ISSN ISSN : 2807-2561 e-ISSN : 2807-2588

An Analysis and Design of Network Security Using Firewall at the Library and Archives Services of Bengkulu Province

Analisis dan Perancangan Keamanan Jaringan Menggunakan Firewall pada Dinas Perpustakaan dan Kearsipan Provinsi Bengkulu

Defri Riyanto [1)]; Khairil [2)]; Eko Prasetiyo Rohmawan [2)]

[1,2)] Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Dehasen Bengkulu

Email: [1)] Defririyanto1998@gmail.com; [2)] Khairil@unived.ac.id; [2)] Prasetiyoeko1@gmail.com

How to Cite :

Riyanto, D., Khairil., Rohmawan, E. P. (2021). An Analysis and Design of Network Security Using Firewall at the Library and Archives Services of Bengkulu province. JURNAL Komitek, *1*(2). DOI: https://doi.org/10.53697/jkomitek.v1i2

ARTICLE HISTORY

Received [11 November 2021]
Revised [15 November 2021]
Accepted [28 November2021]

KEYWORDS

Firewall, IPtablses, LAN, Inlislite

ABSTRAK

Penelitian ini bertitik tolak dari permasalahan yang sering ditemui dilokasi penelitian yaitu bagaimana mengamankan server inlislite dengan merancang kemanan jaringan Menggunakan Packet Filter Firewall Iptables. Tujuan penelitian ini adalah Untuk mengoptimalkan keamanan data sistem inlisliteyang ada di Dinas Perpustakaan Dan Kearsipan Provinsi Bengkulu. Metode yang digunakan adalah metode (NDLC) Network Development Life Cycle suatu siklus tahapan perancangan jaringan yang dapat menuntun sebuah perancangan jaringan, yang bergantung pada besarnya proyek yang akan dilaksanakan dan tujuan dari pembuatan proyek tersebut. Dengan melakukan pengujian serangan Denialof Service (DoS) terhadap inlislite menggunakan hping3 di linux, membuat website inlislite tidak bisa lagi akses. Maka penulis merancang sebuah sistem baru untuk mengamankan server inlislite dari serangan-serangan yang tidak diinginkan menggunakan firewall filter IPTables agar dapat menjadi sebuah firewall yang akan menangkal serangan Distributed Denial Of Service dan Denial of Service terhadap server inlislite. Dari hasil penelitian dan pengujian yang telah dilakukan firewall IPTables sangat bagusuntuk mengamankan server pada dinas perpustakaan dan kearsipan provinsi bengkulu serta menerapkan lebih banyak rules kepada client dalam hal penggunaan internet.

ABSTRACT

This study is based on the problems that are often encountered in the research location, namely how to secure the inlislite server by designing network security using Packet Filter Firewall of IPtables. The purpose of this study is to optimize the data security of the inlislite system in the Library and Archives Service of Bengkulu Province. The method used is the Network Development Life Cycle (NDLC) method, a cycle of network design stages that can guide a network design, which depends on the size of the project to be implemented and the purpose of the project. By testing a Denial of Service (DoS) attack against inlislite using hping3 on linux, the inlislite website can no longer be accessed. Therefore, the author designed a new system to secure the inlislite server from unwanted attacks using the IPTables firewall filter then it can become a firewall that will ward off Distributed Denial of Service and Denial of Service attacks on inlislite servers. From the results of research and testing that has been carried out, the IPTables firewall is very good for securing servers in the Library and Archives Service of Bengkulu Province and applying more rules to clients in terms of internet use.

Penerbit ADM RUMAH PENGETAHUAN
Jurnal KOMITEK
Jurnal Komputer, informasi Dan Teknologi

PENDAHULUAN

Perkembangan teknologi kearah serba digital saat ini semakin pesat pada era digital seperti ini, manusia secara umum memiliki gaya hidup baru yang tidak bisa dilepaskan dari perangkat yang serba elektronik. Teknologi menjadi alat yang mampu membantu sebagian besar kebutuhan manusia. Teknologi telah dapat digunakan oleh manusia untuk mempermudah melakukan tugas dan pekerjaan apa pun. Era digital telah membawa perubahan yang baik sebagai dampak positif yang bisa digunakan sebaik-baiknya. Namun dalam waktu yang bersamaan, era digital juga banyak membawa dampak negatif sehingga menjadi tantangan baru dalam kehidupan manusia di dalam dunia digital ini.

Dinas Perpustakaan Dan Kearsipan Provinsi Bengkulu adalah suatu lembaga yang membantu pemerintah Provinsi dalam mengelola pelayanan dibidang perpustakaan dan kearsipan terhadap masyarakat di Provinsi Bengkulu. Data yang dikelola seperti membuat kartu anggota, menginput buku, peminjaman dan pengembalian buku. Untuk menunjang pekerjaan sehari-hari pada dinas perpustakaan dan kearsipan Provinsi Bengkulu menggunakan aplikasi inlislite yang berbasis WEB dengan antarmuka yang modern sehingga memudahkan pengguna untuk melakukan pencarian buku, peminjaman buku dan pengembalian buku.

Dinas Perpustakaan dan Kearsipan Provinsi Bengkulu menyewa jasa internet Indihome dengan bandwidth 50 Mbps aplikasi yang akan menunjang konektivitas aplikasi. Koneksi jaringan yang ada di dinas perpustakaan menggunakan wireless access point dan kabel UTP didistribusikan melalui Switch tanpa menggunakan Firewall. Wireless access point dipasang sebanyak enam unit di lantai gedung yang berlantai tiga. Dinas perpustakaan juga menyediakan wifi gratis untuk para pengunjung, karena menyediakan layanan wifi gratis maka jaringan di dinas perpustakaan sangat rentan terhadap serangan-serangan dari pihak luar dan pengunjung yang usil atau yang sekedar ingin coba-coba.

LANDASAN TEORI

Jaringan Komputer

Menurut Herman (2018:4) Jaringan komputer adalah sekumpulan komputer (lebih dari satu) yang berhubungan satu dengan lainnya menggunakan media tertentu sehingga memungkinkan antar komputer tersebut untuk berinteraksi, bertukar data, dan berbagi peralatan bersama misalkan printer, *scanner* dan lain-lain.

Macam-Macam Media Jenis Jaringan Komputer

Menurut Yeyen (2017:7) Perangkat keras jaringan komputer adalah perangkat untuk menghubungkan komputer dengan komputer lainnya dalam suatu jaringan yang tujuan utamanya bertukar data dan informasi serta berbagi *peripheral* dalam jaringan. Secara umum suatu jaringan terdiri dari beberapa perangkat keras yaitu :

Network Interface Card (NIC)

Network Interface Card (NIC) atau kartu jaringan merupakan peralatan yang memungkinkan terjadinya hubungan antara jaringan dengan komputer *host* atau jaringan dengan komputer server. NIC berfungsi untuk menghubungkan antara komputer dengan kabel jaringan yang terpasang secara fisik.

Kabel UTP *(Unshielded Twisted Pair)*

Kabel adalah salah satu bentuk bahan yang terbuat dari tembaga, yang berfungsi untuk menyambungkan arus. Sedangkan kabel UTP adalah jenis kabel yang digunakan pada jaringan *ethernet* yaitu sebagai kabel jaringan telepon. Kabel *twisted pair* ini terbagi menjadi dua jenis yaitu *Shielded Twisted Pair* (STP) dan *Unshielded Twisted Pair* (UTP).

Switch

Switch adalah alat yang digunakan untuk menghubungkan beberapa LAN yang terpisah dan untuk meningkatkan kinerja jaringan suatu organisasi dengan cara pembagian jaringan yang besar dalam beberapa jaringan yang lebih kecil. *Switch* adalah perangkat yang lebih pintar daripada *Hub* karena *switch* bekerja dengan cara mempelajari *mac address* yang terhubung padanya dan menyimpan *mac address* tersebut kedalam *database*, sehingga ketika ada *trafik* yang datang *switch* hanya akan meneruskan paket tersebut ke *mac address* tujuan. *Switch* terbagi menjadi 2 jenis yaitu *Switch unmanaged* dan *switch managed,* dimana *switch managed* adalah jenis *switch* yang dapat dikonfigurasi karena terdapat sistem operasi di dalamnya.

Topologi Jaringan Komputer

Menurut Charles (2018:20) Topologi jaringan komputer adalah salah satu aturan bagaimana menghubungkan komputer satu sama lain secara fisik dan pola hubungan antara komponen-komponen yang berkomunikasi media atau peralatan, Seperti server, *workstation, hub/Switch*, dan pemasangan kabel (media transmisi data).

Osi Layer

Menurut Sritrusta (2014:15) OSI adalah referensi komunikasi dari Open *System Interconnection*. OSI model digunakan sebagai titik referensi untuk membahas spesifikasi protokol.

Firewall

Menurut Charles (2018:21) Dalam teknologi jaringan komputer, *firewall* adalah sistem keamanan jaringan yang memantau dan mengontrol lalu lintas jaringan yang masuk dan keluar berdasarkan aturan keamanan yang telah ditentukan sebelumnya. *Firewall* biasanya membuat penghalang antara jaringan terpercaya dan jaringan tidak terpercaya, seperti *Internet*.

Firewall dikategorikan sebagai sistem berbasis jaringan atau berbasis *host*. *Firewall* berbasis jaringan dapat ditempatkan di mana saja dalam LAN atau WAN. *Firewall* berbasis *host* diterapkan langsung pada *host* itu sendiri untuk mengontrol lalu lintas jaringan atau sumber daya komputasi lainnya.

Pengertian *Flowchart*

Menurut Santoso (2017:86) *Flowchart* adalah representasi secara simbolis dari suatu algoritma atau prosedur untuk menyelesaikan suatu masalah, dengan menggunakan *flowchart* akan memudahkan pengguna melakukan pengecekan bagian-bagian yang terlupakan dalam analisa masalah, disamping itu *flowchart* juga berguna sebagai fasilitas untuk berkomunikasi antara pemrograman yang bekerja dalam tim suatu proyek. digunakan simbol-simbol dalam suatu bagan aliran dokumen (*flowchart*) alam bagan alir, arus dokumen ini dapat diakui dengan melihat nomor dalam simbol dalam simbol penghubung pada halaman yang sama. Dalam bagan alir, arus dokumen ini dapat diakui dengan melihat nomer dalam simbol dalam simbol penghubung pada halaman yang sama *(on-page connector).*

METODE PENELITIAN

Network Development Life Cycle (NDLC) merupakan suatu siklus tahapan perancangan jaringan yang dapat menuntun sebuah perancangan jaringan, yang bergantung pada besarnya proyek yang akan dilaksanakan dan tujuan dari pembuatan proyek tersebut. Setiap tahapan siklus merupakan proses yang akan menentukan bagaimana proses kelanjutan dari proyek yang akan dilaksanakan.

1. Analisis
   Pada tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan *user*, dan analisa topologi / jaringan yang sudah ada saat ini.
2. Desain

Dari data-data yang didapatkan sebelumnya, tahap Desain ini akan membuat gambar desain topologi jaringan *interkoneksi* yang akan dibangun. Desain bisa berupa desain struktur topologi, desain akses data, desain tata *layout* perkabelan, dan sebagainya yang akan memberikan gambaran jelas tentang proyek yang akan dibangun.

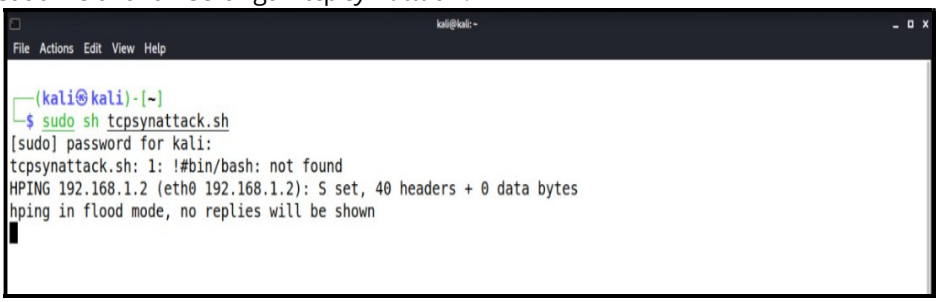
3. Implementation
   Di tahapan ini *network* akan menerapkan semua yang telah direncanakan dan di desain sebelumnya.
4. Pengujian Sistem
   Tahapan Pengujian Sistem merupakan tahapan yang penting, agar jaringan komputer dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan awal dari user pada tahap awal analisis, maka perlu dilakukan kegiatan pengujian sistem.

HASIL DAN PEMBAHASAN

Hasil dan Pembahasan

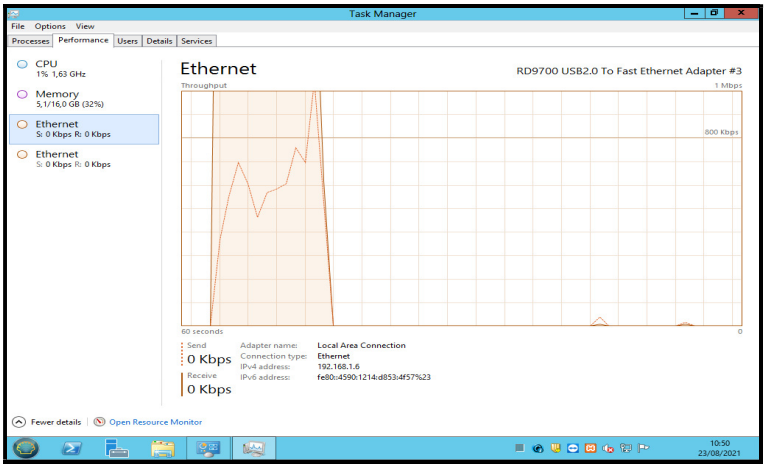
Hasil Pengembangan Sistem

Hasil setelah menggunakan *firewall* pada Dinas Perpustakaan dan Kearsiapan Provinsi Bengkulu menjadi lebih aman terutama untuk server Inlislite penggunjung tidak bisa menyerang server karena adanya *firewall*. Serangan akan di *drop* oleh *firewall*, dapat dilihat pada gambar dibawah ini saat melakukan serangan tcp *syn attack* .



Gambar 1. Serangan *Denial of Service*

Pemantauan kinerja *Bandwidth* dan CPU saat serangan *Denial of Service* berlangsung, CPU dan *Bandwidth* berkerja secara normal karena saat serangan *Denial of Service* berlangsung semua serangan di halangi oleh *firewall.*

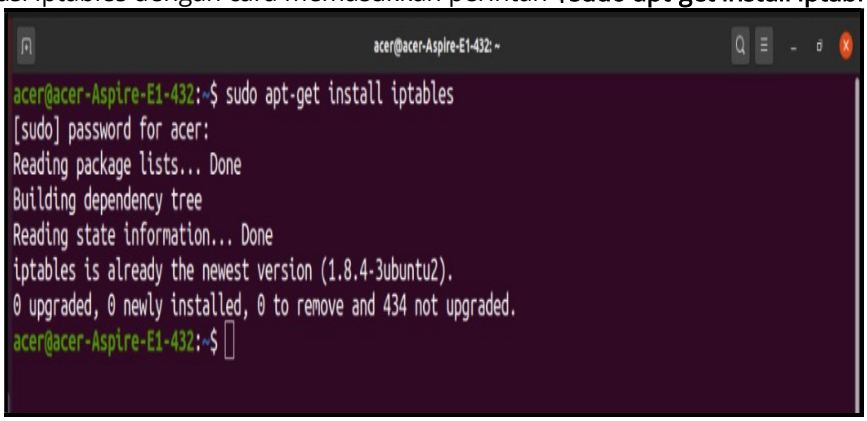


Gambar 2. Pemantauan kinerja *Bandwidth* dan CPU saat serangan DoS

Pembahasan

Menginstal Iptables

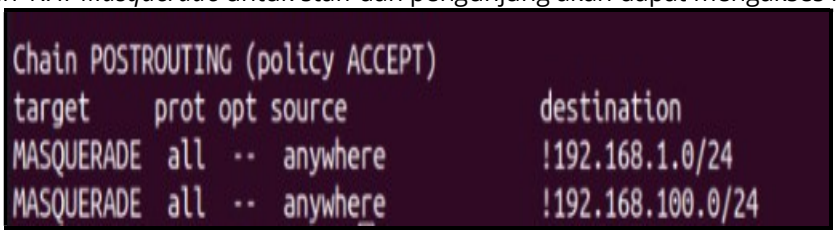
Proses instalasi iptables dengan cara memasukkan perintah **$sudo apt-get install iptables**



Gambar 3. Menginstal Iptables

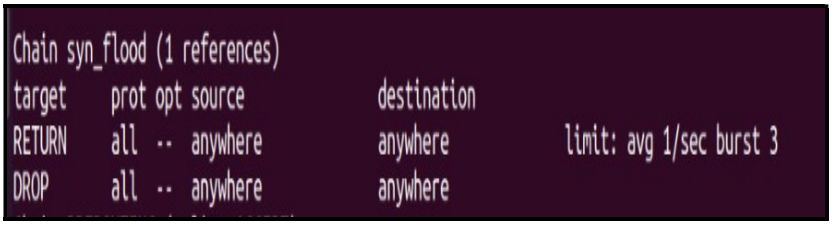
Konfigurasi Rule Iptables

1. Menambahkan *NAT Masquerade* untuk staff dan pengunjung akan dapat mengakses internet.



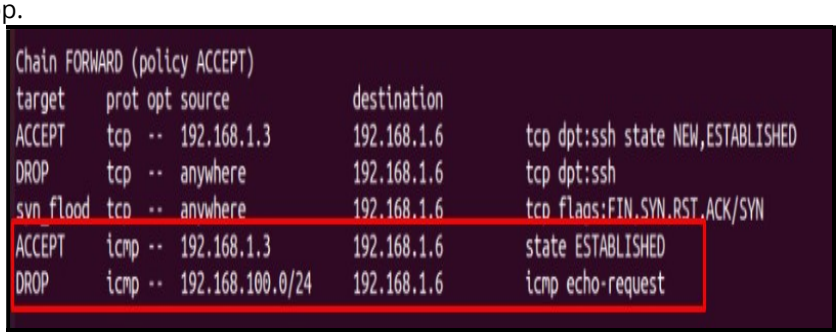
Gambar 4. Konfigurasi staff dan pengujung akses ke internet

2. Membatasi *new packet* TCP menuju server inlislite sebanyak 3 detik, lebih dari 3 detik koneksi akan di *drop.*



Gambar 5. Konfigurasi TCP menuju ke server

3. Membatasi *new packet* ping ICMP menuju server inlislite PC Staff dapat ICMP sedangkan pengujung didrop.



Gambar 6. Konfigurasi ICMP menuju ke server

4. Rule ssh, hanya administrator pada jaringan staff yang dapat mengakses ssh server inlislite. kecuali administrator staff akan didrop.

```
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.1.3          192.168.1.6          tcp dpt:ssh state NEW,ESTABLISHED
DROP       tcp  --  anywhere             192.168.1.6          tcp dpt:ssh
syn_flood  tcp  --  anywhere             192.168.1.6          tcp flags:FIN,SYN,RST,ACK/SYN
ACCEPT     icmp --  192.168.1.3          192.168.1.6          state ESTABLISHED
DROP       icmp --  192.168.100.0/24     192.168.1.6          icmp echo-request
```

Gambar 7. Konfigurasi SSH Staf ke Server

Implementasi Sistem Pengujian

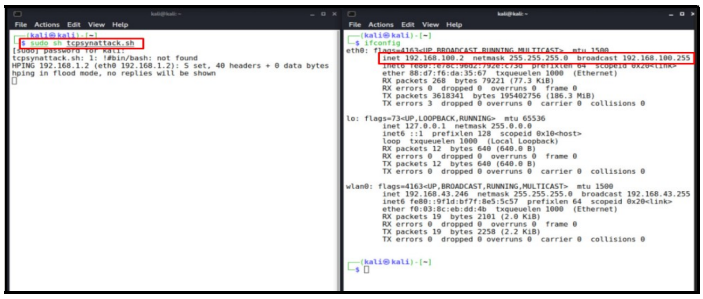
Pengujian akses server service HTTP 80, 443

Semua Host bisa mengakses server inlislite dengan 192.168.1.6/inlislite3/.

Gambar 8. Tampilan *website Inlislite*

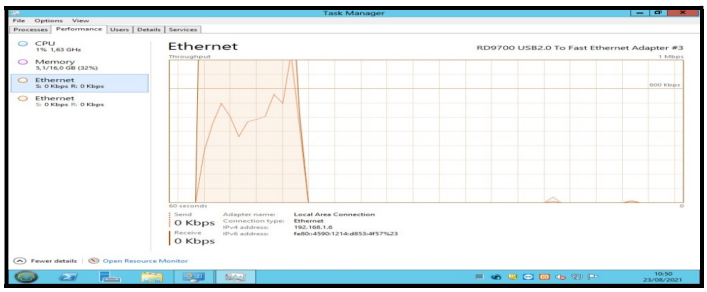
Pengujian TCP menggunakan tcp *syn flood attack* saat menggunakan *firewall*.

Host akan dianggap sah jika mengirim packet *tcp syn attack* kurang dari 3 *attempt* perdetik dan host akan di drop jika mengirim lebih dari *3 attempt* per detik.



Gambar 9. serangan *syn attack* dan IP *Address*

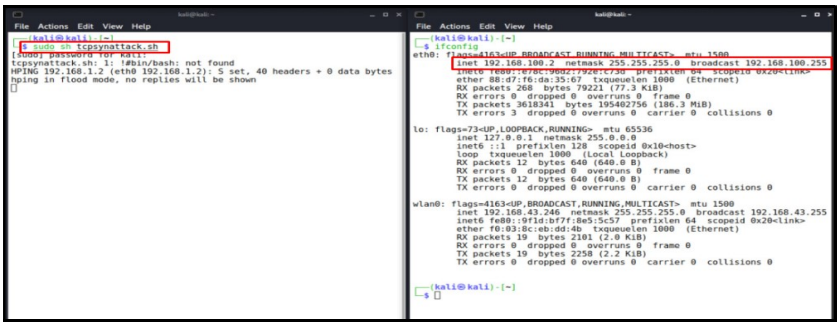
Pemantauan kinerja *Bandwidth* dan CPU saat serangan *Denial of Service* berlangsung, CPU dan *Bandwidth* berkerja secara normal karena saat serangan *Denial of Service* berlangsung semua serangan di halangi oleh *firewall.*



Gambar 10. Pemantauan kinerja Bandwidth saat serangan DoS

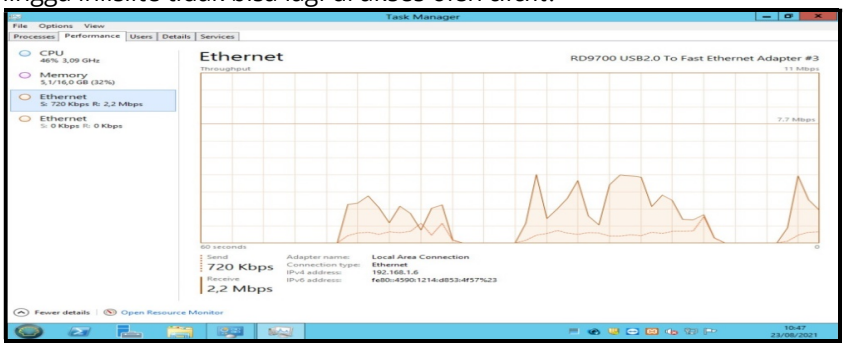
Pengujian TCP menggunakan tcp *syn flood attack* saat tidak menggunakan *firewall*.

Host akan dianggap sah jika mengirim packet *tcp syn attack* kurang dari 3 *attempt* perdetik dan host akan di blok jika mengirim lebih dari *3 attempt* per detik.



Gambar 11. serangan *syn attack* dan IP *Address*

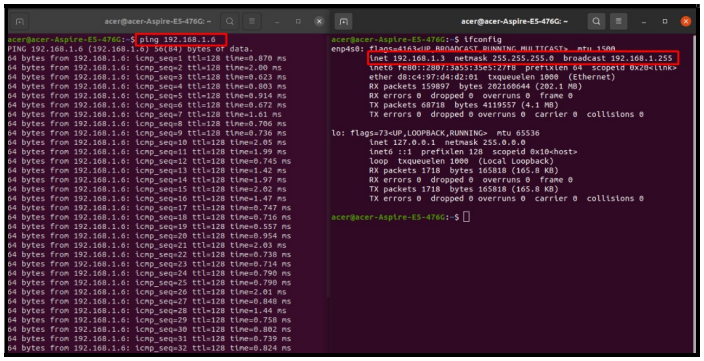
Monitoring Serangan tcp *syn attack* dengan *performance* dari CPU dan *Bandwidth* tidak menggunakan *firewall bandwidth* langsung mengingkat kecepatan *ethernet* dan kinerja CPU menjadi meningkat sehingga inlislite tidak bisa lagi di akses oleh *client*.



Gambar 12. Pemantauan kinerja Bandwidth saat serangan DoS

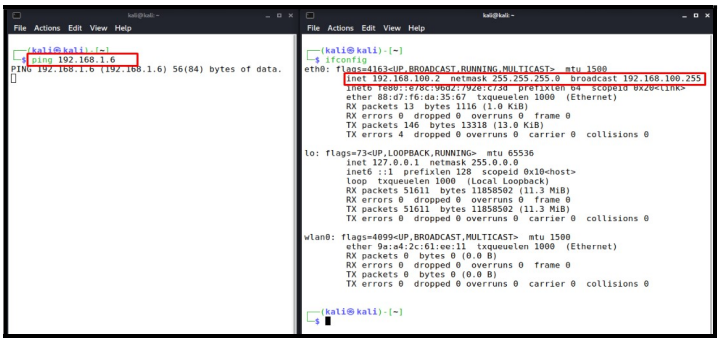
Pengujian Ping service ICMP

Host yang sah akan dapat ICMP *echo reply* dari server dan *host* yang tidak sah akan di *drop*. Pada gambar dibawah dapat dilihat staff bisa ping ke server 192.168.1.6 dan mendapatkan *echo reply*



Gambar 13. Ping ICMP staff ke server dan IP *Address*

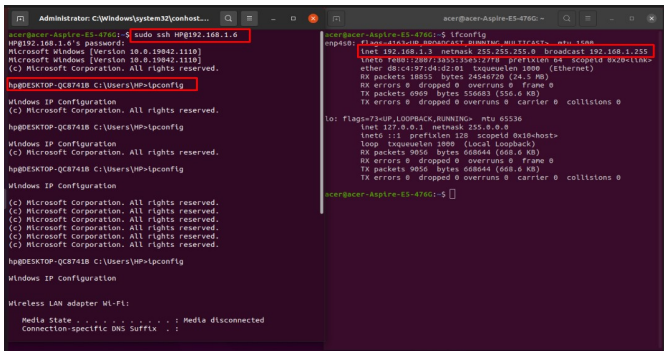
Pada gambar dibawah dapat dilihat pengujung dengan IP *address* 192.168.100.2 ping ke server IP *address* 192.168.1.6 di *drop* oleh *firewall*.



Gambar 14. Ping ICMP pengunjung ke server dan IP *Address*

Pengujian Service SSH

Hanya host *sys admin* yang diterima untuk dapat mengakses server via SSH.



Gambar 15. Staff akes server menggunakan SSH

Tabel 1. Tabel Hasil Pengujian Sistem

NO	Kriteria Pengujian	Hasil Yang Diharapkan	Sukses/ Tidak sukses
1	Pengujian akses server service HTTP 80, 443	Semua Host bisa mengakses server HTTP 80, 443	Sukses dapat dilihat hasil gambar pada halaman 52
2	Pengujian TCP (dalam case ini menggunakan tcp syn flood attack) saat menggunakan *firewall* dan tidak menggunakan *firewall*	Host akan dianggap sah jika mengirimkan packet tcp syn kurang dari 3 attempt per detik dan Host akan di Drop jika mengirimkan lebih dari 3 attempt per detik	Sukses dapat dilihat hasil gambar pada halaman 53-54
3	Pengujian Ping service ICMP	Host yang sah akan dapat icmp echo reply dari server dan Host yang tidak sah akan di Drop	Sukses dapat dilihat hasil gambar pada halaman 55
4	Pengujian service SSH (service SSH di gunakan oleh admin untuk melakukan perubahan konfigurasi pada server)	Hanya Host sysadmin yang diterima untuk dapat mengakses server via SSH	Sukses dapat dilihat hasil gambar pada halaman 56

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil penelitian dan pengujian yang telah dilakukan mengenai Keamanan jaringan menggunakan firewall Iptables pada Dinas Perpustakaan Dan Kearsipan Provinsi Bengkulu harus adanya sebuah firewall. Dalam perancangan filtering firewall menggunakan Iptables sebagai aplikasi dari firewall, dapat membantu mengamankan server inlislite dari serangan Denail of service dengan cara memfilter jaringan dari pemakai yang tidak mempunyai hak akses dan sehingga lebih aman dari serangan.

Saran

1. Perlu adanya *firewall* khusus untuk mengamankan server pada dinas perpustakaan dan kearsipan provinsi bengkulu.
2. Terapkan lebih banyak *rules* kepada *client* dalam hal penggunaan internet.

DAFTAR PUSTAKA

Charles Widodo, Marchellius Yana,. Halim Agung. 2018. Implementasi topologi hybrid untuk pengoptimalan aplikasi Edms pada project office pt phe onwj. Jurnal Teknik Informatika Vol 11 No. 1, april 2018, hal 21.

Sritrusta Sukaridhoto, ST, Ph,D. 2014. Buku Jaringan Komputer I. Politeknik Elektronik Negeri Surabaya. Hal 15.

Santoso dan Radna Nurmalina. 2017. Perencanaan dan Pengembangan Aplikasi Absensi Mahasiswa Menggunakan Smart Card Guna Pengembangan Kampus Cerdas (Studi Kasus Politeknik Negeri Tanah Laut). Jurnal Integrasi: Vol. 9 No. 1. Hal 86.

Septian Geges and Waskitho Wibisosno, 2015. Pengembangan Pemecahan Serangan Terdistributed Denial Of Service (DDOS) Pada Sumber Daya Jaringan dengan Intefrasi Network Behavior Analysis Dan Client Puzzle. hal 54.

Rudy Suwanto, Ikhwan Ruslianto,. Muhammad DiPonegoro. 2019. Implementasi Intrusion Prevition System (IPS) Menggunkan Snort dan IpTable Pada Monitoring Jaringan Local Berbasis Website. Jurnal Dan Aplikasi Volume 07, No.1 (2019), hal 97-107.

Yeyen Ary Wibawa, 2017. Perancangan Dan Analisis Jaringan LAN VLAN DI PT. PERTAMINA (PERSERO) MOR IV SEMARANG. Jurnal unimus.

Yuliandoko Herman. 2018. Jaringan Komputer Wire dan Wireless berserta penerapannya. Jakarta: Deepublish