NASKAH JURNAL

Sistem Keamanan Jaringan Menggunakan Cisco AnyConnect Dengan Metode Network Access Manager

Fathurrahman Dali
Teknik Informatika, Fakultas Ilmu Komputer
Universitas Mercu Buana
E-mail : *fathurdalileo@gmail.com*

ABSTRAK

Pada saat ini perkembangan dalam bidang teknologi dan informasi semakin pesat, hal ini terbukti dengan semakin banyaknya masyarakat yang menggunakan layanan internet. Seiring dengan perkembangan internet yang sedemikian pesat, menjadikan keamanan suatu data atau informasi pada server yang terhubung dengan publik menjadi sangat penting. Banyak perusahaan yang memiliki jaringan komputer dimana jaringan tersebut berfungsi untuk menghubungkan komputer-komputer yang ada didalam ruangan kantor. Adanya jaringan komputer tidak hanya mempermudah kinerja karyawan namun dapat juga memunculkan permasalahan terutama dalam hal keamanan jaringan komputer itu sendiri. Ancaman keamanan jaringan komputer yang dapat merugikan salah satunya terletak pada jaringan internal di PT Lintasarta. Metode penelitian yang digunakan dalam penelitian ini adalah penelitian tindakan atau action research. Hasil dari penelitian ini adalah penggunaan sistem keamanan jaringan menggunakan Cisco ISE dengan metode network access manager tenyata mampu membantu untuk menerapkan standar IT Policy di PT Lintasarta

Kata kunci*—Sistem Keamanan Jaringan, Jaringan Internet, IT Policy, Sistem Otentitkasi Izin Akses.*

http://digilib.mercubuana.ac.id/

1. PENDAHULUAN

Sistem keamanan jaringan komputer adalah cabang dari teknologi yang dikenal sebagai informasi keamanan yang diterapkan pada komputer dan jaringan. Tujuan keamanan komputer meliputi perlindungan informasi dari pihak yang tidak berkepentingan dengan tetap memudahkan akses dan penggunaan oleh para pengguna. Keamanan sistem komputer merupakan mekanisme dan proses kolektif terhadap informasi sensitif dan berharga dan juga layanan yang dilindungi dari publikasi, gangguan atau kehancuran oleh kegiatan yang tidak sah atau individu yang tidak dapat dipercaya dan kejadian-kejadian yang tidak direncanakan masing-masing. Keamanan Jaringan adalah komponen yang paling penting dan vital dalam kemanan informasi karena bertanggung jawab untuk mengamankan semua informasi melewati computer berjejaring[1]. Membuat rancangan jaringan dengan menggunakan pendekatan model proses jaringan[2]. Di dalam mengimplementasikan komponen dari sistem keamanan jaringan seperti firewall yang berfungsi untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak semua hubungan atau kegiatan suatu segemen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya[3]. Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi[4]. Sistem pengamanan yang dapat menangani ancaman dari pihak luar melalui jaringan internet menjadi suatu hal yang mutlak dimiliki sebuah perusahaan atau organisasi[5].

Saat ini, PT Lintasarta sedang melakukan perbaikan besar-besaran dalam segi keamanan infrastruktur IT. Mengingat semakin besarnya dampak dan kemungkinan cyberattack, langkah ini di pandang sebagai langkah strategis untuk meningkatkan efisiensi operasional, mengurangi downtime dan secara tidak langsung, meningkatkan kepuasan terhadap pelanggan. Keamanan jaringan computer sendiri bertujuan untuk mengantisipasi resiko pada jaringan computer berupa bentuk ancaman fisik maupun logic baik langsung ataupun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam jaringan computer[6]. Salah satu dasar dalam pengamanan infrastruktur jaringan dan IT adalah kenyataan bahwa user adalah mata rantai terlemah dalam rantai keamanan. Sebuah perusahaan yang telah menggunakan perangkat security terbaik dan termahal sekalipun dapat ditembus dengan mudah jika usernya tidak memahami masalah security dengan baik. Supaya dapat mengamankan dan mencegah jaringan internet dari berbagai ancaman diperlukan beberapa solusi perancangan suatu sistem keamanan atau multiple layers of security yang dapat bekerja pada lapisan-lapisan jaringan internet[7]. Otentikasi user merupakan hal yang penting harus ada untuk memberikan hak akses kepada user atau client[8]. Cara ini merupakan sistem pengamanan jaringan komputer yang paling efektif dan banyak digunakan[9].

1) Tujuan dan Manfaat

Tujuan yang ingin dicapai pada penelitian ini adalah:

- Dapat memonitoring log session connection pada perangkat kerja user PC dan laptop.
- Mempermudah untuk memberikan hak akses kepada vendor pada saat melakukan preventive maintenance.

2) Batasan Masalah

Adapun perumusan masalah yang ada antara lain:

- Membuat proses standarisasi IT Policy pada sisi end-user
- Memudahkan monitoring kunjungan vendor pada saat preventive maintenance

http://digilib.mercubuana.ac.id/

2. TINJAUAN PUSTAKA

Gambar 1. Cisco Identiy Services Engine

Cisco Identity Services Engine adalah solusi yang cocok untuk bagi perusahaan enterprise dalam menegakkan peraturan keamanan, meningkatkan keamanan infrastruktur, dan merampingkan operasi layanan karena memiliki kemampuan mengumpulkan informasi secara *real-time* dan secara proaktif menegakkan kebijakan *security* dalam infrastruktur jaringan. Secara umum, Cisco ISE menggabungkan layanan AAA (*Authentication Authorization,* dan *Accounting*), *posture*, *profilling* dan layanan manajemen *guest* dalam suatu *platform* tunggal. Administrator dapat secara terpusat membuat dan mengatur kebijakan akses kontrol terhadap pengguna dan perangkat jaringan. Selain itu, Cisco ISE dapat secara otomatis mengenali dan mengklasifikasi perangkat, hak akses user berdasarkan *profile*-nya dan kebijakan *security* yang harus dipenuhi oleh perangkat yang bersangkutan.

Cisco ISE Appliance mempunyai fitur-fitur sebagai berikut:

- Otentikasi dan Otorisasi terhadap pengguna endpoint sesuai dengan *group*-nya
- *Posture Assessment* adalah melakukan validasi endpoint terhadap sistem operasi yang digunakan service pack, hotfixes, versi antivirus, software security lain, registry, termasuk proses-proses yang boleh atau tidak boleh berjalan pada endpoint. Aturan-aturan dalam melakukan posture assessment bisa berbeda antara 1 group dengan group yang lainnya. Aturan untuk posture assessment, seperti hotfixes, service pack, versi antivirus, dapat diperbaharui secara otomatis dan reguler dari pihak Cisco.
- *Quarantine* adalah aturan sementara yang diberikan pada *endpoint* yang tidak memenuhi aturan kebijakan keamanan jaringan pada saat dilakukan *posture assessment*.
- *Automatic remediation* adalah kemampuan memberikan layanan penyembuhan secara otomatis terhadap *endpoint* yang tidak memenuhi aturan kebijakan keamanan jaringan yang ditetapkan, sebagai contoh pengguna endpoint dapat dibimbing langkah demi langkah agar dapat memnuhi kriteria posture assessment tanpa perlu membutuhkan pengetahuan khusus.

3. METHODOLOGI

1) Jenis Penelitian

Penelitian Murni TI, Penelitian jenis ini merupakan penelitian yang berusaha memecahkan permasalahan yang muncul terkait bidang TI dengan mencari solusi-solusi yang bersifat internal. Umumnya penelitian ini banyak berkecimpung mempelajari teori-teori yang ada untuk dapat mengembangkan teori-teori fundamental terkait lainnya.

2) Metode Pengumpulan Data

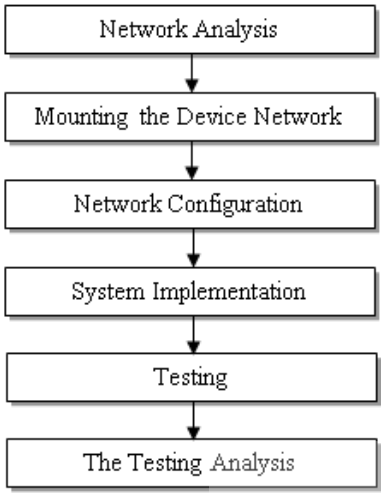
Metode pengumpulan data yang dipakai pada penelitian untuk aplikasi ini adalah metode studi literatur. Studi Literatur merupakan salah satu metode pengumpulan data dengan cara membaca buku-buku dan jurnal sesuai dengan data yang dibutuhkan. Pada penelitian ini penulis memilih studi literatur untuk mengumpulkan referensi dari jurnal-jurnal yang memiliki kemiripan dalam implementasi aplikasi ini dan dari buku putih dokumentasi project implementasi Cisco ISE di PT Lintasarta dan menggunakan mesin pencari google untuk mencari referensi.

3) Tahapan Penelitian

Tahap penelitian merupakan proses menentukan metode dan sistem yang akan berjalan serta

http://digilib.mercubuana.ac.id/

kebutuhan perangkat yang akan digunakan dalam membantu proses penelitian ini.



1) Instrumen Penelitian

Adapun instrumen penelitian yang digunakan dalam penelitan untuk simulasi yaitu :

a. Perangkat Keras

Perangkat keras yang digunakan untuk mengembangkan dan mengumpulkan data pada software ini adalah sebagai berikut:

Tabel 1 Spesifikasi Perangkat Simulasi Cisco ISE

Server VM (Demo)	Client
Dell Vostro	HP Probook
Intel Core i5 2,20GHz	Intel Core i5 2,20GHz
8GB RAM DDR3	8GB RAM DDR3L
500GB Hard Drive	1TB Hard Drive
Integrated Gigabit Ethernet	Integrated Gigabit Ethernet

Switch Cisco Catalyst 2960X Switch 8 Port Manageable[10].

Gambar 2. Switch Catalyst 3560 Series 8 Port

Cisco Catalyst switch 2960C memiliki fitur sebagai berikut:

- Extend a highly secure, intelligent, managed Cisco Catalyst infrastructure with a single Ethernet cable or fiber from the wiring closet.
- Support for advanced security and services, including voice, video, and Cisco Borderless Network services, to remote endpoints.
- Power over Ethernet (PoE) pass-though enables the compact switch to draw power from the wiring closet and pass it to end devces (selected models).
- Attractive, small form factor and fanless operation fit in confined spaces where multiple cable runs could be challenging.
- East to deploy, manage and extend the network loop free.
- Enhanced limited lifetime hardware warranty.

b. Perangkat Lunak

Adapun perangkat lunak yang digunakan dalam aplikasi ini adalah sebagai berikut :

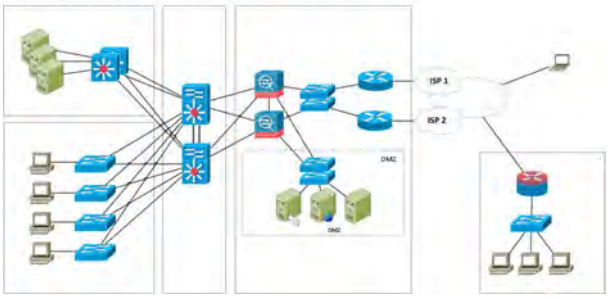
- Cisco ISE Version
- Cisco Any Connect Secure Mobility Agent
- IOS version 12.2(55) SE10
- VMware
- Windows 10 Pro

4. HASIL DAN DISKUSI

Tahapan analisis dan desain sistem berfokus pada menghasilkan sebuah desain menggunakan blok diagram untuk menggambarkan bagaimana cara kerja sistem keamanan jaringan akan dikembangkan secara garis besar.

Tahap awal untuk memperkuat sistem keamanan jaringan untuk IT Policy pada Lintasarta adalah dengan membuat standarisasi keamanan untuk setiap perangkat network dengan mengganti perangkat network pada Layer 2 yang sebelumnya menggunakan switch access unmanaged menjadi switch access managed dari Cisco yang sudah support untuk implementasi fitur dari ISE dan Otentikasi 802.1x..

http://digilib.mercubuana.ac.id/

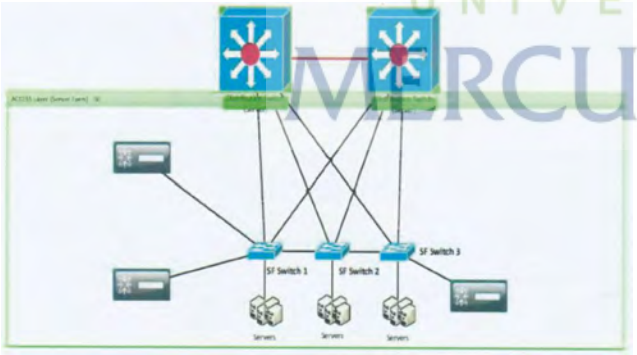


Gambar 3. Topologi Jaringan

Dari hasil analisa gambar topologi di atas dapat dilihat disisi akses hanya dari Access Control List dan pendistribusian dari firewall ke perangkat network yang lainnya. Karena kelemahan pada sistem Access Control List tidak adanya sistem yang mengatur atau manage dari perangkat network hingga ke devices user.

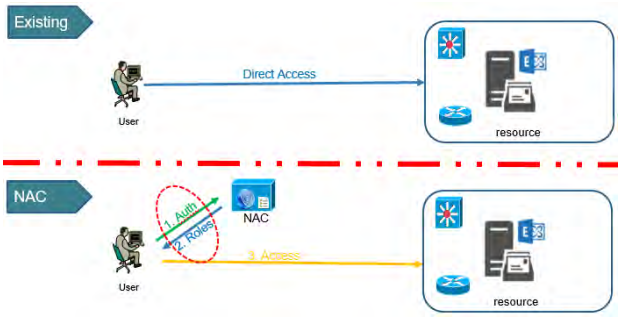
Dan untuk hasil analisa keamanan untuk dari sisi end-user tidak ada ada otentikasi lanjut, sedangkan firewall yang ada hanya untuk melindungi dari sisi internal dari eksternal. Dan untuk standarisasi pada setiap end-device user tidak terminitoring dengan baik.

Dengan menggunakan Network Access Control maka setiap perangkat network dan devices user akan termonitoring secara sistem. Untuk metode Network Access Control dari segi sisi topologi tidak ada yang berubah hanya saja ada pergantian perangkat hardware network dari switch access yang menuju ke end-user.



Gambar 4. Topologi Identity Services Engine (ISE)

Perencanaan Topologi untuk Development ISE setelah pemasangan dan penggantian perangkat network selesai kemudian dapat di implementasikan alur kerja sistem Network Access Manager pada Cisco ISE.

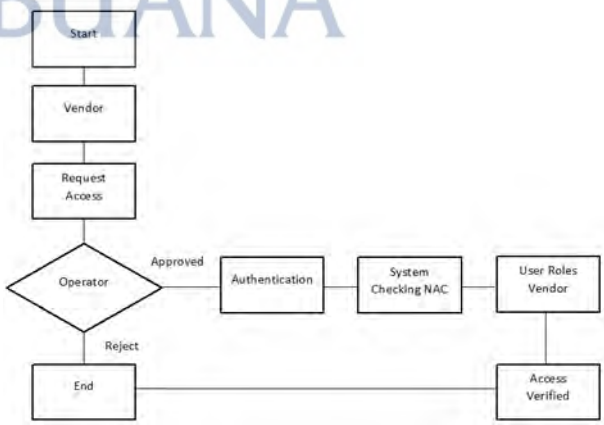


Gambar 5. Alur kerja sistem existing dan rencana Implementasi NAC ISE

Pada Gambar 5 dapat dilihat sistem keamanan yang bekerja melalui rangkaian proses yang cepat karena langsung bisa di akses, sedangkan pada saat sudah di integrasi dengan Network Access Control dapat dibagi ke dalam tiga proses utama, yakni :

1. Proses permintaan autentikasi pada saat ingin menghubungkan ke jaringan internet.
2. Proses pengecekan oleh sistem NAC, apakah user tersebut sudah terdaftar dalam system Active Directory atau tidak jika user tersebut terdaftar maka akan di berikan akses yang sesuai dengan role user tersebut.
3. Setelah proses kedua selesai, baru kemudian user mendapatkan hak aksesnya untuk menggunakan akses aplikasi maupun server, dan lainnya.

Untuk role user dengan vendor rangkaian kerjanya sama namun ada sedikit perbedaan dalam proses awal untuk mengakses jaringan internet :



Gambar 6. Flowchart Skema Sistem Role NAC ISE Untuk Vendor

Untuk Vendor perbedaannya ada di Operator, karena vendor bukan karyawan Lintasarta.

http://digilib.mercubuana.ac.id/

Biasanya vendor menggunakan jaringan Lintasarta untuk keperluan Preventive Maintenance dan gangguan, maka dari itu Karyawan yang bertanggung jawab atas vendor tersebut harus request ke Helpdesk IT untuk meminta akses jaringan.

Gambar 7. Role Sistem NAC ISE

Pada rangkaian di atas Network Access Control untuk vendor dapat dibagi ke dalam tiga proses utama, yakni :

1. Proses permintaan kepada operator atau helpdesk IT dengan mengirimkan email terlebih dulu ke itsupport@lintasarta.co.id .
2. Proses autentikasi ke dalam system NAC untuk persetujuan akses tersebut.
3. Proses pengecekan oleh sistem NAC, apakah user tersebut sudah terdaftar dalam system atau tidak jika user tersebut terdaftar maka akan di berikan akses yang sesuai dengan role user tersebut.

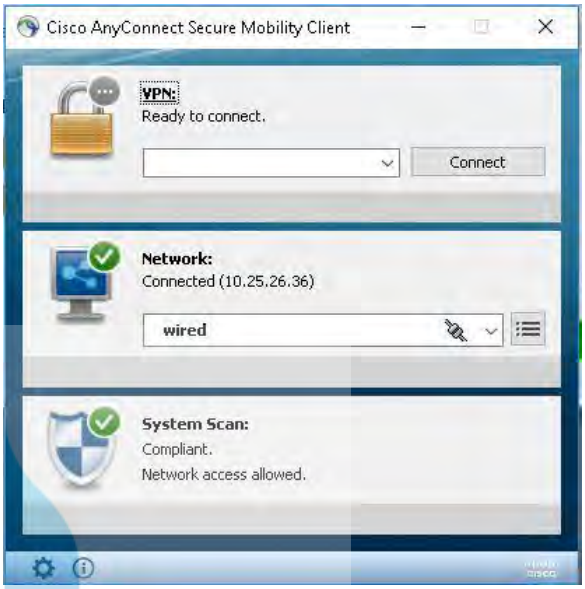
Setelah proses ketiga selesai, vendor mendapatkan hak aksesnya untuk menggunakan akses aplikasi maupun server, dan lainnya untuk keperluan preventive maintenance atau gangguan.

Implementasi Cisco AnyConnect pada sisi devices end-user, dibagian ini dijelaskan bagaimana requirement yang harus dipenuhi untuk instalasi Cisco AnyConnect dari awal hingga selesai dan terhubung dengan server Cisco ISE.

Berikut tahapan-tahapannya :

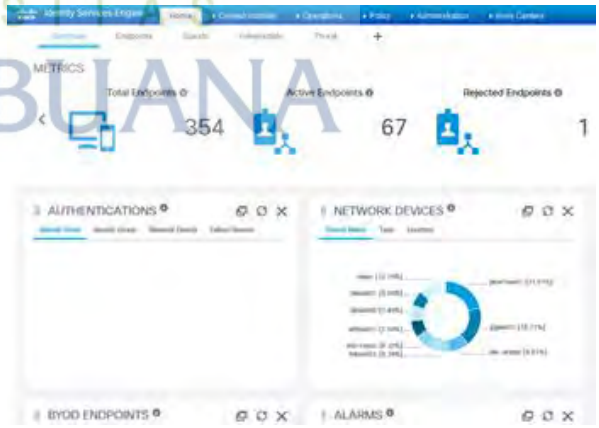
- Join Domain Lintasarta
- Install Software Standard IT
- Install Antivirus Standard IT
- Setting Services Wired Auto Config
- Setting Authentication pada Port LAN
- Lalu Install Cisco AnyConnect pada PC dan Laptop user

Hasil pengujian dilakukan pada satu PC user yang sudah di install Cisco AnyConnect.



Gambar 8. Cisco AnyConnect Secure Mobility Agent

Pada gambar 8 menggambarkan client Cisco AnyConnect, bahwa PC atau laptop tersebut sudah connect dengan network dan statusnya sudah compliant atau sudah terkoneksi dengan sistem ISE.

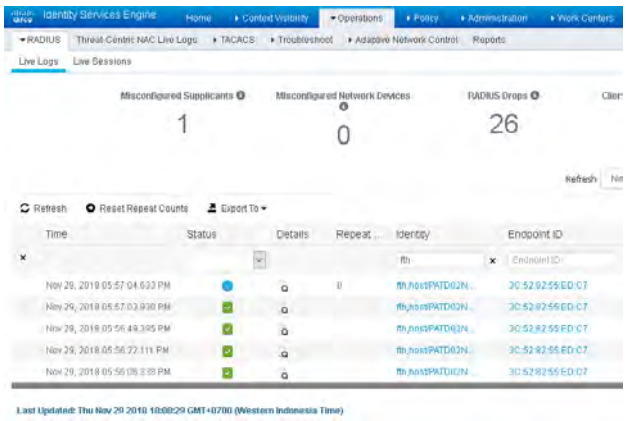


Gambar 9. Dashboard Cisco Identity Service Engine

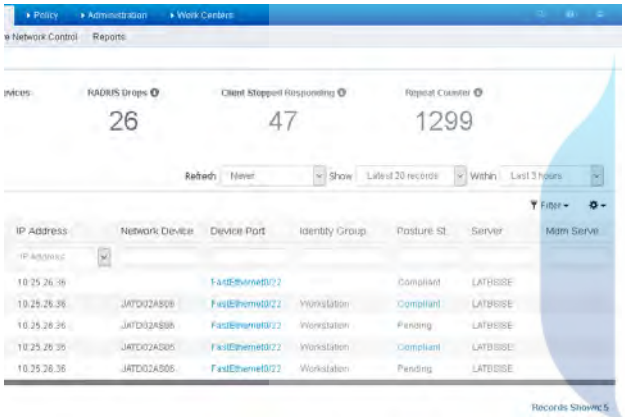
Dashboard Cisco ISE untuk menampilkan dan memonitoring live log dan live session dari setiap perangkat yang sudah terhubung dengan sistem Cisco ISE.

http://digilib.mercubuana.ac.id/

Dapat dilihat hasil autentikasi dari perangkat yang ada di Gambar 8.



Gambar 10. Live Log Monitoring (1/2)



Gambar 11. Live Log Monitoring (2/2)

Dari gambar Live Log di atas bisa di lihat untuk aktivitas dari yang awalnya devices tersebut terhubung dengan jaringan dan proses authentikasi dan sinkronasi dengan server hingga sampai compliant atau connected. Menandakan bahwa sistem Network Access Control dan dengan metode Network Access Manager berfungsi dengan baik untuk memonitoring setiap devices yang terhubung.

5. KESIMPULAN

Berdasarkan hasil percobaan yang telah dilakukan maka didapatkan kesimpulan antara lain:

1. Pada jaringan keamanan existing di dapat hasil berupa sistem keamanan menggunakan metode Access Control List yang dimana belum efisien dari sisi keamanan jaringan sistem pendistribusian akses switch ke setiap devices user. Dengan adanya metode Network Access Control memperbaharui cara sistem kerja keamanan jaringan menjadi lebih baik karena metode tersebut dapat memonitoring dengan baik setiap devices yang terhubung dan dengan metode tersebut bisa memenuhi syarat daripada IT Policy pada perusahaan tersebut.

2. Setelah melakukan implementasi Cisco AnyConnect pada setiap devices user maka bisa di dapatkan berapa total user yang sudah terstandarisasi dan terhubung dengan Cisco ISE. Dengan adanya sistem tersebut maka dapat memudahkan jika ada kunjungan tamu atau vendor yang ingin melakukan troubleshoot ataupun preventive maintenance.

DAFTAR PUSTAKA

[1] M. Syani dan A. M. Ropi, "ANALISIS DAN IMPLEMENTASI NETWORK SECURITY SYSTEM MENGGUNAKAN TEKNIK HOST-BASED INTRUSION DETECTION SYSTEM ANALISIS DAN IMPLEMENTASI NETWORK SECURITY SYSTEM MENGGUNAKAN TEKNIK HOST-BASED INTRUSION DETECTION SYSTEM (HIDS) BERBASIS CLOUD COMPUTING," no. August, 2018.

[2] E. Kusuma *et al.*, "Meningkatkan Keamanan Jaringan Dengan Menggunakan Model Proses Forensik," no. January 2016, 2017.

[3] D. Irawan, "Keamanan jaringan komputer dengan metode blocking port pada laboratorium komputer program diploma-iii sistem informasi universitas muhammadiyah metro," *Manaj. Inform. Progr. Diploma III UM Metro*, vol. 02, no. 05, hal. 1–9, 2015.

[4] Ertie Nur Hartiwati, "Keamanan Jaringan Dan Keamanan Sistem Komputer Yang Mempengaruhi Kualitas Pelayanan Warnet," hal. 27–33, 2014.

[5] B. Heru dan W. Hento, "Keamanan jaringan menggunakan," hal. 48–59.

[6] M. S. Ma'sum, M. A. Irwansyah, dan H. Priyanto, "Analisis perbandingan sistem keamanan jaringan menggunakan snort dan," *J. Sist. dan Teknol. Inf.*, vol. 1, no. 2, hal. 1–5, 2017.

[7] M. Ariq Istiqlal, L. O. Sari, dan I. T. Ali, "Perancangan Sistem Keamanan Jaringan

http://digilib.mercubuana.ac.id/

TCP/IP Berbasis Virtual LAN dan Access Control List," *Jom FTEKNIK*, vol. 3, no. 1, hal. 1–9, 2016.

[8] B. Triandi, "Sistem Keamanan Jaringan Dalam Mencegah Flooding Data Dengan Metode Blocking IP Dan Port," *Semin. Nas. Teknol. Inf. dan Multimed.*, hal. 6–8, 2015.

[9] R. Muzawi, "Aplikasi Pengendalian Port dengan Utilitas Port Knocking untuk Optimalisasi Sistem Keamanan Jaringan Komputer," *SATIN - Sains dan Teknol. Inf.*, vol. 2, no. 1, hal. 52–58, 2016.

[10] O. K. Sulaiman, "Analisis Sistem Keamanan Jaringan Dengan Menggunakan Switch Port Security," *Jar. Komput.*, vol. 1, no. 1, hal. 9–14, 2016.

UNIVERSITAS
MERCU BUANA

http://digilib.mercubuana.ac.id/