

Sistem Keamanan Jaringan Komputer dan Data Dengan Menggunakan Metode *Port Knocking*

Putu Riska¹, Putu Sugiartawan^{*2}, Ichsan Wiratama³

¹Diskominfo Provinsi Bali, Denpasar, Bali

²Fakultas Teknik Informatika, STMIK STIKOM Indonesia

³Fakultas Ilmu Komputer, Universitas AMIKOM Yogyakarta

e-mail: ¹Putu.riska@gmail.com, ^{*2}putu.sugiartawan.85@gmail.com, ³x-sun@amikom.ac.id

Abstrak

Keamanan data dan informasi membuat teknologi informasi harus diperbaharui setiap saat. Seiring dengan perkembangan teknologi Informasi saat ini yang selalu berubah, menjadikan keamanan suatu informasi sangatlah penting. Banyak serangan yang dilakukan oleh orang-orang yang tidak bertanggung jawab melakukan serangan terhadap server. Serangan-serangan 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 knocking. Untuk menghindari serangan yang dilakukan dalam keadaan port terbuka maka digunakan suatu metode Port knocking 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. Sehingga akan membuat orang yang tidak memiliki hak akses tidak memiliki kesempatan untuk memasuki Port-port yang ada.

Kata kunci—Port knocking, port, keamanan jaringan, data

Abstract

Data and information security makes information technology must be updated at all times. Along with the ever-changing information technology development, making information security is very important. Many attacks carried out by irresponsible people to attack the server. These attacks are often performed on open ports, which in turn will allow unauthorized and unauthorized people to easily control ports that have been entered. So to do security on computer network in overcoming attack on ports, one of them is by using Port knocking method. In order to avoid attacks carried out in the open port state a Port knocking method is used and set parameters for this computer device to have no open communication ports to enter, but the device is still accessible from the outside. So as to make people who do not have access rights do not have the opportunity to enter the ports that exist.

Keywords—Port knocking, ports, network security, data

1. PENDAHULUAN

Pesatnya perkembangan teknologi saat ini membuat teknologi sangat berperan penting dalam kehidupan kita saat ini. Seiring dengan perkembangan teknologi informasi saat ini yang selalu berubah menjadikan keamanan suatu informasi sangatlah penting. 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 membuat serangan pada komputer tidak mempunyai hak akses maupun yang tidak berkepentingan dapat dengan mudah mengendalikan *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]. Internet of Things (IoT) lebih rentan terhadap serangan cyber yang ditargetkan daripada infrastruktur Teknologi Informasi (TI) biasa, di mana serangan cyber ini beroperasi pada identifikasi selanjutnya[2]. Salah satunya adalah dengan menggunakan metode *port knocking*. Kerangka kerja *OneTime Knocking* memanfaatkan jaringan seluler seperti GSM atau jaringan CDMA sebagai saluran out-of-band untuk membuat uthentikasi 2-faktor [3]. *Port knocking* adalah teknik pertama yang diperkenalkan mencegah penyerang menemukan dan mengeksploitasi layanan yang berpotensi rentan pada host jaringan, sambil memungkinkan pengguna terotentikasi untuk mengakses layanan ini [1][2][4]. Meskipun berpotensi sebagai alat yang berguna, ia mengalami berbagai kerentanan seperti tayangan ulang TCP, pemindaian *port*, dll. Proyek ini mengusulkan pendekatan baru atas *Port Knocking* yang ada dengan menggunakan urutan *Source Port* yang akan menyederhanakan teknik sistem *port knocking*.

Port knocking merupakan suatu sistem keamanan yang dibuat secara khusus untuk sebuah jaringan. *Port Knocking* (PKn) adalah otentikasi metode di mana data mentransmisikan melalui *port* tertutup [5]. *Port Knocking* adalah konsep penting untuk mengamankan layanan yang disediakan oleh *server* [6]. Dengan mengurutkan *Port Knocking* yang telah ditentukan di identifikasi apakah permintaan tersebut merupakan permintaan sah untuk suatu layanan [6]. Pada dasarnya cara kerja *port knocking* adalah menutup semua *port* yang ada, dan hanya user tertentu saja yang dapat mengakses sebuah *port* yang telah ditentukan, yaitu dengan cara mengetuk terlebih dahulu. Berbeda dengan cara kerja dari Firewall, cara kerja dari Firewall adalah menutup semua *port* tanpa memperdulikan apapun meskipun user tersebut memiliki hak untuk mengakses *port* tersebut. Sehingga user memiliki hak akses tersebut juga tidak bisa untuk mengaksesnya. Evaluasi kinerja dan perbandingan analitis dari tiga algoritma *port knocking* (PK) yang banyak digunakan, Aldaba, FWKNOP dan SIG-2. Analisis komparatif didasarkan pada sepuluh parameter yang dipilih[7][8]. Kelebihan dari *Port knocking* dengan firewell adalah meskipun semua *port* yang ada telah ditutup, tetapi user yang memiliki hak akses dan mengetahui *Knocking* untuk membuka suatu membuka suatu *port* maka user tersebut tetap dapat menggunakan *port* yang telah dibuka [4]. Implementasi *port-knocking* yang ada tidak dapat diskalakan dalam penyebaran penyedia layanan karena penggunaan rahasia bersama. Urutan *knocking* kurang rentan terhadap serangan replay dan brute force jika umurnya lebih pendek [9]. Implementasi *port-knocking* berdasarkan sertifikat x509 bertujuan untuk menjadi sangat skalabel [10]. Namun, *port knocking* sendiri memiliki beberapa kelemahan seperti misalnya TCP replay attacks, *port scan*, ketidak jelasan keamanan dan pengiriman paket tidak sesuai karena latensi jaringan [11]. Permasalahan tersebut dapat diatasi dengan pengaturan keamanan *server*, sehingga serangan dapat ditangkal terlebih dahulu dan menggabungkannya dengan Single Packet Authorization (SPA)[4]. Pada penelitian ini mengimplentasikan sistem keamanan jaringan komputer dengan menggunakan metode *port knocking* untuk mengurangi serangan pada *server*.

2. METODE PENELITIAN

Sebuah Perguruan Tinggi di Denpasar mempunyai lab komputer yang berisi 50 komputer *client* yang dipakai oleh siswa dan terhubung dengan satu *server* memakai jaringan LAN. Lab ini dikelola oleh seorang admin jaringan yang bertanggungjawab atas kinerja

komputer *client* maupun komputer *server*. Admin jaringan dan mahasiswa memiliki hak akses yang berbeda karena didalam *server* juga berisi data-data penting yang tidak boleh diakses oleh siswa. Hak akses pada komputer *server* dapat dibedakan dengan menggunakan metode *port knocking*. *Port knocking* merupakan sebuah metode untuk membangun komunikasi dari mana saja, dengan perangkat komputer yang tidak membuka *port* komunikasi apapun secara bebas. Dengan kata lain, perangkat komputer ini tidak memiliki *port* komunikasi yang terbuka bebas untuk dimasuki, tetapi perangkat ini masih tetap dapat diakses dari luar. Ini dapat terjadi jika pemakai komputer menggunakan metode *Port Knocking*. Koneksi dapat terjadi dengan menggunakan metode pengetukan *port-port* komunikasi yang ada. Pengetukan *port-port* ini dilakukan dengan kombinasi tertentu secara berurutan dalam satu rentan waktu tertentu.

Dengan metode tersebut maka penulis ingin membuat sebuah sistem yang menggunakan metode *Port knocking* untuk membatasi hak akses dari siswa yang memakai komputer di lab. Sistem ini nantinya juga akan membuat admin jaringan akan mempunyai hak akses khusus. Hak akses khusus maksudnya koneksi yang tidak terbuka untuk umum seperti SMTP atau HTTP. Biasanya hak akses khusus ini lebih bersifat administratif dan menggunakan servis-servis seperti telnet, SSH, FTP, TFTP, dan banyak lagi. Hak akses khusus ini akan sangat berbahaya jika dapat juga dilakukan oleh orang lain yang tidak berhak. Dengan menggunakan *Port knocking*, servis-servis tersebut akan tetap tertutup untuk diakses oleh publik dalam hal ini adalah siswa sebagai pemakai komputer di lab, namun masih dapat secara fleksibel di buka oleh siapa saja yang memiliki kombinasi ketukan *port*-nya.

2.1 *Port knocking*

Port-port komunikasi ini biasanya merupakan *port-port* yang ada dalam protokol TCP atau UDP yang merupakan anggota dari *Transportation layer* pada standar OSI [5]. Melalui *port* komunikasi ini, dunia luar dapat menjangkau perangkat Anda. Begitu pula sebaliknya, Anda juga bisa menjangkau mereka yang membuka *port* komunikasi tertentu [12-14]. Komunikasi dapat berjalan dengan lancar, pertukaran informasi menjadi mudah dan kenyamanan Anda berkomputer bertambah dengan terbukanya *Port-port* komunikasi ini. Namun, kadang kala kenyamanan ini sering disalahgunakan oleh sebagian orang. *Port-port* komunikasi ini sering dijadikan sebagai celah untuk dimasuki secara ilegal. *Port-port* yang terbuka digunakan sebagai jalan menuju ke dalam jaringan internal atau ke *server-server* di dalamnya, kemudian mengacaukannya [15].

Keterbukaannya yang bebas ini juga bisa menjadi salah satu ancaman bagi keamanan data Anda. Sangat mungkin penyusup masuk ke dalam komputer Anda, komputer di sebelah Anda, bahkan ke seluruh komputer di jaringan Anda jika dibiarkan terbuka sebebas-bebasnya. Jika jumlah komputer yang terkoneksi ke jaringan sedikit, mungkin tidak akan sulit untuk mengetahui apa saja yang terinstal di masing-masing komputer. Administrator jaringan mungkin tidak akan punya waktu untuk terus-menerus memantau apa yang telah terinstal di komputer-komputer tersebut. Untuk itulah, sebuah firewall sangat dibutuhkan untuk hadir di dalam jaringan Anda. Firewall biasanya memiliki tugas utama melakukan pemblokiran terhadap *Port-port* komunikasi yang terbuka di dalam sebuah jaringan. Di dalam firewall semua komunikasi keluar dan masuk dikontrol.

Port-port yang penting dan berbahaya juga dapat diblokir, sehingga hanya pihak yang Anda izinkan saja yang boleh masuk [16-17]. Metode ini merupakan sistem pengamanan yang paling efektif dan banyak digunakan. Namun terkadang, pemblokiran yang Anda lakukan sering menjadi senjata makan tuan. Ketika Anda butuh untuk menjalin komunikasi dengan apa yang ada di dalam jaringan Anda, firewall tidak mengizinkannya karena mungkin memang Anda berada pada area yang tidak diizinkan. Padahal komunikasi yang ingin Anda lakukan sangatlah penting untuk kelancaran kerja Anda. Misalnya, Anda terkoneksi dengan Internet dan butuh masuk ke dalam *webserver* Anda melalui SSH untuk memperbaiki konfigurasinya, sementara *port* SSH pada *server* tersebut dilarang untuk diakses dari Internet oleh firewall Anda. Tentu ini akan cukup merepotkan. Untuk mengakali kejadian-kejadian seperti ini, ada sebuah metode

yang cukup unik yang dapat dengan efektif menghilangkan masalah senjata makan tuan seperti ini. Metode tersebut diberi nama *Port knocking*.

Secara harafiah, arti dari *Port knocking* adalah melakukan pengetukan terhadap *Port-port* komunikasi yang ada dalam sistem komunikasi data. Fungsi dan cara kerja dari sistem ini tidak jauh berbeda dengan arti harafiahnya [17-18]. *Port knocking* merupakan sebuah metode untuk membangun komunikasi dari mana saja, dengan perangkat komputer yang tidak membuka *port* komunikasi apapun secara bebas. Dengan kata lain, perangkat komputer ini tidak memiliki *port* komunikasi yang terbuka bebas untuk dimasuki, tetapi perangkat ini masih tetap dapat diakses dari luar [18]. Ini dapat terjadi jika Anda menggunakan metode *PortKnocking*. Koneksi dapat terjadi dengan menggunakan metode pengetukan *Port-port* komunikasi yang ada. Pengetukan *Port-port* ini dilakukan dengan kombinasi tertentu secara berurutan dalam satu rentan waktu tertentu. Jika kombinasi dari pengetukan tersebut sesuai dengan yang telah ditentukan, maka sebuah *port* komunikasi yang diinginkan akan terbuka untuk Anda. Setelah terbuka, Anda bebas mengakses apa yang ada dalam jaringan tersebut melalui *port* komunikasi yang baru terbuka tadi. Setelah selesai melakukan pekerjaan dan kepentingan Anda, *port* komunikasi yang tadi terbuka dapat ditutup kembali dengan melakukan pengetukan sekuensialnya sekali lagi. Maka, perangkat komputer dan jaringan Anda akan kembali aman.

Jika dilihat sesaat, *Port knocking* memang tidak terlalu banyak gunanya dan tidak terlalu istimewa. Hanya melakukan buka tutup *port* komunikasi saja tentu tidaklah terlalu banyak gunanya bagi pengguna jaringan lokal. Namun bagi para pekerja telekomuter, para pengguna komputer yang sering bekerja di luar kantor atau para administrator jaringan dan *server* yang harus mengurus *server-server* mereka 24 jam dari mana saja, *Port knocking* merupakan metode yang luar biasa sebagai sebuah jalan penghubung ke perangkat-perangkat komputer mereka. *Port knocking* cocok untuk mereka yang masih ingin memperkuat sistem keamanan komputer dan perangkat jaringannya, sementara tetap pula ingin memiliki koneksi pribadi ke dalamnya secara kontinyu dan dapat dilakukan dari mana saja. Komunikasi pribadi maksudnya koneksi yang tidak terbuka untuk umum seperti SMTP atau HTTP. Biasanya komunikasi pribadi ini lebih bersifat administratif dan menggunakan servis-servis seperti telnet, SSH, FTP, TFTP, dan banyak lagi. Komunikasi pribadi ini akan sangat berbahaya jika dapat juga dilakukan oleh orang lain yang tidak berhak. Dengan menggunakan *Portknocking*, servis-servis tersebut akan tetap tertutup untuk diakses oleh publik, namun masih dapat secara fleksibel di buka oleh siapa saja yang memiliki kombinasi ketukan *port-nya*.

Port knocking bekerja seperti halnya brankas dengan kunci kombinasi angka putar. Pada brankas tersebut, Anda diharuskan memutar kunci kombinasi beberapa kali hingga tepat seperti yang ditentukan. Sebenarnya Anda memutar lapisan-lapisan kunci di dalam brankas. Dalam lapisan-lapisan kunci tersebut terdapat sebuah lubang kunci. Jika sebuah putaran tepat, maka sebuah lubang terbuka. Jika seluruh putaran dilakukan dengan kombinasi yang benar, maka seluruh lubang terbuka dan menciptakan sebuah jalur khusus yang bebas tidak ada hambatan sama sekali. Jalur lubang kunci tadi tidak lagi menjadi penghalang pintu brankas untuk dibuka, sehingga pintu dapat terbuka dengan mudah.

2. 2 Jaringan Komputer

Formulir Jaringan komputer adalah sebuah kumpulan komputer, printer dan peralatan lainnya yang terhubung. Informasi dan data bergerak melalui kabel-kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan data, mencetak pada printer yang sama dan bersama sama menggunakan hardware/software yang terhubung dengan jaringan. Tiap komputer, printer atau periferal yang terhubung dengan jaringan disebut node. Sebuah jaringan komputer dapat memiliki dua, puluhan, ribuan atau bahkan jutaan node.

Sebuah jaringan biasanya terdiri dari 2 atau lebih komputer yang saling berhubungan diantara satu dengan yang lain, dan saling berbagi sumber daya misalnya CDROM, Printer, pertukaran file, atau memungkinkan untuk saling berkomunikasi secara elektronik. Komputer yang terhubung tersebut, dimungkinkan berhubungan dengan media kabel, saluran telepon,

gelombang radio, satelit, atau sinar infra merah

2. 2.1 Sejarah Jaringan Komputer

Sejarah jaringan komputer bermula dari lahirnya konsep jaringan komputer pada tahun 1940-an di Amerika yang digagas oleh sebuah proyek pengembangan komputer MODEL I di laboratorium Bell dan group riset Universitas Harvard yang dipimpin profesor Howard Aiken. Pada mulanya proyek tersebut hanyalah ingin memanfaatkan sebuah perangkat komputer yang harus dipakai bersama. Untuk mengerjakan beberapa proses tanpa banyak membuang waktu kosong dibuatlah proses beruntun (Batch Processing), sehingga beberapa program bisa dijalankan dalam sebuah komputer dengan kaidah antrian.

Kemudian ditahun 1950-an ketika jenis komputer mulai berkembang sampai terciptanya super komputer, maka sebuah komputer harus melayani beberapa tempat yang tersedia (terminal), untuk itu ditemukan konsep distribusi proses berdasarkan waktu yang dikenal dengan nama TSS (Time Sharing Sistem). Maka untuk pertama kalinya bentuk jaringan (*network*) komputer diaplikasikan. Pada sistem TSS beberapa terminal terhubung secara seri ke sebuah komputer atau perangkat lainnya yang terhubung dalam suatu jaringan (*host*) komputer. Dalam proses TSS mulai terlihat perpaduan teknologi komputer dan teknologi telekomunikasi yang pada awalnya berkembang sendiri-sendiri. Departemen Pertahanan Amerika, U.S. Defense Advanced Research Projects Agency (DARPA) memutuskan untuk mengadakan riset yang bertujuan untuk menghubungkan sejumlah komputer sehingga membentuk jaringan organik pada tahun 1969. Program riset ini dikenal dengan nama ARPANET. Pada tahun 1970, sudah lebih dari 10 komputer yang berhasil dihubungkan satu sama lain sehingga mereka bisa saling berkomunikasi dan membentuk sebuah jaringan. Dan pada tahun 1970 itu juga setelah beban pekerjaan bertambah banyak dan harga perangkat komputer besar mulai terasa sangat mahal, maka mulailah digunakan konsep proses distribusi (Distributed Processing). Dalam proses ini beberapa host komputer mengerjakan sebuah pekerjaan besar secara paralel untuk melayani beberapa terminal yang tersambung secara seri disetiap host komputer. Dalam proses distribusi sudah mutlak diperlukan perpaduan yang mendalam antara teknologi komputer dan telekomunikasi, karena selain proses yang harus didistribusikan, semua host komputer wajib melayani terminal-terminalnya dalam satu perintah dari komputer pusat .

2. 2.2 Jenis-jenis jaringan komputer

Jenis-jenis jaringan komputer berdasarkan cakupan areanya dapat dibedakan menjadi beberapa jenis yaitu PAN, LAN, MAN dan WAN.

PAN (Personal Area Network), Pada saat kita saling menghubungkan komputer atau perangkat lain seperti handphone, PDA, keyboard, mouse , headsetwireless, camera dan peralatan lain yang jaraknya cukup dekat (4-6 meter) maka kita telah membentuk suatu Personal Area Network. Hal yang paling penting bahwa dalam PAN ini kita sendiri yang mengendalikan (authoritas) pada semua peralatan tersebut. Selain dihubungkan langsung ke komputer lewat *port* USB atau FireWire, PAN juga sering dibentuk dengan teknologiwireless seperti bluetooth, Infrared atau WiFi.

LAN (*Local Area Network*) adalah jaringan komputer yang mencakup wilayah kecil; seperti jaringan komputer kampus, gedung, kantor, dalam rumah dan sekolah.

Sebuah LAN, adalah jaringan yang dibatasi oleh area yang relatif kecil, umumnya dibatasi oleh area lingkungan seperti sebuah Perkantoran di sebuah gedung, atau sebuah sekolah, dan biasanya tidak jauh dari sekitar 1 km persegi.

Beberapa model konfigurasi LAN, satu komputer biasanya dijadikan sebuah file *server*. Yang mana digunakan untuk menyimpan perangkat lunak (*software*) yang mengatur aktifitas jaringan, ataupun sebagai perangkat lunak yang dapat digunakan oleh komputer yang terhubung ke dalam *network*. Komputer-komputer yang terhubung ke dalam jaringan (*network*) itu biasanya disebut dengan workstation. Biasanya kemampuan workstation lebih di bawah dari file *server* dan

mempunyai aplikasi lain di dalam harddisk-nya selain aplikasi untuk jaringan. Kebanyakan LAN menggunakan media kabel untuk menghubungkan antara satu komputer dengan komputer lainnya

Sebuah MAN, biasanya meliputi area yang lebih besar dari LAN, misalnya antar wilayah dalam satu propinsi. Dalam hal ini jaringan menghubungkan beberapa buah jaringan-jaringan kecil ke dalam lingkungan area yang lebih besar, sebagai contoh yaitu : jaringan Bank dimana beberapa kantor cabang sebuah Bank di dalam sebuah kota besar dihubungkan antara satu dengan lainnya. Misalnya Bank BNI yang ada di seluruh wilayah Denpasar atau Surabaya.

Wide Area Networks (WAN) adalah jaringan yang lingkupnya biasanya sudah menggunakan sarana Satelit ataupun kabel bawah laut sebagai contoh keseluruhan jaringan BANK BNI yang ada di Indonesia ataupun yang ada di Negara-negara lain. Menggunakan sarana WAN, Sebuah Bank yang ada di Bandung bisa menghubungi kantor cabangnya yang ada di Hongkong, hanya dalam beberapa menit. Biasanya WAN agak rumit dan sangat kompleks, menggunakan banyak sarana untuk menghubungkan antara LAN dan WAN ke dalam Komunikasi Global seperti Internet. Tapi bagaimanapun juga antara LAN, MAN dan WAN tidak banyak berbeda dalam beberapa hal, hanya lingkup areanya saja yang berbeda satu diantara yang lainnya.

2. 3 Port

Dalam satu waktu, sebuah device bisa saja menjalankan berbagai beberapa proses sekaligus. Masing-masing proses mungkin bisa menggunakan protokol dari *transport* layer misalnya TCP atau UDP. Untuk bisa membedakan satu proses dan proses lainnya di jaringan, digunakan *portnumber*. *Port* number memiliki ukuran 16 bit sehingga penomoran yang memungkinkan yaitu mulai dari 0 sampai dengan 65535. Penggunaan nomor pada *port* diatur oleh Internet Assigned Number Authority (IANA). Berikut pengaturan yang dilakukan oleh IANA :

1. Well-know *ports* : 0 sampai dengan 1023 Penomoran dan penggunaan *port – port* ini diatur sepenuhnya oleh IANA. Jika diperlukan, sebuah *port* bisa di dimanfaatkan oleh TCP dan UDP sekaligus.
2. Registered *port* : 1024 sampai dengan 49151 IANA tidak sepenuhnya mengatur penggunaan *port – port* ini, tetapi IANA menyediakan *port* ini untuk dimanfaatkan oleh perusahaan atau komunitas – komunitas.
3. Dynamic atau private *port* : 49152 sampai dengan 65535. IANA tidak mengatur *port – port* ini. *Port* ini bisa dengan bebas digunakan dan biasanya disebut *ephemeral port*.

2. 4 Keamanan Jaringan Komputer dan Firewall

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 disalahgunakan. Sistem keamanan membantu mengamankan jaringan tanpa menghalangi penggunaannya dan menempatkan antisipasi 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 dibuat. Jika mereka tidak memahami hal tersebut, maka mereka akan menciptakan lubang (*hole*) keamanan pada jaringan.

Ada dua elemen utama pembentuk keamanan jaringan :

1. Tembok pengamanan, baik secara fisik maupun maya, yang ditaruh diantara piranti dan layanan jaringan yang digunakan dan orang-orang yang akan berbuat jahat.
2. Rencana pengamanan, yang akan diimplementasikan bersama dengan user lainnya, untuk menjaga agar sistem tidak bisa ditembus dari luar.

Segi-segi keamanan didefinisikan dari kelima point ini.

- a) Confidentiality Mensyaratkan bahwa informasi (data) hanya bisa diakses oleh pihak yang memiliki wewenang.

- b) Integrity Mensyaratkan bahwa informasi hanya dapat diubah oleh pihak yang memiliki wewenang.
- c) Availability Mensyaratkan bahwa informasi tersedia untuk pihak yang memiliki wewenang ketika dibutuhkan.
- d) Authentication Mensyaratkan bahwa pengirim suatu informasi dapat diidentifikasi dengan benar dan ada jaminan bahwa identitas yang didapat tidak palsu.
- e) Nonrepudiation Mensyaratkan bahwa baik pengirim maupun penerima informasi tidak dapat menyangkal pengiriman dan penerimaan pesan.

2. 5 Rancangan Implementasi Port knocking

Rancangan implementasi sistem untuk *port knocking* ditunjukkan pada Gambar 1. pada Gambar 1 menunjukkan proses yang terjadi pada program *port knocking*. Urutan proses yang terjadi antara lain:

1. Setelah program dijalankan maka user diminta untuk memasukkan IP *server*.
2. Selanjutnya program meminta masukan urutan *port* yang akan diketuk.
3. Setelah itu sistem akan memvalidasi IP *server* apabila salah maka program akan meminda IP *server* kembali apabila benar maka sistem akan melanjutkan ke proses selanjutnya.
4. Berikutnya sistem akan memvalidasi *port* yang telah dimasukkan, apabila urutan *port* salah maka sistem akan kembali ke proses memasukkan *port*, apabila benar maka sistem akan melanjutkan ke proses selanjutnya.
5. Setelah validasi bernilai true and true maka barulah proses *knocking* terjadi

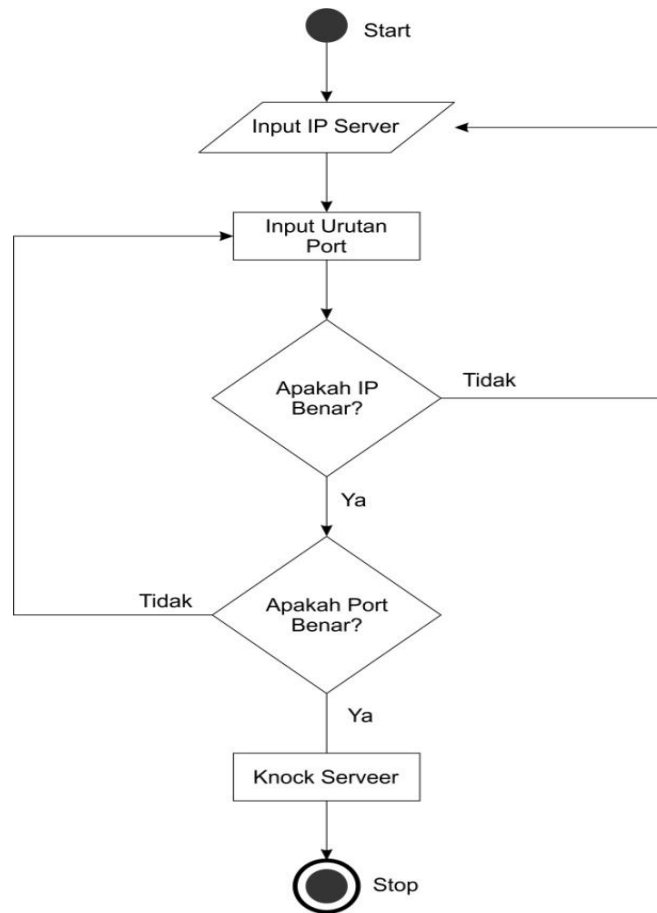
Program *port knocking* ini akan berjalan dengan ideal apabila kebutuhan sistemnya sudah terpenuhi. Kebutuhan sistem yang diperlukan antara lain:

1. Sistem operasi yang mendukung pada pemasangan program ini. Dalam hal ini kebutuhan sistem operasi minimal microsoft *windows XP* atau yang lebih baik untuk *client*. Pilihan lain sistem ini juga dapat digunakan pada sistem operasi linux ubuntu 12.04 atau versi ubuntu yang lebih baru.
2. Kebutuhan yang lainnya adalah RAM (*Random Acces Memory*) sebesar 512MB. Fungsi dari RAM dalam sebuah sistem ini adalah sebagai sebuah perangkat atau media yang mempunyai fungsi untuk menyimpan data sementara pada sebuah komputer. Jadi, memori ini memang difungsikan untuk menyimpan data sementara agar ketika komputer sedang bekerja, komputer tidak perlu mengakses terus menerus ke hardisk ketika mengolah data dan mencari data.
3. Sistem ini membutuhkan ruangan harddisk kosong sebesar 200MB. Fungsi perangkat harddisk secara umum adalah untuk menyimpan data yang dihasilkan oleh pemrosesan perangkat komputer/laptop. Di dalamnya, terdapat sebuah ruang simpan utama dalam sebuah komputer. Dimana di situlah setiap data dan informasi disimpan olehnya.
4. Sistem ini dibuat dengan bahasa pemrograman java maka pada sistemnya harus berisi JRE (*Java Runtime Environment*) yakni satu teknologi yang dibuat dan dikembangkan oleh Oracle. dengan Java Runtime Environment JRE, anda dimungkinkan untuk menjalankan aplikasi yang disebut "Applet" yang ditulis dalam bahasa pemrograman berbasis Java.
5. Kebutuhan lain diluar sistem yakni hak akses Administrator karena admin lah yang akan menjalankan program ini dan yang mengatur *port* mana saja yang boleh diakses oleh *client*.

2. 6 Use Case Diagram Sistem Port knocking

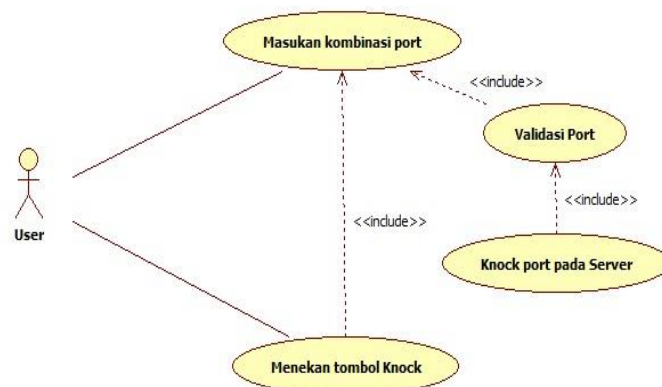
Use case diagram digunakan untuk memodelkan proses berdasarkan perspektif pengguna system. Use case merepresentasikan operasi-operasi yang dilakukan oleh actor. Use case digambarkan berbentuk elips dengan nama operasi dituliskan di dalamnya. Actor yang melakukan operasi dihubungkan dengan garis lurus ke use case. Pada Gambar 2 menunjukkan

gambaran use case diagram yang menggambarkan proses yang terjadi didalam system *port knocking*.



Gambar 1 Rancangan sistem pengujian *port knocking*

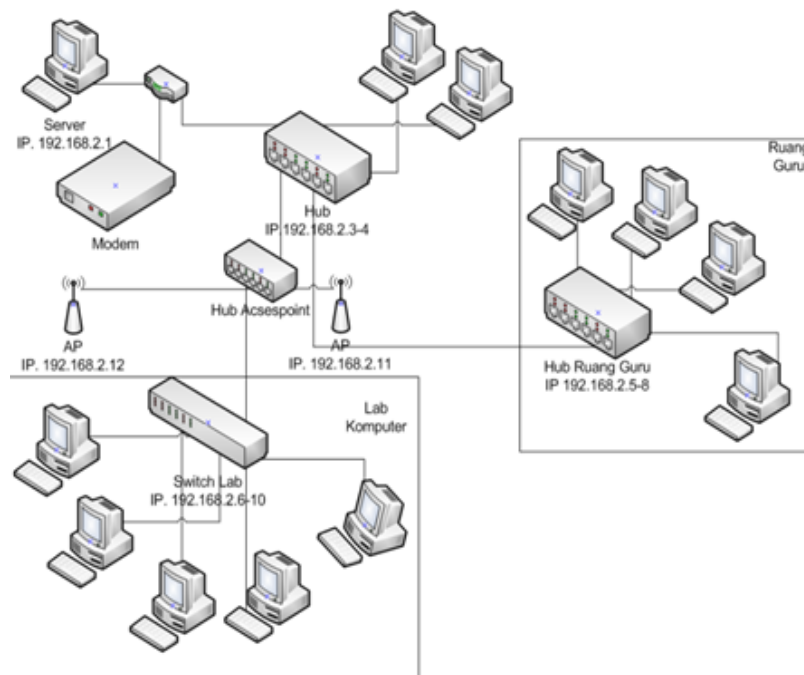
Dalam use case pada Gambar 2 diterangkan kegiatan yang dilakukan oleh user yakni menekan tombol knock yang membutuhkan memasukkan *port* kombinasi terlebih dahulu. Setelah itu sistem akan memvalidasi kombinasi *port* saat kombinasi tersebut bernilai true maka sistem baru akan melakukan *port knocking* pada server.



Gambar 2 Use Case System

2. 7 Skenario Pengujian

Program *port knocking* akan diuji cobakan pada arsitektur komputer yang ditunjukkan pada Gambar 3. Program masing-masing dipasang di *server* dan di salah-satu *client* yang terhubung dalam satu jaringan LAN. Pada *server* program dijalankan lebih dahulu untuk memberi aturan ketukan dan mengatur *port* yang akan dibuka ataupun ditutup. Setelah program di *server* dijalankan barulah program di *client* dijalankan. Ketukan di *client* disesuaikan pada ketukan di *server* apabila tidak sesuai maka akan ada *error control*. Dalam pengujian yang telah dilakukan *client* dengan IP 192.169.1.33 akan mengetuk *port* 445 pada *server*.



Gambar 3. Topologi jaringan penelitian

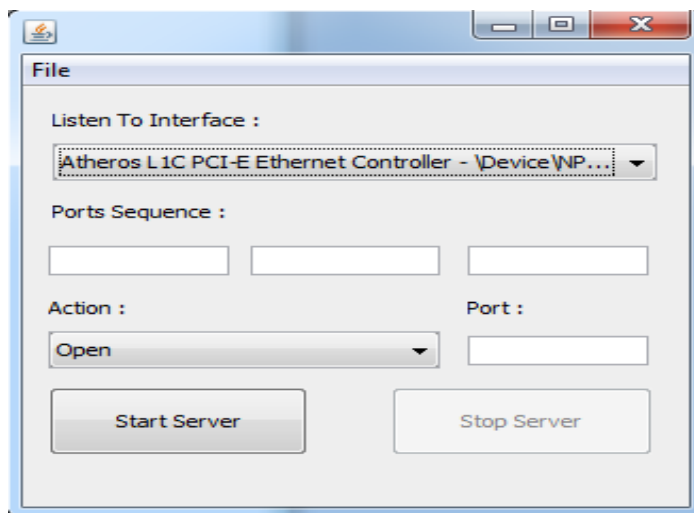
Tujuan dari pengujian ini adalah membuktikan metode *port knocking* sekaligus menguji apakah implementasi program yang telah dibuat sudah sesuai dengan yang diinginkan. Selanjutnya pengujian ini dilakukan juga untuk menguji apakah *client* yang dalam satu jaringan mendapatkan hak akses setelah berhasil menjalankan program secara benar. Pengujian hak akses dilakukan dengan sharing file dari *server* yang dapat dibuka oleh *client*.

Terdapat 2 buah access point dengan IP masing-masing IP 192.168.2.11 dan IP 192.168.2.12 yang dapat berhubungan dengan beberapa komputer di masing-masing ruangan. Sehingga satu buah *server* dapat berhungan dengan masing-masing komputer di setiap ruangan dan di masing-masing komputer di setiap ruangan dapat saling berhubungan dengan ruangan lainnya menggunakan Switch Hub. Program *port knocking* hanya dibuat untuk komunikasi antara *server* dan ruangan lab. Program *port knocking* berfungsi agar *client* yang mempergunakan komputer di lab tidak dapat secara leluasa mengakses data pada komputer *server*.

3. HASIL DAN PEMBAHASAN

Pada tampilan implementasi utama program PkServer ini berisikan *combo box* dengan label “Listen To Interface” yang akan memunculkan semua piranti jaringan yang ada pada komputer *server*. Dibawahnya terdapat tiga input box dengan label “Ports Sequence”. Pada input box tersebut akan dimasukkan urutan *port Sequence*. Setelah itu ada *combo box* dengan label “Action:” yang memiliki dua isi yakni Open artinya memberikan status Open pada *port* yang ditentukan dan Close yang berarti memberikan perintah untuk menutup *port* yang telah

ditentukan. Disebelah kanan ada input box yang memiliki label “Port” disana kita akan mengisi *port* berapa yang akan dibuka ataupun ditutup pada *server*. Dibawahnya ada dua tombol yang masing-masing berisi label “Start Server” dan “Stop Server”. Start Server berfungsi untuk menjalankan konfigurasi *port knocking* yang telah diisi dan stop server berfungsi untuk menghentikan konfigurasi *port knocking* pada *server* yang tadinya telah dijalankan.



Gambar 4. Implementasi sistem port knocking

3.1 Port Sequence Error Control

Setelah memilih *interface* selanjutnya administrator diminta memasukkan *port sequence*. Dalam memasukkan urutan *port* program ini memiliki dua error yakni apabila urutan *port* ini diisi dengan huruf maka akan muncul *message box* yang berisi kata-kata “Invalid Port Number!”. Dalam input box diatur untuk hanya menerima angka saja, dan program tidak akan berjalan apabila inputan ini belum sesuai.

Port sequence yang dapat diterima adalah urutan *port* yang ditentukan secara acak oleh administrator yang sesuai dengan Well-known *Port* yang berkisar antara 0 hingga 1023. Urutan *port sequence* tidak boleh diluar dari kisaran 0 hingga 1023 dan pada sisi *client* harus sama dengan *port sequence* yang ditentukan oleh administrator

3.2 Rule Allow

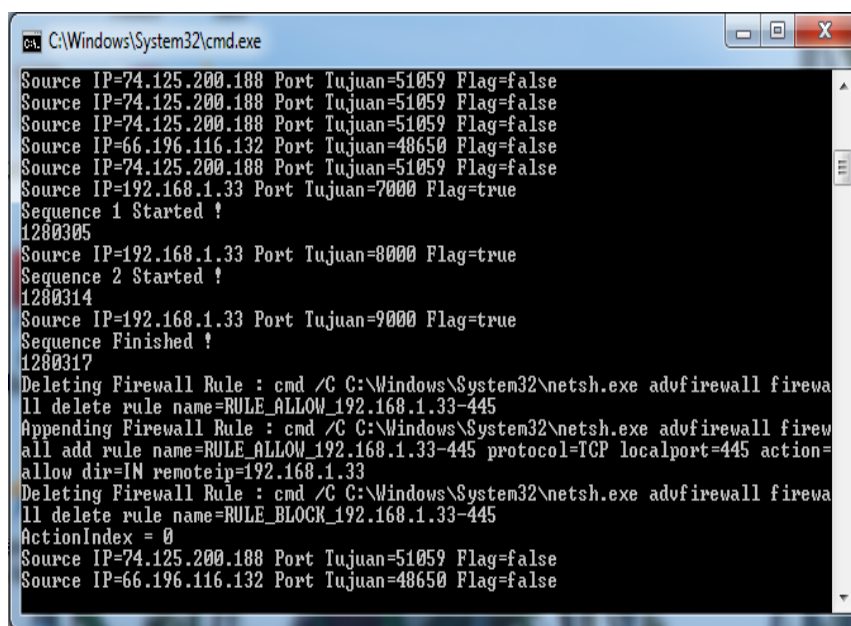
Setelah program *server* dijalankan maka *server* tinggal menunggu program *knocking* dari *client*. Saat *client* sudah menjalankan program dan memilih *port* yang diijinkan maka pada CMD akan muncul pemberitahuan bahwa ada *client* yang ingin masuk.

Dalam CMD akan muncul baris pemberitahuan seperti “add rule: RULE_ALLOW_192.168.1.33-445 protocol=TCP localport= 445 action=allow dir=IN remoteip=192.169.1.33” pemberitahuan tersebut berarti program ini memasukkan aturan baru bernama “RULE_ALLOW_192.168.1.33-445” dengan berisi IP *client* dan *port* yang dituju. Selanjutnya berisi protocol yang dipakai yakni protocol TCP. Selanjutnya berisi *port* yang dituju pada percobaan yang telah dilakukan *client* mengakses *port* 445. Selanjutnya berisi action, action ada tiga jenis yakni allow, block, dan bypass. Allow berarti paket jaringan yang sesuai dengan semua kriteria yang ditentukan dalam peraturan ini diizinkan melalui firewall. Block berarti paket jaringan yang sesuai dengan semua kriteria yang ditentukan dalam peraturan ini yang diblok oleh firewall.

Bypass dalam opsi ini hanya berlaku untuk aturan yang memiliki satu atau lebih accounts yang tercantum dalam *rmtcomputergrp* dan *rmtusrgrp* opsional. Selanjutnya berisi “dir=IN” baris ini berarti Aturan yang cocok hanya *inbound* lalu lintas jaringan yang tiba di

komputer. Aturan ini muncul dalam Windows Firewall dengan Advanced Security MMC snap-in di bawah Inbound Rules. Selanjutnya ada “remoteip=192.169.1.33” ini berarti bahwa paket jaringan dengan pencocokan alamat IP sesuai dengan aturan ini. remoteip dibandingkan dengan IP bidang alamat tujuan dari sebuah paket jaringan outbound. Hal ini dibandingkan dengan field alamat IP sumber dari sebuah paket jaringan inbound.

Selain pemberitahuan di CMD, Rule ini juga akan muncul di jendela firewall, dalam firewall akan muncul aturan baru yang bernama “RULE_ALLOW_192.168.1.33-445” dengan parameter profile=all, Enable=yes, Action=allow. Ditunjukkan pada Gambar 5.



```

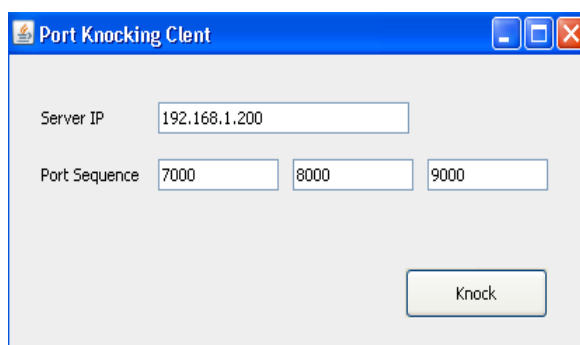
C:\Windows\System32\cmd.exe
Source IP=74.125.200.188 Port Tujuan=51059 Flag=false
Source IP=74.125.200.188 Port Tujuan=51059 Flag=false
Source IP=74.125.200.188 Port Tujuan=51059 Flag=false
Source IP=66.196.116.132 Port Tujuan=48650 Flag=false
Source IP=74.125.200.188 Port Tujuan=51059 Flag=false
Source IP=192.168.1.33 Port Tujuan=7000 Flag=true
Sequence 1 Started !
1280305
Source IP=192.168.1.33 Port Tujuan=8000 Flag=true
Sequence 2 Started !
1280314
Source IP=192.168.1.33 Port Tujuan=9000 Flag=true
Sequence Finished !
1280317
Deleting Firewall Rule : cmd /C C:\Windows\System32\netsh.exe advfirewall firewall delete rule name=RULE_ALLOW_192.168.1.33-445
Appending Firewall Rule : cmd /C C:\Windows\System32\netsh.exe advfirewall firewall add rule name=RULE_ALLOW_192.168.1.33-445 protocol=TCP localport=445 action=allow dir=IN remoteip=192.168.1.33
Deleting Firewall Rule : cmd /C C:\Windows\System32\netsh.exe advfirewall firewall delete rule name=RULE_BLOCK_192.168.1.33-445
ActionIndex = 0
Source IP=74.125.200.188 Port Tujuan=51059 Flag=false
Source IP=66.196.116.132 Port Tujuan=48650 Flag=false

```

Gambar 5. Rule Allow

3.3 Client Side

Pada sisi *client* terdapat program untuk *knocking* ke *server*, seperti yang ditunjukkan Pada Gambar 5. pada program ini berisi dua parameter yakni mengisi *Server IP* tujuan dan *Port Sequence* yang harus sama dengan *port sequence* yang ada pada *server*. Dalam kasus ini IP *server* adalah 192.168.1.200 dan *port sequence* 7000, 8000, 9000. Setelah parameter tersebut diisi maka administrator dapat menekan tombol *Knock*. yang ditunjukkan pada Gambar 6



Gambar 6. Port knocking client

4. KESIMPULAN

Sesuai dengan perancangan dan pembangunan program *port knocking* maka didapat beberapa kesimpulan antara lain, Program *port knocking* dapat menentukan *port* yang dapat

diakses oleh *client*, Program *port knocking* dapat menentukan *port* yang tidak dapat diakses oleh *client*, Apabila tidak mendapat akses *client* tidak dapat melakukan sharing file atau berkomunikasi dengan *server*.

DAFTAR PUSTAKA

- [1] M. Khader, A. Hadi, and A. Hudaib, "Covert Communication Using *Port Knocking*," *2016 Cybersecurity Cyberforensics Conf.*, pp. 22–27, 2016.
- [2] B. Mahbooba and M. Schukat, "Digital Certificate-based *Port Knocking* for Connected Embedded Systems," *2017 28th Irish Signals Syst. Conf.*, pp. 1–5, 2017.
- [3] J. Liew, S. Lee, and I. Ong, "One-Time *Knocking* Framework using SPA and IPsec," *2010 2nd Int. Conf. Educ. Technol. Comput.*, vol. 5, pp. V5-209-V5-213, 2010.
- [4] F. H. M. Ali, R. Yunus, and M. A. M. Alias, "Simple *port knocking* method: Against TCP replay attack and *port scanning*," in *International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, 2012, pp. 247–252.
- [5] M. Pourvabab, R. E. Atani, and L. Boroumand, "SPKT : Secure *Port Knock-Tunneling* , an Enhanced *Port Security Authentication Mechanism*," *2012 IEEE Symp. Comput. Informatics*, pp. 145–149, 2012.
- [6] V. Srivastava, A. K. Keshri, A. D. Roy, V. K. Chaurasiya, and R. Gupta, "Advanced *Port Knocking Authentication Scheme* with QRC using AES," *2011 Int. Conf. Emerg. Trends Networks Comput. Commun.*, pp. 159–163, 2011.
- [7] B. W. Moedeen and A. S. H. Jeerooburkhan, "Evaluating the strategic role of Social Media Analytics to gain business intelligence in Higher Education Institutions," *2016 IEEE Int. Conf. Emerg. Technol. Innov. Bus. Pract. Transform. Soc.*, pp. 303–308, 2016.
- [8] Z. A. Khan, N. Javaid, M. H. Arshad, A. Bibi, and B. Qasim, "Performance Evaluation of Widely used *Portknocking Algorithms*," *2012 IEEE 14th Int. Conf. High Perform. Comput. Commun. 2012 IEEE 9th Int. Conf. Embed. Softw. Syst.*, pp. 903–907, 2012.
- [9] T. Popeea, V. Olteanu, L. Gheorghe, and R. Rughiniş, "Extension of a *port knocking client-server architecture* with NTP synchronization," *2011 RoEduNet Int. Conf. 10th Ed. Netw. Educ. Res.*, pp. 1–5.
- [10] D. Sel, S. H. Totakura, and G. Carle, "sKnock : *Port-Knocking for Masses*," *2016 IEEE 35th Symp. Reliab. Distrib. Syst. Work.*, pp. 1–6, 2016.
- [11] A. Narayanan, "A critique of *port knocking*," *Linux J.*, vol. 1, no. 1, 2004.
- [12] Boroumand, L., Shiraz, M., Gani, A., and Khokhar, R, "Virtualization Technique for Port Knocking in Mobile Cloud Computing". *Ist.J.Advance.Soft.Comput.Appl*, 6(1), 2014
- [13] I. Marzuki, "Perancangan dan Implementasi Sistem Keamanan Jaringan Komputer Menggunakan Metode Port Knocking Pada Sistem Operasi Linux," *J. Teknol. Inf. Indones.*, vol. 2, no. 2, pp. 18–24, 2017.
- [14] R. Muzawi, "Aplikasi Pengendalian Port dengan Utilitas Port Knocking untuk Optimalisasi Sistem Keamanan Jaringan Komputer," *SATIN – Sains dan Teknol. Inf.*, vol. 2, no. 1, 2016.
- [15] Yewale, M. P. R. "A Modified Hybrid Port Knocking Technique for Host Authentication : A Review". *IJRITCC International Journal on Recent and Innovation Trends in Computing and Communication*, 2(3), 673–677, 2014.
- [16] Sahu, P., Singh, M., & Kulhare, D. "Implementation of Modified Hybrid Port Knocking (MHPK) with Strong Authentication ", *International Journal of Computer Applications*, 64(22), 31–36, 2013.
- [17] Saleh, M., Fajri, H., Suhatman, R., Putra, Y. E., Studi, P., Informatika, TCaltex, P, "Analisa Port Knocking Pada Sistem Operasi Linux Ubuntu Server", 2(1), 59–67, 2014.
- [18] Prihanto, A., and Knocking, P., "Implementasi Port-Knocking di Mikrotik dengan Menggunakan Komponen Delphi TcpClient". *Prosiding Seminar Teknik Elektro Dan Pendidikan Teknik Elektro, (Ste)*, 533–538, 2013.