TELCOMATICS, Vol.4 No. 1, April 2019, pp. 1-6
e-ISSN: 2541-5867

Analisis Sistem Pengamanan Akses Autentikasi Jaringan dengan Metode Port Knocking dan Action Tarpit pada Router Mikrotik

Yefta Christian
Sistem Informasi, Fakultas Ilmu Komputer, Universitas Internasional Batam, Jl. Gajah Mada, Batam, 29442, Indonesia
e-mail: yefta@uib.ac.id

Abstract

The use of mikrotik router in the process of forming a network system in a company both internally and externally is a common thing in the world of work, this is in line with the rapid development of technology today. In this study, researchers designed user permissions on ports using mikrotik routers as well as testing the security of port knocking methods and action tarpit firewalls. Port knocking method is a technique that temporarily closed port access. With the method of port knocking researchers can test the security of a port using a knocking port on the router mikrotik, so it can be known how safe port knocking method to protect certain ports. Port knocking used in mikrotik this router using winbox to see it, and also by using web service on winbox webfig already provided by party mikrotik router.
***Keywords**: port knocking, action tarpit*

Abstrak

Penggunaan pemakaian mikrotik router dalam proses membentuk sistem jaringan dalam suatu perusahaan baik secara internal maupun eksternal merupakan sebuah hal yang biasa dalam dunia kerja, hal ini sejalan dengan perkembangan teknologi yang pesat saat ini. Dalam penelitian ini, peneliti merancang hak akses user pada port menggunakan mikrotik router serta melakukan uji coba akan keamanan metode port knocking dan firewall action tarpit. Metode port knocking merupakan sebuah teknik yang menutup akses port sementara. Dengan metode port knocking peneliti dapat melakukan uji coba terhadap keamanan dari sebuah port yang menggunakan port knocking di mikrotik router, sehingga dapat diketahui seberapa aman metode port knocking untuk melindungi port tertentu. Port knocking yang digunakan di mikrotik router ini menggunakan winbox untuk melihatnya, dan juga dengan memakai layanan web pada webfig winbox yang sudah di sediakan oleh pihak mikrotik router.
***Katakunci**: port knocking, action tarpit*

I. LATAR BELAKANG

Perkembangan teknologi informasi yang semakin pesat terutama perkembangan yang signifikan di sektor jaringan komputer semakin memudahkan para penggunanya mulai dari perorangan dan korporasi, akan tetapi perkembangan teknologi tidak hanya memberikan semua dampak positif, namun dapat memberikan dampak yang negative pula seperti kurangnya atau lambatnya pergerakan didalam suatu jaringan.

Cybercrime [1] adalah sesuatu dari bentuk kejahatan virtual dengan memanfaatkan media komputer yang terhubung melalui jaringan internet, dan mengekploitasi komputer lain yang terhubung dengan internet juga. Adanya lubang-lubang keamanan pada sistem operasi menyebabkan kelemahan dan terbukanya lubang yang dapat digunakan para Hacker, Cracker dan Script Kiddies untuk menyusup kedalam komputer tersebut.

Salah satunya bagi seorang administrator server, seorang administrator akan menyediakan layanan service remote login agar komputer

TELCOMATICS, Vol.4 No. 1, April 2019, pp. 1-6
e-ISSN: 2541-5867

server tersebut dapat diakses dari mana saja. Dengan kata lain administrator menginstall service secure shell (SSH) [2] agar bisa mengakses komputer server dari tempat lain. Agar administrator dapat mengakses komputernya, maka dari itu administrator harus menjalankan service daemon hal ini dapat menyebabkan aplikasi melakukan listen pada port yang sudah sesuai sehingga hal ini dapat membuat port tersebut terbuka.

Dengan adanya keadaan seperti ini dapat memberikan keuntungan bagi pihak lain diluar dari pihak administrator dan ini bisa menimbulkan dampak yang serius seperti ancaman bagi komputer server. Pihak yang bukan seorang administrator adalah seorang attacker yang mencoba mengakses komputer server dengan metode yang sudah dikuasai oleh pihak lain seperti percobaan eksploitasi dengan menggunakan metode brute force [3] dan lain sebagainya.

Percobaan-percobaan eksploitasi tersebut dapat menimbulkan dampak buruk terhadap komputer server apabila attacker tersebut berhasil melakukan percobaan eksploitasi ini antara lainnya adalah attacker dapat mempunyai hak akses tertinggi dikomputer atau bahkan attacker dapat merusak system server yang ada. Untuk mengatasi keadaan seperti ini, sistem server akan membutuhkan pengamanan yang mampu mengatasi aksi penyerangan dari pihak yang tidak memiliki akses ke komputer server yaitu memasang firewall. Firewall akan melakukan blokir terhadap user yang mencoba masuk dengan melintasi port yang terbuka [4]. Hal ini juga dapat menyebabkan seorang administrator tidak dapat mengakses komputer. Agar administrator dapat melakukan akses ke komputer server, dibutuhkan system autentikasi agar firewall memberikan izin mengakses komputer server melalui dengan meng-Ping sebelumnya.

Namun dengan keadaan seperti ini, diperlukan suatu solusi yang tepat agar administrator tetap dapat mengakses komputer tersebut. Solusi tersebut adalah dengan menerapkan metode autentikasi port knocking. Metode autentikasi ini bekerja dengan system "buka port kepada suatu klien bila klien itu meminta, dan tutup kembali bila klien telah selesai".

Berdasarkan penelitian di atas, penulis akan menggunakan port knocking dan mengkombinasikan dengan mikrotik router. System operasi yang digunakan adalah linux ubuntu 14.04, windows 7 yang akan diujikan dalam lingkungan local Area Network dan winbox di windows 7 yang bertugas sebagai server dan target serangan menggunakan virtualisasi.

Adapun rumusan masalah pada penelitian yang telah diuraikan diatas adalah sebagai berikut:1) Bagaimana model implementasi sistem keamanan jaringan komputer dapat mendeteksi serangan Attacker memasuki port dan secara otomatis memblokir port yang akan dimasuki; 2) Perbandingan kinerja autentikasi dengan menggunakan layanan jaringan port knocking, firewall action tarpit dan layanan standar pada port FTP, SSH, WebFig, dan Winboxv.

II. AKSES AUTENTIKASI JARINGAN

Sistem keamanan pada jaringan menggunakan port knocking menggunakan mikrotik sebelumnya sudah dianalisa dan dibangun. Pada penelitian tersebut digunakan router RB750 dan 1 laptop untuk penelitiannya. Tahap akhir dalam penelitiannya adalah pengujian terhadap sistem port knocking menggunakan mikrotik. Pengujian tersebut dilakukan untuk mengetahui apakah pencegahan penyerang dari pemindai sistem yang mudah di eksploitasi seperti SSH dengan melakukan port scanning. Pengujian port knocking adalah pengujian yang di design untuk menutup port-port yang terbuka. Pengujian port knocking dilakukan dengan menutup sementara port yang sudah diketahui. Hasil akhir dari penelitian menunjukkan aplikasi router yang menggunakan mikrotik berhasil dengan menunjukan bahwa beberapa port berstatus filtered dan setelah berhasil dilakukan knocking maka port tersebut berstatus open.

Jaringan komputer bukanlah sesuatu yang baru saat ini [5]. Jaringan Komputer adalah sekumpulan komputer yang saling terhubung satu sama lain dan bekerja secara otomatis. Hampir di setiap perusahaan terdapat jaringan komputer untuk memperlancar arus informasi dalam perusahaan tersebut. Internet yang mulai popular sejak beberapa tahun terakhir ini adalah suatu jaringan komputer raksasa yang saling terhubung dan dapat saling berinteraksi. Hal ini dapat terjadi karena adanya perkembangan teknologi jaringan yang sangat pesat, sehingga dalam beberapa tahun saja jumlah pengguna

jaringan komputer yang tergabung dalam internet telah menjadi berlipat ganda. Jaringan yang terhubung dengan internet, masalah kecepatan upload maupun download merupakan hal yang sangat penting untuk memperlancar transmisi data. Banyak hal yang dapat mempengaruhi kecepatan dua proses tersebut, diantaranya yaitu besarnya bandwidth yang digunakan jaringan tersebut dan seberapa efektif bandwidth tersebut bisa dimanfaatkan. Bandwidth adalah suatu ukuran dari banyaknya informasi yang dapat mengalir dari satu tempat ke tempat lain dalam satu waktu tertentu.

Jaringan komputer adalah salah satu himpunan interkoneksi sejumlah komputer autonomous. Dalam bahasa yang popular dapat dijelaskan bahwa jaringan komputer adalah sekumpulan beberapa komputer dan perangkat lain seperti printer, hub, dan sebagainya, yang saling terhubung satu sama lain melalui media perantara. Media perantara ini biasa berupa media kabel ataupun media tanpa kabel (nirkabel). Informasi berupa data akan mengalir dari suatu komputer ke komputer lainnya atau dari satu komputer ke perangkat lain, sehingga masing-masing komputer yang terhubung tersebut biasa bertukar data atau berbagi perangkat keras.

Jaringan komputer yang saling terhubung ke suatu komputer server dengan menggunakan topologi tertentu, biasanya digunakan dalam kawasan satu gedung atau kawasan yang jaraknya tidak lebih dari 1 km.

Mencakup daerah geografis yang luas, seringkali mencakup negara atau benua. WAN [6] terdiri dari kumpulan mesin yang bertujuan untuk menjalankan program-program (aplikasi) pemakai. Mesin ini disebut HOST. HOST dihubungkan oleh sebuah subnet komunikasi atau cukup disebut SUBNET. Tugas subnet adalah membawa pesan dari satu host ke host lainnya. Pada sebagian besar WAN subnet terdiri dari 2 komponen: kabel transmisi dan element switching.

Client Server [7] merupakan model jaringan yang menggunakan satu atau beberapa komputer sebagai server yang memberikan resource-nya kepada komputer lain (client) dalam jaringan, server akan mengatur mekanisme akses resource yang boleh digunakan, serta mekanisme komunikasi antar node dalam jaringan.

Selain pada jaringan lokal, sistem ini bisa juga diterapkan dengan teknologi internet. Dimana ada suatu unit komputer) berfungsi sebagai server yang hanya memberikan pelayanan bagi komputer lain, dan client yang juga hanya meminta layanan dari server. Akses dilakukan secara transparan dari client dengan melakukan login terlebih dulu ke server yang dituju.

Client hanya bisa menggunakan resource yang disediakan server sesuai dengan otoritas yang diberikan oleh administrator. Aplikasi yang dijalankan pada sisi client, bisa saja merupakan resource yang tersedia di server. Namun hanya bisa dijalankan setelah terkoneksi ke server. Pada implementasi software aplikasi yang di-install di sisi client berbeda dengan yang digunakan di server.

Peer artinya rekan sekerja. Peer-to-peer network [8] adalah jaringan komputer yang terdiri dari beberapa komputer, terhubung langsung dengan kabel crossover atau wireless atau juga dengan perantara hub/switch. Peer to peer adalah suatu model dimana tiap PC dapat memakai resource pada PC lain atau memberikan resource-nya untuk dipakai PC lain, Tidak ada yang bertindak sebagai server yang mengatur sistem komunikasi dan penggunaan resource komputer yang terdapat dijaringan, dengan kata lain setiap komputer dapat berfungsi sebagai client maupun server pada periode yang sama.

Keamanan pada jaringan komputer pada saat ini menjadi sebuah topik tersendiri dan bidang ilmu tersendiri didalam jaringan komputer, yang khususnya yang mempelajari tentang berbagai jenis ancaman keamanan dan kejahatan komputer dan jaringan komputer serta sejumlah solusi yang diberikan di dalamnya. Faktor keamanan menjadi factor penentu dari layanan yang disediakan di dalam jaringan komputer (khususnya internet) bagaimana sebuah keamanan suatu negara atau pemerintahan, apabila data-data penting didalamnya berhasil dicuri.

Keamanan komputer dibangun dapat memiliki beberapa tujuan yang diantaranya: 1) Confidentiality, bisa disebut juga dengan sebuah kerahasiaan yang bertujuan utamanya untuk menjaga dari keamanan komputer dan keamanan jaringan computer; 2) Integrity, berupa upaya untuk menjaga sebuah keamanan data pada komputer yang bertujuan agar data dan informasi oleh pihak yang tidak berhak untuk mengubahnya; 3) Availability, upaya untuk menyediakan akses kepada pihak yang berhak untuk mengetahui data dan informasi tersebut.

Ada beberapa penyebab kenapa komputer bisa terkena serangan baik berupa virus ataupun

TELCOMATICS, Vol.4 No. 1, April 2019, pp. 1-6
e-ISSN: 2541-5867

attacker, yaitu: 1) Kelengahan dari pengguna dimana penyebab paling utama adalah karena kelengahan atau kesalahan dari pengguna komputer tersebut. Contohnya pada hal yang paling besar adalah akibat dari mendownload suatu file, jika file tersebut terdapatvirus, tanpa di sadari virus telah masuk ke dalam komputer; 2) Komputer dengan kurangnya sistem keamanan yang baik tanpa anti virus

Penyebab lainnya adalah dimana disaat meng-copy atau memindah kan data dari flashdisk atau cd-room yang belum ter-scan sehingga terdapat virus didalamnya, sehingga virus pun dapat menyerang ke komputer seperti adanya shortcut, dan lain-lain; 3) Lubang-lubang dalam sistem operasi yang digunakan atau port, dimana penyebab yang tidak berhubungan langsung dengan pengguna adalah lubang-lubang sekuriti seperti port yang terbuka yang terdapat pada sistem operasi yang digunakan pada computer; 4) Faktor-faktor lainnya, dimana salah satu dari penyebab lainnya adalah tidak berhubungan sama sekali dengan kepenggunaan dan pada saat pengguna komputer menggunakan komputer di tempat umum seperti warnet. Bisa saja komputer tersebut menggunakan keylogger atau penyimpanan kunci password tanpa sepengetahuan user. Pengguna tanpa sadar memasukan data-data rahasia seperti password, PIN, maupun data lainnya yang sangat penting.

Keamanan system [9] adalah termasuk juga pada jaringan komputer, secara umum terbagi atas tiga aspek utama. Ketiga aspek utama tersebut meliputi aspek sistem (System), aspek kebijakan (Policy), dan aspek pengguna (User).

Penjelasannya adalah sebagai berikut: Aspek sistem (System), dimana aspek ini terdiri dari atas semua perangkat keras dan perangkat lunak komputer, termasuk juga yang digunakan di dalam jaringan. Bagian inilah yang paling banyak dibahas oleh hampir sebagian besar pengguna computer; Aspek kebijakan (Policy), dimana aspek ini memegang peranan penting, sebelum proses implementasi kedalam sistem dan pemberlakuan aturan tersebut kepada para pengguna; Aspek pengguna (User) dimana aspek ini mencakup semua pengguna yang terlibat didalam sistem pada jaringan komputer adalah aspek pengguna (User). Aspek pengguna (User) mencakup semua pengguna yang terlibat didalam sistem pada jaringan komputer, baik sebagai pengguna tertinggi (administrator) hingga yang biasa.

Suatu serangan kedalam server jaringan komputer dapat terjadi kapan saja. Baik administrator bekerja atau tidak. Ada berbagai tipe macam penyerangan yang terjadi pada jaringan, sebagai berikut:1) Port Scanning, [10] merupakan suatu proses untuk mencari dan membuka port pada suatu jaringan komputer. Dari hasil scanning akan didapat letak kelemahan sistem tersebut. Pada dasarnya sistem port scanning mudah untuk dideteksi, tetapi penyerang akan menggunakan beberapa cara metode untuk menyembunyikan serangan; 2) Teardrop

Penyerangan dengan menggunakan proses disassembly reassembly paket data. Dialam jaringan internet sering kali data harus dipotong menjadi paket yang lebih kecil untuk menjamin reliabilitas dan proses multiple akses jaringan; 3) IP spoofing, dimana teknik ini bekerja dengan mengganti alamat IP pengguna yang lain yang bukan penyerang sebenarnya. Hal ini terjadi karena salah rancang (design flaw) bagian urutan nomor (sequence number) dari paket TCP / IP. Dalam beberapa kasus, penyerang menggunakan satu alamat IP sumber yang spesifik pada semua paket IP yang keluar untuk membuat semua pengembalian paket IP dan pesan ICMP ke pemilik alamat tersebut; 4) ICMP flood

Pengolahan data-data paket yang menggunakan ICMP, untuk mengantisipasi flood data yang disebabkan oleh paket yang menggunakan protocol ICMP; 5) UDP flood dimana UDP flood sama seperti halnya ICMP pengiriman paket melalui UDP juga merupakan jenis pengiriman paket berupa datagram, yang pada sekala normal dan juga merupakan paket data yang berukuran kecil; 6) Packet interception, dimana gangguan jenis ini dilakukan dengan membaca paket di saat paket tersebut sedang mengalami packet sniffing. Packet interception merupakan cara penyerang untuk mendapatkan informasi yang ada di dalam paket tersebut. Hal ini dapat dicegah dengan mengenkripsi terlebih dahulu, sehingga penyerang akan mengalami kesulitan untuk membuka paket tersebut; 7) Brute force, dimana serangan terhadap sebuah sistem keamanan jaringan komputer yang digunakan dengan percobaan terhadap semua kunci yang akan memungkinkan untuk menemukan user dan password tersebut.

Model referensi jaringan terbuka OSI atau *OSI Reference Model for open networking* [11] adalah sebuah model arsitektural jaringan yang

dikembangkan oleh badan International Organization for Standardization (ISO) di Eropa pada tahun 1977. OSI sendiri merupakan singkatan dari Open System Interconnection. Model ini disebut juga dengan model "Model tujuh lapis OSI" (OSI seven-layer model).

Sebelum munculnya model referensi OSI, sistem jaringan komputer sangat tergantung kepada pemasok (vendor). OSI berupaya membentuk standar umum jaringan komputer untuk menunjang interoperatibilitas antar pemasok yang berbeda. Dalam suatu jaringan yang besar biasanya terdapat banyak protokol jaringan yang berbeda. Tidak adanya suatu protokol yang sama, membuat banyak perangkat tidak bisa saling berkomunikasi.

Model referensi ini pada awalnya ditujukan sebagai basis untuk mengembangkan protokol-protokol jaringan, meski pada kenyataannya inisiatif ini mengalami kegagalan. Kegagalan itu disebabkan oleh beberapa faktor berikut: a) Standar model referensi ini, jika dibandingkan dengan model referensi DARPA (Model Internet) yang dikembangkan oleh Internet Engineering Task Force (IETF), sangat berdekatan. Model DARPA adalah model basis protokol TCP/IP yang populer digunakan; b) Model referensi ini dianggap sangat kompleks. Beberapa fungsi (seperti halnya metode komunikasi connectionless) dianggap kurang bagus, sementara fungsi lainnya (seperti flow control dan koreksi kesalahan) diulang-ulang pada beberapa lapisan; c) Pertumbuhan Internet dan protokol TCP/IP (sebuah protokol jaringan dunia nyata) membuat OSI Reference Model menjadi kurang diminati.

Pemerintah Amerika Serikat mencoba untuk mendukung protokol OSI Reference Model dalam solusi jaringan pemerintah pada tahun 1980-an, dengan mengimplementasikan beberapa standar yang disebut dengan Government Open Systems Interconnection Profile (GOSIP). Meski demikian, Usaha ini akhirnya ditinggalkan pada tahun 1995 dan implementasi jaringan yang menggunakan OSI Reference model jarang dijumpai di luar Eropa.

OSI Reference Model pun akhirnya dilihat sebagai sebuah model ideal dari koneksi logis yang harus terjadi agar komunikasi data dalam jaringan dapat berlangsung. Beberapa protokol yang digunakan dalam dunia nyata, semacam TCP/IP, DECnet dan IBMSystems Network Architecture (SNA) memetakan tumpukan protokol (protocol stack) mereka ke OSI Reference Model.OSI Reference Model pun digunakan sebagai titik awal untuk mempelajari bagaimana beberapa protokol jaringan di dalam sebuah kumpulan protokol dapat berfungsi dan berinteraksi.

Struktur tujuh lapis model OSI, bersamaan dengan protocol data unit pada setiap lapisan

III. Analisis Sistem Pengamanan Akses

Setelah melakukan serangkaian analisis dan perancangan sistem pada bab-bab sebelumnya, maka pada bab ini akan dilakukan implementasi sistem sesuai dengan yang telah direncanakan pada bab sebelumnya. Implementasi ini mencakupi dari instalasi dan konfigurasi perangkat lunak.

Dari hasil pengujian sebelum dan sesudah menggunakan port knocking didapatkan analisa dan evaluasi sebagai berikut. Pada pengujian serangan menggunakan hydra brute force attack pada port FTP, SSH, dan HTTP bahwa password dan user dapat oleh aplikasi hydra dan ini bisa menyebabkan attacker masuk kedalam sistem autentikasi atau masuk kedalam port FTP dan SSH yang nantinya akan mempengaruhi dampak perubahan sistem didalamnya atau penghapusan data didalam sistem mikrotik router.

Pada pengujian scanning port bahwa serangan scanning sebelum dan sesudah memakai port knocking dan firewall action tarpit terdapat banyak perbedaan diantaranya adalah ketika sebelum memakai port knocking, scanning port memberitahu bahwa terdeteksi port SSH, FTP, dan HTTP. Ketika sudah memakai port knocking scaaning port sama sekali tidak bisa mendeteksi satu pun port yang ada, dan ketika dikombinasikan dengan firewall action tarpit ada sekitar 1023 port yang terdeteksi termasuk port FTP akan tetapi ini akan membinggungkan attacker untuk menentukan port-port yang akan diserang.

Di pengujian selanjutnya menggunakan nmap/zenmap dengan menggunakan port knocking sebelum, sesudah, dan dikombinasi kan dengan firewall action tarpit, port yang berstatus open ketika sistem tidak menggunakan port knocking, dan status port berubah menjadi filtered ketika memakai port knocking, selanjutnya memakai firewall action tarpit status tidak dilihatkan tetapi nmap memberitahu bahwa port discovery open port, akan tetapi port yang discovered open port ada banyak sehingga membingungkan attacker untuk memulai serangan port. Dan ini membuat sistem autentikasi port akan aman dari serangan.

TELCOMATICS, Vol.4 No. 1, April 2019, pp. 1-6
e-ISSN: 2541-5867

IV. KESIMPULAN

Metode port knocking dapat meminimalisir terjadinya penyusupan yang tidak mempunyai hak akases dan sangat membantu administrator dalam menjaga keamanan akses pada port autentikasi. Metode port knocking dapat bekerja dengan baik dimana metode ini dapat meport knocking port autentikasi sehingga harus melalu izin masuk ke port tersebut. Pengkombinasian port knocking dan action tarpit penyusup mau pun administrator tidak akan bisa masuk dan login melalui layanan remote login seperti SSH. Berdasarkan pengujian dari penulis, hasil evaluasi dari kinerja port knocking menunjukan hasil yang baik, dimana penyerangan menggunakan brute force attack tidak berhasil menemukan user dan password dari layanan port tersebut. Hasil pengujian dari scanning port, tahap scanning dapat menunjukan hasil yang baik dimana status pada port tersebut ada filtered yang maksudnya adalah harus izin terlebih dahulu sebelum memasuki port tersebut. Berdasarkan pengujian dari scanning port, metode port knocking dan action tarpit dari hasil evaluasi ini port knocking dapat meminimalkan dan membingungkan penyerangan pada port FTP, SSH, dan HTTP. Kinerja dari port knocking dan Tarpit, dimana aplikasi Bitvise SSH Client atau service remote login tidak dapat melakukan login setelah melakukan ping dan sebelum melakukan ping aplikasi dari Bitvise SSH Client tetap tidak bisa Login, dan seorang admin harus masuk melalui fitur WINBOX (GUI yang telah disediakan oleh mikrotik). Penyerangan yang dilakukan pada port 8291 sama sekali tidak terjadi apa-apa, akan tetapi port 8291 adalah port winbox , dimana port tersebut merupakan login ke sistem mikrotik, akan tetapi ada cara lain selain memasuki port winbox, yaitu dengan memasuki port SSH dan HTTP dikarenakan winbox bisa diremote melalui SSH dan winbox juga tersedia dalam layanan WEB.

REFERENSI

[1] A. S. Poonia, "Cybercrime: Challenges and Its Classification," International Journal of Emerging Trends & Technology in Computer Science, vol. 3, no. 6, 2014.

[2] A. P. S. D. Y. M. S. D. Aniket Burande, "Wireless Network Security by SSH Tunneling," International Journal of Scientific and Research Publications, vol. 4, no. 4, 2014.

[3] P. Wiyanto, A. Hamzah and M. Sholeh, "Aplikasi Monitoring Keamanan Jaringan Dengan Menggunakan IDS dan Router Mikrotik," Jurnal JARKOM, vol. 2, no. 1, 2014.

[4] G. Sondakh, M. E. I. Najoan and A. S. Lumenta, "Perancangan Filtering Firewall Menggunakan Iptables Di Jaringan Pusat Teknologi Informasi Unsrat," E-journal Teknik Elektro dan Komputer, 2014.

[5] E. Lauren A. Menard and P. Diane F. Olivier, "New Technologies in Professional Learning Networks," International Journal for Service Learning in Engineering, vol. 9, no. 2, 2014.

[6] S. N. Khasanah, "Perancangan dan Implementasi Wide Area Network (WAN) dengan IP VPN," Jurnal Techno Nusa Mandiri, vol. 11, no. 2, 2014.

[7] A. Latubessy and W. Agus, "Analisa dan Perancangan Sistem Pemasaran UMKM Terintegrasi Berbasis Cloud Server," Jurnal SIMETRIS, vol. 5, no. 1, 2014.

[8] M. Zunaidi, B. Andika and Saniman, "Membentuk Jaringan Peer to Peer Menggunakan Kabel Firewire IEEE-1394 dengan Metode Bridge," Jurnal Ilmiah Saintikom, vol. 13, no. 2, 2014.

[9] A. J. Alnawaiseh, "Security Information System of The Computer Center in Mu'tah University," European Scientific Journal, vol. 10, no. 27, 2014.

[10] S. A. Prihasmoro, Y. Rachmawati and E. Fatkhiyah, "Simulasi Sistem Deteksi Penyusup dalam Jaringan Komputer Berbasis Web Interface Serta Pencegahan Untuk Meningkatkan Keamanan," Jurnal JARKOM, vol. 2, no. 1, 2014.

[11] G. Bora, S. Bora, S. Singh and S. M. Arsalan, "OSI Reference Model: An Overview," International Journal of Computer Trends and Technology (, vol. 7, no. 4, 2014.