

IMPLEMENTASI MANAGEMENT NETWORK SECURITY PADA LABORATORIUM CISCO UNIVERSITAS BINA DARMA

Edi Surya Negara
Dosen Universitas Bina Darma
Jalan Jenderal Ahmad Yani No.12, Palembang
Sur-el: e.s.negara@mail.binadarma.ac.id

Abstract: *The development of computer network technology as a medium for data communications to this increase. The need for the use of shared resources on the network both software and hardware has resulted in the emergence of a variety of network technology development itself. Along with the high level of need and the increasing number of network users who want some form of network that can deliver maximum results, in terms of both efficiency and increase network security itself, the improvement efforts continue to be made by the various parties. One measure of the quality of the computer network management and network security is good. By it because they needed a real action to create a system management and network security is good. So with the management and security of the network that will either guide to good computer network.*

Keywords: *Computer Networks, Network Management, and Network Security.*

Abstrak: *Perkembangan teknologi jaringan komputer sebagai media komunikasi data hingga saat ini semakin meningkat. Kebutuhan atas penggunaan bersama resources yang ada dalam jaringan baik software maupun hardware telah mengakibatkan timbulnya berbagai pengembangan teknologi jaringan itu sendiri. Seiring dengan semakin tingginya tingkat kebutuhan dan semakin banyaknya pengguna jaringan yang menginginkan suatu bentuk jaringan yang dapat memberikan hasil maksimal, baik dari segi efisiensi maupun peningkatan keamanan jaringan itu sendiri, maka upaya-upaya penyempurnaan terus dilakukan oleh berbagai pihak. Salah satu tolak ukur dari jaringan komputer yang berkualitas adalah management dan keamanan jaringan yang baik. Oleh karena itu dibutuhkan suatu tindak nyata untuk membuat suatu sistem management dan pengamanan jaringan yang baik. Sehingga dengan adanya management dan keamanan jaringan yang baik akan menciptakan jaringan komputer yang berkualitas.*

Kata kunci: *Jaringan Komputer, Management Jaringan, dan Keamanan Jaringan*

1. PENDAHULUAN

Perkembangan teknologi jaringan komputer telah merubah cara interaksi sosial, komersial, politik, dan pribadi mengikuti evolusi jaringan komputer secara global. Salah satu bentuk nyata evolusi jaringan komputer itu adalah perkembangan jaringan *internet*. Meningkatnya penggunaan *internet* di dunia bisnis mendorong semakin berkembang dan beragam *content-content* di *internet*.

Pada saat sebuah badan usaha atau instansi baik pemerintah atau swasta

mengintegrasikan jaringannya ke jaringan publik atau yang lebih kita kenal dengan istilah *internet*, maka akan timbul suatu masalah baru yang sangat mengancam yaitu masalah keamanan jaringan atau sering disebut dengan *network security*. Ancaman keamanan ini banyak sekali ditemukan oleh pengguna seperti *Virus, Trojan, Worm, DoS, Hacker, Sniffing* dan sebagainya dengan apapun istilah *underground* yang sering kita dengar, yang pasti akan menyusahkan kita pada saat ancaman-ancaman ini menyerang sistem kita. Semakin besar skala suatu jaringan maka semakin kompleks administrasi dari

jaringan itu, oleh karena itu diperlukan suatu mekanisme keamanan dan metode untuk dapat mengoptimalkan sumber daya jaringan tersebut.

Sejalan dengan hal di atas, Universitas Bina Darma telah memiliki sistem jaringan komputer yang telah diimplementasikan di masing-masing unit kerja. Seperti sistem jaringan komputer di pusat pengolahan data, atau jaringan komputer di masing-masing laboratorium. Jaringan komputer yang telah diimplementasikan dengan baik di Universitas Bina Darma harus memiliki sistem keamanan yang baik untuk dapat melindungi seluruh data dan informasi penting yang selalu dicari oleh pihak-pihak yang ingin mencoba menyusup atau bahkan merusak sistem informasi dan jaringan komputer Universitas Bina Darma.

Menurut Howard dalam Sofana (2010) dalam buku yang berjudul *CISCO CCNA & Jaringan Komputer mengemukakan tentang computer security*. “ *Computer security is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks.*” (Howard dan Weaver, “*An Analysis Of Security Incidents On The Internet 1989 – 1995*)”.

Menurut Garfinkel (1995) keamanan komputer mencakup empat aspek yaitu, *privacy, integrity, authentication, dan availability*.

1) *Privacy* atau *confidentiality*. *Privacy* mencakup kerahasiaan informasi. Inti aspek *privacy* adalah bagaimana menjaga informasi agar tidak dilihat atau diakses oleh orang yang tidak berhak. Sebagai contoh, *e-mail* seorang pemakai tidak boleh dibaca orang lain bahkan administrator. Salah satu usaha yang dapat dilakukan yaitu penggunaan

enkripsi. Kita dapat menggunakan enkripsi untuk setiap dokumen atau informasi lainnya yang dianggap rahasia dan hanya kita sendiri yang dapat membukanya menggunakan kunci yang tepat.

2) *Integrity*. *Integrity* atau integritas mencakup keutuhan informasi. Inti aspek *integrity* ini adalah bagaimana menjaga informasi agar tetap utuh. Informasi tidak boleh diubah, baik ditambah atau pun dikurangi, kecuali jika mendapat izin dari pemilik informasi. *Virus, Trojan horse*, atau pemakai lain yang mengubah informasi tanpa izin pemiliknya merupakan contoh masalah yang mengganggu aspek ini. Penggunaan anti virus, enkripsi, dan *digital signature*, merupakan contoh usaha untuk mengatasi masalah ini.

3) *Authentication*. *Authentication* atau otentikasi berkaitan dengan keabsahan pemilik informasi. Harus ada cara untuk mengetahui bahwa informasi benar-benar asli, kemudian yang mengakses informasi adalah orang-orang yang berhak, dan hanya yang berhak saja yang boleh memberikan informasi tersebut kepada orang lain. Penggunaan *access control* seperti *login* dan *password* merupakan usaha yang dilakukan untuk memenuhi aspek ini. *Digital signature* dan *watermarking* juga merupakan salah satu usaha untuk melindungi *intellectual property* yang sesuai dengan aspek *authentication*.

4) *Availability*. Aspek ini berhubungan dengan ketersediaan informasi. Informasi harus tersedia manakala dibutuhkan. Contoh serangan terhadap aspek ini yaitu “*Denial of*

Service attack“ atau *DoS attack*. Misalkan, *server* dikirim *request* palsu secara bertubi-tubi sehingga tidak dapat melayani permintaan lain. Contoh lain yaitu *mailbomb*, dimana seorang pemakai dikirim ribuan bahkan jutaan *e-mail* sehingga pemakai tidak dapat membuka *e-mail* miliknya atau kesulitan mengakses *e-mail*, terutama jika akses *internet* dilakukan melalui saluran telephon.

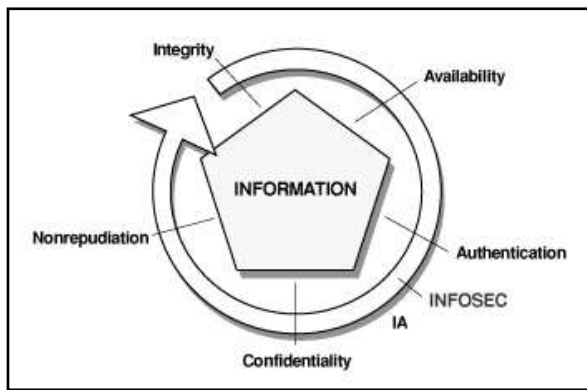
Management network security pada Universitas Bina Darma sebagian besar sudah diimplementasikan dengan baik. Akan tetapi akan lebih baik lagi apabila seluruh bagian terkecil dari jaringan Universitas Bina Darma diimplementasikan *management network security*, khususnya jaringan *intranet* yang akan menuju jaringan *internet* (dari *internal network* ke *external network*) sehingga akan membantu kinerja *server* yang telah ada di unit kerja MIS_CUT dalam pengamanan *network*.

Salah satu bagian dari jaringan komputer tersebut adalah laboratorium komputer. Laboratorium merupakan salah satu pintu masuk pihak-pihak yang tidak bertanggung jawab untuk merusak jaringan Universitas Bina Darma. Sehingga dibutuhkan mekanisme pengamanan yang nyata pada seluruh laboratorium komputer Universitas Bina Darma. Oleh sebab itu penulis bermaksud untuk mengimplementasikan *management network security* pada salah satu laboratorium komputer di Universitas Bina Darma dengan memanfaatkan berbagai sumber daya jaringan yang ada di laboratorium CISCO seperti *Router Cisco 2600 series* dan *Switch Catalyst 2950*. Adapun judul penelitian ini adalah “*Implementasi Management Network*

Security Pada Laboratorium CISCO Universitas Bina Darma”.

Penelitian ini bertujuan untuk mengimplementasikan *managemet network security* pada laboratorium CISCO Universitas Bina Darma agar keamanan jaringan pada laboratorium tersebut semakin meningkat dan meminimalisir ancaman-ancaman keamanan jaringan pada Universitas Bina Darma serta mengevaluasi secara singkat dampak dari implementasi.

Keamanan Informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis (*business continuity*), meminimasi risiko bisnis (*reduce business risk*) dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis (ISO 27001 dalam Sarno dan Iffano (2009). Menurut Syafrizal, M, (2007) Keamanan informasi terdiri dari perlindungan terhadap aspek-aspek berikut: 1) *Confidentiality* (kerahasiaan) aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.; 2) *Integrity* (integritas) aspek yang menjamin bahwa data tidak dirubah tanpa ada ijin pihak yang berwenang (*authorized*), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek *integrity* ini.; 3) *Availability* (ketersediaan) aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana diperlukan).



Gambar 1. Information Assurance Model

Target *network security* adalah bagaimana mencegah dan menghentikan berbagai *threats* (potensi serangan) agar tidak memasuki dan menyebar pada suatu *network* (Sofana 2010). Pada dasarnya banyak *threats* (potensi serangan) yang mengancam *network security*, seperti yang telah dipaparkan oleh Sofana dalam bukunya yang berjudul *Cisco CCNA & Jaringan Komputer* (2010) berbagai *threats* yang mengancam *network security* dapat digolongkan menjadi beberapa golongan, diantaranya adalah: 1) *Viruses, Worms, and Trojan horses*; 2) *Spyware and adware*; 3) *Zero-day attacks (zero-hour) attacks*; 4) *Hacker attacks*; 5) *Denial of service attacks (DoS)*; 6) *Data interception and theft*; 7) *Identity theft*.

Implementasi *Management Network Security* pada Laboratorium CISCO Universitas Bina Darma meliputi aspek-aspek sebagai berikut: 1) Implementasi *Access Control* pada seluruh komputer *client* yang ada di laboratorium CISCO Universitas Bina Darma.; 2) Implementasi dan konfigurasi *Network Address Translation (NAT)* pada Router Cisco 2600 series.; 3) Implementasi dan konfigurasi *Virtual Local Area Network (VLAN)* pada Router Cisco 2600 series dan implementasi Metode Variabel

Length Subnet Mask (VLSM) untuk penghematan *host*.; 4) Implementasi dan konfigurasi sistem keamanan pada Router Cisco 2600 series dan Switch Cisco Catalyst 2960 antara lain: membatasi Control Access ke Router dan Switch, Membatasi *access telnet* ke Router dan Switch, *Block spoof /* paket-paket berbahaya, seperti *block traffic virus* pada Router Cisco 2600 series, membatasi *Simple Network Management Protocol (SNMP)* pada Router Cisco 2600 series, mengenskripsi semua *password* pada Router dan Switch, menonaktifkan semua layanan yang tidak digunakan, membuat *LOG* pada Router Cisco 2600 series untuk mencatat seluruh kegiatan *router*.

2. METODOLOGI PENELITIAN

Metodologi adalah ilmu yang digunakan untuk memperoleh kebenaran menggunakan penelusuran dengan tatacara tertentu dalam menemukan kebenaran, tergantung dari realitas yang sedang dikaji. Dalam penelitian ini metode yang digunakan adalah penelitian tindakan atau *action research*, dalam penelitian tindakan mendeskripsikan, menginterpretasi dan menjelaskan suatu situasi pada waktu yang bersamaan dengan melakukan perubahan atau intervensi dengan tujuan perbaikan atau partisipasi.

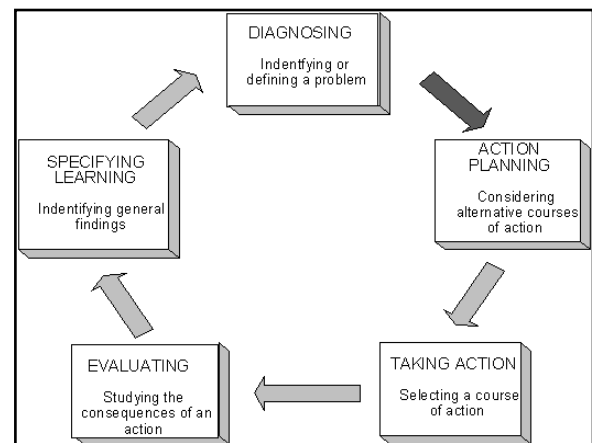
Menurut Davison, Martinson & Kock (2004), menyebutkan penelitian tindakan sebagai metode penelitian, didirikan atas asumsi bahwa teori dan praktek dapat secara tertutup diintegrasikan dengan pembelajaran dari hasil intervensi yang direncanakan setelah diagnosis

yang rinci terhadap konteks masalahnya. 5 tahapan yang merupakan siklus dari *action research*:

- 1) Melakukan *diagnose* (*Diagnosing*). Melakukan identifikasi masalah-masalah pokok yang ada guna menjadi dasar kelompok atau organisasi sehingga terjadi perubahan.
- 2) Membuat rencana tindakan (*Action Planning*). Penelitian dan partisipan bersama-sama memahami pokok masalah yang ada kemudian dilanjutkan dengan menyusun rencana tindakan yang tepat untuk menyelesaikan masalah yang ada.
- 3) Melakukan tindakan (*Action Taking*). Peneliti dan partisipan bersama-sama mengimplementasikan rencana tindakan dengan harapan dapat menyelesaikan masalah.
- 4) Melakukan evaluasi (*Evaluating*). Setelah masa implementasi (*action taking*) dianggap cukup kemudian peneliti bersama partisipan melaksanakan evaluasi hasil dari implementasi.
- 5) Pembelajaran (*Learning*). Tahap ini merupakan bagian akhir siklus yang telah dilalui dengan melaksanakan *review* tahap pertahap yang telah berakhir kemudian penelitian ini dapat berakhir.

Seluruh kriteria dalam prinsip pembelajaran harus dipelajari, perubahan dalam situasi organisasi dievaluasi oleh peneliti dan dikomunikasikan kepada *client*, peneliti dan *client* merefleksikan terhadap hasil proyek, yang nampak akan dilaporkan secara lengkap dan hasilnya secara eksplisit dipertimbangkan dalam hal implikasinya terhadap penerapan *Canonical*

Action Research (CAR). Untuk hal tertentu, hasilnya dipertimbangkan dalam hal implikasinya untuk tindakan berikutnya dalam situasi organisasi lebih-lebih kesulitan yang dapat dikaitkan dengan pengimplementasian perubahan proses.



Gambar 2. Action Research Mode

3. HASIL DAN PEMBAHASAN

3.1 Analisis Kebutuhan Perangkat Keras (*Hardware*)

Perangkat keras yang dibutuhkan untuk mengimplementasikan *management network security* pada laboratorium CISCO Universitas Bina Darma antara lain: *Cisco Router 2600 Series, Switch Cisco Catalyst 2950, Switch D-link 16 Port, Personal Computer*.

3.2 Analisis Kebutuhan Perangkat Lunak (*Software*)

Kebutuhan perangkat lunak: 1) *Microsoft Windows XP SP-2* dan *Ubuntu 10.04* sebagai

sistem operasi *client*; 2) *Cisco Internetwork Operating System Software (IOS) version 12.0(5)T1 (Router 2600 series)*; 3) *Cisco Internetwork Operating System Software (IOS) version 12.1(22)EAI (Switch catalyst 2950)*.

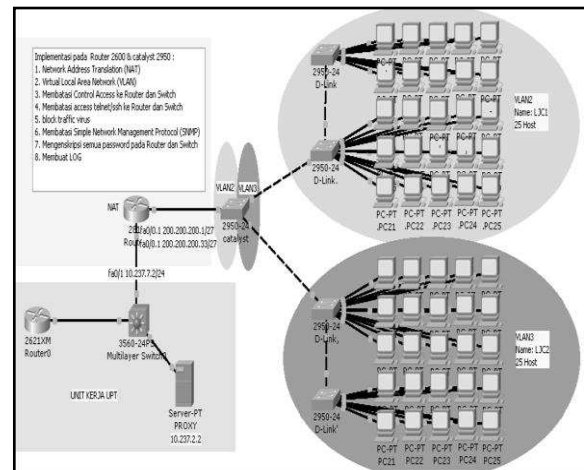
3.3 Perancangan *Management Network Security* Pada Laboratorium CISCO

Analisis yang dilakukan terhadap peta jaringan laboratorium CISCO menghasilkan beberapa rancangan pengembangan. Salah satu rancangan pengembangan yang akan diimplementasikan adalah pengembangan *management network security laboratorium CISCO*. Rancangan pengembangan ini bertujuan untuk meningkatkan keamanan *network* pada laboratorium tersebut, sehingga nantinya diharapkan dapat membantu kinerja *firewall* yang telah diimplementasi pada unit pelayanan teknis (UPT). Disamping itu implementasi ini diharapkan memberikan efek yang baik untuk peningkatan proses belajar mengajar pada laboratorium CISCO. Pengembangan yang akan dilakukan antara lain adalah:

- 1) Pengembangan *network topologi* dengan menggunakan *Cisco Router 2600 series* dan *Switch catalyst 2950*.
- 2) *Implementasi Access Control* pada seluruh komputer *client* yang ada di laboratorium CISCO Universitas Bina Darma.
- 3) Implementasi dan konfigurasi *Network Address Translation (NAT)* pada *Router Cisco 2600 series*.
- 4) Implementasi dan konfigurasi *Virtual Local Area Network (VLAN)* pada *Router Cisco*

2600 series dan implementasi *Metode Variabel Length Subnet Mask (VLSM)* untuk penghematan host.

- 5) Implementasi dan konfigurasi sistem keamanan pada *Router Cisco 2600 series* dan *Switch Cisco Catalyst 2960*.



Gambar 3. Rancangan Implementasi *Management Network Security* pada Laboratorium CISCO

Untuk menerapkan *Management Network Security* pada jaringan computer laboratorium CISCO ada beberapa tahapan yang harus konfigurasi. Tahapan-tahapan tersebut antara lain:

- 1) Konfigurasi *Hostname, Line Console, Line VTY* serta *Banner* dan mengenskripsi semua *password*.
- 2) Konfigurasi *Network Address Translation (NAT)*.
- 3) Konfigurasi *Virtual Local Area Network (VLAN)*.
- 4) Konfigurasi *Control Access* ke *Router* dan *Switch*.
- 5) Membatasi *access telnet* ke *Router* dan *Switch*.
- 6) *Block traffic virus*.

Semakin tinggi kualitas jaringan komputer yang ada di laboratorium CISCO maka akan semakin aman user dalam menggunakan komputer client. Penggunaan *Ubuntu* 10.10 mampu meminimalisir ancaman keamanan yang ada di laboratorium CISCO khususnya dari serangan virus-virus jaringan.

Implementasi *Network Address Translation* pada laboratorium CISCO Universitas Bina Darma adalah untuk menghubungkan jaringan *virtual local area network* dengan menggunakan IP Address private pada laboratorium CISCO terhadap jaringan *public*. Sehingga seluruh komputer *client* yang ada di jaringan laboratorium CISCO bisa mengakses jaringan internet. Ide utama dari penggunaan NAT ini adalah untuk menghemat alamat global internet dan untuk meningkatkan keamanan jaringan dengan menyembunyikan alamat IP internal dari luar.

Konfigurasi *Network Address Translation* telah dilakukan pada *Cisco Router 2600 Series* sehingga seluruh komputer *client* yang menggunakan *IP Address private* dapat di *route* ke jaringan *outside*. Selanjutnya konfigurasi dilakukan pada komputer *client* dengan mengkonfigurasi *IP Address* client dengan menggunakan *IP Address* 200.200.200. 2 *Subnet Mask* 255.255.255.224.

Pembatasan control access ke *Cisco Router 2600 Series* dan *Switch Catalyst 2950* telah dikonfigurasi di masing-masing *device*. Sehingga untuk melakukan *remote* ke *Cisco Router 2600 Series* dan *Switch Catalyst 2950* harus telah memiliki *username* dan *password* yang telah didaftarkan pada *Cisco Router 2600 Series* dan *Switch Catalyst 2950*. Ini merupakan

salah satu *manajement network security* yang telah diimplementasikan pada laboratorium CISCO dengan memanfaatkan *authentication authorized account (AAA)*. Pembatasan akses *telnet* ke *Cisco Router 2600 Series* dan *Switch Catalyst 2950* telah diimplementasikan, di mana terdapat beberapa *IP Address* saja yang bisa melakukan *telnet* ke *Cisco Router 2600 Series* dan *Switch Catalyst 2950*. Selain dari itu seluruh *IP Address* *deny* untuk melakukan *telnet* ke *Cisco Router 2600 Series* dan *Switch Catalyst 2950*.

Dari implementasi ini diharapkan akan maningkatkan keamanan terhadap akses yang dilakukan ke *Cisco Router 2600 Series* dan *Switch Catalyst 2950*. Di bawah ini adalah gambar akses ke *router* dan *switch* dengan menggunakan *username* edi.

Blocking terhadap *traffic virus* telah dilakukan pada *Cisco Router 2600 Series*. Salah satu jenis virus jaringan adalah *virus blaster*. Virus ini menggunakan *TCP port 135*, virus ini dapat memenuhi jaringan dan menyebabkan aplikasi di jaringan menjadi lambat atau bahkan hang. Paket ini akan terus memenuhi jaringan walaupun kondisi komputer sedang tidak melakukan aktivitas. Selain itu jenis virus blaster yang lain menggunakan *TCP port 445*, 139 dan *UDP port 137* ada juga yang menggunakan port 138. Dibawah ini adalah gambar *LOG Cisco Router 2600* yang sedang melakukan *filtering* terhadap *port-port* yang biasa digunakan oleh virus.

Seluruh *password* yang telah dikonfigurasi pada *Cisco Router 2600 Series* dan *Switch Catalyst 2950* telah dienskripsi. Ini bertujuan untuk lebih meningkatkan keamanan pada *Cisco*

Router 2600 Series dan *Switch Catalyst 2950*.

4. SIMPULAN

Kesimpulan yang didapat dari penelitian implementasi *management network security* dengan memanfaatkan Cisco Router 2600 Series dan Switch Catalyst 2950 untuk meningkatkan keamanan *network* pada laboratorium CISCO adalah:

- 1) *Cisco Router 2600 Series* mampu mentranslasikan komputer *client* yang ada di laboratorium dengan menggunakan alamat *private* ke jaringan *public* dengan menggunakan *Network Address Translation*.
- 2) *Cisco Router 2600 Series* dan *Switch Catalyst 2950* mampu melakukan *management* terhadap *network* dengan menggunakan *virtual local area network*.
- 3) *Cisco Router 2600 Series* mampu melakukan *filter traffic* terhadap *packet-packet* yang tidak diinginkan seperti *packet virus* dan lain-lain.
- 4) Implementasi *Management Network Security* pada laboratorium CISCO meningkatkan keamanan *network* pada laboratorium CISCO Universitas Bina Darma.

DAFTAR RUJUKAN

- Davison, R.M., Martinsons, M.G., Kock, N. 2004. *Principels of Canonical Action reserch*. Info Systems J. 14, 65–86.
- Howard, J. dan Waver, G. 1995. *An Analisis of Security Incidents on the Internet*. Software Engineering Institute.
- Garfinkel, S. 1995. *PGP: Pretty Good Privacy*. O'Reilly & Associ-ates.
- Sarno, R. dan Iffano, I. 2009. *Sistem Manajemen Keamanan Informasi*. ITS Press. Surabaya.
- Syafrizal, M. 2007. *Information Security Management System (ISMS) Menggunakan Standar isofiec 27001:2005*.
- Sofana. I. 2010. *CISCO CCNA & Jaringan Komputer*. Informatika. Bandung.