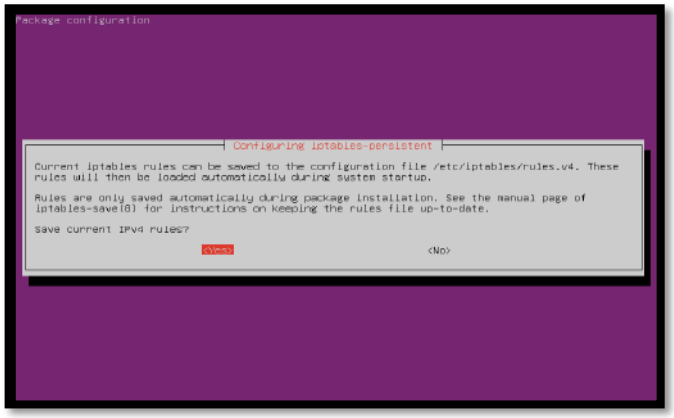
5) Proses instalasi linux ubuntu.

Gambar 16. Proses Instalasi Linux Ubuntu

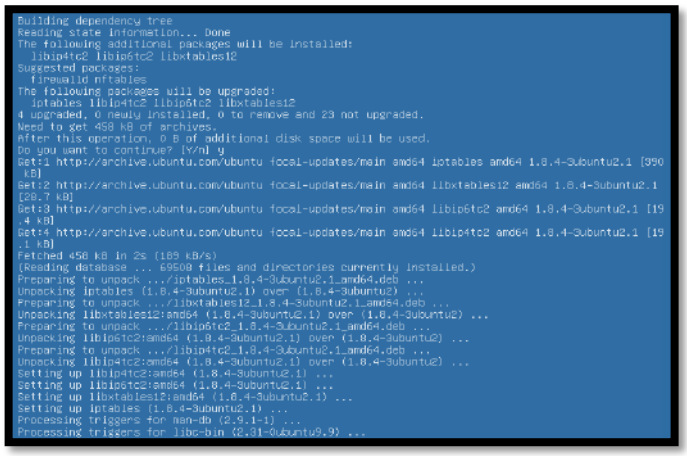
Setelah instalasi linux ubuntu server berhasil, maka langkah selanjutnya yaitu melakukan instalasi iptable melalui perintah berikut :

apt-get install iptables iptables-persistent

Dan proses instalasi iptables pada sistem operasi linux ubuntu server



Gambar 17. Instalasi Iptables (1)



Gambar 18. Instalasi Iptables (2)

Kemudian melihat status awal dari iptables dengan perintah iptables -t filter -L, sehingga menampilkan rule/aturan iptables

p-ISSN 1858-2680
e-ISSN 2723-4673

```
root@nopriserver:/home/nopri# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Gambar 19. Status Iptables

Setelah itu melakukan konfigurasi iptables untuk memasukkan aturan-aturan pada iptables, sebagai berikut :

1) Memblokir jika terdapat permintaan ping dalam jaringan (serangan *ping of death*)

Pada tahap ini dilakukan definisi rule/aturan untuk memblokir permintaan ping dalam jaringan dengan cara mengetik rule/aturan seperti :

Iptables -A INPUT -p icmp --icmp-type 8 -m contrack -ctstate NEW -j DROP

Dari kode tersebut diperuntukkan untuk disimpan pada chain INPUT.

```
root@nopriserver:~# iptables -A INPUT -p icmp --icmp-type 8 -m conntrack --ctstate NEW -j DROP
```

Gambar 20. Rule Iptables Blokir Permintaan Ping

Pada Gambar 20. terlihat bahwa rules iptables yang telah dibuat untuk memblokir ping sudah didefinisikan dengan cara melihat list rule iptables melalui perintah : iptables -t filter -L

Dari perintah tersebut, akan menampilkan rules yang telah didefinisikan

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  anywhere             anywhere             icmp echo-request ctstate NEW

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain STREAM (0 references)
target     prot opt source               destination
```

Gambar 21. Rule Iptables Ping Yang Telah Didefinisikan

Rules untuk blokir ping terdapat pada ChainINPUT dimana terlihat bahwa :

a) Target = drop, mendefinisikan untuk memutuskan koneksi paket
b) prot = icmp, mendefinisikan protokol yang digunakan
c) source = anywhere, mendefinisikan sumber yang akan melakukan ping, dimana telah di setting anywhere berarti dimana saja yang masih terhubung dengan server iptables
d) destination = anywhere, mendefinisikan tujuan yang diping dimana telah di setting anywhere berarti dimana saja yang masih terhubung dengan server iptables
2) Memperbolehkan akses hanya client dengan IP Address 192.168.0.100 yang dapat mengakses port 22 SSH pada server iptables 192.168.1.21.

Pada tahap ini dilakukan definisi rule/aturan untuk mengizinkan akses hanya client dengan IP Address 192.168.0.100 yang dapat mengakses port 22 SSH pada server iptables dengan cara mengetik rule/aturan seperti :

Iptables -A INPUT -s 192.168.0.100 -p tcp –dport 22 -j ACCEPT

Dari kode tersebut diperuntukkan untuk disimpan pada chain INPUT,

Gambar 22. Rule Iptables Perbolehkan Akses Port 22

Terlihat bahwa rules iptables yang telah dibuat untuk akses port SSH sudah didefinisikan dengan cara melihat list rule iptables melalui perintah :

iptables -t filter -L

Dari perintah tersebut, akan menampilkan rules yang telah didefinisikan

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  anywhere             anywhere             icmp echo-request ctstate NEW
ACCEPT     tcp  --  192.168.0.100        anywhere             tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain STREAM (0 references)
target     prot opt source               destination
```

Gambar 23. Rule Iptables SSH Yang Telah Didefinisikan

Tersebut terlihat bahwa port 22 ssh telah didefinisikan hanya dapat diakses oleh IP Address 192.168.0.100 pada Chain INPUT dimana :

a) Target = Accept, mendefinisikan untuk menerima paket yang masuk
b) Prot = tcp, mendefinisikan protokol yang digunakan
c) Source = 192.168.0.100, mendefinisikan bahwa sumber atau source yang dapat melakukan akses ke port 22 hanya IP 192.168.0.100
d) Destination = anywhere, mendefinisikan tujuan yang akan diakses port SSHny disetting anywhere, berarti dimana saja yang masih terhubung dengan server iptables.

p-ISSN 1858-2680
e-ISSN 2723-4673

3) Memperbolehkan seluruh network bisa mengakses port 80 pada server

Pada tahap ini dilakukan definisi rule/aturan untuk memperbolehkan seluruh jaringan bisa mengakses port 80 HTTP dengan cara mengetik rule/aturan seperti :

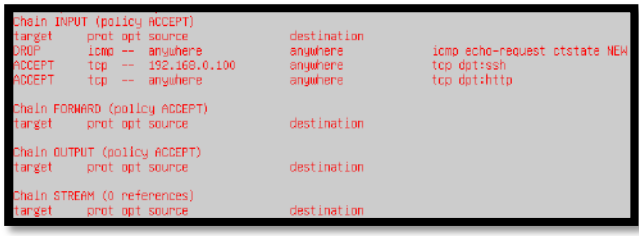
Iptables -A INPUT -s 0/0 -p tcp --dport 80 -j ACCEPTDari kode tersebut diperuntukkan untuk disimpan pada chain INPUT,

Gambar 24. Rule Iptables Perbolehkan Akses Port 80

Terlihat bahwa rules iptables yang telah dibuat untuk akses port HTTP sudah didefinisikan dengan cara melihat list rule iptables melalui perintah :

iptables -t filter -L

Dari perintah tersebut, akan menampilkan rules yang telah didefinisikan

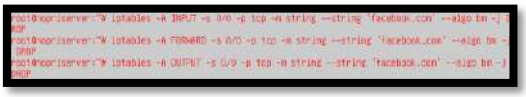


Gambar 25. Rule Iptables HTTP Yang Telah Didefinisikan

Tersebut terlihat bahwa port 80 HTTP telah didefinisikan agar dapat diakses pada Chain INPUT dimana :

a) Target = Accept, mendefinisikan untuk menerima paket yang masuk
b) Prot = tcp, mendefinisikan protokol yang digunakan
c) Source = anywhere, mendefinisikan sumber yang akan melakukan akses HTTP, dimana telah di setting anywhere berarti dimana saja yang masih terhubung dengan server iptables
d) Destination = anywhere, mendefinisikan tujuan yang akan diakses akses HTTP disetting anywhere, berarti dimana saja yang masih terhubung dengan server iptables.
4) Menutup semua akses jaringan sehingga tidak dapat mengakses situs facebook.com

Dalam menutup akses pada situs web facebook.com, terdapat chain yang didefinisikan yaitu INPUT, FORWARD, dan OUTPUT dengan perintah



Gambar 26. Rule Iptables Menutup Akses Facebook.com

Terlihat bahwa rules iptables yang telah dibuat untuk memblokir akses facebook.com sudah didefinisikan dengan cara melihat list rule iptables melalui perintah :

iptables -t filter -L

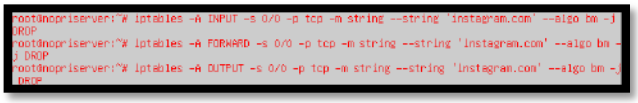
Dari perintah tersebut, akan menampilkan rules yang telah didefinisikan

Gambar 27 Rule Iptables Facebook.com Yang Telah Didefinisikan

Terlihat bahwa semua source tidak dapat mengakses facebook.com yang telah didefinisikan agar dapat diakses pada Chain INPUT, FORWARD, OUTPUT dimana :

a) Target = Drop, mendefinisikan untuk memutuskan koneksi paket
b) Prot = tcp, mendefinisikan protokol yang digunakan
c) Source = anywhere, mendefinisikan sumber yang akan melakukan akses ke facebook.com, dimana telah di setting anywhere berarti dimana saja yang masih terhubung dengan server iptables
d) Destination = anywhere, mendefinisikan tujuan yang akan diakses akses facebook.com disetting anywhere, berarti dimana saja yang masih terhubung dengan server iptables.
5) Menutup semua akses jaringan sehingga tidak dapat mengakses situs instagram.com

Dalam menutup akses pada situs web instagram.com, terdapat chain yang didefinisikan yaitu INPUT, FORWARD, dan OUTPUT dengan perintah seperti Gambar 4.26



Gambar 28. Rule Iptables Menutup Akses Instagram.com

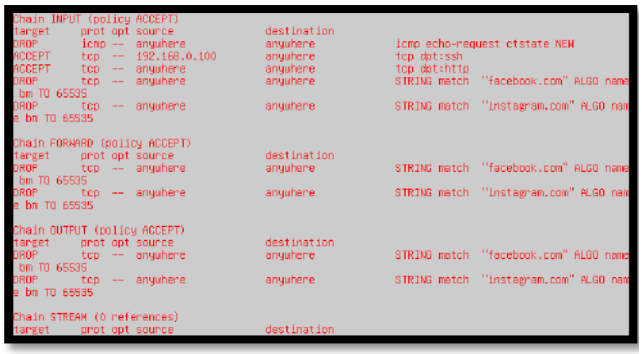
Pada Gambar 4.26. terlihat bahwa rules iptables yang telah dibuat untuk memblokir akses

p-ISSN 1858-2680
e-ISSN 2723-4673

instagram.com sudah didefinisikan dengan cara melihat list rule iptables melalui perintah :

iptables -t filter -L

Dari perintah tersebut, akan menampilkan rules yang telah didefinisikan



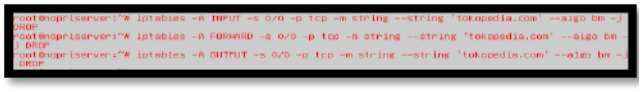
Gambar 29. Rule Iptables Instagram.com Yang Telah Didefinisikan

Tersebut terlihat bahwa semua source tidak dapat mengakses instagram.com yang telah didefinisikan agar dapat diakses pada Chain INPUT, FORWARD, OUTPUT dimana :

a) Target = Drop, mendefinisikan untuk memutuskan koneksi paket
b) Prot = tcp, mendefinisikan protokol yang digunakan
c) Source = anywhere, mendefinisikan sumber yang akan melakukan akses ke instagram.com, dimana telah di setting anywhere berarti dimana saja yang masih terhubung dengan server iptables
d) Destination = anywhere, mendefinisikan tujuan yang akan diakses akses instagram.com disetting anywhere, berarti dimana saja yang masih terhubung dengan server iptables.

6) Menutup semua akses jaringan sehingga tidak dapat mengakses situs tokopedia.com

Dalam menutup akses pada situs web tokopedia.com, terdapat chain yang didefinisikan yaitu INPUT, FORWARD, dan OUTPUT dengan perintah

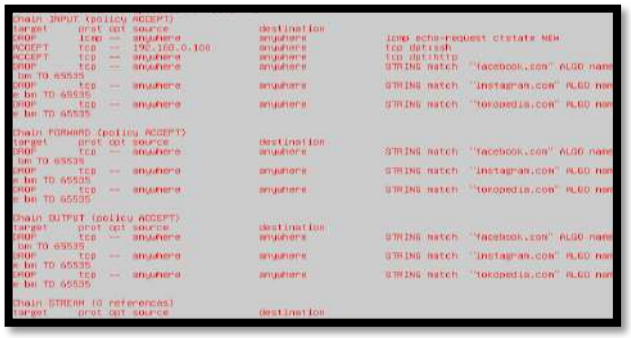


Gambar 30 Rule Iptables Menutup Akses Tokopedia.com

Terlihat bahwa rules iptables yang telah dibuat untuk memblokir akses instagram.com sudah didefinisikan dengan cara melihat list rule iptables melalui perintah :

iptables -t filter -L

Dari perintah tersebut, akan menampilkan rules yang telah didefinisikan

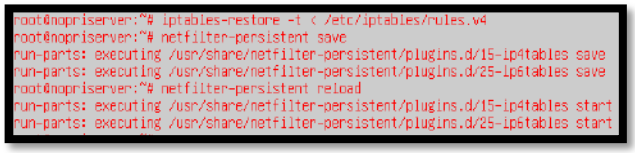


Gambar 31 Rule Iptables Tokopedia.com Yang Telah Didefinisikan

Terlihat bahwa semua source tidak dapat mengakses instagram.com yang telah didefinisikan agar dapat diakses pada Chain INPUT, FORWARD, OUTPUT dimana :

a) Target = Drop, mendefinisikan untuk memutuskan koneksi paket
b) Prot = tcp, mendefinisikan protokol yang digunakan
c) Source = anywhere, mendefinisikan sumber yang akan melakukan akses ke instagram.com, dimana telah di setting anywhere berarti dimana saja yang masih terhubung dengan server iptables
d) Destination = anywhere, mendefinisikan tujuan yang akan diakses akses instagram.com disetting anywhere, berarti dimana saja yang masih terhubung dengan server iptables.

7) Setelah semua rule/aturan iptables telah didefinisikan pada server, langkah selanjutnya menyimpan rule tersebut dengan perintah



Gambar 32. Menyimpan Rule Iptables

Tersebut terlihat bahwa terdapat perintah untuk menyimpan rules yang telah didefinisikan pada iptables agar masuk kedalam ip4tables dan ip6tables dalam sistem.

8) Kemudian restart service iptables dan melihat status iptable dengan perintah

p-ISSN 1858-2680
e-ISSN 2723-4673

Gambar 33. Restart dan Melihat Status Service Iptables

C.Pengujian Sistem

Pada tahap ini dilakukan pengujian terhadap Penerapan Firewall pada sistem keamanan jaringan komputer di Sekolah SMK Negeri 5 Seluma apakah berjalan dengan baik atau tidak. Pengujian dilakukan sistem keamanan jaringan komputer di Sekolah SMK Negeri 5 Seluma

Tabel 2. Hasil Pengujian

Pengujian	Hasil Pengujian	Keterangan
Melakukan serangan ping of death dalam jaringan	Sistem berhasil meblokir serangan ping of death dalam jaringan	Sesuai harapan
Mengakses port 22 SSH pada jaringan	Sistem berhasil mengakses port 22 pada jaringan	Sesuai harapan
Mengakses port 80 HTTP pada jaringan	Sistem berhasil mengakses port 80 pada jarngan	Sesuai harapan
Mengakses situs web facebook.com	Sistem berhasil memblokir situs web facebook.com	Sesuai harapan
Mengakses situs web instagram.com	Sistem berhasil memblokir situs web instagram.com	Sesuai harapan
Mengakses situs web tokopedia.com	Sistem berhasil memblokir situs web tokopedia.com	Sesuai harapan

Berdasarkan pengujian yang telah dilakukan, maka dapat disimpulkan bahwa penerapan firewall pada sistem keamanan jaringan komputer di SMK Negeri 5 Seluma mampu memblokir serangan ping of death dan juga mampu membuka serta menutup akses beberapa port dalam jaringan dan memblokir situs web facebook.com, instragram.com, dan tokopedia.com

V.KESIMPULAN DAN SARAN

1. Kesimpulan

Berdasarkan hasil dan pembahasan serta pengujian, maka dapat disimpulkan bahwa :

1. Keamanan jaringan menggunakan iptables terkait terhadap 3 aspek yang diamankan yaitu *confidentiality*, *integrity*, dan *availability*. Dari ketiga aspek keamanan jaringan tersebut, telah diterapkan ke dalam iptables dengan membuat rule/aturan untuk mengizinkan, memblokir koneksi masuk dan keluar pada jaringan di SMK Negeri 5 Seluma.
2. Rule/aturan yang telah diterapkan dengan 3 aspek keamanan tersebut, antara lain :
   a) User tidak dapat mengakses ping dalam jaringan
   b) Hanya mengizinkan IP 192.168.0.100 saja yang dapat mengakses port 22 SSH
   c) Mengizinkan semua user untuk mengakses port 80 HTTP
   d) Tidak mengizinkan semua user untuk mengakses beberapa situs web (facebook, instagram, dan tokopedia).
3. Berdasarkan pengujian yang telah dilakukan, maka dapat disimpulkan bahwa penerapan firewall mampu memblokir serangan ping of death dan juga mampu membuka serta menutup akses beberapa port dalam jaringan dan memblokir situs web facebook.com, instragram.com, dan tokopedia.com

B.Saran

Berdasarkan kesimpulan, maka penulis menyarankan agar dapat menggunakan firewall ini untuk membantu mengamankan jaringan di SMK Negeri 5 Seluma.

DAFTAR PUSTAKA

[1]Amien, J. A. & Mukhtar, H., 2020. *Implementasi Jaringan Komputer*. Yogyakarta: Penerbit Deepbulish.

[2]Anggraini, M. A. N., 2018. Uji Fitur Intrusion Prevention Pada Firewall Untangle Dengan Pengujian DOS dan SSH Brute Force. *Jurnal Manajemen Informatika*, Volume Vol.9 No.1.

[3]Anggrawan, A., 2018. *Algoritma dan Pemrograman Implementasi Pada VB.Net dan Java*. Pertama penyunt. Yogyakarta: Andi Publisher.

[4]Hanafi, M. & Habibi, R., 2020. *Cara Mudah Desain Sistem Operasi Linux Ubuntu 16.04*

p-ISSN 1858-2680
e-ISSN 2723-4673

LTS Edition Dalam 5 Jam. Bandung: Kreatif Industri Nusantara.

[5]Hendry, 2018. Implementasi Samba Server Untuk Mendukung Sharing Printer di SD Swasta Al-Washliyah 6/39 Medan. *Jurnal Ilmiah Core IT* , Volume Vol.6 No.1 e-ISSN:2548-3528.

[6]Husen, Z. & Surbakti, M., 2020. *Membangun Server dan Jaringan Komputer Dengan Linux Ubuntu.* Aceh: Syiah Kuala University Press.

[7]Husni, 2020. *Membangun dan Mengamankan Layanan Jaringan Menggunakan Linux.* Malang: Media Nusa Creative.

[8]Sahal, M., 2018. *Administrasi Infrastruktur Jaringan Untuk SMK/MAK Kelas XII.* Jakarta: PT. Gramedia Widiasarana Indonesia.

[9]Santoso, J. D., 2017. Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System. *INFOS Journal,* Volume Vol.1 No.3 e-ISSN:2655-142X.

[10]Santoso & Nurmalina, R., 2017. Perencanaan dan Pengembangan Aplikasi Absensi Mahasiswa Menggunakan Smart Card Guna Pengembangan Kampus Cerdas (Studi Kasus Politeknik Negeri Tanah Laut). *Jurnal Integrasi* , Volume Vol.9 No.1 . E-ISSN : 2548-9828.

[11]Sastradipraja, C. K. & Segar, S., 2022. *E-Niaga Konsep Dasar dan Teknologi Pendukung.* Bandung: Kaizen Media Publishing.

[12]Simargolang, M. Y., Widarma, A. & Irawan, M. D., 2021. *Jaringan Komputer.* Medan: Yayasan Kita Menulis.

[13]Sondakh, G., Najoan, M. & Lumenta, A., 2014. Perancangan Filtering Firewall Menggunakan Iptables di Jaringan Pusat Teknologi Informasi Unsrat. *E-Journal Teknik Elektro dan Komputer,* Volume ISSN:2301-8402.