OPTIMALISASI KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN METODE KNOCKING PORT BERBASIS MIKROTIK (Studi Kasus: CV. Mitra Indexindo Pratama)

Abdul Jamalul'ain, Odi Nurdiawan, Martanto
Program Studi Teknik Informatika, STMIK IKMI Cirebon
abdul14jamal@gmail.com

ABSTRAK

Di zaman modern sekarang ini perkembangan Teknologi Informasi (TI) sangat pesat, dibuktikan dengan semakin canggihnya dunia Teknologi Informasi dari waktu ke waktu yang memberikan kemudahan bagi manusia dalam berkomunikasi. Jaringan komputer digunakan hampir oleh semua orang tanpa terkecuali termasuk para craker. Penelitian ini bertujuan, bagaimana meningkatkan keamanan jaringan komputer dan mengurangi serangan dari craker. Penelitian ini menggunakan metode port knocking, dimana port ini merupakan suatu sistem keamanan yang bertujuan memfilter akses ke port yang digunakan menggunakan firewall pada perangkat jaringan menjadi alternatif dalam mengamankan server. Penggunaan metode port knocking dalam instalasi firewall sangat mudah digunakan, sehingga proses membuka dan menjalankan firewall pada mikrotik cukup stabil dan tidak memakan resource yang banyak. Hasil pengujian hipotesis penelitian tes awal dan tes akhir di peroleh nilai thitung = 4.714 dan nilai ttabel =0,3550. Maka thitung > ttable. Dengan demikian dapat disimpulkan bahwa Ha diterima dan Ho ditolak. Metode knocking port berbasis mikrotik dapat mengoptimalkan keamanan jaringan computer (Ha diterima).

Kata kunci: *Mikrotik, Port knocking, Telnet, SSH*

1. PENDAHULUAN

Pada zaman modern seperti sekarang ini, perkembangan Teknologi Informasi (TI) sangat pesat, dibuktikan dengan semakin canggihnya dunia Teknologi Informasi dari waktu ke waktu. Dengan semakin canggihnya Teknologi Informasi saat ini memberikan kemudahan pada manusia dalam berkomunikasi. Jaringan komputer digunakan hampir semua orang semua orang tanpa terkecuali para *craker*. Adanya maksud dan tujuan tertentu *cracker* melakukan penyusupan melalui port-port yang terdapat pada jaringan sehingga dapat merugikan pemilik server dan jaringan komputer. Banyak organisasi menggunakan jaringan komputer untuk saling bertukar informasi dalam bentuk data, suara, video, dan masih banyak lagi. Sehingga menjadi kebutuhan yang sangat penting dalam mendukung kegiatan organsisasi, baik yang berupah organisasi individual, komersil, perguruan tinggi maupun pemerintahan. Dengan demikian yang harus diperhatikan oleh para pengelola jaringan ialah meningkatkan keamanan pada jaringan supaya celah-celah yang terdapat pada jaringan tidak dapat disisipi maupun dilihat oleh orang yang tidak bertanggung jawab.

Banyak serangan sering dilakukan pada suatu *port-port* yang dalam keadaan terbuka. Seperti halnya virus *Wannacry ransomware,* yang menyerang data di komputer melalui port yang terbuka. Pengamanan pada port komputer nantinya akan membuart serangan pada komputer tidak mempunyai hak akses maupun yang tidak berkepentingan dapat dengan mudahmengendalikan *port-port* yang telah ia masuki. Maka untuk melakukan keamanan pada jaringan komputer dalam mengatasi serangan pada *port-port* dan memaksakan kebutuhan untuk mengembangkan teknik komunikasi baru dan tersembunyi untuk melindungi data sensitif yang ditransfer melalui internet [1].

Berdasarkan penlitian terdahulu yang dibuat oleh Muhamad Ryansyah, Muhammad Sony Maulana, Vol. 6, No.3, Juli 2018 yang berjudul "Malware Security Menggunakan *Filtering Firewall* dengan Metode *Port Block*ing pada Mikrotik RB 1100AHx2" Salah satu dampak adanya malware dalam jaringan kampus adalah *overload traffic bandwidth*, sehingga menyebabkan kendala bandwidth yang cepat habis atau lalu lintas transfer data baik yang masuk maupun yang keluar menjadi lambat dari biasanya. Umumnya sebuah kampus atau universitas memiliki struktur jaringan yang didalamnya dikelola oleh satu atau lebih router di dalam mengelola jaringan dan bandwidth. Beberapa router memiliki kemampuan pengaturan *firewall* yang sudah cukum mumpuni namun perlu dikelola lebih spsesifik berdasarkan kebutuhan skala jaringan dan bandwidth yang tersedia. Dengan menciptakan *rule-rule* yang baik di dalam *firewall* akan lebih mudah dalam melakukan *filtering* terhadap lalu lintas trafik jaringan dan bandwidth sehingga dapat menciptakan keamanan dan kenyamanan pengguna jaringan dan *bandwidth*. Hasil penelitian ini menunjukkan kinerja dari mikrotik router board RB 1100 AHx2 yang dapat memfilter aktivitas malware dengan rule yang telah ditanamkan jaringan menjadi lebih aman, cepat dan stabil dan *adminnistrator* dapat mengetahui port yang harus dibuka atau ditutup untuk menutup akses *malware* pada jaringan [2].

Berdasarkan penelitian terdahulu yang dibuat oleh Efrahim Sinyo Rio Ola Balen Langobelen, Rr. Yuliana Rachmawati, Catur Iswahyudi, Vol. 7 No. 2 Desember 2019 yang berjudul "Analisis Dan Optimasi Dari Simulasi Keamanan Jaringan Menggunakan *Firewall* Mikrotik Studi Kasus di Taman Pintar Yogyakarta" Penerapan konsep *firewall* terlihat cukup sederhana yaitu bila ada *traffic* yang datang dan menuju suatu jaringan, *firewall* kemudian akan melakukan pemeriksaan serta control terhadap *traffic* tersebut kemudian dikirimkan ke tujuannya. Kemanan jaringan yang ada di Taman Pintar Yogyakarta masih membutuhkan pengembangan agar terbaharui dengan perkembangan teknologi dan mampu meminimalisir segala bentuk serangan yang mungkin bisa masuk ke dalam sistem jaringan. Menyikapi keamanan tersebut dipandang perlu untuk menerapkan kebijakan teknis yang digunakan untuk mengelola user, yakni mencegah akses yang tidak perlu yang nantinya dapat membebani jaringan. Metodologi yang digunakan dalam penelitian ini menggunakan konsep *Prepare Plan Design Implement Operate and Optimize* (PPDIOO) yaitu metologi *Life Cycle* yang secara berkesinambungan terus dilakukan dalam proses pengembangan dan implementasi jaringan. Metode ini sangat cocok digunakan dalam pengembangan sistem keamanan jaringan karena keamanan jaringan setiap saat terus berkembang seiring dengan cepatnya perkembangan teknologi. Secara umum penelitian ini menghasilkan konfigurasi untuk sistem keamanan jaringan komputer. Taman Pintar Yogyakarta mengunakan *firewall* router Mikrotik yang meliputi konfigurasi untuk *firewall*, pengelolaan *service port* serta konfigurasi *Filter* untuk *Bridge*. Penelitian ini menerapkan empat konfigurasi *firewall* yang difungsikan untuk memblokir aktivitas pengguna atau serangan dari luar yang dapat membahayakan sistem keamanan jaringan. Konfigurasi tersebut yaitu blokir penggunaan aplikasi geratis VPN, blokir penggunaan aplikasi torrent, blokir seragan *DDOS* serta melakukan penyamaran untuk *scaning port* menggunakan NMAP [3].

Berdasarkan penlitian terdahulu Putu Riska, Putu Sugiartawan, Ichsan Wiratama, Vol.1, No.2, December 2018, pp. 53~64 yang berjudul "Sistem Keamanan Jaringan Komputer dan Data Dengan Menggunakan Metode *Port Knocking*" Seiring dengan perkembangan teknologi Informasi saat ini yang selalu berubah, menjadikan keamanan suatu informasi sangatlah penting. Banyak serangan yang dilakukanoleh orang-orang yang tidak bertanggung jawab melakukan serangan terhadap server. Seranganserangan tersebut sering dilakukan pada suatu *port–port* yang dalam keadaan terbuka, sehingga nantinya akan membuat orang–orang yang tidak mempunyai hak akses maupun yang tidak berkepentingan dapat dengan mudah mengendalikan port–port yang telah dimasuki. Maka untuk melakukan keamanan pada jaringan computer dalam mengatasi serangan pada *port-port*, salah satunya adalah dengan menggunakan metode *Port knoking*. Untuk menghindari serangan yang dilakukan dalam keadaan port terbuka maka digunakan suatu metode *port knoking* dan mengatur parameter-parameter agar perangkat komputer ini tidak memiliki port komunikasi yang terbuka bebas untuk dimasuki, tetapi perangkat ini masih tetap dapat diakses dari luar. Sehinggaakanmembuat orang yang tidak memiliki hak akses tidak memiliki kesempatan untuk memasuki *port-port* yang ada [4].

Berdasarkan penlitian terdahulu Frengky Novrian, Catur Iswahyudi, Prita Haryani, Vol. 7 No. 2 Desember 2019 yang berjudul "Perancangan Jaringan Komputer Lokal Menggunakan Model Hierarki di Kampus 1 Institut Teknologi Yogyakarta", Konsep jaringan internet yang terpasang pada kampus Institut Teknologi Yogyakarta belum memiliki interkoneksi antara kampus 1, 2, 3 dan 4 dan jaringan komputer lokal yang belum memenuhi kebutuhan kampus. Tentunya hal itu tidak baik dan dapat mempengaruhi kinerja kampus. Terhubungnya antar kampus 1, 2, 3 dan 4 dan perancangan jaringan komputer lokal diharapkan dapat meningkatkan kecepatan kinerja dalam bertukar dan mengirim data didalam kampus 1 dan antar kampus dan meningkatkan kinerja operasional kampus Institut Teknologi Yogyakarta. Sistem yang dibangun adalah perancangan jaringan komputer lokal menggunakan model hierarki. Penyusunan meliputi dengan prosedur antara identifikasi masalah, analisis data, perancangan interkoneksi, perancangan arsitektur jaringan, perancangan logical dan perancangan topologi fisik Sistem yang dibangun adalah perancangan jaringan komputer lokal menggunakan model hierarki. Penyusunan meliputi dengan prosedur antara identifikasi masalah, analisis data, perancangan interkoneksi, perancangan arsitektur jaringan, perancangan logical dan perancangan topologi fisik [5].

Beberapa fitur-fitur yang dapat digunakan pada Mikrotik, seperti pada tabel di bawah ini:

Tabel 1. Fitur - Fitur Mikrotik

No	NAMA FITUR	KETERANGAN
1	Address List	Pengelompokan IP Address berdasarkan nama
2	Asynchronous	Mendukung serial PPP dial-in / dial-out, dengan otentikasi CHAP, PAP,MSCHAPv1 dan MSCHAPv2, Radius, dial on demand, modem pool hingga 128 ports.
3	BONDING	Mendukung dalam pengkombinasian beberapa antarmuka ethernet kedalam 1 pipa pada koneksi cepat.
4	BRIDGE	Mendukung fungsi bridge spinning tree, multiple bridge interface, bridging firewalling.
5	Data Rate Management	QoS berbasis HTB dengan penggunaan burst, PCQ, RED, SFQ, FIFO queue, CIR, MIR, limit antar peer to peer.

No	NAMA FITUR	KETERANGAN
6	DHCP	Mendukung DHCP tiap antarmuka; DHCP Relay,DHCP Client, multiple
7	Firewall dan NAT	Mendukung pemfilteran koneksi peer to peer, source NAT dan destination NAT. Mampu memfilter berdasarkan MAC, IP address, range port, protokol IP, pemilihan opsi protokol seperti ICMP, TCP Flags dan MSS.
8	Hotspot	Hotspot gateway dengan otentikasi RADIUS. Mendukung limit data rate,SSL ,HTTPS.
9	IPSec	Protokol AH dan ESP untuk IPSec; MODP Diffie-Hellmann groups 1, 2, 5, MD5 dan algoritma SHA1 hashing; algoritma enkirpsi menggunakan DES, 3DES, AES-128, AES-192, AES-256; Perfect Forwarding Secresy (PFS) MODP groups 1, 2,5.
10	ISDN	Mendukung ISDN dial-in/dial-out. Dengan otentikasi PAP, CHAP, MSCHAPv1 dan SCHAPv2, Radius. Mendukung 128K bundle, Cisco, HDLC, x751,x75ui, x75bui line protokol.
11	Routing	Routing statik dan dinamik; RIP v1/v2, OSPF v2, BGP v4.
12	Simple Tunnel	Tunnel IPIP dan EoIP (Ethernet over IP).

Penelitian dibuat untuk melindungi jaringan computer dari segala bentuk ancaman yang akan datang baik langsung maupun tidak langsung yang mengganggu kegiatan yang sedang beroperasi. Dalam rangka melindungi kemungkinan serangan-serangan tersebut perlu di terapkan konsep *firewall*. Dimana *firewall* dirancang untuk mencegah akses yang tidak diinginkan yang datang baik dari internal maupun *external* jaringan. Penerapan konsep *firewall* terlihat cukup sederhana yaitu bila ada *traffic* yang datang dan menuju suatu jaringan, *firewall* kemudian akan melakukan pemeriksaan serta control terhadap traffic tersebut kemudian dikirimkan ke tujuannya.

Kemanan jaringan yang ada di CV. Mitra Indexindo Pratama masih membutuhkan pengembangan agar terbaharui dengan perkembangan teknologi dan mampu meminimalisir segala bentuk serangan yang mungkin bisa masuk ke dalam sistem jaringan. Menyikapi keamanan tersebut dipandang perlu untuk menerapkan kebijakan teknis yang digunakan untuk mengelola user, yakni mencegah akses yang tidak perlu yang nantinya dapat membebani jaringan.

Dengana alasan yang telah diuraikan, penulis mengambil penelitian ini dengan judul "Optimalisasi Keamanan Jaringan Komputer Menggunakan Metode *Knocking Port* Berbasis Mikrotik (Studi Kasus: CV. Mitra Indexindo Prtama)" MikroTik router adalah salah satu sistem operasi yang dapat digunakan sebagai router jaringan yang handal, mencakup berbagai fitur lengkap untuk jaringan dan wireless. Selain itu MikroTik dapat juga berfungsi sebagai firewall. akan dibahas bagaimana merancang sistem keaman jaringan komputer dengan menerapkan konsep *firewall* berbasis Miktorik dengan tujuan dapat mengurangi resiko ancaman yang akan mengganggu aktifitas yang yang sedang berlangsung, disesuaikan dengan kondisi di CV. Mitra Indexindo Pratama.

2. TINJAUAN PUSTAKA

Menurut Heri Gunawan, 2019 jurnal yang berjudul "Ancaman Keamanan Jaringan Pada Server Untuk Membatasi Website Tertentu Menggunakan Mikrotik" membahas Mikrotik RouterOs™ adalah sistem operasi dan perangakat lunak yang dapat di gunakan untuk menjadikan komputer menjadi router network yang handal. Didesain untuk memberikan kemudahan bagi penggunanya administrasinya bisa dilakukan melalui *Windows application* (Winbox). Internet banyak memberikan konten yang bermanfaat apabila penggunanya menggunakan internet secara baik, disamping itu internet juga dapat memberikan dampak negatif bagi penggunanya apabila internet di gunakan untuk hal yang negatif yang akan berdampak pada generasi muda yang akan merangkul negeri ini untuk menjadi penerus bangsa ini digunakan diluar norma yang berlaku. Saat ini internet sudah banyak beragam jenis situs jejaring sosial yang telah digunakan oleh banyak orang, tujuannya atau Salah satu solusinya yaitu agar pengguna internet tidak mengakses yang berdampak negatif atau merugikan dirinya sendiri,menggunakan metode *Scientific of Inquiry* dengan membatasi akses terhadap website-website tertentu untuk upaya pencegahan dalam mengakses situs internet yang berbau negatif dalam hal ini mengandung konten pornografi adalah dengan memblokir situs-situs negatif tersebut secara permanen menggunakan web proxy yang berfungsi untuk memblokir beberapa website yang tidak boleh di akses oleh klien melalui browser pada router Mikrotik Fakultas teknik Universitas Ibn khaldun [6].

Menurut Julianto, Suwanto Raharjo, Catur Iswahyudi, Vol. 09 No. 01 Juni 2021 jurnal yang berjudul "Analisis Keamanan Jaringan Mikrotik ISP Indonesia Menggunakan *Search Engine Scada Shodan* Dengan Metode *Exploit Winbox Critical Vulnerability*" Mikrotik sudah sangat familiar bagi pengguna internet di Indonesia sebagai sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer biasa menjadi router network. Disamping itu masalah yang sering terjadi pada router mikrotik terhadap sisi pengguna tidak meningkatkan versi mikrotik yang memiliki celah kerentanan mikrotik v6.42-v6.28 sehingga mudah diexploit. Penelitian ini bertujuan untuk menganalisis sistem keamanan akses router mikrotik serta melakukan cara mitigasi atau pencegahan dan solusi keamanan dari serangan *Exploit*. Metode yang digunakan dalam penelitian ini menggunakan metode eksperimen, studi pustaka dan simulasi. Dalam melakukan ujicoba, penelitian ini menggunakan teknik *Exploit* winbox critical vulnerability terhadap perangkat mikrotik yang diketahui masih memiliki celah keamanan dengan memanfaatkan search engine

scada shodan sebagai pencari Ip publik dari mikrotik. Hasil dari penelitian yang dilakukan yaitu menyimpulkan dan memberikan solusi bagaimana cara menanggulangi dan mencegah kembali serangan terhadap masalah keamanan akses router mikrotik dari serangan exploit dalam hal ini bisa menjadi bahan pertimbangan bagi IT *security* instansi atau perusahaan untuk mengamankan router mikrotik dari serangan exploit [7].

Menurut Andik Saputro, Nanang Saputro, Hendro Wijayanto, Vol. 3, No. 2, November 2020, hlm. 22-27, jurnal yang berjudul "Metode *Demilitarized Zone dan Port Knocking* Untuk Keamanan Jaringan Komputer" Saat ini cara komunikasi jaringan sudah banyak berubah. Seluruh aspek menjadi sangat bergantung pada layanan online. Karyawan dapat bekerja dari rumah, dan siswa dari segala usia mengambil kelas secara online. Semakin publik bergantung untuk tetap terhubung dengan jaringan, semakin besar potensi serangan jaringan yang terjadi. Dalam jaringan komputer jika tidak dilindungi akan menyebabkan kerugian berupa kehilangan data atau file, kerusakan system server, tidak maksimal dalam melayani user atau bahkan kehilangan aset berharga institusi. Serangan yang paling sering digunakan dalam jaringan adalah Port Scanning dan DDoS (*Distributed Denial of Service*). Dalam penelitian ini menggabungkan metode DeMilitarized Zone dan Port Knocking untuk mengamankan jaringan komputer. Implemetasi teknik *DeMilitarized Zone* digunakan untuk mengakses server lokal agar bisa diakses dari luar dengan teknik *Port Knocking*. *Port Knocking* juga dapat diimplementasikan pada jaringan lokal maupun interlokal dengan dipadukan time limit ping request yang menjadikan lebih aman, sehingga jika penyerang ingin mengakses router, dan tidak mengetahui aturan dari remote maka yang terjadi adalah penolakan terhadap akses port tersebut [8].

Menurut Sumardi Jayanto, Ahmad Tantoni, Hasyim Asyari VOL. 1 NO. 2 tahun 2021 jurnal yang berjudul "Implementasi Keamanan Jaringan dengan *Packet Filtering* Berbasis Mikrotik Untuk Internet Positif Di SMKN 1 Praya" SMKN 1 Praya adalah salah satu sekolah di NTB yang berstandar nasional. Sekolah ini memiliki lingkungan yang sangat luas Di SMKN 1 Praya yang menjadi masalah utamanya adalah pemakaian data jaringan internet oleh siswa digunakan untuk bermain games dan media sosial pada saat jam belajar sehingga dibutuhkan sebuah sistem yang mampu menjadi proteksi agar user tidak dapat menggunakan internet untuk bermain games dan sosial media pada saat jam belajar. Berdasarkan hal tersebut maka penelitian ini bertujuan untuk menguji implementasi kemanan jaringan dengan *packet filtering* berbasis mikrotik pada SMKN 1 Praya. Secara umum penelitian ini menunjukkan keberhasilan pemblokiran terhadap beberapa aplikasi games online seperti mobile legend, free fire, TOT dan sosial media seperti facebook [9].

Menurut Lutvi Riyandari, Tri Wahyuningsih, dan Joko Purnomo, jurnal yang berjudul "Rancang Bangun Jaringan Internet Dengan Memperhatikan Etika Profesi TI Menggunakan Web *Filtering* Pada Router Mikrotik 951g-2hnd" Dengan tingkat permintaan yang lebih tinggi dan meningkatnya jumlah pengguna jaringan menginginkan bentuk jaringan yang dapat memberikan hasil yang maksimal baik dari segi efisiensi dan peningkatan keamanan network itu sendiri. Penelitian yang dilakukan di SMK di Banyumas, dalam penelitian ini metode yang digunakan untuk membangun jaringan komputer menggunakan *Network Development* Model siklus hidup (NDLC). Apakah desain jaringan internet menyanyikan Router Mikrotik 951G-2HnD sebagai *web filtering* di SMK di Banyumas kinerjanya mengacu pada atribut Dimensi Kualitas barang? Setelah jaringan dibangun dan diimplementasikan, peneliti menguji sistem dengan dua tes: uji produk dan uji manfaat, mengambil sampel responden untuk uji produk yaitu 5 ahli jaringan komputer dan 40 dari pengguna internet di Sekolah Menengah Kejuruan untuk tes manfaat. Setelah tes statistik yang sukses dengan skor di atas nilai uji produk ditentukan yaitu 75% dan hasilnya adalah 86,66%. Skor uji manfaat juga di atas skor tes manfaat yang telah ditentukan dari 75% dan hasil tes enefit adalah 99,37% [10].

Menurut Suryanto, VOL. 3. NO. 2 FEBRUARI 2018 jurnal yang berjudul "Pengaturan Pemakaian Bandwidth dan Akses Jaringan Komputer Menggunakan Mikrotik Router" Jaringan komputer sudah menjadi kebutuhan bagi perusahaan atau organisasi era digital saat ini, namun penggunaannya harus diatur agar dapat menunjang kinerja perusahaan. Adanya ancaman keamanan dan penyalagunaan jaringan yang bukan untuk kepentingan kerja kerap menjadi persoalan yang dihadapi oleh perusahaan, untuk itu dibutuhkan suatu metode untuk mengatur agar pemanfaatan dan penggunaan jaringan sesuai dengan peruntukannya. Teknik pengaturan aksesdan pengaturan pemakaian *bandwith* dengan menggunakan aturan (r*ule*) yang sudah ditentukan perusahaan menjadi solusi yang bisa diambil untuk mengatasi permasalahan yang dihadapi. Aturan tersebut dapat diterapkanpadarouter mikrotikdi jaringan dengan menggunakan IPTABLES dan aturan tersebut dapat ditujukan pada sebuah *IP address*, protokol, ataupun content, agar jaringan tersebut diperbolehkan atau tidak untuk diakses. Metode yang digunakan pada penelitian ini adalah metode *experimental* yang merancang, membuat dan menguji pengaturan pemakaian *bandwidth* dan pembatasan akses pada suatu jaringan. Dari hasil penelitian ini menunjukan bahwa pengaturan pemakaian bandwidth dan pembatasan akses pada jaringan komputer dapat berjalan dengan baik dan aturan dalam penggunaan sumber daya jaringan bisa dijalankan [11].

3. METODOLOGI

3.1. Jenis Penelitian

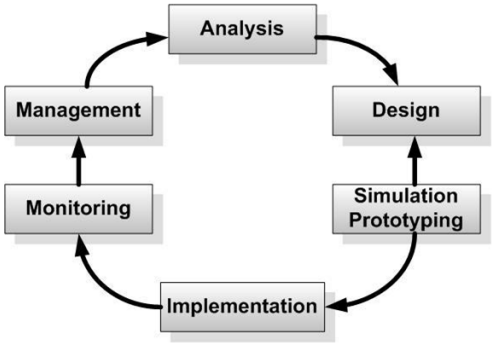
Jenis penelitian yang digunakan pada penelitian ini adalah metode analisis kualitatif dan metode survey. Metode analisis kualitatif adalah metode penelitian yang digunakan untuk melihat sistem yang ada pada objek penelitian yang akan diteliti, dengan berdasarkan analisis yang difokuskan pada fungsi kualitas dari sistem yang ada pada lokasi penelitian.

Penelitian ini menggunakan metode penelitian survey. Penelitian survey adalah penelitian yang dilakukan pada populasi besar maupun kecil, tetapi data yang dipelajari adalah dari sampel yang diambil dari populasi tersebut, sehingga ditemukan kejadian-kejadian relative, distribusi, dan hubungan-hubungan antar variabel sisiologis, maupun psikologis.

Pada penelitian ini penulis melakukan analisis pada sistem jaringan komputer dengan menggunakan metode *port knocking*. Selain analisis kualitatif, proses penelitian akan dilakukan dengan metode studi kasus dimana pada proses ini, penulis mengumpulkan data-data yang telah didapatkan pada saat proses penelitian di lakukan di lokasi, kemudian memberikan kesimpulan tentang hasil dari penelitian yang dilakukan, dimana pada penelitian ini hasil yang ingin dicapai adalah apakah sistem jaringan di lokasi penelitian aman melalui port jaringan.

3.2. Tahap Penelitian

Peneliti Menggunakan Tahapan pada *Network Development Life Cycle (NDLC)*



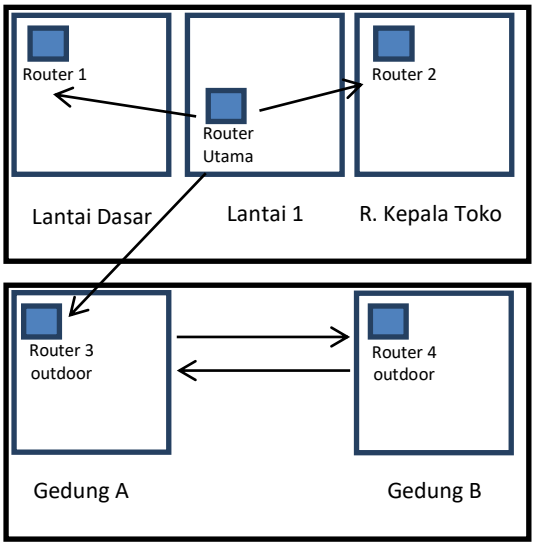
Gambar 2. *Network Development Life Cycle (NDLC)*

Berikut ini adalah tahapan penilitan yang dilakukan sebagai berikut:

1. Analisis
   Pada tahap ini dilakukan beberapa analisa kebutuhan, analisa masalah yang muncul, keinginan user, dan analisa topologi. Ada beberapa metode yang digunakan antara lain:
   a. Survey Lapangan.
   b. Wawancara kepada pihak terkait.
   c. Membaca dokumentasi dari pengembang sebelumnya.
   d. Menelaah setiap data data diperoleh sebelumnya.
2. Design
   Dari data yang telah didapatkan, tahap selanjutnya membuat desain jaringan atau topologi dari jaringan yang akan dibangun, seperti kebutuhan hardware, software dan estimasi biaya yang diperlukan.
3. Simulation Prototyping
   Pada tahap ini, dilakukan simulasi atau gambaran terhadap topologi yang telah dirancang menggunakan GN3 atau Visio untuk melihat gambaran implementasi dari topologi yang akan dibuat.
4. Implementation
   Dalam tahap implementasi, dilakukan penerapan topologi yang telah dibuat di lapangan.
5. Monitoring
   Setelah melakukan implentasi jaringan, maka perlu dilakukan monitoring jaringan agar jaringan terpasang dengan baik dan sesuai tidak dengan kebutuhan user.
6. Management
   Pada tahap manajemen, perlu adanya kebijakan – kebijakan untuk mengatur sistem yang telah dibangun agar dapat berjalan dengan baik dan semestinya.

3.3. Analisis Keadaan jaringan

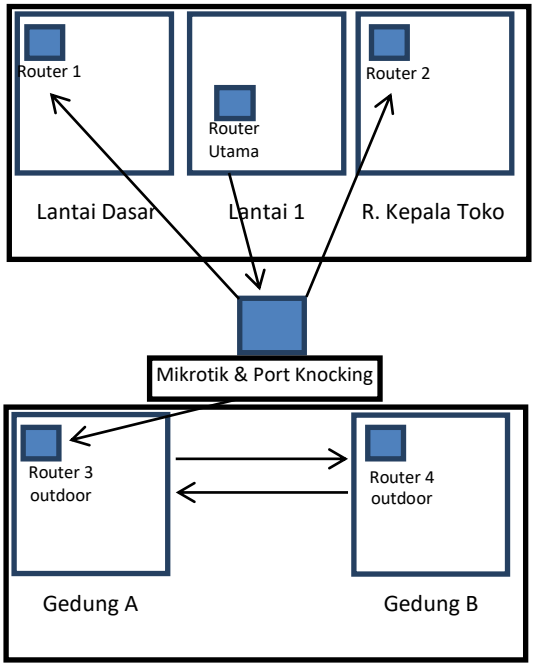
Secara umum, sebuah jaringan pada instansi seperti intansi toko hanya menggunakan sistem yang standar, seperti pada lokasi penlitian, dimana sistem jaringan yang digunakan yang berasal dari provider, kemudian digunakan sebagai media jaringan internet melalui perantara modem, dengan menambahkan perangkat jaringan berupa modem, sebagai alat untuk konfigurasi tambahan pada jaringan tanpa kabel (*wireles*) dalam proses berbagai data maupun melakukan pencarian informasi. Penggunaan jarinngan yang intenss digunakan pada ruangan kepala toko, kemudian ruangan service, dan toko terdekat sebagai gambar



Gambar 3. Topologi awal

3.4. Desain

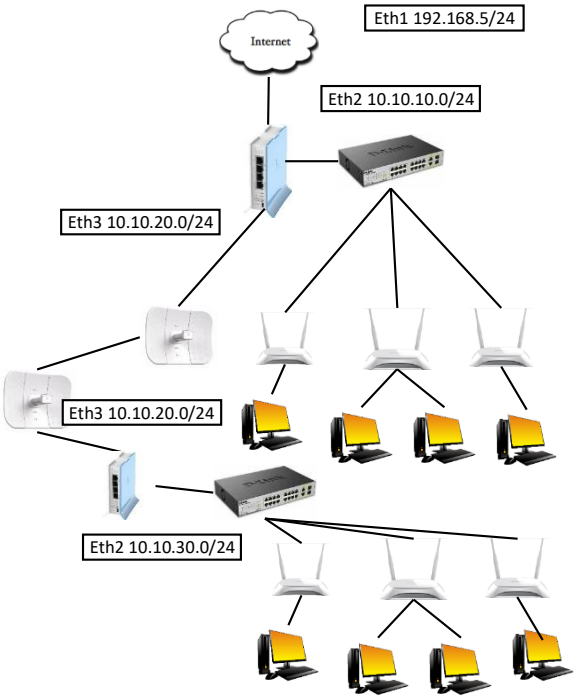
Untuk desain perancangan jaringan yang akan dibuat berdasarkan denah toko pada gambar sebelumnya, berikut adalah desain jaringan CV. Mitra Indexindo Pratama. Desain ditujukan untuk melakukan pengamatan terhadap sistem keamanan yang diterapkan oleh instansi terkait, dimana focus desain dilakukan pada perangkat mikrotik sebagai sentral sistem yang berjalan pada jaringan di lokasi penelitian, analisis yang dilakukan berupa hak akses setiap komputer yang terkoneksi ke dalam jaringan, kemudian proses port knocking yang dilakukan peneliti untuk melihat atau meninjau keamanan akses port pada jaringan yang sedang berjalan, dengan menganalisa port yang terbuka di sistem jaringan di lokasi, dapat diketahui apakah jaringan yang ada di lokasi penelitian dapat dikategorikan sebagai jaringan aman atau tidak, sebagaimana pada gambar di bawah ini



Gambar 4. Desain Topologi Jaringan

3.5. Prototype jaringan

Pada tahap simulasi prototype jaringan ini menggunakan software menggunakan Visio. Tujuan menggunakan aplikasi ini adalah sebagai simulasi sehingga dapat dilakukan uji coba tanpa menggunakan hardware yang sedang digunakan. Karena berjalan secara terpisah dengan jaringan yang sudah ada. Berikut merupakan gambaran jaringan di CV. Mitra Indexindo Pratama.

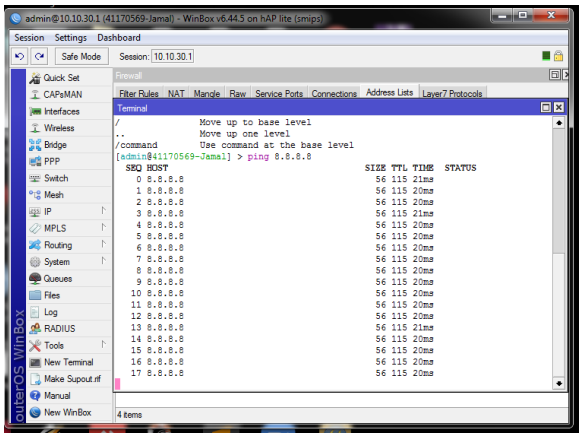


Gambar 5. Prototipe Topologi Jaringan

4. HASIL DAN PEMBAHASAN

4.1. Mikrotik Sebagai Gateway

Setelah dikonfigurasikan mikrotik sebagai gateway, sehingga setiap client dapat terhubung ke internet melewati mikrotik sebagai gateway.

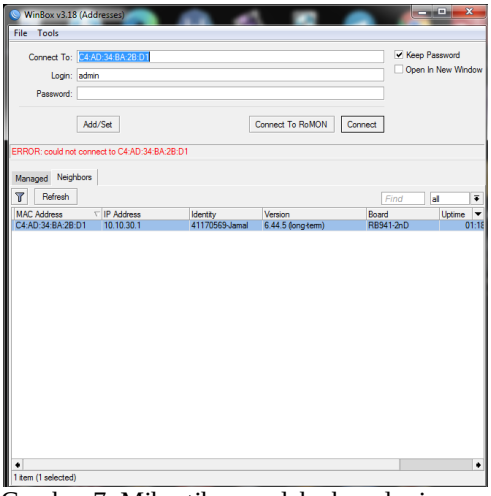


Gambar 6. Ping Server Google via terminal Mikrotik

Ping ke server google berhasil, menandakan jaringan mikrotik telah terhubung ke internet

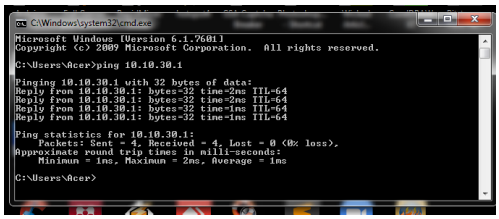
1. Pengujian Sistem
   Pada tahap ini melakukan pengujian sistem yang telah dibuat dengan proses langkah – langkah sebagai berikut:
   a. Melakukan percobaan *login ke winbox*
   b. Lakukan *ping Ip Address Mikrotik*
   c. Melakukan *ping ke Scure Shell* (SSH)
   d. Melakukan *ping ke Telnet*
   e. Jika langkah–langkah telah sesuai dengan rule maka dapat mengakses Mikrotik

2. Hasil Metode *Port Knocking* pada Mikrotik
   a. Melakukan percobaan *Login* ke Winbox tanpa melewati tahap *ping*.
   Hasil Implementasi mencoba mengakses mikrotik melalui winbox tanpa *melakukan* rules yang telah diterapkan, hasilnya mikrotik menolak akses yang diminta.

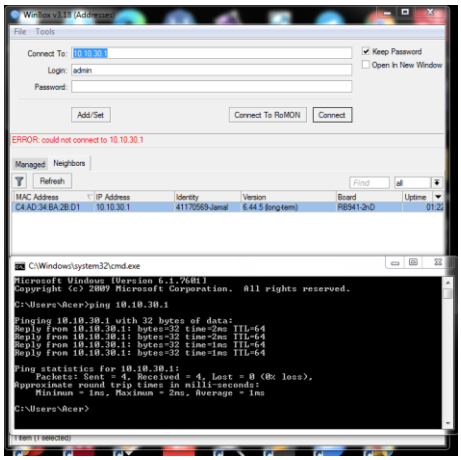


Gambar 7. Mikrotik menolak akses login user

   b. Lakukan ping Ip *Address Mikrotik*
   Melakukan *Ping adress mikrotik* via cmd dan mencoba mengakses mikrotik melalui winbox menggunakan salah satu rules yang telah diterapkan, hasilnya mikrotik menolak akses yang diminta.

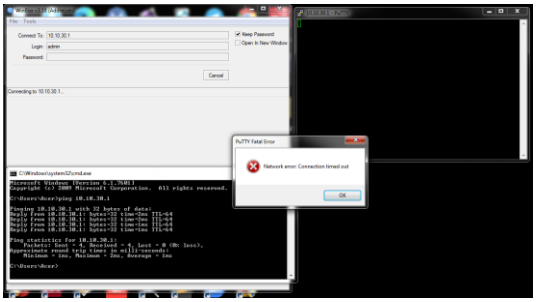


Gambar 8. Mikrotik menolak akses login karena rule tidak lengkap



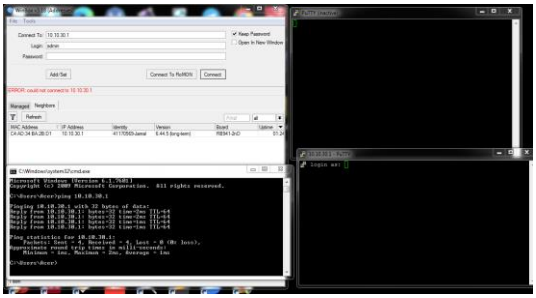
Gambar 9. Mikrotik menolak akses login karena rule tidak lengkap

   c. Melakukan ping adrress mikrotik via putty ke Telnet
   Melakukan Ping adress mikrotik via cmd, putty ke telnet dan mencoba mengakses mikrotik melalui winbox menggunakan dua rules yang telah diterapkan, hasilnya mikrotik menolak akses yang diminta.



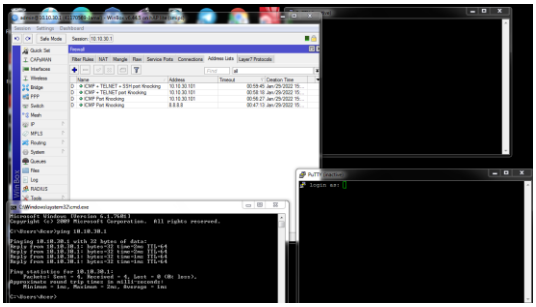
Gambar 10. Mikrotik menolak akses login karena rule tidak lengkap

   d. Melakukan ping adrress mikrotik via putty ke SSH
   Melakukan Ping adress mikrotik via cmd, putty ke telnet, putty ke SSH dan mencoba mengakses mikrotik melalui winbox menggunakan ketiga rules yang telah diterapkan dan sesuai urutan, hasilnya mikrotik menerima akses yang diminta.



Gambar 11. Mikrotik menerima akses login karena rule sudah lengkap

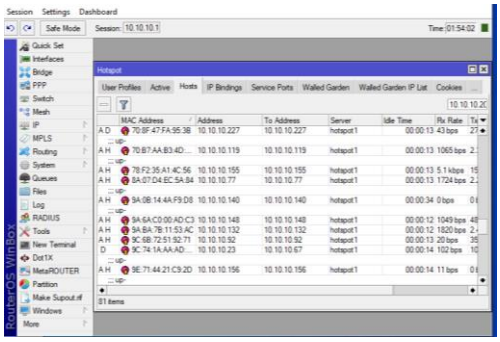
Tampilan rules yang telah dibuat.



Gambar 12. Tampilan hasil port knocking

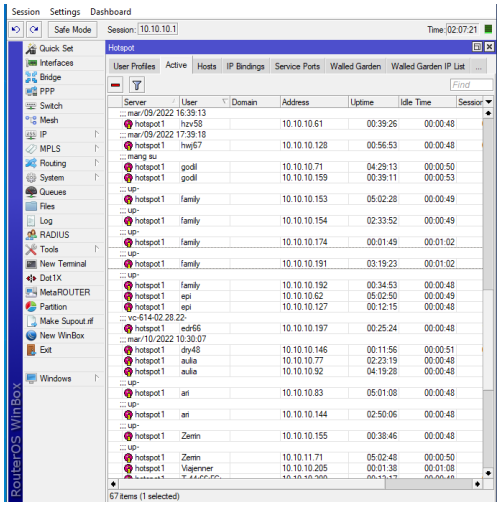
Monitoring

Pada tahap ini dilakukan monitoring apakah jaringan internet berjalan dengan baik atau tidak.

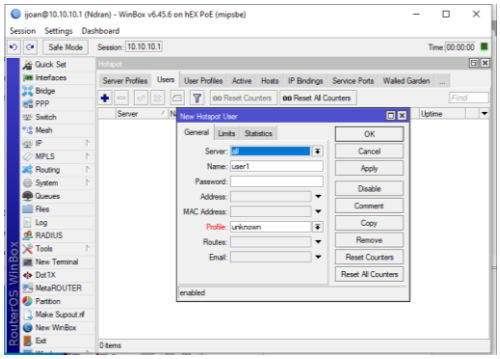


Gambar 13. Host

Host befungsi untuk mengetaui pengguna yang sedang aktif (mendapatkan internet), stanby (terhubung tapi tidak mendapatkan akses internet) belum login dan untuk mengetahui trafik modem/ user yang dibinding.



Gambar 14. User Active

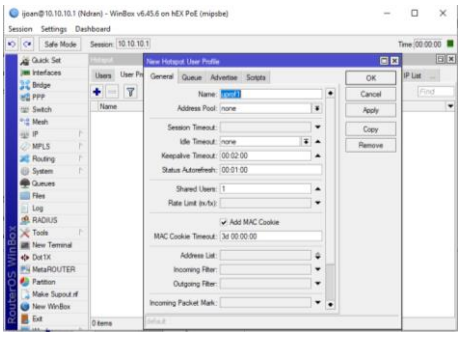


Gambar 15. Pembuatan User

User aktif mengetahui user yang berhasil login di jaringan dan akan menampilkan mac address.
Management.

Pada tahap management ini perlu dilakukan pengaturan user agar internet berjalan dengan baik dan lancar.

Pembuatan user berfungsi untuk membuat user untuk memanage agar orang yang terdaftar yang hanya bias menggunakan jaringan internet dan meminimalisir akses ilegal.



Gambar 16. User Profil

User profil berfungsi sebagai template pengaturan bandwith, akses, dan waktu untuk mengatur user yang dibuat.

4.2. Hasil Pembahasan

Data dalam penelitian ini dikumpulkan melalui metode survei dengan menyebarkan kusioner pada karyawan CV. MITRA INDEXINDO PRATAMA. Kusioner yang digunakan adalah kuesioner yang telah dikembangkan oleh peneliti sebelumnya. Total item pernyataan dalam kusioner sebanyak 16 item pertanyaan, yang terdiri dari 3 item pertanyaan mengenai *Functional Requirements* dan 13 item persyaratan *non fungsional*.

Kusioner disebarkan sebanyak 35 kusioner kepada responden yang merupakan karyawan CV. MITRA INDEXINDO PRATAMA. Penyebaran kuesioner dilakukan secara online oleh peneliti. Peneliti menyebarkan kuesioner dengan cara membuat *Google from* oleh peneliti dan menyebarkan dengan cara mengirim link kepada masing masing karyawan.

4.3. Uji Validitas

Pengujian Validitas dilakukan untuk mengetahui valid tidaknya suatu kuesioner dari masing-masing variabel tersebut. Uji validitas yang telah dilakukan dalam penelitian ini ditampilkan dalam tabel berikut:

Tabel 2. Uji Validitas X

Correlations					
		X1	X2	X3	TOTAL
X1	Pearson Correlation	1	.178	.589**	.801**
	Sig. (2-tailed)		.330	.000	.000
	N	32	32	32	32
X2	Pearson Correlation	.178	1	.296	.639**
	Sig. (2-tailed)	.330		.100	.000
	N	32	32	32	32
X3	Pearson Correlation	.589**	.296	1	.823**
	Sig. (2-tailed)	.000	.100		.000
	N	32	32	32	32
Total X	Pearson Correlation	.801**	.639**	.823**	1
	Sig. (2-tailed)	.000	.000	.000	
	N	32	32	32	32

Tabel 3. Uji Validitas Y

Correlations

		Y1	Y2	Y3	Y4	Y5	Y6	Y7	Y8	Y9	Y10	Y11	Y12	Y13	Total Y
Y1	Pearson Correlation	1	.250	-.082	.102	-.077	.153	.203	.246	-.036	.203	-.081	-.193	.149	.313
	Sig. (2-tailed)		.168	.655	.580	.675	.402	.265	.176	.844	.266	.659	.289	.415	.081
	N	32	32	32	32	32	32	32	32	32	32	32	32	32	32
Y2	Pearson Correlation	.250	1	.254	.346	.099	.310	.079	.633	.462	.468	.104	.097	.451	.713
	Sig. (2-tailed)	.168		.161	.052	.591	.084	.667	.000	.008	.007	.572	.598	.010	.000
	N	32	32	32	32	32	32	32	32	32	32	32	32	32	32
Y3	Pearson Correlation	-.082	.254	1	-.008	.119	.126	-.019	.207	.183	-.222	-.109	.042	-.231	.183
	Sig. (2-tailed)	.655	.161		.964	.516	.492	.919	.256	.316	.222	.554	.820	.204	.317
	N	32	32	32	32	32	32	32	32	32	32	32	32	32	32
Y4	Pearson Correlation	.102	.346	-.008	1	.139	.595**	.252	.157	.665	.484	.465	.208**	.242	.735
	Sig. (2-tailed)	.580	.052	.964		.448	.000	.164	.392	.000	.005	.007	.253	.182	.000
	N	32	32	32	32	32	32	32	32	32	32	32	32	32	32
Y5	Pearson Correlation	-.077	.099	.119	.139	1	.111	.186	.005	.067	-.187	.165	.038	-.039	.298
	Sig. (2-tailed)	.675	.591	.516	.448		.546	.309	.978	.716	.305	.367	.836	.833	.097
	N	32	32	32	32	32	32	32	32	32	32	32	32	32	32
Y6	Pearson Correlation	.153	.310	.126	.595**	.111	1	.534	.382	.432	.194**	.201	.222	.097	.670
	Sig. (2-tailed)	.402	.084	.492	.000	.546		.002	.031	.014	.288	.270	.221	.596	.000
	N	32	32	32	32	32	32	32	32	32	32	32	32	32	32
Y7	Pearson Correlation	.203	.079	-.019	.252	.186	.534**	1	.200	.065	.053	.381	-.116**	.413	.530
	Sig. (2-tailed)	.265	.667	.919	.164	.309	.002		.271	.723	.774	.031	.572	.019	.002
	N	32	32	32	32	32	32	32	32	32	32	32	32	32	32
Y8	Pearson Correlation	.246	.633**	.207	.157	.005	.382*	.200	1**	.212	.131	.092	-.092*	.296	.513**
	Sig. (2-tailed)	.176	.000	.256	.392	.978	.031	.271		.245	.475	.616	.616	.100	.003
	N	32	32	32	32	32	32	32	32	32	32	32	32	32	32
Y9	Pearson Correlation	-.036	.462**	.183	.665**	.067	.432*	.065	.212**	1	.321**	.129	.196*	.007	.577**
	Sig. (2-tailed)	.844	.008	.316	.000	.716	.014	.723	.245		.073	.480	.282	.970	.001
	N	32	32	32	32	32	32	32	32	32	32	32	32	32	32
Y10	Pearson Correlation	.203	.468**	-.222	.484**	-.187	.194	.053	.131**	.321	1**	.402	-.024	.498	.528**
	Sig. (2-tailed)	.266	.007	.222	.005	.305	.288	.774	.475	.073		.023	.898	.004	.002
	N	32	32	32	32	32	32	32	32	32	32	32	32	32	32
Y11	Pearson Correlation	-.081	.104	-.109	.465**	.165	.201	.381	.092	.129	.402**	1	-.173	.385	.489
	Sig. (2-tailed)	.659	.572	.554	.007	.367	.270	.031	.616	.480	.023		.343	.030	.005
	N	32	32	32	32	32	32	32	32	32	32	32	32	32	32
Y12	Pearson Correlation	-.193	.097	.042	.208	.038	.222	-.116	-.092	.196	-.024	-.173	1	-.090	.185
	Sig. (2-tailed)	.289	.598	.820	.253	.836	.221	.527	.616	.282	.898	.343		.624	.310
	N	32	32	32	32	32	32	32	32	32	32	32	32	32	32
Y13	Pearson Correlation	.149	.451	-.231	.242	-.039	.097	.413	.296	.007	.498	.385	-.090	1	.512
	Sig. (2-tailed)	.415	.010	.204	.182	.833	.596	.019	.100	.970	.004	.030	.624		.003
	N	32	32	32	32	32	32	32	32	32	32	32	32	32	32
Total Y	Pearson Correlation	.313	.712	.183	.735	.298	.670	.530	.513	.577	.528	.489	.185	.512	1
	Sig. (2-tailed)	.081	.000	.317	.000	.097	.000	.002	.003	.001	.002	.005	.310	.003	
	N	32	32	32	32	32	32	32	32	32	32	32	32	32	32

Secara keseluruah total kuesioner yang dibustrikan sebanyak 35 kusioner, namun hanya 32 responden yang bersedia mengirimkan jawaban dari kuesioner yang disebarkan, jadi r table dengan mengunakan rumus sebagai berikut:

$$n = \frac{N}{1 + N(e)^2}$$

Keterangan:

n = Jumlah sampel yang diperlukan

N = Jumlah populasi

e = Tingkat kesalahan sampel (sampling error), biasanya 5%

Penjumlahannya yaitu:

$$n = \frac{32}{1+32(0{,}05)^2} = 29$$

Nilai dari r table dari 29 responden adalah 0.3550

Tabel 4. Uji Daya Beda

No	Pertanyaan	Uji Validitas	Tabel R	Hasil
1	X1	0.801	0,3550	Valid
2	X2	0.639	0,3550	Valid
3	X3	0.823	0,3550	Valid
4	Y1	0,313	0,3550	Tidak Valid
5	Y2	0,713	0,3550	Valid
6	Y3	0,183	0,3550	Tidak Valid
7	Y4	0,735	0,3550	Valid
8	Y5	0,298	0,3550	Tidak Valid
9	Y6	0,670	0,3550	Valid
10	Y7	0.530	0,3550	Valid
11	Y8	0.513	0,3550	Valid
12	Y9	0,577	0,3550	Valid
13	Y10	0.528	0,3550	Valid
14	Y11	0.489	0,3550	Valid
15	Y12	0.185	0,3550	Tidak Valid
16	Y13	0.512	0,3550	Valid

Dari hasil analisis dapat dilihat bahwa untuk semua nilai yang kurang dari r table, terdapat 12 item yang nilainya lebih dari 0,3550 maka dapat disimpulkan bahwa butir instrumen tersebut valid.

Sedangkan 4 item lainnya yang mendapat nilai kurang dari 0,3550 maka butir instrumen tersebut tidak valid.

4.4. Uji Realibitas

Azwar (2011) mendefenisikan reliabilitas dengan sejauh mana hasil pengukuran dapat dipercaya apabila dalam beberapa kali pelaksanaan pengukuran terhadap kelompok subjek yang sama diperoleh hasil yang relatif sama selama aspek dalam diri subjek yang diukur belum berubah. Suatu alat ukur mempunyai reliabilitas tinggi apabila alat ukur tersebut stabil dan dapat diandalkan. Uji reliabilitas alat ukur ini menggunakan pendekatan konsistensi internal (*Cronbach's alpha coeffecient*), yaitu suatu bentuk tes yang hanya memerlukan satu kali pengenaan tes tunggal pada sekelompok individu sebagai subjek dengan tujuan untuk melihat konsistensi antar item atau antar bagian dalam skala. Teknik ini dipandang ekonomis dan praktis (Azwar, 2009). Penghitungan koefisien reliabilitas dalam uji coba dilakukan dengan menggunakan program *SPSS version 20 For Windows*.

Tabel 5. Hasil Uji Realibitas

Reliability Statistics

Cronbach's Alpha	N of Items
.835	12

Hasil uji reabilitas berdasarkan Cronbach's Alpha sebesar 0.835 yang diketahui dari 12 item valid dan 4 item yang gugur menunjukkan bahwa hasil yang diperoleh reliabel.

4.5. Uji Normalitas

Uji normalitas ini digunakan untuk mengetahui apakah populasi data berdistribusi normal atau tidak. Dalam penelitian ini, peneliti menggunakan metode uji normalitas yaitu uji Liliefors. Data dinyatakan berdistribusi normal jika signifikansi lebih besar dari 0,05.

Tabel 6. Uji Normalitas

Tests of Normality

	Kolmogorov-Smirnova			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Fungsional	.196	32	.003	.887	32	.003
Non Fungsional	.122	32	.200*	.951	32	.155

*. This is a lower bound of the true significance.
a. Lilliefors Significance Correction

Berdasarkan uji normalitas menggunakan Kolmogorov-Smirnov. Data dinyatakan normal jika Signifikansi > 0.05. Dari Tabel 4.10 diatas dapat diketahui bahwa nilai signifikansi untuk funtional requirements 0.003 dan non functional requirements sebesar 0.200. Karena signifikansi untuk variabel non functional requirements lebih besar dari variabel functional requirements maka dapat disimpulkan bahwa penyebaran data berdistribusi normal.

4.6. Uji Hipotesis

Pada bagian ini akan dijelaskan hasil pengujian hipotesis dengan regresi linear sederhana untuk membuktikan hipotesis penelitian. Hasil uji hipotesis dapat dilihat pada tabel 7 sebagai berikut:

Tabel 7 Hasil Uji Hipotesis

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.652[a]	.425	.406	2.069

a. Predictors: (Constant), Total_Y

Coefficients[a]

		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-2.850	2.829		-1.007	.322
	Fungsional	.298	.063	.652	4.714	.000

a. Dependent Variable: Total_X

Berdasarkan tabel di atas, uji Hipotesis dapat dilakukan antara lain:

1. Menentukan Hipotesis:
   Ho : Metode knocking port berbasis mikrotik tidak dapat mengoptimalkan keamanan jaringan komputer
   Ha : Metode knocking port berbasis mikrotik dapat mengoptimalkan keamanan jaringan komputer
2. Menentukan tingkat signfikansi:
   Tingkat signifikasi menggunakan 0,05
3. Menentukan t hitung:
   Berdasrkan output diatas diperoleh thitung sebesar 4.714
4. Menentukan t table:
   Table distribusi t dicari pada a =5%. Dengan pengujian n 1 sisi (signifikasi = 0,05) hasil diperoleh untuk t table sebesar 0,3550
5. Kriteria pengujian
   Ho diterima jika t hitung ≤ t table
   Ho ditolak jika t hitung > t table
6. Membandingkan t hitung dengan t table:
   Thitung 4.714 ≥ ttabel 0,3550
7. kesimpulan
   Metode knocking port berbasis mikrotik dapat mengoptimalkan keamanan jaringan computer (Ha diterima)

5. KESIMPULAN DAN SARAN

Berdasarkan kegiatan penelitian yang telah peneliti lakukan, maka ada beberapa simpulan yang dapat diambil, antara lain: Metode *Port Knocking* dapat menjadi salah satu alternatif dalam melindungi atau mengamankan server. Hasil analisis dapat memenuhi kebutuhan intansi, lembaga atau perusahan terhadapat sistem pengamanan server. Dalam penggunaan dan instalasi *firewall* dengan metode *port knocking* sangat mudah, proses membuka dan menjalankan *firewall* pada mikrotik cukup stabil dan tidak memakan resource yang banyak.Selanjutnya

untuk Hasil pengujian hipotesis penelitian tes awal dan tes akhir di peroleh nilai thitung 4.714 dan nilai ttabel pada α = 0,05 n = $\frac{32}{1+32(0,05)^2}$ = 29 di peroleh harga sebesar 0,3550. Dengan demikian thitung lebih besar dari t table (thitung = 4.714 > ttabel = 0,3550). Berdasarkan kriteria pengujian bahwa diterima: Jika thitung > ttabel. Dengan demikian dapat disimpulkan bahwa Ha diterima dan Ho ditolak. Jadi dapat disimpulkan bahwa dengan menggunakan Optimalisasi Keamanan Jaringan Komputer Menggunakan Metode Knocking Port Berbasis Mikrotik memberikan pengaruh positif terhadap keamanan jaringan. Sehingga hipotesis berbunyi terdapat Pengaruh Optimalisasi Keamanan Jaringan Komputer Menggunakan Metode Knocking Port Berbasis Mikrotik Terhadap Peningkatan keamana jaringan di CV. Mitra Indexindo Pratama dapat diterima dan terjawab. Sistem autentifikasi remote server dengan metode port knocking ini tentu tidak terlepas dari beberapa kekurangan. Oleh sebab itu, untuk pengemabnagn selanjutnya yang lebih baik, penulis menyarankan beberapa di antaranya adalah: Diperlukannya adanya modifikasi lanjut agar konfigurasi bisa dapat mendeteksi laptop user agar bisa langsung meminta akses login tanpa meminta autentifikasi terlebih dahulu. Meski sistem konfigurasi sudah dirancang sudah begitu bagus, akan tetapi tetap diperlukan adanya pengembangan sistem sehingga mampu memberikan keamanan yang lebih baik mengikuti perkembangan zaman.

DAFTAR PUSTAKA

[1] A. H. M. Khader, A. Hadi, "Covert Communication Using Port Knocking," *Cybersecurity Cyberforensics Conf*, pp. 22–27, 2016

[2] M. S. Maulana and M. Ryansyah, "Malware Security Menggunakan Filtering Firewall Dengan Metode Port Blocking Pada Mikrotik RB 1100AHx2," *J. Sist. dan Teknol. Inf.*, vol. 6, no. 3, p. 112, 2018, doi: 10.26418/justin.v6i3.26716

[3] E. S. R. O. B. Langobelen, Y. Rachmawati, and C. Iswahyudi, "Analisis Dan Optimasi Dari Simulasi Keamanan Jaringan Menggunakan Firewall Mikrotik Studi Kasus Di Taman Pintar Yogyakarta," *J. JARKOM*, vol. 7, no. 2, pp. 95–102, 2019

[4] P. Riska, P. Sugiartawan, and I. Wiratama, "Sistem Keamanan Jaringan Komputer Dan Data Dengan Menggunakan Metode Port Knocking," *J. Sist. Inf. dan Komput. Terap. Indones.*, vol. 1, no. 2, pp. 53–64, 2018, doi: 10.33173/jsikti.12

[5] H. Di, K. Institut, and T. Yogyakarta, "Jurnal JARKOM Vol . 7 No . 2 Desember 2019 PERANCANGAN JARINGAN KOMPUTER LOKAL MENGGUNAKAN MODEL Jurnal JARKOM Vol . 7 No . 2 Desember 2019," vol. 7, no. 2, pp. 103–111, 2019

[6] H. Gunawan, "Ancaman Keamanan Jaringan Pada Server Untuk Membatasi Website Tertentu Menggunakan Mikrotik," *Inova-Tif*, vol. 2, no. 1, p. 22, 2020, doi: 10.32832/inova-tif.v1i2.2749

[7] J. Julianto, "Analisis Keamanan Jaringan Mikrotik Isp Indonesia Menggunakan Search Engine Scada Shodan Menggunakan Exploit Winbox …," vol. 09, no. 01, pp. 56–62, 2021

[8] A. Saputro, N. Saputro, H. Wijayanto, and P. S. Informatika, "METODE DEMILITARIZED ZONE DAN PORT KNOCKING UNTUK DEMILITARIZED ZONE AND PORT KNOCKING METHODS FOR COMPUTER," vol. 3, no. 2, pp. 22–27, 2020

[9] D. C. Dewi, V. Y. Utami, and S. Y. M. Yusuf, "Jurnal Ranah Publik Indonesia Kontemporer," no. 1, pp. 1–12, 2021

[10] L. Riyandari, T. Wahyuningsih, and J. Purnomo, "RANCANG BANGUN JARINGAN INTERNET DENGAN MEMPERHATIKAN ETIKA PROFESI TI MENGGUNAKAN WEB FILTERING PADA ROUTER MIKROTIK 951G-2HND"

[11] Suryanto, "Pengaturan Pemakaian Bandwidth dan Akses Jaringan Komputer Menggunakan Mikrotik Router," *J. Ilmu Pengetah. Dan Teknol. Komput.*, vol. 3, no. 2, pp. 167–172, 2018

.