TUGAS AKHIR

RANCANG BANGUN SISTEM KEAMANAN JARINGAN MENGGUNAKAN FIREWALL FILTERING DAN PORT KNOCKING DENGAN NOTIFIKASI TELEGRAM

DISUSUN OLEH :

ASNATUN AINI

193510330

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS ISLAM RIAU

PEKANBARU

2024

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh. Alhamdulillah puji syukur penulis panjatkan ke hadirat Allah SWT atas rahmat, karunia, dan hidayahnya sehingga penulis dapat menyelesaikan penyusunan proposal ini yang berjudul " **RANCANG BANGUN SISTEM KEAMANAN JARINGAN MENGGUNAKAN FIREWALL FILTERING DAN PORT KNOCKING DENGAN NOTIFIKASI TELEGRAM".** Proposal skripsi ini disusun untuk memenuhi persyaratan memperoleh gelar Sarjana Teknik dengan strata1 (Proposal skripsi telah penulis susun dengan maksimal dan mendapatkan bantuan dari berbagai pihak).

Dalam penyusunan skripsi ini, tentunya penulis sadar bahwa tanpa bantuan dan bimbingan berbagai pihak maka laporan ini sulit untuk terwujud. Untuk itu dalam kesempatan ini penulis ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Ayahanda Syukur beliau yang menjadi tulang punggung keluarga. Meskipun beliau tidak sempat merasakan pendidikan hingga bangku perkuliahan namun beliau mampu mendidik saya menjadi lebih baik sehingga penulis mampu menyelesaikan studinya sampai sarjana.
2. Ibunda Sri Fajar indah pintu surgaku. Beliau sangat berperan penting dalam menyelesaikan program studi penuli dan beliau mampu mendidik saya menjadi perempuan yang kuat dan tegar dalam segala rintangan dan doa beliau lah sehingga saya mampu menyelesaikan studi hingga sarjana. Makasi mami sudah bertahan sejauh ini untuk mbak.
3. Kepada adik saya alvindo dan aqilah yang selalu menghibur penulis dan selalu memberikan doa supaya saya cepat menyelesaikan studi.
4. Kepada pembimbing saya Bapak Apri Siswanto S.Kom., M.Kom yang telah membimbing penulis hingga menyelesaikan studi nya, serta jajaran staff/karyawan Universitas Islam Riau.
5. Kepada teman-teman saya Putri Ramadhani,Fadia,Rahmi,Sri Kemuning,Annisa yang selalu mendukung saya dan memberikan semangat kepada saya dalam menyelesaikan skripsi ini hingga selesai.

Penulis menyadari bahwa dalam penyusunan laporan skripsi ini masih jauh dari kata sempurna. Oleh karena itu dengan segala kerendahan hati penulis berharap saran dan kritik yang sifatnya membangun guna memperbaiki laporan skripsi ini. Akhir kata semoga laporan skripsi ini dapat menambah ilmu pengetahuan dan bermanfaat bagi semua pihak yang membacanya

Pekanbaru, 12 Oktober 2023

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

RANCANG BANGUN SISTEM KEAMANAN JARINGAN MENGGUNAKAN FIREWALL FILTERING DAN PORT KNOCKING DENGAN NOTIFIKASI TELEGRAM

Asnatun Aini
Jurusan Teknik Informatika Fakultas Teknik Universitas Islam Riau
Email: asnatun2@student.uir.ac.id

ABSTRAK

Kominfo kabupaten kepulauan meranti merupakan salah satu lembaga instansi pemerintahan. Permasalahan di instansi ini belum menerapkan metode port knocking dan firewall filtering yang dimana dapat meminimalisir serangan dan memfiltering jaringan yang mencurigakan. Pada rancangan ini digunakan metode penetration test dengan tool snort yang dimana mampu meminimalisir serangan pada jaringan. Pada pengujian ini digunakan konfigurasi alamat IP address snort terlebih dahulu dan selanjutnya kalilinux sebagai pantester selanjutnya telegram disini berfungsi sebagai gateway notifikasi yang mampu memberi peringatan kepada admin jika ada yang akan masuk ke dalam jaringan. Kemudian untuk uji serangan menggunakan metode penyerangan ICMP,Port Scanning,DDos. Hasil dari penetration test ini menunjukkan hasil bahwa penyerangan dapat terdeteksi dan telegram mampu memberikan alert (peringatan) kepada admin.

Kata Kunci: Konfigurasi,Port Knocking, Firewall Filtering, Penetration Test,Snort,Kalilinux, Telegram,ICMP,Port Scanning,Ddos,Alert.

NETWORK SECURITY SYSTEM DESIGN USING FIREWALL FILTERING AND PORTS KNOCKING WITH TELEGRAM NOTIFICATION

Asnatun Aini
Departement of Informatics Engineering Faculty of Engineering
Islamic University of Riau
Email: asnatun2@student.uir.ac.id

ABSTRACT

Meranti Islands District Ministry of Communication and Information is one of the government agencies. The problem is that this agency has not implemented port knocking and firewall filtering methods which can minimize attacks and filter suspicious networks. In this design, the penetration test method is used with the snort tool which is able to minimize attacks on the network. In this test, Snort IP address configuration is used first and then Kalilinux as Pantester, then Telegram here functions as a notification gateway which is able to warn the admin if someone enters the network. Then to test the attack using the ICMP, Port Scanning, DDos attack method. The results of this penetration test show that attacks can be detected and Telegram is able to provide alerts to admins.

Keywords: Konfigurasi,Port Knocking, Firewall Filtering, Penetration Test,Snort,Kalilinux, Telegram,ICMP,Port Scanning,Ddos,Alert.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Rancang Bangun sistem Keamanan jaringan komputer adalah suatu sistem untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jaringan komputer. Langkah-langkah pencegahan membantu menghentikan pengguna yang tidak sah yang disebut "penyusup" untuk mengakses setiap bagian dari sistem jaringan komputer . Tujuan rancang bangun system Keamanan jaringan komputer adalah untuk mengantisipasi resiko jaringan komputer berupa bentuk ancaman fisik maupun logik baik langsung ataupun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer.

Satu hal yang perlu diingat bahwa tidak ada jaringan yang anti sadap atau tidak ada jaringan komputer yang benar-benar aman. Sifat dari jaringan adalah melakukan komunikasi. Setiap komunikasi dapat jatuh ke tangan orang lain dan disalah gunakan. Sistem keamanan membantu mengamankan jaringan tanpa menghalangi penggunaannya dan mengantisipasi ketika jaringan berhasil ditembus. Selain itu, pastikan bahwa user dalam jaringan memiliki pengetahuan yang cukup mengenai keamanan dan pastikan bahwa mereka menerima dan memahami rencana keamanan yang kita buat. Jika mereka tidak memahami hal tersebut, maka mereka akan menciptakan lubang (hole) keamanan pada jaringan kita.

Penelitian ini menggunakan metode *firewall filtering* dan *Port Knocking* yang dimana objek penelitian nya memiliki beberapa kelemahan dan kelebihan dimana pada metode *firewall filtering* ini memiliki performa yang cepat selain itu

memiliki dampak yang kecil pada jaringan komputer yang harga nya juga sangat terjangkau sedangkan kekurangan dari *firewall filtering* ini dapat mempengaruhi kinerja jaringan dan memperlambat lalu lintas data jika tidak dikonfigurasi dengan benar. Selanjutnya metode *port knocking* memiliki teknik perlindungan yang dapat digunakan sebagai lapisan keamanan ekstra pada system keamanan computer sedangkan kekurangan pada port knocking tidak dapat digunakan sebagai keamanan yang berdiri sendiri.

Proses penyaluran jaringan membutuhkan router sebagai penghubung dari , salah satu router yang digunakan pada saat ini adalah router mikrotik. Dalamproses routing,jaringan diilustrasikan sebagai sebuah graf dengan bobot, di mana setiap koneksi antara titik-titik dalam jaringan memiliki nilai atau bobot tertentu. Bobot ini mencakup faktor-faktor seperti bandwidth, network delay, hop count, path cost, beban (load), dan kehandalan (reliability). Setiap router bertugas untuk mencari rute dengan biaya terendah untuk mengirimkan paket data dengan efisiensi yang optimal. (Nugroho, 2023).

Router mikrotik membantu pekerjaan administrator yang memiliki fungsi konfigurasi, monitoring dan troubleshooting pada sistem. (Ariyanto et al., 2020; Dwi Prayogo & Arif Wibaw a, 2012; ismi, 2020). Permasalahan yang terjadi adalah administrator tidak dapat mengetahui apabila terjadi gangguan-gangguan yang dapat menghambat dan mengurangi kinerja dari router mikrotik. Gangguan tersebut merupakan langkah awal pemerosesan pencurian data / merusak data, apabila terlaksana dan terjadi terhadap router mikrotik , hal tersebut dapat menganggu kinerja.

Disini yang harus dilakukan ialah memberikan keamanan pada system router mikrotik yang dimana penerapan fitur *port knocking* ini pada sistem login dengan autentifikasi kesepakatan memiliki tujuan sebagai bentuk meminimalisir atau menghambat ketika serangan ssh, telnet dan winbox , fitur firewall melakukan filtering pada jaringan apabila terdapat kejanggalan dalam login, melakukan pemblokan ip secara otomatis, menonaktifkan pada serangan dan pemberian notifikasi serangan dengan memanfaatkan sosial media Telegram sebagai platform yang terhubung router mikrotik terhadap administrator.

Telegram dirancang untuk memudahkan pengguna saling berkirim pesan teks, audio, video, gambar dan sticker dengan aman (Fahana & Ridho, 2018). Jumlah pengguna aktif bulanan Telegram global telah mencapai 700 juta orang hingga awal Juni 2022. Jumlah tersebut telah meningkat 40% dibandingkan pada Januari 2021.

Kominfo Kabupaten Kepulauan Meranti merupakan salah satu lembaga instansi pemerintahan yang belum menggunakan metode *port knocking* yang dimana dapat meminimalisir serangan dan memfiltering jaringan yang mencurigakan yang dimana notifikasi nya dengan bantuan *social* media telegram dalam antisipasi serangan pada router mikrotik.

Dalam rangka mengatasi masalah tersebut, penulis merancang suatu"rancang bangun system keamanan jaringan menggunakan *firewall filtering* dan *port knocking* dengan notifikasi telegram", sehingga dapat meningkatkan produktifitas dalam instansi tersebut. Router mikrotik dipilih karena memiliki performa yang baik dalam pengembangan *bandwith* internet. Dengan adanya pengelolaan

jaringan dengan mikrotik ini diharapkan dapat meningkatkan keamanan jaringan pada Kominfo sehingga dapat membantu proses pekerjaan.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah dijelaskan diatas maka didapatkan identifikasi masalah ini adalah:

Kominfo Kabupaten Kepulauan Meranti belum memiliki system keamanan dengan metode *port knocking* untuk meminimalisir serangan dan memfiltering jaringan yang mencurigakan serta melakukan pemberian notifikasi dengan bantuan *social* media telegram dalam antisipasi serangan pada router mikrotik yang dimana dapat membantu dalam proses melakukan pekerjaan.

1.3 Rumusan Masalah

Adapun rumusan masalah dari rancang bangun system keamanan jaringan di Kominfo Kabupaten Kepulauan Meranti ini adalah sebagai berikut:

a. Bagaimana cara menerapkan keamanan pada router mikrotik untuk serangan *Port Scanning* Dan *DDos*?
b. Bagaimana cara penerapan *firewall filtering* dan *Port knocking* pada sistem?
c. Bagaimana cara penerapan telegram sebagai notifikasi sistem peringatan?

1.4 Batasan Masalah

Batasan masalah dalam proses rancang bangun system keamanan jaringan di Kominfo Kabupaten Kepulauan Meranti sebagai berikut:

a. Sistem dibangun pada jaringan LAN (Local Area Network).

b. Sistem dijalankan dengan 4 user yaitu router (mikrotik versi 7.1.1), attacker 1 (kali linux 13.0), attacker 2 (Windows 10 pro), log server dan telegram gateway (ubuntu), administrator (Windows 7) dan winbox versi 3.40.

c. Sistem keamanan *firewall filtering* digunakan sebagai mengatasi (*Port Scanning, DDoS).*

d. Notifikasi serangan dengan telegram versi 91.108.9.52

1.5 Tujuan Penelitian

Tujuan dari rancang bangun system keamanan jaringan ini adalah sebagai berikut:

a. Peneliti merancang bangun system keamanan router mikrotik yang dimana bisa mengantisipasi setiap serangan pihak yang tidak bertanggung jawab dan meningkatkan keamanan data dengan mengimplementasikan *firewall* dan fitur lainnya.

b. Implementasi telegram disini sebagai notifikasi awal dalam antisipasi serangan pada router mikrotik yang terjadi pada jaringan.

c. Penggunaan router mikrotik juga memiliki fitur monitoring jaringan yang dapat membantu administrator jaringan untuk memantau meninjau kinerja jaringan, memperbaiki masalah, dan mengoptimalkan kinerja jaringan secara keseluruhan.

1.6 Manfaat Penelitian

a. Penelitian ini menghasilkan notifikasi yang dapat digunakan untuk mempercepat informasi dan meminimalisir terjadinya serangan pada router mikrotik pada Kominfo Kabupaten Kepulauan Meranti.

b. Penelitian ini dapat memperbaiki kualitas keamanan jaringan di Kominfo Kabupaten Kepulauan Meranti.

BAB II

LANDASAN TEORI

2.1 Tinjauan Pustaka

Penelitian mengenai rancang bangun system keamanan jaringan pada Kominfo Kabupaten Kepulauan Meranti adalah dengan cara melakukan studi pustaka. Sehingga studi pustaka ini dapat menjadi bahan pertimbangan dan memperkaya literature dalam penelitian ini. Pengumpulan data pendapat dari para peneliti terdahulu mengenai objek yang akan di teliti, di antaranya dari beberapa jurnal yang dikutip.

Penelitian yang dilakukan Randi & Ruuhwan (2020) yang membahas mengenai implementasi keamanan jaringan menggunakan metode *port blocking* dan *port knocking* pada mikrotik RB-941. Permasalahan yang terdapat pada penelitian ini adalah ketika keamanan jaringan sering terjadi kerusakan yang dimana apabila seseorang atau pihak lain memungkinkan mengakses suatu data bahkan mengubah isi data tersebut melalui jaringan komputer yang terhubung dengan komputer lainnya yang mengakibatkan adanya port yang terbuka atau akses yang illegal, secara autentikasi dan otorisasi dapat mengakibatkan mudahnya user yang tidak valid dapat mengakses sistem tersebut secara illegal. Pembahasan keamanan jaringan pada penelitian ini menggunakan metode port dengan fungsi untuk melindungi, memfilter, membatasi atau menolak semua hubungan jaringan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan area ruang lingkupnya. Tujuan dari penelitian ini adalah untuk melindungi dari serangan yang berfungsi melakukan pemindaian port dan pembatasan hak akses user, sehingga hanya user yang legitimate yang bisa

mengkases secara penuh untuk membuka dan menutup akses port yang telah dikonfigurasi.

Penelitian selanjutnya dilakukan oleh Iqbal & Arini (2020) yang membahas mengenai analisa dan simulasi keamanan jaringan *Ubuntu server* dengan *port knocking,honeypot,iptables,icmp* Keamanan jaringan komputer sangatlah penting untuk menjaga kerahasiaan data dan informasi yang terdapat pada server. Data dan informasi ini hanya ditujukan untuk administrator dan user yang berhak mengakses saja melalui port layanan. Membiarkan port penting terbuka adalah kesalahan fatal yang dapat mengakibatkan serangan terhadap server, umumnya teknik yang sering dilakukan adalah scan portdan bruteforce. Hal lain untuk melindungi server dengan firewall adalah salah satu metode yang dapat diterapkan pula, namun penggunaan firewall tidak efektif dikarenakan akan memblok semua layanan tanpa memperdulikan siapapun termasuk administrator, oleh karena itu penelitian ini dilakukan menggunakan port knocking yang digabungkan dengan Honeypot, IPtables dan ICMP. IPtables menggantikan peran dari firewall, untuk menentukan aturan portmana yang akan di filter, sehingga setiap paket yang masuk pada filtered portakan di-refused. Port knocking berfungsi untuk menentukan ketukan rahasia terhadap portlayanan server. Honeypot untuk mengalihkan server port pada port tiruan dan sengaja terbuka untuk mengetahui apa saja upaya yang dilakukan untuk memasuki server, dan ICMP berfungsi sebagai ping request dari client terhadap server yang bersangkutan .Pengembangan selanjutnya dapat dengan menggunakan static chiper knock dalam penelitian ini fokus pada protokol TCP, SSH port, keamanan mencakup DoS Attack, Port Scandan port/sniffer pada Ubuntu serta

menambahkan protokol ICMP input dan output), NAT(3 chain yaitu output, pre-rouitng dan post-routing), Mangle(5 chain : forward, output, input, postrouting dan presouting). Chain ini untuk TCP protocol Packet Quality of Service saat sebelum proses routing dilakukan. Hasil yang dilakukan pada penelitian ini diharapkan dapat mencegah terjadinya serangan ke server utama dan dapat mengetahui apa saja upaya yang dilakukan untuk masuk kedalam serta mengganti peran dari firewall dengan IPtables, juga menggunakan ICMP protokol.

Selanjutnya referensi yang berjudul desain keamanan jaringan pada mikrotik router OS menggunakan metode port knocking Amarudin & Faruq (2018), Dalam penelitian ini dapat mengembangkan keamanan jaringan komputer dengan cara penggunaan port knocking adapun untuk mempermudah dalam mendesain dan menguji jaringan yang akan dibangun perlu adanya simulator GNS3 untuk mendesain dan mensimulasikan topologi keamanan jaringan. Berdasarkan penelitian yang sudah dilakukan simulator GNS3 dapat dengan mudah diterapkan dalam mendesain topologi jaringan maupun dalam mensimulasikan pengujian keamanan jaringan khususnya pada metode keamanan port knocking. Hasil penelitian yang dilakukan juga didapatkan hasil bahwa metode port knocking dapat diterapkan untuk mengamankan router dari akses orang lain yang tidak berhak mengakaesnya.

Berikutnya penelitian yang dilakukan oleh Desmira & Roni (2022) yang berjudul rancang bangun keamanan port secure shell (SSH) menggunakan metode port knocking, Penelitian ini menerapkan OS linux dari serangan keamanan jaringan. Dalam sistem keamanan ini hanya membutuhkan beberapa

konfigurasi dalam port SSH dan port knocking. Fungsi dari system yang dibuat penulis merupakan akses khusus keamanan jaringan yang didalam pengelolaan dan pengawasan dari setiap akses jaringan internet yang ada dalam lingkungan perusahaan,karna kemudahan dalam pengelolaan dan akses rahasia yang dapat digunakan hanya administrator tertentu. PORT SSH (Secure Shell) SSH banyak digunakan dalam kemanan jaringan komputer bahkan digunakan dalam keamanan jaringan sebuah perusahaan-perusahaan besar di indonesia.

Berikutnya penelitian yang dilakukan oleh Tito (2022) yang berjudul pemanfaatan metode port knocking dan blocking untuk keamanan jaringan BPKAD Sumatera Selatan, Dalam penelitian ini penulis melakukan pengujian pemanfaatan metode *portknocking* dan *port blocking* pada sistem keamanan jaringan di BPKAD Provinsi Sumatera Selatan menggunakan Mikrotik Routerboard. Dikarenakan keamanan jaringan di BPKAD Prov Sumsel belum terdapat sistem keamanan pada akses layanan port (*port service*) dalam mengatasi serangan khususnya pada port 8291 (winbox), 80 (webfig) dan 23 (telnet). Layanan port tersebut berfungsi agar administrator jaringan dapat mengakses ke router dalam rangka melakukan pengelolaan jaringan di instansi BPKAD Provinsi Sumatera Selatan, hasil penelitian yang dilakukan Rules knocking yang dibuat menjadi tambahan pengamanan autentikasi untuk terhubung ke *router*, Kemudian *Service port* yang terbuka dapat diamankan dengan cara melakukan *blocking port* sehingga menjadi ter-*filtered* yang selanjutnya metode *port knocking* dan *blocking* dapat meningkatkan keamanan sistem jaringan terutama dari akses yang illegal.

Kemudian penelitian yang dilakukan oleh Eva (2014) yang berjudul analisis dan perancangan pengontrolan trafik jaringan internet terhadap user menggunakan mikrotik dan server linux yang di penelitian ini menjelaskan mengenai pengontrolan dan penerapan jaringan internet untuk memantau situs yang telah diakses oleh user. Sistem kontrol dan monitoring trafik jaringan sangat cocok untuk diterapkan di SMP Negeri 2 Depok Sleman Yogyakarta, dikarenakan sekolah tersebut belum memiliki fasilitas yang dapat mengontrol aktifitas kegiatan siswa,karyawan dan guru yang berhubungan dengan akses internet. Adanya system seperti ini, di harapkan dapat mengurangi kekhawatiran orang tua saat orang tua jauh dari anak-anaknya. Dibawah ini merupakan referensi penelitian jurnal yang telah dijelaskan diatas:

Tabel 2. 1 Penelitian

Peneliti	Hasil Penelitian	Kelebihan/Kekurangan
Randi & Ruuhwan (2020)	Hasil dari penelitian ini adalah untuk melindungi dari serangan yang berfungsi melakukan pemindaian port yang tidak dikenali.	Kelebihan pada penelitian ini hanya user yang bisa mengakses secara penuh untuk membuka dan menutup port. Kekurangan didalam penelitian ini hanya bisa diakses di ruang lingkupnya.
Iqbal & Arini (2020)	Hasil dari penelitian ini mencegah terjadinya serangan ke server	Kelebihan pada penelitian ini dapat mengetahui apa saja upaya yang perlu dilakukan agar tidak terjadinya

	utama	serangan. Kekurangan pada penelitian ini adalah penggunaan firewall tidak efektif dikarenakan akan memblok semua layanan termasuk administrator.
Amarudin & faruq (2018)	Hasil dari penelitian ini didapatkan bahwa pada metode port knocking dapat diterapkan untuk mengamankan router dari akses orang lain yang tidak berhak mengaksesnya	Kelebihan pada penelitian ini sudah menggunakan simulator GNS3 untuk mendesain dan mensimulasikan topologi jaringan. Kekurangan dalam penelitian ini kurangnya membangun role yang lebih kompleks yang membuat jaringan mudah diretas oleh hacker.
Desmira & Roni (2022)	Hasil penelitian yang dilakukan oleh peneliti yaitu membuat akses khusus keamanan jaringan dalam pengelolaan dan pengawasan menggunakan remote server.	Kelebihan pada penelitian ini didapatkan pemanfaatan port SSH yang mudah konfirtible dan praktis dalam memantau jaringan internet pada server. Kekurangan nya masih ada beberapa port yang system windows nya tidak dapat terlihat aktifitas port ssh pada jaringan server.
Tito (2022)	Hasil penelitian yang dilakukan oleh peneliti	Kelebihan pada penelitian ini yaitu rules knocking yang dibuat menjadi

	yaitu pengelolaan jaringan di instansi BPKAD Sumsel dilakukan rules knocking yang dimana menjaditambahan autentikasi untuk terhubung ke router yang dapat meningkatkan keamanan system jaringan terutama dari akses illegal	tambahan autentikasi untuk terhubung ke router dan service port yang terbuka dapat diamankan dengan melakukan blocking port sehingga menjadi ter-filtered. Kekurangan pada penelitian ini di beberapa port masih ada system computer yang hanya bisa dibuka dengan cara mengetuk nya terlebih dahulu.
Eva (2014)	Hasil penelitian ini bisa mengontrol aktifitas kegiatan siswa,guru yang berhubungan dengan akses internet.	Kelebihan pada penelitian ini adalah pengontrolan trafik jaringan internet terhadap user yang dimana dapat memantau situs yang telah diakses oleh user.mengakses hal yang terlarang.

2.2 Dasar Teori

2.2.1 Jaringan

Menurut Sharon & Supardi (2014) mengatakan juga bahwa jaringan adalah sistem yang terdiri dari media komunikasi perangkat keras dan perangkat

lunak yang diperlukan untuk menghubungkan antara dua atau lebih sistem komputer dan peralatan. Menurut Jafar Noor Yudianto (2007) jaringan komputer adalah sebuah sistem yang terdiri atas komputer-komputer yang didesain untuk dapat berbagi sumber daya (printer, CPU), berkomunikasi (surel, pesan instan), dan dapat mengakses informasi (peramban web). Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya, Di setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan (service). Pihak yang meminta atau menerima layanan disebut klien (client) dan yang memberikan/mengirim layanan disebut peladen (server). Desain ini disebut dengan sistem client-server, dan digunakan pada hampir seluruh aplikasi jaringan komputer.

Dari beberapa pengertian jaringan menurut para ahli di atas dapat diambil kesimpulan bahwa jaringan adalah sebuah sistem yang terdiri atas sekumpulan komputer untuk menunjang terhubungnya komunikasi antara satu perangkat komputer dengan perangkat komputer lainnya.

2.2.2 CIA Triad

Menurut perrin (2008) CIA Triad (Confidentiality, Intergrity,Availbility) adalah model terkenal yang pengembangan kebijakan keamanan nya digunakan untuk mengidentifikasi masalah dan solusi yang diperlukan untuk keamanan dan system informasi. CIA Triad bisa didefinisikan sebagai sebuah rancangan model yang digunakan untuk menjadi panduan atau membantu seseorang baik secara individu maupun organisasi tertentu dalam membentuk atau membuat sebuah aplikasi,system,prosedur, atau kebijakan yang berhubungan dengan keamanan

informasi. Menurut Asriyanik (2016) konsep keamanan harus memenuhi minimalnya 3 aspek yaitu :

a. Confidentiality(Kerahasiaan)

Dapat menjamin bahwa data bersifat rahasia, maksudnya hanya dapat diakses oleh pihak yang berhak dan memastikan bahwa informasi hanya dapat di akses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan. Metode yang digunakan pada penelitian ini adalah: Encryption, Access Controls, Steganografi dan Obfuscation.

b. Keutuhan (Integrity)

Dapat menjamin bahwa data tetap utuh dan lengkap, dan dapat menjaga dari kerusakan atau ancaman lain yang mengakibatkan berubah informasi dari aslinya. Metode yang digunakan antara lain hasing dengan menggunakan MD5, SHA, HMAC, Tanda tangan digital 2 (dua).

c. Ketersediaan (Availability)

Dapat menjamin pengguna dapat mengakses informasi kapanpun tanpa adanya gangguan dan tidak dalam format yang tidak bisa digunakan, salah satu metode adalah patching, backup Data.

2.3 Keamanan Sistem

Menurut Revva et al (2018) Sistem Keamanan Jaringan adalah proses untuk mencegah dan mengidentifikasi pengguna yang tidak sah penyusup dari jaringan komputer.Tujuannya adalah untuk mengantisipasi resiko jaringan komputer yang dapat berupa ancaman fisik maupun logik. Yang dimaksud ancaman fisik itu adalah yang merusak bagian fisik komputer atau hardware computer sedangkan

ancaman logik yaitu berupa pencurian data atau penyusup yang membobol akun Seseorang. Keamanan jaringan harus didasarkan pada prinsip keamanan yang kokoh, termasuk enkripsi yang kuat, pengelolaan kunci yang baik, dan pemantauan yang terus-menerus terhadap ancaman. Keamanan jaringan komputer sendiri merupakan praktik yang bertujuan untuk mencegah dan mendeteksi penggunaan jaringan komputer yang tidak sah dimana pada keamanan suatu jaringan dapat mengidentifikasi potensi bahaya yang dapat mengganggu operasi jaringan komputer baik secara langsung maupun tidak disengaja. Selain itu, keamanan jaringan komputer juga bertujuan untuk melindungi data sistem komputer dari berbagai risiko yang mungkin terjadi.

2.3.1 Mikrotik

Menurut penelitian yang dilakukan oleh Samsuar & Hadi (2018) MikroTik RouterOS dan perangkat kerasnya banyak digunakan oleh ISP *(Internet Service Provider),* penyedia layanan Wi-Fi, perusahaan, institusi pendidikan, dan bahkan oleh pengguna rumahan yang memiliki kebutuhan jaringan yang kompleks.

2.3.2 Firewall Filtering

Menurut Rendra Towidjojo (2013) *firewall* merupakan perangkat yang berfungsi untuk memeriksa dan menentukan paket data yang dapat keluar atau masuk dari sebuah jaringan, dengan kemampuan menentukan apakah sebuah paket data bisa masuk dan keluar dari suatu jaringan maka *firewall* berperan untuk melindungi jaringan dari serangan yang berasal dari luar jaringan, selain ditujukan untuk melindungi jaringan, firewall juga dapat

difungsikan untuk melindungi sebuah host atau yang biasa disebut single host.

Menurut Mardiyati (2014) *Firewall* memiliki beberapa tugas yang perlu dilaksanakan :

1. Pertama, firewall harus menerapkan kebijakan keamanan dalam jaringan (site security policy). Jika tindakan tertentu tidak sesuai dengan kebijakan ini, firewall harus memastikan bahwa semua upaya yang mewakili tindakan tersebut gagal atau dicegah. Dengan demikian, semua akses ilegal antar jaringan yang tidak diotorisasi akan ditolak.
2. *Firewall* melakukan filtering dengan mewajibkan semua lalu lintas data melewati firewall untuk semua proses penyediaan dan penggunaan layanan informasi. Dalam konteks ini, paket data yang mengalir ke dan dari firewall diseleksi berdasarkan alamat IP, nomor port, atau arahnya, dan disesuaikan dengan kebijakan keamanan yang ada.
3. Firewall juga harus mampu merekam atau mencatat kejadian mencurigakan serta memberitahu administrator tentang upaya-upaya yang mencoba melanggar kebijakan keamanan. Namun, ada beberapa hal yang tidak dapat dilakukan oleh firewall. Pertama, firewall tidak dapat melindungi dari serangan yang berasal dari dalam jaringan (serangan orang dalam). Kedua, firewall tidak dapat melindungi dari serangan yang tidak melewati firewall tersebut (bypassing the choke point). Misalnya, jika ada layanan dial-up yang terpasang, jaringan dapat diakses melalui modem tersebut.

4. Firewall tidak dapat melindungi jaringan internal dari seranganserangan model baru. firewall tidak dapat melindungi jaringan dari serangan virus.

2.3.3 IP Address

Menurut Varianto & Badrul (2015) "IP Address merupakan singkatan dari Internet Protocol Address, IP Address adalah identitas numeric yang diberikan kepada suatu alat seperti komputer, router atau printer yang terdapat dalam suatu jaringan komputer yang menggunakan internet. Adanya IP Address berfungsi agar setiap perangkat yang menggunakan koneksi internet bisa menghubungi satu sama lain. Cara kerja ip Address ini adalah ISP akan mengubah data tersebut ke dalam datagram. Datagram ini akan dikirim ke server website untuk masuk ke tahap screening oleh IP address. Jika datagram tersebut dirasa aman, maka situs website yang diminta akan dapat muncul pada halaman web browser pengguna.

2.3.4 Block IP Address

Menurut penelitian Widyatama (2014) block ip address bisa digunakan untuk memfilter traffic koneksi yang keluar masuk berdasarkan alamat IP serta port. Block ip Address sendiri didesain untuk memblok IP dalam suatu koneksi yang terjadi dalam suatu jaringan. Kejahatan didunia maya yang beragam jenisnya mulai dari spamers, hacker dan lainnya

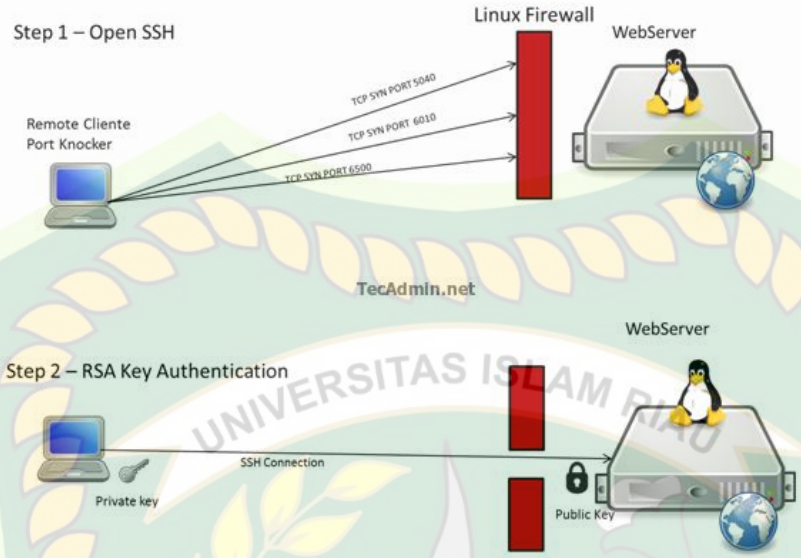
2.3.5 Drop IP Address

Disini merupakan panduan langkah menambahkan aturan filter menggunakan Winbox:

1. Buka IP>Firewall;
2. Pilih Tab “Filter Aturan”;
3. Klik pada + untuk menambahkan aturan baru;
4. Pilih tab “umum”;
5. Pilih Rantai: Masukan;
6. Pilih src. Alamat-masukkan IP yang diinginkan;
7. Pilih tab “Tindakan”;
8. Pilih Tindakan: Jatuhkan;
9. Klik OK dan alamat ip yang dituju akan diblokir filtering

2.4 Port Knocking

Menurut Amarudin (2018) port knocking adalah proses menyembunyikan layanan jarak jauh didalam sebuah firewall yang memungkinkan akses ke port tersebut hanya untuk mengetahui service setelah klien berhasil diautentikasi ke firewall yang dimana port knocking ini merupakan metode untuk mengakses port yang telah diblok dengan mengirimkan packet atau koneksi sesuai dengan aturan knocking yang telah dibuat. Yang dimana port knocking merupakan suatu system keamanan router mikrotik yang bertujuan untuk membuka atau menutup akses port tertentu dengan menggunakan firewall pada perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu. Seperti lebih jelasnya bisa dilihat pada gambar 2.1



Gambar 2. 1 Port Knocking

2.4.1 Topologi

Menurut penelitian yang dilakukan Madcomps (2015), Topologi jaringan merupakan gambaran pola hubungan antara komponen-komponen jaringan, yang meliputi komputer server, komputer client (workstation), hub (switch), Pengkabelan, dan komponen jaringan yang lain". Topologi jaringan komputer merujuk pada cara menghubungkan komputer satu dengan yang lain untuk membentuk jaringan. Saat ini, terdapat beberapa cara yang umum digunakan, seperti bus, token ring, dan star. Pilihan topologi jaringan komputer akan mempengaruhi kecepatan komunikasi di dalamnya. Oleh karena itu, penting untuk memperhatikan kelebihan dan kekurangan masing-masing topologi berdasarkan karakteristiknya. Topologi jaringan yaitu dengan bentuk paling dasar memiliki tiga jenis yaitu topologi diantaranya bus, star, ring.

a. Topologi*Bus*

Topologi Bus merupakan suatu konfigurasi jaringan yang memiliki satu

kabel utama sebagai jalur utama yang terhubung ke beberapa node atau perangkat lainnya. Kabel yang digunakan dalam topologi ini adalah kabel koaksial dengan konektor BNC. Untuk setiap sambungan antara kabel utama dan node, digunakan T-Connector. Di sisi akhir kabel utama yang tidak terhubung ke perangkat jaringan, digunakan terminator atau end-connector.

b. Topologi Star

Topologi Star adalah suatu konfigurasi jaringan yang memiliki bentuk seperti bintang. Pada topologi ini, terdapat sebuah hub atau switch yang berfungsi sebagai pusat dari jaringan. Semua perangkat jaringan terhubung ke hub/switch tersebut. Hub atau switch memiliki peran yang sangat penting dalam topologi ini. Topologi Star merupakan salah satu topologi yang paling mudah dalam hal pemeliharaan, sehingga banyak digunakan. Selain itu, topologi ini menggunakan kabel UTP dan konektor RJ-45.

c. Topologi Ring

Topologi Ring adalah suatu konfigurasi jaringan yang memiliki bentuk lingkaran, di mana setiap perangkat terhubung langsung dengan dua perangkat lainnya. Dengan demikian, setiap node memiliki dua kabel yang terhubung. Topologi ini menggunakan kabel koaksial dengan konektor BNC. Berbeda dengan topologi Bus, topologi Ring tidak menggunakan end-connector karena setiap kabel langsung terhubung dengan perangkat jaringan.

2.4.2 Internet Service Provider

Menurut Wijaya (2016) Penyedia Layanan Internet (ISP) adalah perusahaan atau entitas bisnis yang menjual akses internet atau layanan serupa kepada pelanggan. ISP sering dikaitkan dengan jaringan telepon karena mereka menyediakan akses internet melalui jaringan telepon, contohnya Telkomnet instant dari Telkom. Namun, perkembangan teknologi ISP tidak terbatas pada jaringan telepon saja, melainkan juga mencakup teknologi lain seperti serat optik dan nirkabel. Selain itu, ISP memiliki jaringan yang mencakup koneksi domestik dan internasional, sehingga pengguna dapat terhubung ke internet global melalui koneksi yang disediakan oleh ISP. Jaringan ini menggunakan media transmisi seperti kabel dan frekuensi radio untuk mengalirkan data.

2.4.3 Winbox

Winbox merupakan sebuah perangkat lunak yang digunakan untuk mengkonfigurasi Mikrotik RouterOS melalui antarmuka grafis (*GUI*). Dengan menggunakan GUI ini, pengaturan konfigurasi menjadi lebih mudah. Winbox dapat dijalankan di sistem operasi *Windows* dan merupakan sebuah aplikasi *biner portabel*. Oleh karena itu, ukuran Winbox umumnya lebih kecil dan tidak menghabiskan banyak memori. Winbox juga dapat berjalan di MacOS (OSX) dan Linux, namun memerlukan aplikasi tambahan bernama Wine.

WinBox merupakan sebuah aplikasi grafis yang dikembangkan oleh MikroTik dengan tujuan untuk mengonfigurasi dan mengelola perangkat jaringan MikroTik. Aplikasi ini menyediakan antarmuka pengguna yang intuitif dan mudah digunakan untuk mengatur berbagai pengaturan pada router MikroTik. Dengan menggunakan WinBox, pengguna dapat dengan mudah melakukan

konfigurasi jaringan, mengelola pengguna, memantau kinerja jaringan, dan menangani tugas-tugas administratif lainnya. WinBox menyediakan berbagai fitur yang bermanfaat, termasuk kemampuan untuk melihat dan mengedit pengaturan jaringan, mengkonfigurasi firewall, mengatur keamanan, mengelola antarmuka, dan banyak lagi. Aplikasi ini telah menjadi pilihan populer di kalangan pengguna MikroTik karena antarmuka yang sederhana dan fungsionalitas yang lengkap. Meskipun tidak ada informasi khusus mengenai pandangan para ahli tentang WinBox, namun aplikasi ini telah dikenal luas dan dianggap sebagai alat yang berguna untuk mengkonfigurasi dan mengelola perangkat MikroTik RouterOS dengan cara yang mudah dan efisien.

2.4.4 Telegram Bot

Menurut penelitian yang dilakukan oleh Angga Dwi Mulyanto (2020) bot telegram merupakan akun telegram khusus yang didesain dapat meng- handle pesan secara otomatis. Pengguna dapat berinteraksi dengan bot dengan mengirimkan command tertentu melalui pesan private maupun group. Akun ini hanya bertugas sebagai antarmuka dari kode yang berjalan di sebuah server. Ada dua cara dalam pembuatan bot telegram, yaitu dengan menggunakan metode long-polling dan webhook. Metode long-polling artinya server bot tersebut bisa diakses menggunakan laptop sendiri sebagai server dan database nya, server akan mengecek aktivitas bot secara periodik. Jika ada pesan yang masuk maka server akan melakukan eksekusi berdasarkan pesan request yang dikirim pengguna. Jika tidak ada pesan maka kondisi server idle. Apabila menggunakan metode webhook server bot telegram harus di hosting dan memakai https, yang artinya bot yang berada di server bisa diakses oleh user lain.

2.4.5 Jenis serangan pada jaringan komputer

2.6.1 Port Scanning

Menurut penelitian yang dilakukan Mulyanto et al (2022) port scanning adalah proses penjelajahan sistem atau jaringan untuk mengidentifikasi port yang aktif atau terbuka pada perangkat tujuan. Yang dimana port forwarding ini menginstruksikan router untuk mengirim permintaan tersebut ke PC tertentu di jaringan yang akan memenuhi permintaan tersebut sebagai contoh ketika kita meminta router untuk menerima permintaan luar dari PC dengan alamat IP 192.168.1.103 dan port terbuka :80.

2.6.2 DDos

Menurut Penelitian yang dilakukan oleh Gregorius Hendita Artha Kusuma (2022) Serangan DDoS merupakan Serangan Distribusi Layanan (DDoS) yang bertujuan untuk membuat jaringan atau layanan tidak tersedia dengan membanjiri lalu lintas jaringan atau sumber daya dengan serangan dari banyak perangkat yang terdistribusi Hal ini dapat mengakibatkan gangguan berat pada operasi jaringan.

2.5 Linux

Linux adalah sebuah system operasi yang menggunakan kernel sebagai system operasi yang berisikan sebuah script yang ada. Selanjutnya linux memiliki terdapat banyak user juga yang mempunyai masalah besar dalam perkembangan system operasi linux ini. Pada dasarnya linux banyak digunakan untuk pentest dalam sebuah pengujian system keamanan jaringan karena linux mempunyai

banyak tools yang memudahkan dalam pengujian system keamanan.Untuk keseluruhan dari system operasi ini adalah yang berbasis General Public License (GPL) yang ditetapkan pada tahun 1983 oleh Richard Stallman. Menurut Harjo (2016) pengaruh GNU yang sangat besar karena sebagai pelopot munculnya nama alternative GNU/Linux.

2.6 Snort

Snort merupakan sebuah tool keamanan yang berfungsi untuk mendeteksi intrusi-intrusi jaringan (penyusupan,pemindaian,penyerangan,dan beragam bentuk ancaman lainnya) sekaligus untuk pencegahan. Dalam pratiknya snort sangat handal untuk membentuk logging paket-paket dan analisis trafik secara real-time dalam jaringan berbasis TCP/IP. Sehingga snort merupakan suatu system yang mendeteksi secara realtime terhadap adanya serangan jaringan dengan hasil alert dari serangan jaringan tersebut. Menurut Kerry J & Cristhopher (2004) snort dapat dioperasikan dalam 4 mode yaitu diantara nya :

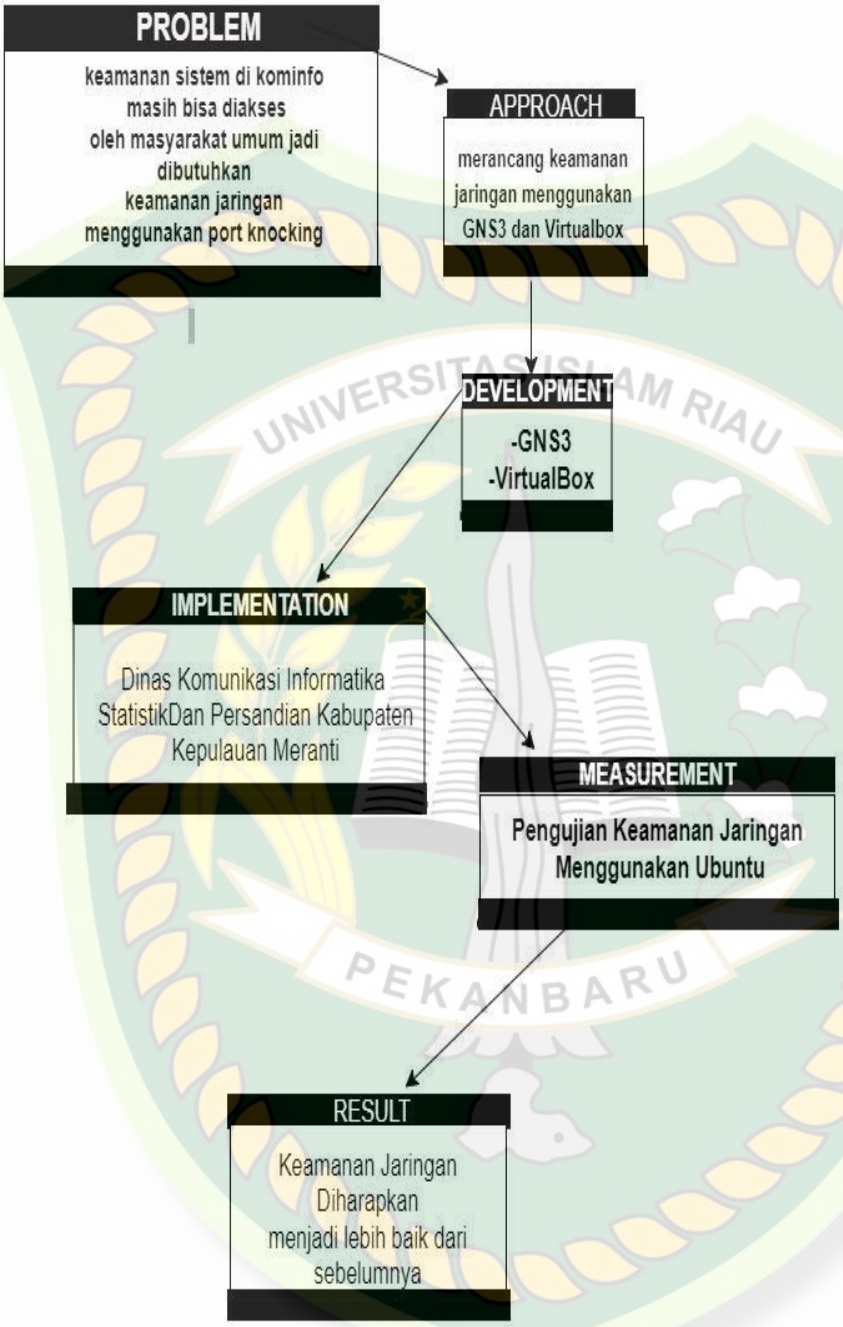
1. Sniffer mode pada mode ini snort melakukan tugasnya untuk menangkap seluruh data yang lewat dan snort dapat melihat seluruh paket data pada sebuah jaringan.
2. Logger mode pada mode ini snort bertugas mencatat semua paket data yang lewat dari sebuah jaringan sehingga dapat dianalisis.
3. Intrusion detection mode pada mode ini snort akan bertugas sebagai pendeteksi sebuah tindakan jaringan komputer
4. Inline mode pada mode ini snort bertugas membandingkan sebuah paket data dengan aturan iptables dan libpcap kemudian dapat menentukan iptables untuk melakukan penjatuhan paket yang berisi serangan atau

paket normal yang bisa juga menerima paket berdasarkan aturan snort yang lebih baik lagi. Penempatan snort sebagai IDS dalam jaringan dapat dilakukan dengan IDS Placement tergantung kebutuhan dan ketersediaan perangkat yang ada konsep penerapan IDS dalam jaringan adalah sebagai berikut:

1. Network Intrusion Detection system ini melakukan monitoring paket data pada sebuah perangkat jaringan yang telah dipasang snort, dan juga terhadap semua bentuk lalu lintas sebuah jaringan yang berada didalam segmen jaringan dimana snort itu berada. Kelebihan dari system NIDS ini meliputi cakupan jaringan yang diawasi cukup luas sehingga dalam melakukan pengamanan pada sebuah jaringan yang memilki system IDS maka mempunyai jangkauan yang lebih luas sedangkan kekurangan dari system NIDS ini meliputi jaringan komputer yang menggunakan IDS skan mempunyai lalu lintas jaringan yang sangat banyak.

2.7 Kerangka Pemikiran

Pada gambaran kerangka pemikiran yang dibuat oleh penulis ketika ada seseorang yang hendak mencoba untuk memasuki sebuah system keamanan jaringan dengan cara yang tidak sah dan penerimaan notifikasi dapat dilihat oleh server melalui telegram Hasil yang diharapkan adalah ketika hacker akan memasuki system keamanan maka internet yang akan di peroleh mengalami pemblokan internet. Untuk penjelasan yang lebih jelas bisa di lihat pada Gambar 2.2 Kerangka Pemikiran



Gambar 2. 2 Kerangka Pemikiran

BAB III

METODOLOGI PENELITIAN

3.1 Tinjauan Tempat Penelitian

Metodologi penelitian merupakan cara untuk mengetahui hasil dari suatu masalah yang spesifik, dalam hal ini masalah tersebut juga berkaitan dengan permasalahan penelitian yang dimana didalam penelitian ini menjelaskan bagaimana cara merancang suatu keamanan jaringan menggunakan *firewall filtering dan port knocking* seperti pengumpulan data dan bahan yang digunakan, menentukan spesifikasi kebutuhan software dan hardware. Metodologi penelitian ini juga merancang bangun system keamanan yang dimana bisa mengantisipasi setiap serangan yang tidak bertanggung jawab dan meningkatkan keamanan data dengan mengimplementasikan *firewall filtering* dan fitur lainnya pada Kominfo Kabupaten Kepulauan Meranti.

3.1.1 Sejarah Tempat Penelitian

Dinas komunikasi dan informatika sebelumnya bernama "Departemen Penerangan" (1945-1999), Selanjutnya ditahun (2001-2005) menjadi Kementerian Negara Komunikasi dan informasi, Dan pada tahun (2005-2009) Diganti menjadi Departemen Komunikasi dan Informatika disingkat Dep Kominfo yang dimana Departemen atau Kementerian dalam Pemerintah Indonesia yang membidangi urusan Komunikasi dan Informatika. Pada mulanya bagian Komunikasi dan Informatika (KOMINFO) berada di Dinas Perhubungan (DISHUB-DISHUB KOMINFO) dan berdasarkan PERBUP OPD SETDA NO 29 TAHUN 2016 KOMINFO menjadi bagian tersendiri di Sekretariat Daerah. Bagian Komunikasi

dan Informatika dibentuk berdasarkan PERBUP OPD SETDA NO 29 TAHUN 2016/25/November tentang kedudukan,susunan organisasi, tugas pokok dan fungsi serta tata kerja Sekretariat Daerah Kabupaten Kepulauan Meranti. Bagian Komunikasi dan Informatika Kabupaten Kepulauan Meranti merupakan lembaga Pemerintah daerah yang mempunyai tugas untuk menyelenggarakan urusan Pemerintah di bagian Komunikasi Dan Informatika yang dimana bisa membantu dalam menyelenggarakan Pemerintahan Negara. Lembaga ini terletak dikomplek Perkantoran Terpadu JL.Dorak, Kecamatan Tebing Tinggi, Kabupaten Kepulauan Meranti Provinsi Riau.

3.2 Metode Penelitian

Penelitian ini menggunakan metode penetration test yang dimana merupakan bentuk penelitian pengujian serangan secara langsung menggunakan simulasi serangan jaringan untuk mengetahui kerentanan jaringan pada instansi terkait. Pada penelitian ini menggambarkan sebuah IP address client/korban yang dilakukan penyerangan dengan menggunakan kalilinux sehingga snort mendeteksi adanya serangan. Snort merupakan tool keamanan untuk mengetahui adanya serangan atau penyusupan jaringan dan pencegahan.

3.2.1 Metode Pengumpulan Data

a. Metode Observasi

Metode observasi penulis melakukan pengamatan terhadap jaringan lokal di KOMINFO Kabupaten Kepulauan Meranti yang dimana penulis juga melakukan pengetesan/pantester secara langsung di KOMINFO Kabupaten Kepulauan Meranti.

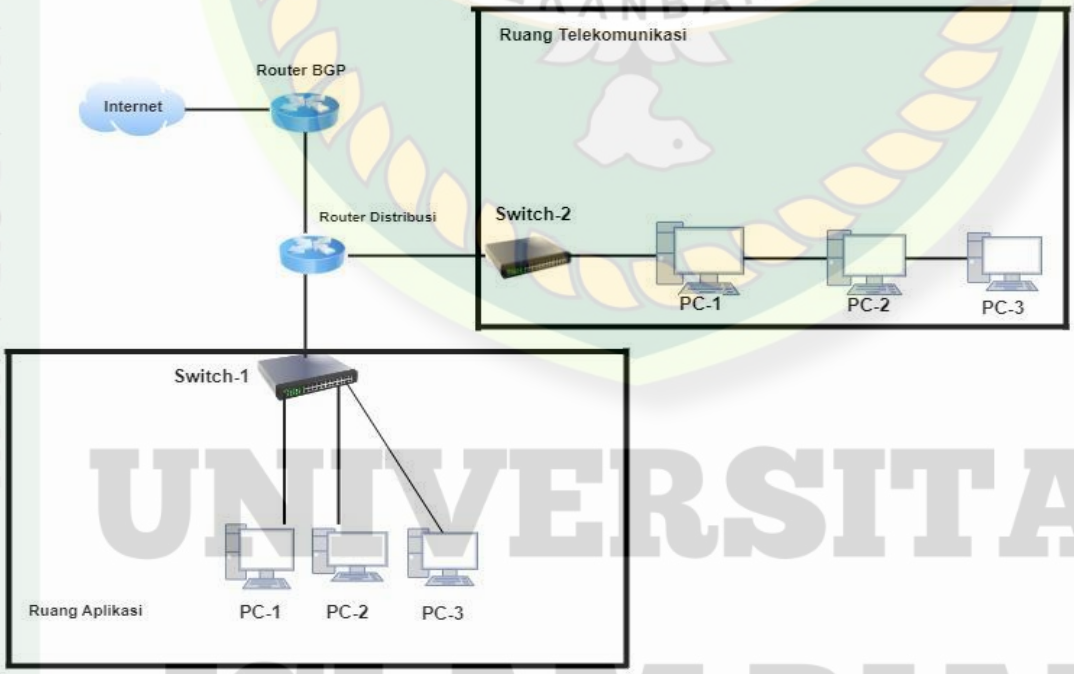
b. Metode Wawancara

Metode Wawancara Penulis peroleh dengan interaksi secara langsung pada tanggal 6 November 2023 dengan Pengawas Teknologi Informasi. Beberapa pertanyaan diajukan mengenai prosedur keamanan system pada KOMINFO Kabupaten Kepulauan Meranti yang dimana belum ada penggunaan sebelumnya yang menggunakan Port Knocking.

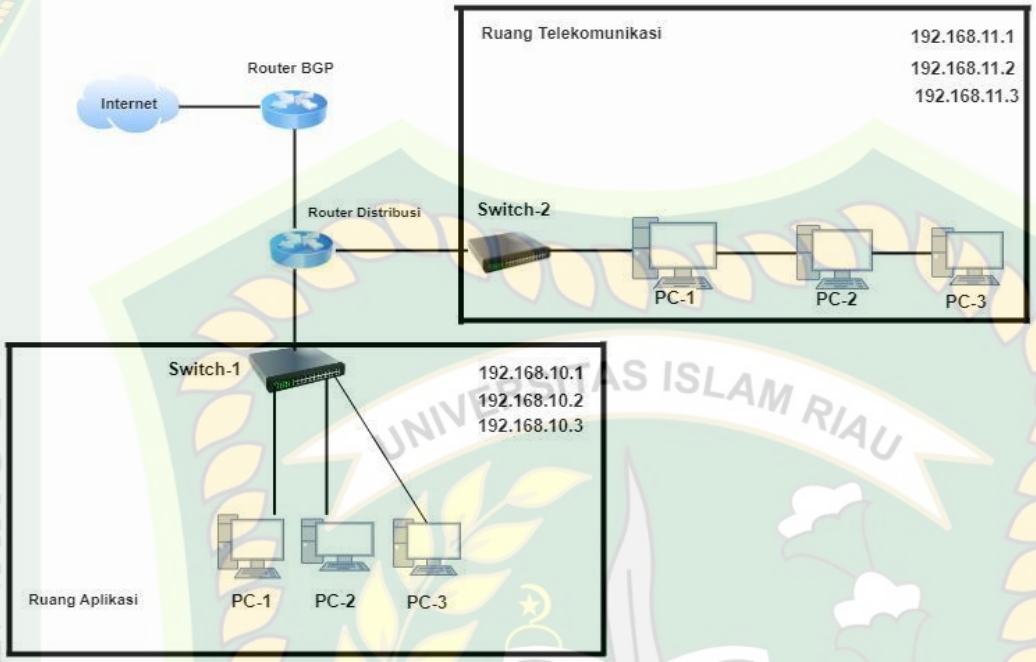
3.3 Skema Jaringan Saat ini

3.3.1 Topologi Jaringan

Topologi jaringan yang digunakan pada Kominfo Kabupaten Kepulauan Meranti yaitu topologi *star* karena setiap komputer menggunakan satu kabel jaringan apabila ada satu komputer yang rusak maka jaringan dikomputer yang lain tidak terganggu berikut ini merupakan topologi *fisik* dan topologi *logic* dikominfo kabupaten kepulauan meranti.



Gambar 3. 1 Topologi Logic



Gambar 3. 2 Topologi Fisik

3.3.2 Spesifikasi Hardware dan Software Jaringan

Spesifikasi perangkat keras (Hardware) dan perangkat lunak (Software) harus memiliki spesifikasi kebutuhan dari sistem yang digunakan, berikut sistem spesifikasi hardware dan software yang digunakan:

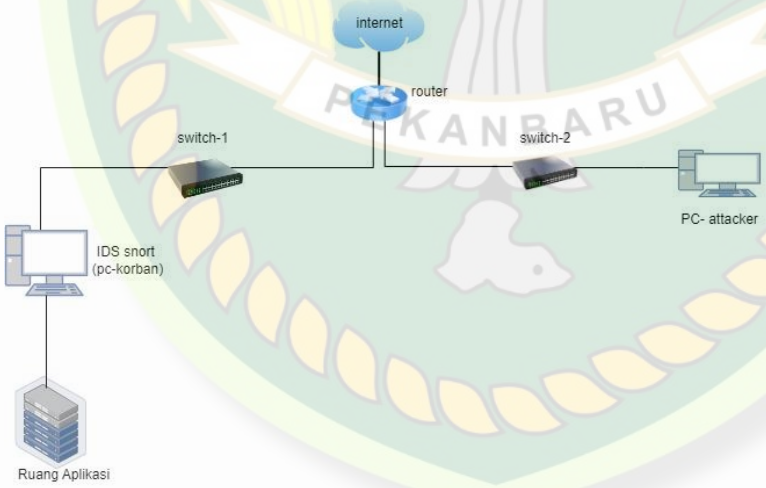
Tabel 3. 1 Spesifikasi Hardware dan Software Jaringan

	Alat, Komponen, Bahan	Spesifikasi
1	Laptop	Processor: Core i5 RAM :8GB Harddisk :500 GB
2	Winbox	3.40 (64bit)

3	Virtualbox	6.1 (64bit)
4	GNS3	2.2.44.1 (32bit)
5	Telegram Bot	10.3.2

3.3.3 Arsitektur Jaringan

Didalam system IDS penelitian ini memiliki arsitektur jaringan yang memberikan gambaran secara jelas mengenai interkoneksi antar perangkat satu dengan yang lainnya. Didalam arsitektur untuk mengatasi permasalahan yang ada diinstansi terkait meliputi pengawasan terhadap keamanan jaringan melalui tool/software yang berguna untuk pencegahan terhadap serangan jaringan yang mungkin bisa saja dilakukan saat tidak terduga. Software bisa meliputi snort yang bertujuan untuk mendeteksi adanya serangan dan menangkap paket data.

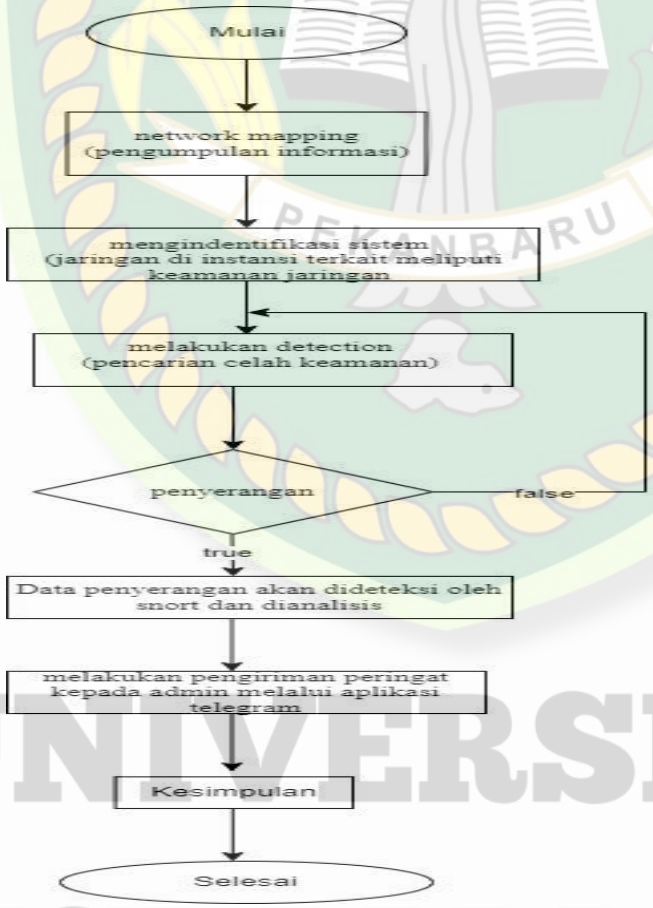


Gambar 3. 3 Impelementasi system IDS snort

Pada gambar 3.3 diatas ini merupakan tahapan pengujian yang dimana penyerang akan melakukan pengujian kekomputer client/korban yang terhubung keruang aplikasi kominfo kabupaten kepulauan meranti. Sehingga saat penyerang melakukan pengujian maka snort akan mendeteksi adanya ancaman atau serangan.

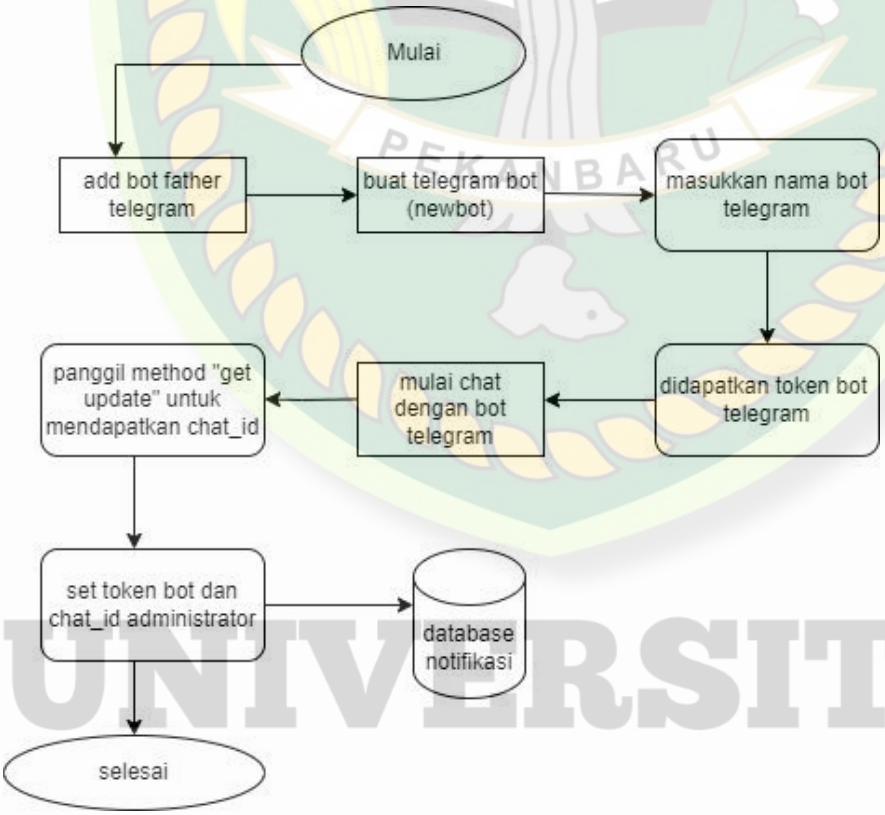
3.3.4 Usulan Perancangan Sistem

Pada penelitian ini perancangan system yang dimana dapat untuk mengatasi permasalahan yang ada pada instansi Kominfo Kabupaten Kepulauan Meranti terkait dengan pengawasan terhadap serangan keamanan jaringan yang kapan saja bisa terjadi. Dipenelitian ini *software* snort yang bertujuan untuk mendeteksi adanya serangan jaringan dan dapat menangkap paket-paket data. *Penetration test* merupakan metode yang banyak digunakan yang dimana tujuan dari metode ini adalah menguji/mengetest keamanan yang baru dirancang meliputi pada jaringan local. Pada gambar dibawah ini merupakan proses dalam *penetration test.*



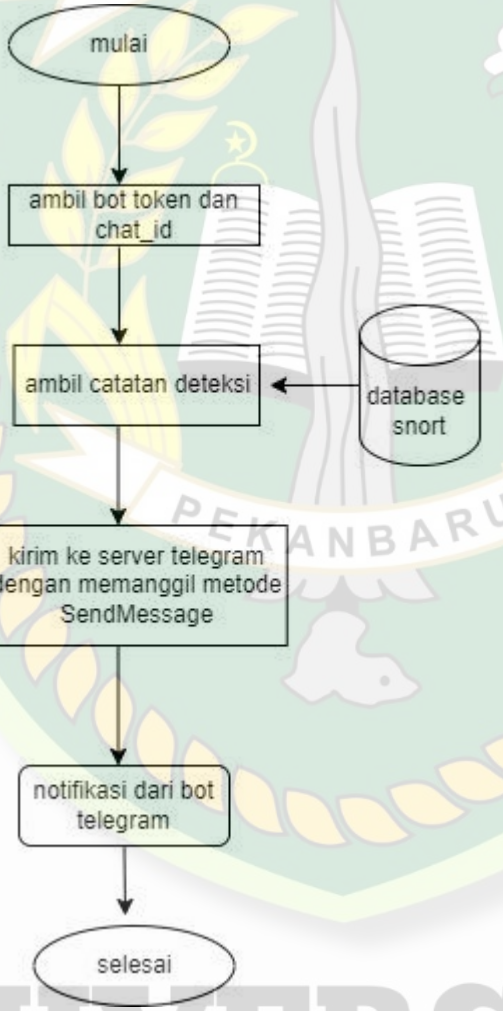
Gambar 3.4 Flowchart Penetration test

Untuk tahap selanjutnya yaitu proses pembuatan bot telegram yang dimana pada proses pembuatan dimulai dengn meminta akun resmi pada @botfather dengan memasukkan perintah bot baru sehingga bisa mendapatkan token dari bot yang digunakan sebagai media peringatan pendeteksi pada snort agar diketahui oleh admin. Pada notifikasi yang dikirimkan oleh bot telegram sepenuhnya berasal dari satu database yang sama dengan yang digunakan untuk menampung alert snort. Disini untuk mengetahui id pengguna, admin harus terlebih dahulu memulai chat terhadap bot yang kemudian mengunjungi situs telegram dengan alamat http://api.telegram.org/bot<token>/getupdates <token> diisi dengan token bot telegram yang dapat dari botfather yang dimana dapat dilihat pada gambar dibawah ini.



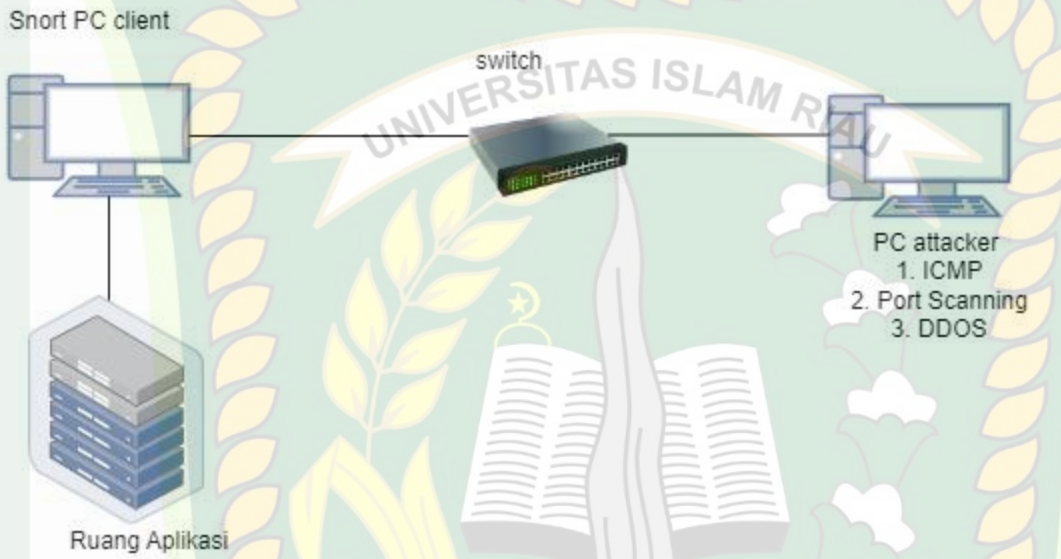
Gambar 3.5 Flowchart pembuatan bot telegram

Langkah selanjutnya yaitu pengiriman notifikasi yang dikirim berdasarkan dari satu database yang sama dengan tool snort untuk menyimpan hasil pendeteksian nya. Token dari bot telegram ini berfungsi untuk mengakses API telegram yang dimana tidak sembarang orang bisa mengakses bot yang dijadikan sebagai media pengiriman peringatan dari snort. Untuk lebih jelasnya dapat dilihat pada gambar 3.6 dibawah ini.



Gambar 3.6 Flowchart pengiriman notifikasi telegram

Langkah selanjutnya yaitu pengujian system untuk melakukan uji atau evaluasi dari penelitian ini yang dimana bertujuan untuk menentukan efektif dari snort sebagai system pendeteksi dari ancaman serangan jaringan. Untuk skema pengujian dapat dilihat pada gambar 3.7 dibawah ini.



Gambar 3.7 Tahapan pengujian system

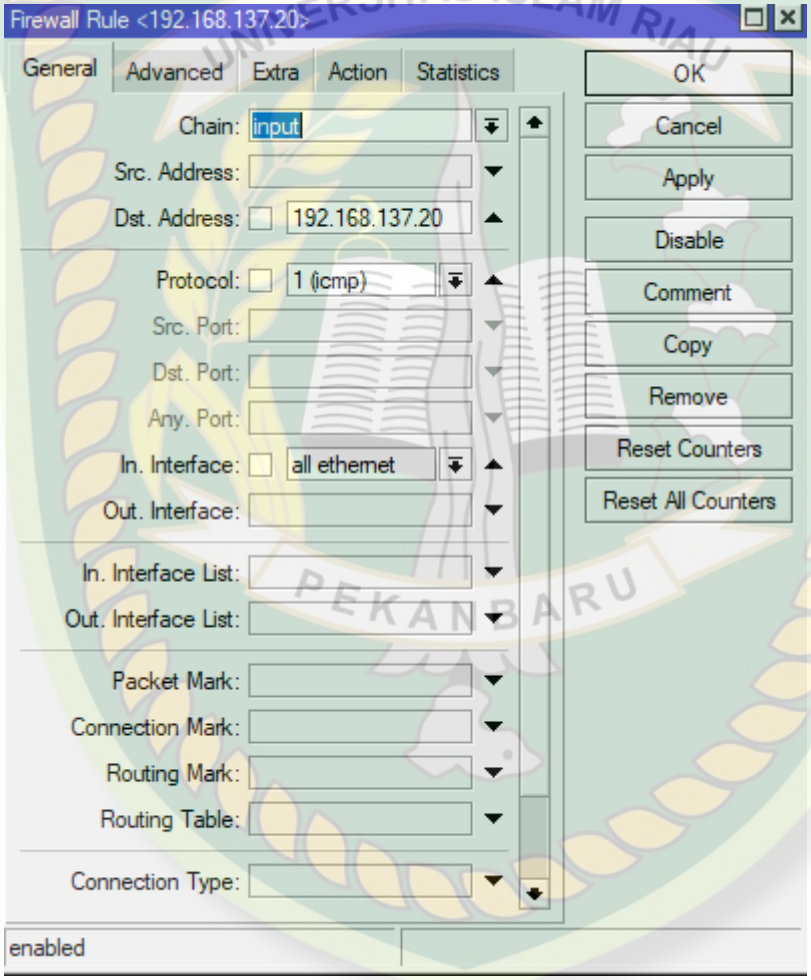
3.3.5 Skema Jaringan

Skema jaringan di Kominfo kabupaten kepulauan meranti saat ini yaitu menggunakan topologi star, yang dimana sumber ISP nya berasal dari NAP Telkom yang setiap komputer menggunakan satu kabel jaringan apabila ada satu komputer yang rusak maka jaringan dikomputer yang lain tidak terganggu Selanjutnya jaringan tersebut dicabangkan melalui switch yang bisa diakses oleh monitor kantor ke bagian bidang aplikasi, Selanjutnya ke bidang telekomunikasi.

3.3.6 Keamanan Jaringan

Pada kominfo kabupaten kepulauan meranti keamanan jaringan yang ada pada mikrotik menggunakan firewall. Firewall dimikrotik berperan sebagai fitur perlindungan untuk mengamankan jaringan dari serangan yang tidak diinginkan

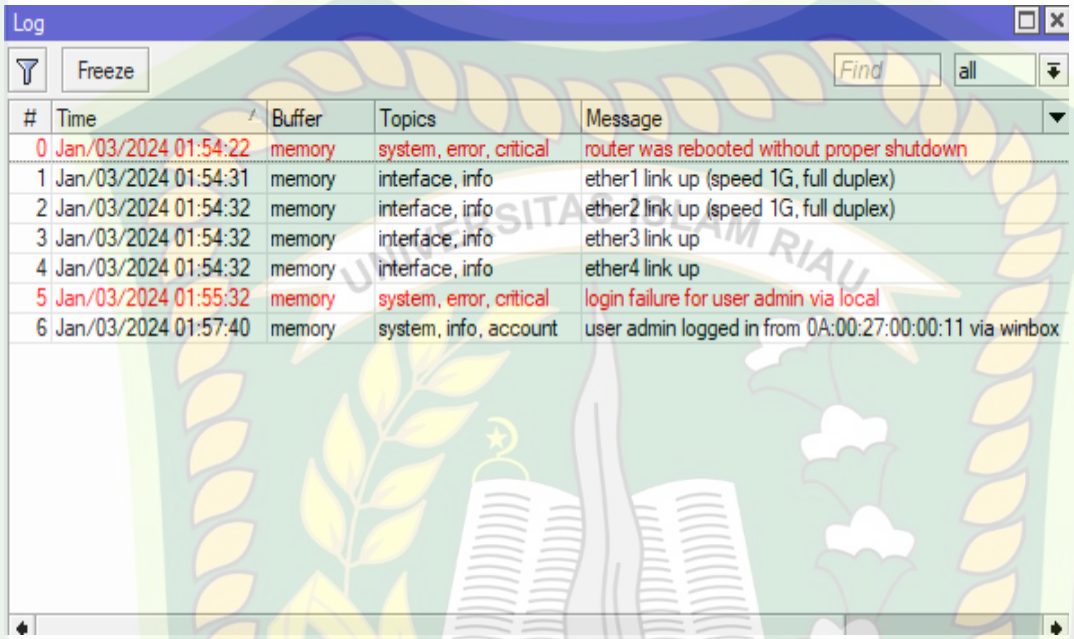
atau ancaman keamanan potensial. Keamanan jaringan komputer diperhatikan dan dianggap penting sejak adanya penyerangan komputer dengan cara menyebarkan virus dan banyak contoh lainnya. Keamanan jaringan komputer pada umumnya sudah banyak dilakukan pencegahan serta penanggulangannya jika sudah diretas hingga ke server.



Gambar 3.8 *Firewall Filtering*

Pada Kominfo Kabupaten Kepulauan Meranti keamanan jaringan yang ada pada mikrotik menggunakan *firewall*. *Firewall* di MikroTik berperan sebagai fitur perlindungan untuk mengamankan jaringan dari serangan yang

tidak diinginkan atau ancaman keamanan potensial. Disini Penulis melakukan konfigurasi pada firewall untuk memblokir siapa saja yang mencoba masuk.



Gambar 3. 9 Contoh Penyerangan Yang Disaring Firewall Filtering

3.4 Permasalahan

Jaringan Internet yang mudah untuk diakses, sangat mengganggu kegiatan para karyawan Kominfo dan pemenuhan media komunikasi yang dilakukan di kantor. Tentunya kendala tersebut menjadi masalah dan mengganggu kegiatan-kegiatan yang ada. DIkarenakan sistem yang sangat mudah diakses oleh pihak luar dan bisa saja di hack data data karyawan yang ada dikantor tersebut.

3.5 Alternatif Pemecahan Masalah

Alternatif pemecahan masalah di penelitian ini adalah melakukan proses routing di dalam mikrotik. Dikarenakan dikantor Kominfo ini belum ada fitur tambahan seperti port knocking untuk memblok siapa saja yang mengakses jaringan internet, maka penulis melakukan konfigurasi terhadap mikrotik. Setelah

melakukan konfigurasi penulis memulai melakukan konfigurasi ulang pada router mikrotik dengan winbox.

BAB IV

HASIL DAN PEMBAHASAN

Penelitian ini dilakukan untuk dapat mengetahui keamanan yang ada didalam sebuah jaringan di KOMINFO Kabupaten Kepulauan Meranti. Keamanan jaringan komputer di KOMINFO Kabupaten Kepulauan Meranti memerlukan peningkatan keamanan seperti *firewall filtering* dan *port knocking* yang dapat membantu dikarenakan memiliki jaringan yang terhubung ke server yang dimana pada server tersebut menyimpan data-data penting terkait informasi dan pembagian jaringan di KOMINFO Kabupaten Kepulauan Meranti. Sehingga dapat melakukan pengujian keamanan jaringan terhadap serangan yang dilakukan oleh pihak yang tidak bertanggung jawab. Dimana dalam melakukan pengujian ini memiliki ip address dan ip penyerang.

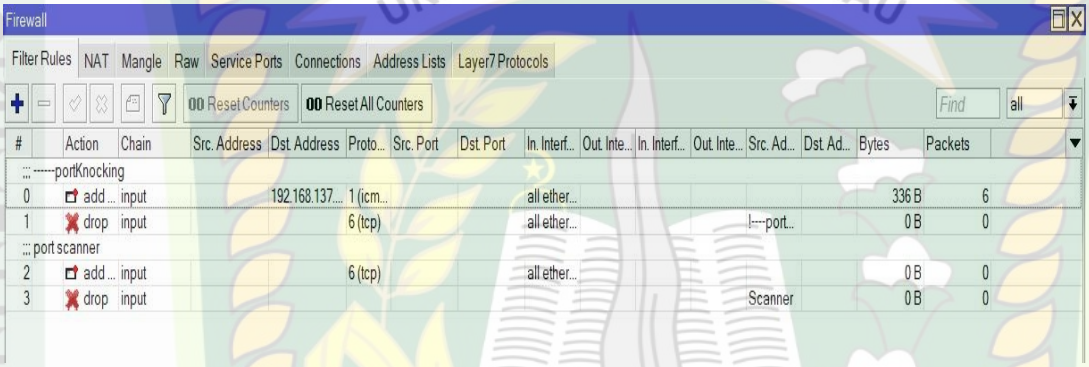
Tabel 4.1 IP address

NO	IP address penyerang	IP address korban
1	192.168.10.22	192.168.10.44

4.1 Analisa Hasil Penelitian

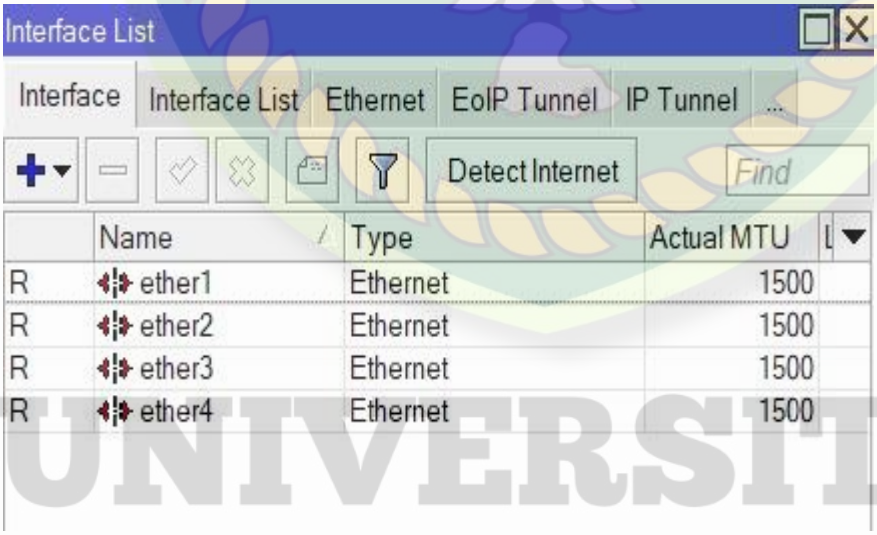
Hasil dari penelitian ini menggunakan dua metode keamanan jaringan yaitu firewall filtering yang digunakan untuk mengatur lalu lintas jaringan serta memblokir jaringan yang dianggap mencurigakan dan port knocking berfungsi sebagai lapisan keamanan jaringan dalam upaya meningkatkan keamanan jaringan yang dimana dalam penelitian ini juga mencakup notifikasi telegram sebagai bentuk pemberitahuan kepada admin jaringan ketika terjadi sesuatu yang

mencurigakan.Evaluasi kinerja dari system dilakukan dengan skenario uji coba serangan dan analisis menggunakan snort. Snort merupakan system yang dapat untuk mendeteksi adanya serangan atau penyalahgunaan jaringan sehingga diperlukan percobaan dengan melakukan penyerangan terhadap jaringan yang sudah dipasang snort. Berikut pada gambar 4.1 merupakan pemasangan firewall filtering dan port knocking.



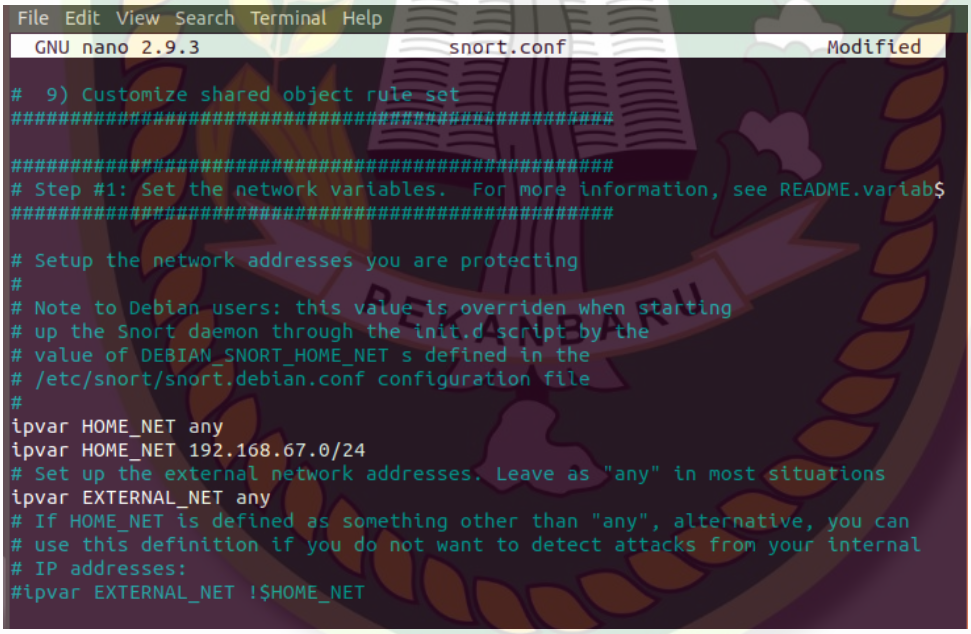
Gambar 4.1 Pemasangan Port Knocking

Pada gambar 4.1 diatas merupakan pemasangan dari fitur port knocking dan firewall filtering yang dimana menggunakan mikrotik winbox.



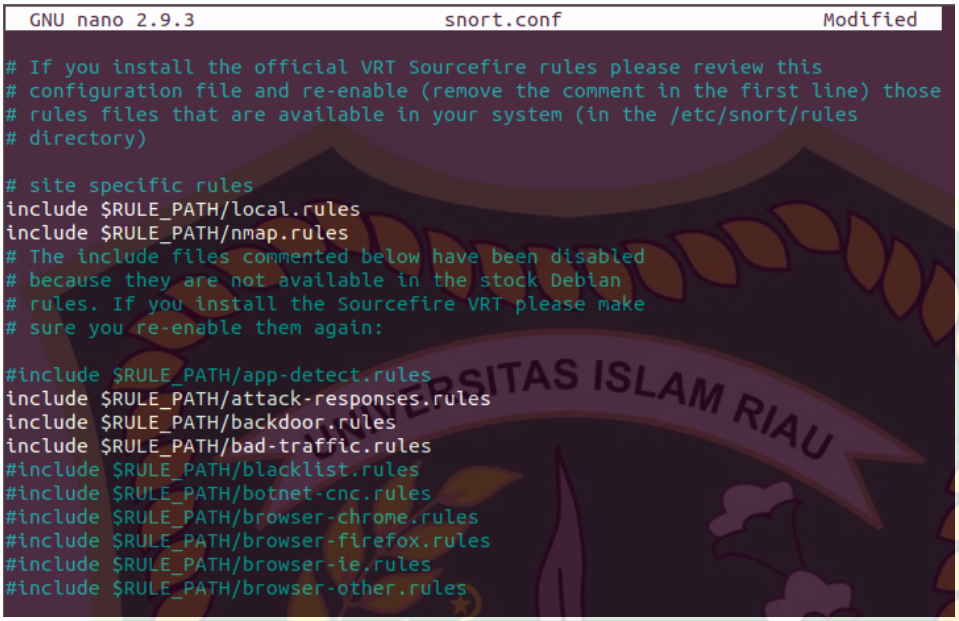
Gambar 4.2 Interface List

Sebelum memulai tahapan pengujian ada beberapa hal yang perlu dilakukan dalam pendeteksian snort apakah snort tersebut berjalan sesuai dengan yang diharapkan yang diantaranya melakukan pembuatan rule snort terkait dengan adanya ancaman hingga dapat terdeteksi oleh snort. Selanjutnya konfigurasi snort sehingga snort dapat bekerja sebagai IDS untuk mendeteksi serangan didalam konfigurasi snort ada beberapa hal penting yang harus dilaksanakan seperti untuk memasukkan IP address client yang dilindungi pada folder snort.conf dan debian.conf sehingga snort dapat mendeteksi jika adanya perobaan penyerangan terhadap ip client. Untuk dapat dilihat lebih jelas pada gambar 4.3 dibawah ini.



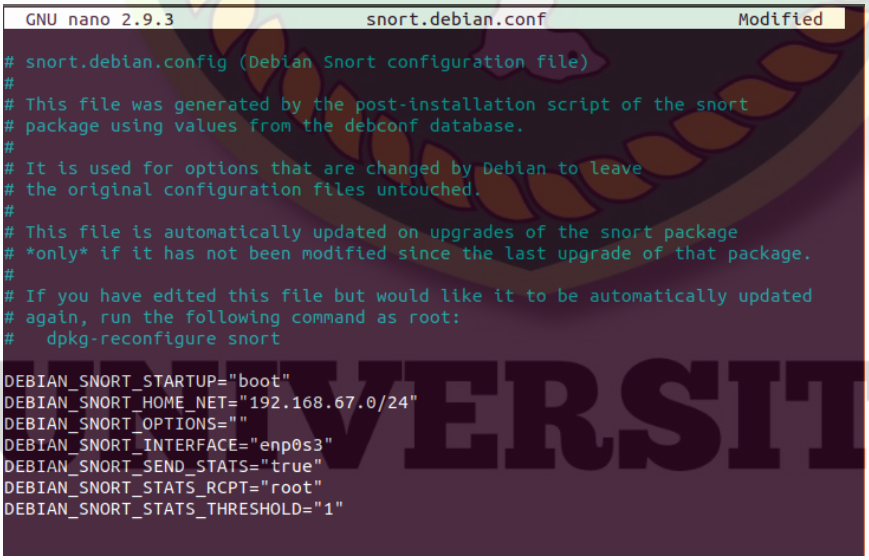
Gambar 4.3 Tampilan Konfigurasi IP Address Snort

Pada gambar 4.3 diatas dapat dilihat IP address yang dilindungi oleh snort yang IP nya 192.168.67.0/24. Selanjutnya yaitu memilih rules- rules snort yang akan diaktifkan pada gambar 4.4 dibawah ini.



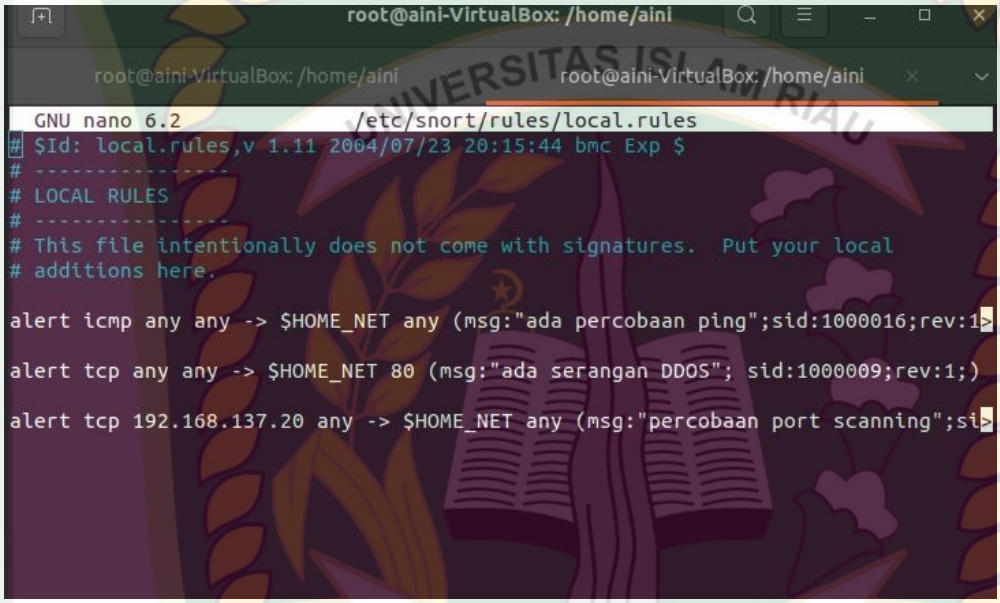
Gambar 4.4 Konfigurasi Pengaktifan Rule Snort

Pada langkah selanjutnya yaitu konfigurasi pada folder snort.debian.conf dalam konfigurasi difolder ini sama hal nya dengan folder.snort.conf yang dimana memasukkan IP address yang akan dilindungi dan untuk lebih jelasnya dapat dilihat pada gambar 4.5 dibawah ini.



Gambar 4.5 Konfigurasi folder snort.debian.conf

Setelah melakukan konfigurasi terhadap folder snort.conf dan snort.debian.conf langkah selanjutnya yaitu membuat rule snort yang dimana pada rule snort tersebut bisa mendeteksi serangan. Untuk lebih jelas dapat dilihat pada gambar 4.6 dibawah ini.



Gambar 4.6 Rules Snort

Langkah selanjutnya yaitu konfigurasi snort dan telegram yang dimana jika terjadi penyerangan snort dapat mendeteksi adanya serangan dan melakukan pengiriman peringatan kepada admin KOMINFO Kabupaten Kepualauan Meranti melalui telegram. Pada gambar 4.7 dibawah ini merupakan konfigurasi untuk membuat snort terhubung ke API telegram.

```
 GNU nano 2.9.3                    bot-tele.sh                         Modified

#init
initCount=0
logs=/home/server/log-tele.txt

#File
msg_caption=/tmp/telegram_msg_caption.txt

#chatid dan bot token telegram
chat_id="-477165501"
token="1940663511:AAEqdaOuCsGDtaQ88ni3dFSKCV-HFirPHcs"

#kirim
function sendAlert
{
        curl -s -F chat_id=$chat_id -F text="$caption"
https://api.telegram.org/bot$token/sendMessage #> /dev/null 2&>1
}
while true
do
    lastCount=$(wc -c $logs | awk '{print $1}') #getSizeFileLogs
    #DEBUG ONLY
    #echo before_last $lastCount #ex 100 #after reset 0
```

Gambar 4.7 Konfigurasi Snort Ke Telegram

Pada gambar 4.7 dapat dilihat pada konfigurasi ini memasukkan chat_id dan token yang ditemukan dari telegram yang dimana snort dapat terhubung ke telegram. Pada gambar 4.8 dibawah ini merupakan tampilan kata kata yang akan ditampilkan pada interface telegram admin.

```
 GNU nano 2.9.3                    bot-tele.sh                         Modified

    #echo before_last $lastCount #ex 100 #after reset 0
    #echo before_init $initCount #ex 0
    #echo "--------------------"

    if(($(($lastCount)) > $initCount));
       then
        #DEBUG
        #echo "Kirim Alert..."
        msg=$(tail -n 2 $logs) #GetLastLineLog
        echo -e "Halo Admin \n Telah Terjadi ada nya Penyerangan pada jaringan$
        Server Time : $(date +"%d %b %Y %T")\n\n"$msg > $msg_caption
        #set Caption / Pesan
        caption=$(<$msg_caption) #set Caption
        sendAlert #Panggil Fungsi di function
        echo "Alert Terkirim"
        initCount=$lastCount
        rm -f $msg_caption
        sleep 1
    fi
    sleep 2 #delay if Not Indication
done
```

Gambar 4.8 Tampilan Interface Telegram

Untuk menjalankan perintah snort seperti pada gambar 4.9 dibawah ini. Yang perintah untuk mengaktifkan nya sudo snort -I enp0s3 -c /etc/snort/snort.conf -l /var/log/snort -d -A console>/home/aini/log-tele.txt.

```
root@aini-VirtualBox:/home/aini# sudo snort -i enp0s3 -c /etc/snort/snort.conf-l
 /var/log/snortv-d -A console > /home/aini/log-tele.txt
```

Gambar 4.9 Perintah Mengaktifkan Snort

Untuk menjalankan peringatan snort yang dimana terhubung dengan telegram dapat dilihat pada gambar 4.10 dibawah ini.

```
root@aini-VirtualBox:/home/aini# ./bot-tele.sh
```

Gambar 4.10 Perintah Menghubungkan Snort Ke Telegram

Selanjutnya yaitu IP address client yang akan di serang oleh penyerang yang menuliskan ipconfig pada terminal linux ubuntu maka akan menampilkan 192.168.10.22 sebagai client/korban. Berikut lebih jelasnya dapat dilihat pada gambar 4.11 dibawah ini

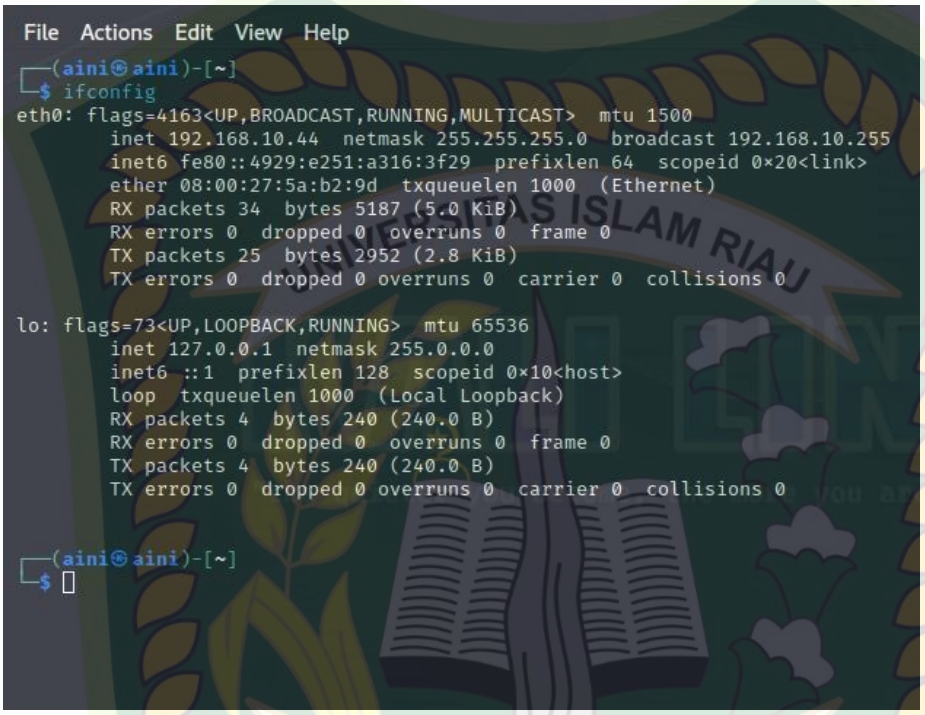
```
aini@aini-VirtualBox:~$ sudo su
[sudo] password for aini:
root@aini-VirtualBox:/home/aini# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.22  netmask 255.255.255.0  broadcast 192.168.10.255
        inet6 fe80::cd8d:d868:b84a:f288  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ff:c9:9b  txqueuelen 1000  (Ethernet)
        RX packets 61  bytes 7529 (7.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 288  bytes 25781 (25.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 345  bytes 28359 (28.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 345  bytes 28359 (28.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@aini-VirtualBox:/home/aini#
```

Gambar 4.11 IP Address Client

Berikut pada gambar 4.12 dibawah ini merupakan IP address jaringan komputer sebagai penyerang.

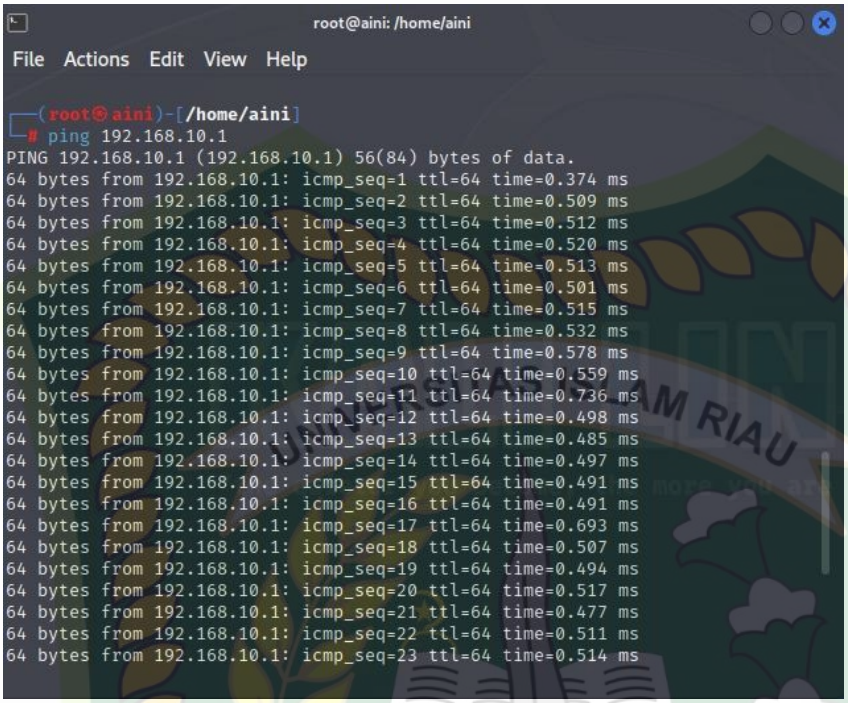


Gambar 4.12 IP Address Penyerang

4.2 Tahapan Pengujian

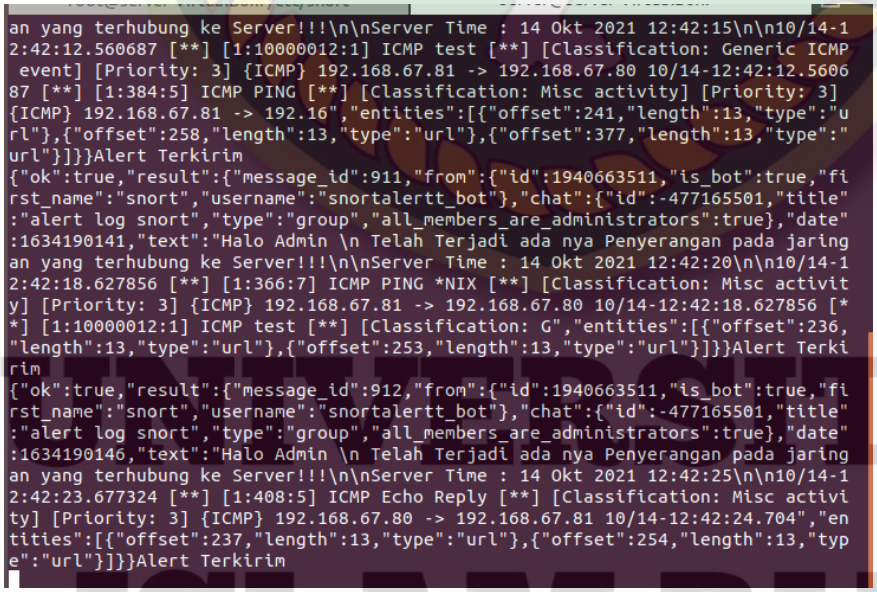
4.2.1 ICMP (Internet Control Message Protocol)

Komputer yang sudah dipasang snort akan mendeteksi adanya serangan dan aktifitas yang mencurigakan yang terdapat didalam jaringan yang langsung terhubung ke server, ICMP sendiri merupakan sebuah protocol yang dimana bertugas untuk mengirimkan pesan kesalahan. Pada gambar 4.13 dibawah ini merupakan tampilan ping dari jaringan penyerang ke jaringan client maka jika komputer client sudah terpasang oleh snort akan muncul tampilan pendeteksi atau adanya aktifitas ping.



Gambar 4.13 Ping IP address Client Dari Penyerang

Selanjutnya pada gambar 4.14 merupakan tampilan interface client yang sudah terpasang snort yang dimana akan menampilkan alert (peringatan) yang terdapat aktifitas ping, dikarenakan itu telah dibuat berdasarkan rule snort sehingga menampilkan perintah pendeteksian snort.



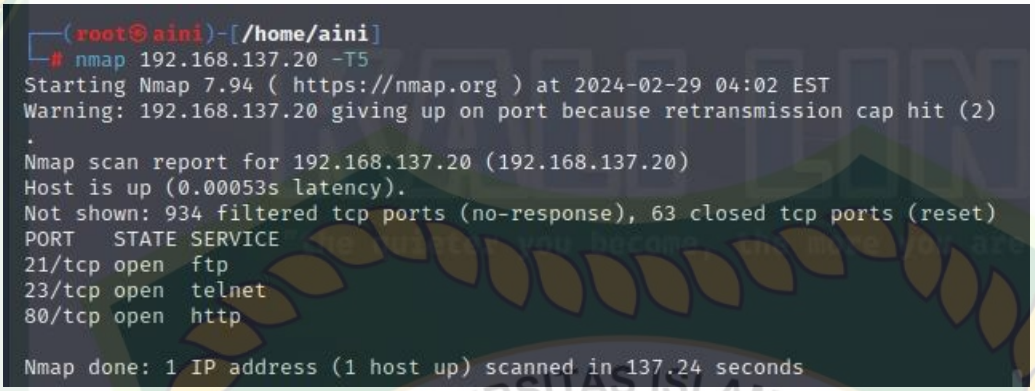
Gambar 4.14 ICMP snort

Komputer yang sudah terpasang oleh snort dapat mendeteksi adanya serangan ping untuk mengetahui snort sudah terkoneksi atau tidak dengan hasil reply dari 192.168.10.44. Selanjutnya setelah snort mendeteksi adanya serangan jaringan maka snort akan mengirimkan peringatan kepada admin melalui aplikasi telegram yang dapat dilihat pada gambar dibawah ini.

Gambar 4.15 Notifikasi Serangan ping dari Telegram

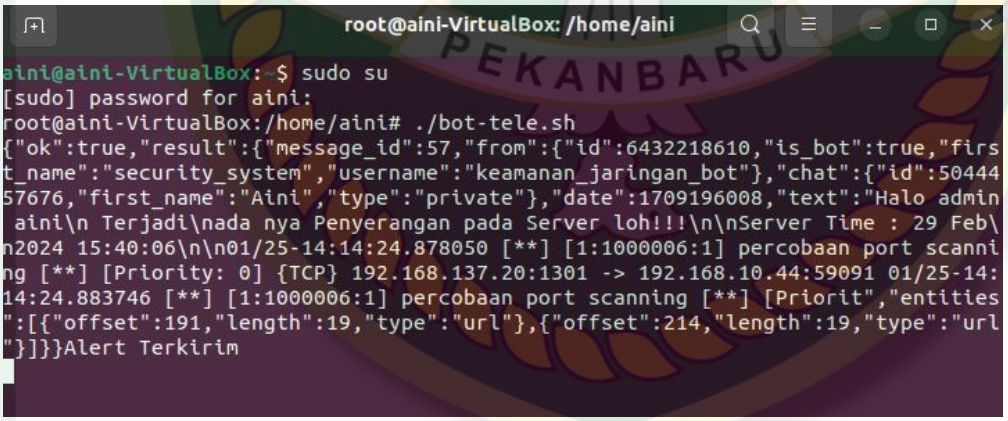
4.2.2 Nmap (*PortScanning*)

Komputer yang sudah terpasang oleh snort selanjutnya akan dicoba untuk melakukan metode penyerangan *nmap* yaitu merupakan serangan *port scanning* dari komputer penyerang. Pada gambar 4.16 dibawah ini dilakukan pengujian ke snort yang dimana apakah snort dapat membaca serangan *nmap*.



Gambar 4.16 *Port Scanning* ke IP client

Pada gambar 4.16 diatas setelah melakukan *port scanning* ke jaringan client maka jaringan client tersebut memiliki 3 port yang terbuka diantaranya 21 ftp, 23 telnet,80 http yang dimana ini merupakan sebuah celah dimana penyerang dapat masuk kedalam jaringan. Pada gambar 4.17 dibawah ini merupakan tampilan linux ubuntu yang telah terpasang oleh snort yang dimana snort akan mendeteksi adanya serangan atau aktifitas yang mencurigakan didalam jaringan.



Gambar 4.17 Snort Mendeteksi Adanya *Port Scanning*

Selanjutnya setelah snort mendeteksi adanya serangan maka snort akan mengirimkan peringatan telah terjadinya port scanning ketelegram admin. Yang dapat dilihat pada gambar 4.18 dibawah ini.

Gambar 4.18 Tampilan Telegram *Port Scanning*

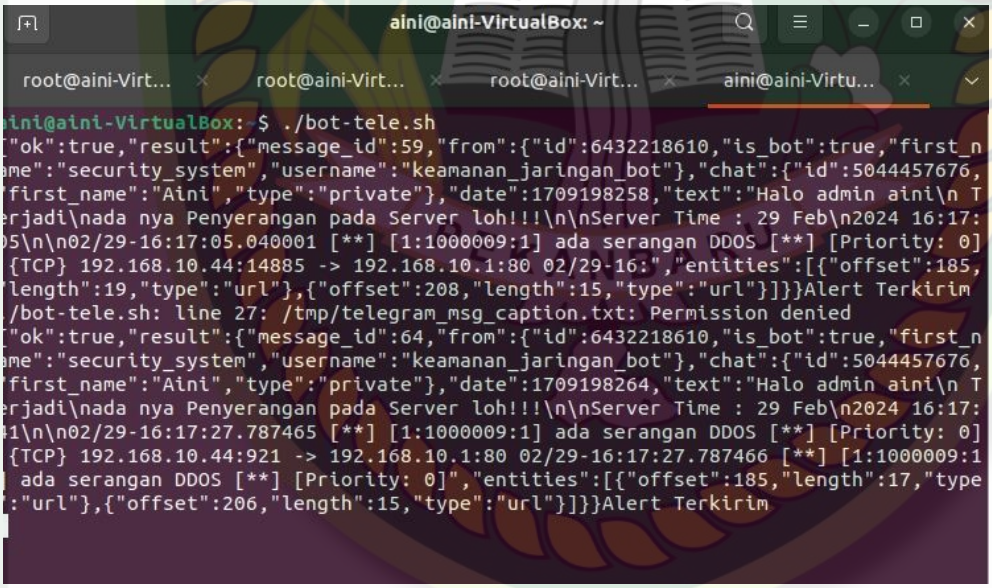
4.2.3 DDOS (Distributed Denial Of Service)

Selanjutnya komputer yang sudah terpasang oleh snort akan dicoba untuk melakukan metode penyerangan DDOS yaitu merupakan serangan yang dimana membanjiri lalu lintas jaringan internet yang terhubung ke server atau jaringan. Berdasarkan dari pengujian *port scanning* diatas, DDOS ini akan membanjiri lalu lintas jaringan berdasarkan port yang terbuka sehingga dalam penelitian ini dilakukan pengujian system keamanan snort yang telah terhubung kedalam jaringan yang dimana meliputi pengujian serangan DDOS dengan metode TCP. Berikut pada gambar 4.19 dibawah ini merupakan penyerangan DDOS yang dilakukan dengan menggunakan kalilinux dan snort dapat mendeteksi adanya serangan DDOS kemudian memberikan alert(peringatan) kepada admin melalui aplikasi telegram.

```
┌──(root㉿aini)-[/home/aini]
└─# hping3 -S 192.168.10.1 --flood -p 80
HPING 192.168.10.1 (eth0 192.168.10.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.10.1 hping statistic ---
588003 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Gambar 4.19 Kalilinux melakukan serangan DDOS dengan metode TCP

Pada gambar 4.19 dapat dilihat penyerangan dengan IP client dilakukan pada port 80 dengan metode TCP. Pada gambar 4.20 dibawah ini merupakan tampilan hasil snort yang mendeteksi adanya serangan jaringan yang dimana jenis serangan ini merupakan serangan TCP dan snort mendeteksi adanya penyerangan kemudian mengirimkan peringatan kepada admin telegram.

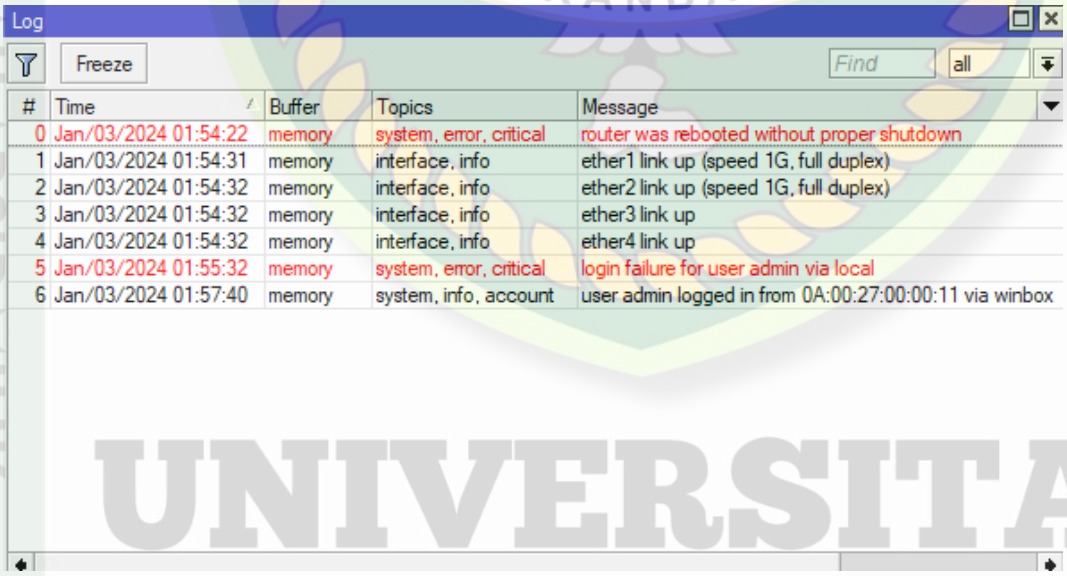


Gambar 4.20 Hasil Serangan DDOS menggunakan TCP

Untuk hasil dari serangan TCP snort akan mengirimkan peringatan ke admin telegram yang dapat dilihat pada gambar 4.21 dibawah ini.

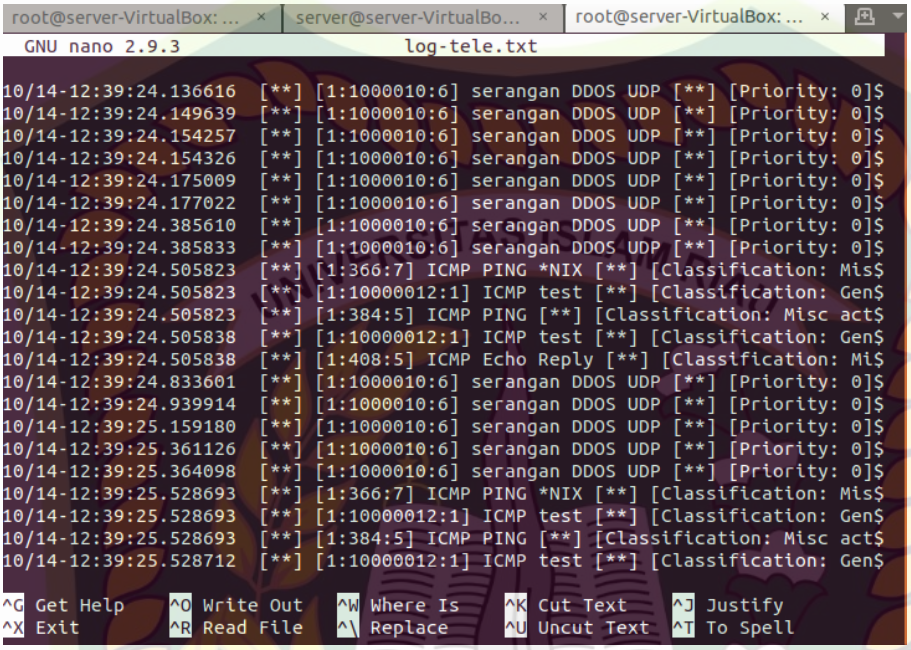
Gambar 4.21 Tampilan Serangan Notifikasi Telegram

Pada gambar 4.22 dibawah ini merupakan tampilan log dari mikrotik yang telah dipasang *port knocking* yang dimana merupakan lapisan keamanan yang memblokir siapa saja yang mencoba masuk ke jaringan.



Gambar 4.22 Tampilan Log yang sudah diterapkan Port Knocking

Pada gambar 4.23 dibawah ini merupakan tampilan log snort yang ada di dalam file log-tele.txt yang dimana berguna untuk dianalisis oleh admin.

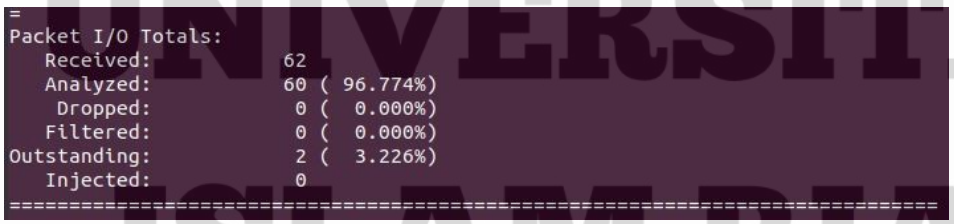


Gambar 4.23 Tampilan log-tele.txt

4.3 Hasil Pengujian

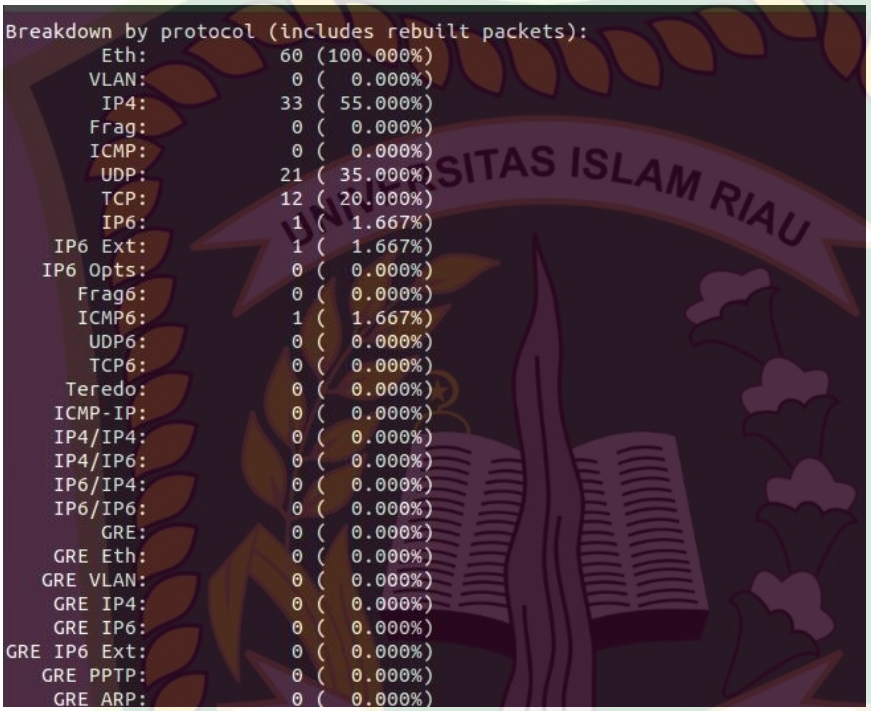
4.3.1 Analisis Snort

Hasil dari pengujian menggunakan snort ini terbukti bahwa snort dapat mendeteksi adanya aktifitas yang tidak wajar didalam jaringan. Dimana pada gambar 4.24 dibawah ini merupakan analisis dari snort terhadap adanya serangan-serangan dan snort menangkap sejumlah serangan dari penyerang ke client selama 15 menit yang dimana snort menerima paket 62 dan snort menganalisis paket serangan sehingga menghasilkan (96.774%) dan paket yang jatuh (0.000%).



Gambar 4.24 Analisis Snort

Selanjutnya yaitu pada gambar 4.25 dibawah ini dapat dilihat analisis dari paket detail snort yang merekam untuk penyerangan yang berada didalam jaringan.



Gambar 4.25 Analisis Detail Packet Snort

Selanjutnya pada gambar 2.26 dibawah ini merupakan hasil total snort sebanyak 60 dengan presentase (96.774%).

Gambar 4.26 Analisis Total Snort

4.3.2 Hasil Penetration Test

Hasil dari penetration test yang dilakukan secara keseluruhan dari waktu pengujian keamanan jaringan LAN (Local Area Network) di KOMINFO Kabupaten Kepulauan Meranti pada tanggal 2 januari 2024 – 01 Maret 2024 dapat dilihat pada table dibawah ini.

Tabel 4.2 Waktu Pengujian

NO	Jenis Serangan	Awal serangan	Waktu Terdeteksi	Terkirim
1	ICMP	15.26.34	15.26.35	15.26.36
2	Port Scanning	07.20.17	07.20.18	07.20.19
3	DDOS	16.17.40	16.17.41	16.17.42

Sehingga hasil penetration test ini berhasil dalam pengujian yang dapat dilihat pada table 4.3 dibawah ini.

Tabel 4.3 Hasil Penetration Test

NO	Jenis Serangan	Hasil Pengujian Sistem	Kesimpulan
1	ICMP	Terdeteksi	Berhasil
2	Port Scanning	Terdetaksi	Berhasil
3	DDOS	Terdeteksi	Berhasil

Dan dapat dilihat pada table 4.3 diatas seluruh pengujian mendapatkan hasil yang sangat sesuai yang diharapkan system tersebut yang dimana dapat mendeteksi adanya serangan yang dilakukan oleh attacker.

BAB V

SIMPULAN DAN SARAN

5.1 Simpulan

Berdasarkan hasil dari pengujian bab IV penulis membuat simpulan sebagai berikut ini.

1. Dari hasil penelitian yang diperoleh peningkatan keamanan router mikrotik dengan menggunakan firewall filtering dan port knocking terbukti efektif dalam mencegah terjadinya serangan port scanning dan DDOS.
2. *Firewall filtering* dan *Port Knocking* terbukti efektif dalam mencegah terjadinya serangan pada mikrotik yang dimana firewall berfungsi untuk menyaring paket data yang masuk kedalam jaringan sedangkan *port knocking* sebagai lapisan keamanan untuk melindungi jaringan.
3. Dalam penerapan telegram sebagai notifikasi system peringatan yang dimana membantu admin apabila terjadinya serangan pada jaringan.

5.2 Saran

Dalam penelitian ini penulis berharap dapat ditingkatkan lagi mulai dari firewall filtering dan port knocking serta snort yang berperan penting sebagai tool pantester serta dapat untuk memperbarui rules secara otomatis dan system IDS ini dapat untuk memblokir serangan secara otomatis. Selanjutnya system IDS ini merupakan metode yang tepat untuk melakukan pendeteksian serangan jaringan. Dan penulis berharap penelitian ini dapat dikembangkan lagi terutama pada peringatan ke aplikasi telegram supaya secara otomatis memberikan peringatan kepada admin.

DAFTAR PUSTAKA

Aji, R. P. (2022). Analisis Log Serangan BruteForce Terhadap Web Server Nginx. *Vol .10 Nomor 27 November 2022, 10*, 56-63.

Amarudin&Faruq. (2018). Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking. *Jurnal TEKNOINFO, Vol. 12, No. 2, 2018, 12*, 72-75.

Asriyanik. (2016). Penilaian Keamanan Sistem Informasi Akademik Universitas Muhammadiyah Sukabumi Dengan Menggunakan ISO 27001. *Volume 6 No 2 Desember 2016, 6*, 501-506.

Desmira&Roni. (2022). Rancang Bangun Keamanan Port Secure Shell(SSH) Menggunakan Metode Port Knocking. *Vol.5 No.1 Maret 2022, 5*, 28-33.

Iqbal & Arini. (2020). Analisa Dan Simulasi Keamanan Jaringan Ubuntu Server Dengan Port Knocking,HoneyPot, Iptables, ICMP. *Vol.3, No. 1, Mei 2020, 3*, 27-32.

Kusuma, G. H. (2022). Sistem Firewall untuk Pencegahan DDOS Attack Di Masa Pandemi Covid-19. *Vol. 3 No.1, Mei 2022, 3*, 52-56.

Mardiyanti. (2014). Mengoptimalkan Suatu Sistem Firewall Pada Jaringan Skala Global. *Vol 7(1): 72-83, 2014, 7*, 72-83.

Mulyanto, A. D. (2020). Pemanfaatn Bot Telegram Untuk Media Informasi Penelitian. *Vol 12, No 1 (2020), 12*, 49-54.

Nugroho. (2023). Studi Performansi Protokol Routing ISIS Pada Arsitektur Jaringan Software Defined Network (SDN). *Vol.10, No.2 April 2023, 10*, 1-11.

Pilendia, D. (2020). *Pemanfaatn Adobe Flash Sebagai Dasar Pengembangan Bahan Ajar Fisika Studi Literatur* (Vol. 2). 2020.

Randi&Ruuhwan. (2020). Impelementasi Keamanan Jaringan Menggunakan Metode Port Blocking Dan Port Knocking Pada Mikrotik RB-941. *Vol. 19, No.1, Juli 2020, pp.1-8, 19*, 1-8.

Ridho, F. &. (2018). Pemanfaatan Telegram Sebagai Notifikasi Serangan untuk Keperluan Forensik Jaringan. *Agrin Vol. 15, No.1,April 2018, 15*, 54-63.

Samsuar & Hadi. (2018). Pengembangan Jaringan Komputer Nirkabel (WiFi) Menggunakan Mikrotik Router. *Vol. 4 No. 1 MARET 2018, 4*, 1-9.

Sharon & Supardi. (2014). Membangun Jaringan Wireless Local Area Network (WLAN). *Vol. 10 No. 1, Februari 2014, 10*, 35-41.

Towidjojo, R. (2013). Perancangan Dan Implementasi Sistem Keamanan Jaringan Menggunakan Firewall Dan Web Proxy Berbasis Mikrotik. *VOL 2. NO.1 JUNI 2018, 2*, 28-32.

Varianto & Badrul. (2015). VOL. 1 NO. 1 FEBRUARI 2015. *Impelementasi Virtual Private Network Dan Sever Menggunakan Clear OS, 1*, 54-65.

Fathoni, W. F. (2016). Deteksi Penyusupan Pada Jaringan Komputer MenggunakanIds Snort. *E-Proceeding of Engineering*, 1169–1172.

Febrison, Y. (Nov 2020). Analisa Dan Perancangan Keamanan Jaringan Lokal Menggunakan Security . *Journal of Information System and Technology*, Vol.01 No.02,37-61.

Harahap, M. H. (2018). Implementasi Snort Intrusion Detection System (IDS) Pada Sistem Jaringan Komputer. *Informatika : Fakultas Sains dan Teknologi*, vol6. No.3.

Akbar, M. (2018). Perancangan Software Ids Snort Untuk Pendeteksian (Netcut) Serangan Interruption Pada Jaringan Wireless. *Jurnal Instek (Informatika Sains Dan Teknologi)*, 121–129.