BUKU AJAR

TEKNIK ELEKTRO

SRI HARTANTO

KEAMANAN DAN KEHANDALAN JARINGAN

PENERBIT CV. MITRA ILMU

IKAPI
IKATAN PENERBIT INDONESIA
No. 041/SSL/I022

BUKU AJAR TEKNIK ELEKTRO

KEAMANAN DAN KEHANDALAN JARINGAN

BUKU AJAR TEKNIK ELEKTRO

KEAMANAN DAN KEHANDALAN JARINGAN

SRI HARTANTO

PENERBIT
CV MITRA ILMU
MAKASSAR
Anggota IKAPI No. 041/SSL/2022

Perpustakaan Nasional: Katalog Dalam Terbitan (KDT)

Sri Hartanto

Keamanan dan Kehandalan Jaringan/Sri Hartanto.
—Ed. 1, Cet. 1.—Makassar: Penerbit CV Mitra Ilmu, 2023.
viii, 140 hlm., 21 cm.
Bibliografi: hlm. 141
ISBN 978-623-145-089-0

2023.0519 SRI
Sri Hartanto

KEAMANAN DAN KEHANDALAN JARINGAN

Cetakan ke-1, Mei 2023

Editor : Ujang Wiharja
Setter : Sri Hartanto
Desain Cover : Sulaiman

Dicetak di Gilby Jaya Printing

PENERBIT CV MITRA ILMU

Anggota IKAPI

Kantor Pusat:
Jl. Kesatuan 3 No. 11 Kelurahan Maccini Parang
Kecamatan Makassar Kota Makassar 90144
Telpon : 081342345219
E-mail : mitrailmu@mitrailmumakasaar.com
http: //www. mitrailmumakasaar.com

KATA PENGANTAR

Alhamdulillahi robbil ‘alamiin.

Segala puji syukur dipanjatkan ke hadirat ALLAH SWT atas segala petunjuk, rahmat dan hidayah-Nya sehingga dapat disusun Buku Ajar Keamanan dan Kehandalan Jaringan ini sebagai bahan pembelajaran bagi mahasiswa yang mengikuti perkuliahan Keamanan dan Kehandalan Jaringan.

Tidak ada gading yang tidak retak, maka diharapkan saran dan masukan dari pembaca untuk perbaikan buku ini ke depannya. Diharapkan, buku ajar ini dapat bermanfaat bagi mahasiswa yang mempelajari dan mengikuti perkuliahan Keamanan dan Kehandalan Jaringan. Selain itu, buku ini juga ditujukan untuk memenuhi Tri Dharma Perguruan Tinggi dalam menyediakan Buku Ajar untuk Program Studi Teknik Elektro, khususnya untuk mata kuliah Keamanan dan Kehandalan Jaringan.

Terimakasih disampaikan kepada semua pihak yang telah membantu dalam penyusunan buku ini, baik pimpinan, karyawan maupun mahasiswa sehingga buku ini dapat diselesaikan dengan baik dan dapat diterbitkan.

Penyusun,

Sri Hartanto

DAFTAR ISI

BAB I
KONSEP DASAR

1.1. Pemahaman Keamanan dan Kehandalan Jaringan

Keamanan jaringan telekomunikasi adalah keamanan yang berkaitan dengan perlindungan jaringan telekomunikasi yang meliputi semua perangkat yang digunakan untuk melaksanakan komunikasi. Keamanan jaringan telekomunikasi bertujuan untuk mencegah kemungkinan terjadinya ancaman atau gangguan terhadap jalannya komunikasi (*preventive*). Selain itu, keamanan jaringan telekomunikasi juga meliputi pendeteksian dan perbaikan jaringan terhadap kemungkinan ancaman yang memasuki jaringan telekomunikasi (*detection and post attack recovery*).

Kehandalan jaringan telekomunikasi adalah bagian yang tidak terpisahkan dari keamanan jaringan telekomunikasi. Kehandalan jaringan telekomunikasi adalah kemampuan jaringan telekomunikasi untuk menyediakan layanan informasi dan komunikasi ke pengguna tanpa adanya gangguan baik dari sistem itu sendiri maupun gangguan karena faktor di luar sistem. Dengan terjaminnya kehandalan jaringan telekomunikasi, maka semua perangkat komunikasi yang digunakan dapat bekerja dengan baik dan memberikan tingkat kualitas layanan/*Quality of Service* (QoS) yang tinggi.

Keamanan jaringan telekomunikasi dapat diklasifikasikan menjadi:

1. Keamanan bersifat fisik (*physical security*), yang meliputi akses orang ke gedung, peralatan, dan media yang

BAB II
KRIPTOGRAFI DAN STEGANOGRAFI

2.1. Metode Pengamanan Informasi

Untuk mengelola suatu jaringan telekomunikasi, perlu memperhatikan aspek pengamanan informasi (*information security*), dimana informasi hanya dapat diakses oleh pengelola (pembuat) informasi serta pihak-pihak yang diberi hak untuk mengaksesnya. Selain itu, perlu juga diperhatikan aspek perolehan informasi (*information intellegence*), sehingga hanya pihak-pihak yang memiliki hak akses informasi yang dapat mengetahui dan mencari keberadaan informasi tersebut. Metode pengamanan informasi dapat dibedakan atas Steganografi (*Steganography*) dan Kriptografi (*Cryptography*).

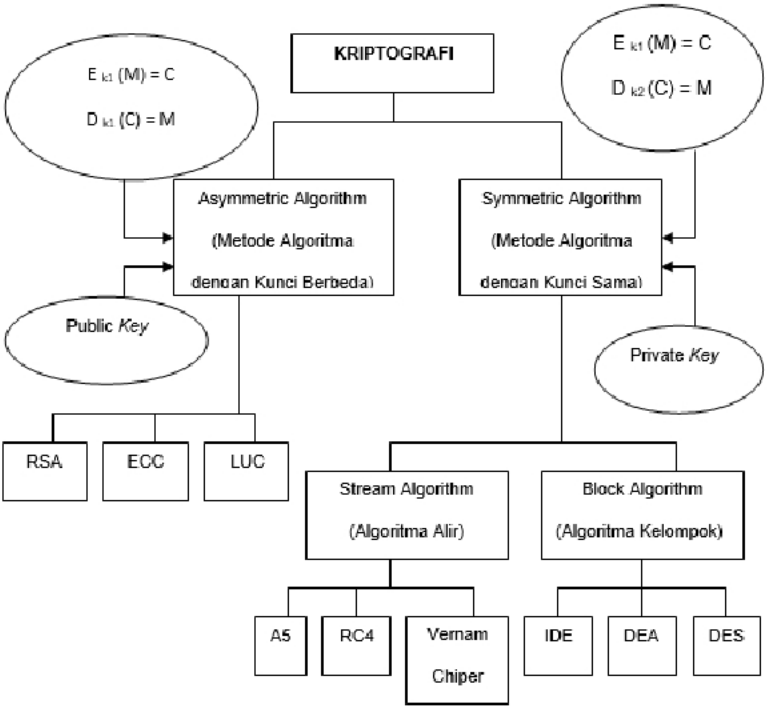
Steganografi (*Steganography*) adalah metode untuk membuat informasi sulit ditemukan, dengan menyembunyikan suatu informasi sehingga menjadi tidak terlihat (tidak dapat diakses). *Steganography* berasal dari bahasa Yunani, yaitu dari kata *stegano*, yang berarti tersembunyi dan *graphein*, yang berarti gambar yang mengandung pengertian tertentu (tulisan), sehingga steganografi didefinisikan secara lengkap sebagai metode untuk menyembunyikan tulisan (informasi). Dalam penerapannya, meskipun informasi berada pada media penyimpanan atau media transmisi yang dapat dikases, tetapi pihak lain tidak dapat menemukan dengan mudah informasi tersebut (*intelligence access*).

Kriptografi (*Cryptography*) adalah metode untuk membuat informasi yang dapat ditemukan (dapat diakses)

BAB III
KUNCI ENKRIPSI DAN DEKRIPSI

3.1. Klasifikasi Kunci Enkripsi dan Dekripsi

Klasifikasi kunci enkripsi dan dekripsi diperlihatkan dalam Gambar 3.1. berikut.



Gambar 3.1. Klasifikasi Kunci Enkripsi dan Dekripsi

Kunci enkripsi dan dekripsi dapat digolongkan atas dua

BAB IV
EVALUASI KEAMANAN JARINGAN

4.1. Deteksi Probing

Meskipun suatu jaringan telekomunikasi sudah dirancang memiliki perangkat pengamanan, dalam operasinya, keamanan jaringan telekomunikasi harus selalu dimonitor, karena:

1. Dapat ditemukannya lubang keamanan jaringan telekomunikasi (*security hole*) yang baru.
2. Kesalahan konfigurasi.
3. Penambahan perangkat baru (perangkat keras dan/atau perangkat lunak) yang menyebabkan menurunnya tingkat keamanan atau berubahnya metoda untuk mengoperasikan sistem.

Lubang keamanan jaringan telekomunikasi (*security hole*) dapat terjadi karena beberapa hal; seperti: kesalahan dalam perancangan, kesalahan dalam implementasi, kesalahan konfigurasi, dan kesalahan penggunaan. Administrator jaringan telekomunikasi membutuhkan perangkat bantu otomatis, yang dapat membantu menguji atau mengevaluasi keamanan jaringan telekomunikasi yang dikelola.

Layanan di internet umumnya dilakukan dengan menggunakan protokol TCP atau UDP. Setiap layanan dijalankan dengan menggunakan *port* yang berbeda, misalnya:

1. SMTP, untuk mengirim dan menerima *email* (TCP *port* 25),
2. DNS, untuk domain (UDP dan TCP *port* 53),
3. HTTP, untuk web *server* (TCP *port* 80),

BAB V
KEAMANAN JARINGAN BERBASIS SERVER

5.1. Pengaturan Akses Layanan

Salah satu cara yang umum digunakan untuk mengamankan informasi adalah dengan mengatur akses ke informasi melalui mekanisme "*authentication*" dan "*access control*". Implementasi dari mekanisme ini antara lain dengan menggunakan "*password*". Dalam sistem operasi Linux, *password* pengguna disimpan dalam *file text* yang terletak di /etc/passwd, sedangkan dalam sistem operasi Windows, *password* pengguna terletak di c:\windows\sistem32\config dimana *file password* tersebut telah menggunakan algoritma enkripsi.

Kata kunci (*Password*) digunakan sebagai fasilitas untuk mengatur hak akses pengguna dalam menggunakan perangkat dan fasilitas jaringan telekomunikasi. Kriteria pembuatan *password* yang sudah umum diketahui adalah:

1. Jangan menggunakan nama *login*, nama pertama atau akhir beserta variasinya dan nama pasangan atau anak.
2. Jangan menggunakan informasi lainnya yang mudah didapat tentang diri pribadi seperti nomor telepon, tanggal lahir.
3. Gunakan *password* yang merupakan kombinasi antara huruf kapital dan huruf kecil dan angka.
4. Gunakan special "32 karakter ALT", diketikkan dengan menahan tombol Alt ketika mengetik angka antara 128 and 255 pada tombol angka dengan indikator *Num Lock*

BAB VI
ANCAMAN TERHADAP KEAMANAN JARINGAN

6.1. Pengelolaan Resiko

Pengelolaan terhadap keamanan jaringan telekomunikasi dapat dilihat dari sisi pengelolaan resiko (*risk management*). Terdapat tiga komponen yang memberikan kontribusi terhadap resiko kemanan jaringan, yaitu: kepengelolaan (*asset,*) kelemahan/kerentanan yang ditemui dalam suatu jaringan (*vulnerabilities*) dan ancaman keamanan yang berasal dari luar (*threats*).

Terdapat beragam permasalahan dalam jaringan telekomunikasi yang perlu diperhatikan dan ditangani, di antaranya adalah yang berkaitan dengan keamanan informasi atau informasi yang dikirimkan melalui jaringan telekomunikasi, serta kehandalan suatu jaringan lokal memberikan layanan bagi pengguna atau pelanggan agar dapat berkomunikasi dengan baik. Dalam mempelajari keamanan dan kehandalan pada suatu jaringan telekomunikasi, terdapat enam aspek utama yang perlu diperhatikan dalam pengelolaan suatu jaringan telekomunikasi.

6.2. Kategori Ancaman Terhadap Jaringan

Ancaman terhadap keamanan jaringan telekomunikasi, yang diakibatkan oleh adanya beragam ancaman (*threats*) dan kelemahan (*vulnerabilities*) dari sistem jaringan telekomunikasi, di antaranya adalah:

BAB VII
KEAMANAN JARINGAN BERBASIS PROTOKOL KOMUNIKASI

7.1. Pengamanan Berbasis OSI Layer

Untuk dapat memahami keamanan jaringan telekomunikasi, terlebih dahulu memahami aturan/tata cara berkomunikasi antara suatu perangkat dengan perangkat lainnya yang dihubungkan oleh suatu media transmisi. Aturan/tata cara berkomunikasi dapat disebut sebagai protokol komunikasi. *Open System Interconnection* (OSI) adalah protokol komunikasi yang distandarisasi oleh Badan Standar Internasional (*International Standard Organization*) yang dibagi menjadi tujuh tahapan atau tujuh lapisan (*seven layers*), yaitu:

1. Lapisan 1: Lapisan Fisik (*Physical Layer*)
   Lapisan atau tahapan komunikasi ini berkaitan dengan perangkat komunikasi dan media transmisi. Perangkat komunikasi dibedakan atas: terminal atau *Data Terminal Equipment (DTE)* dan penghubung atau *Data Communication Equipment (DCE).* Wujud dari terminal dapat berupa perangkat, tablet, smartphone dan lain sebagainya, baik yang berfungsi sebagai *client* (penerima layanan) maupun *server* (pengatur layanan). Wujud dari penghubung di antaranya adalah konektor-konektor, *hub, switch, bridge, router, modem* dan sebagainya. Untuk media transmisi dapat dibedakan atas: media transmisi dengan kabel (*on wire*) dan tanpa kabel (*wireless*). Untuk

BAB VIII
FIREWALL

8.1. Pengertian dan Perbandingan Firewall

Firewall merupakan suatu perangkat yang diletakkan antara internet dengan jaringan lokal. Informasi yang keluar atau masuk harus melalui *firewall* ini. Tujuan adanya *firewall* adalah untuk mencegah (*prevent*) agar akses (ke dalam maupun ke luar) dari orang yang tidak berwenang (*unauthorized access*) tidak dapat dilakukan.

Firewall bekerja dengan mengamati paket IP (*Internet Protocol*) yang melewatinya. Berdasarkan pada konfigurasi *firewall* maka akses dapat diatur berdasarkan *IP Address*, *port*, dan arah informasi. Detail konfigurasi bergantung pada masing-masing *firewall* dan kebijaksanaan (*policy*) organisasi yang bersangkutan, yang dapat dibagi menjadi dua jenis:

1. *Prohibitted*, yaitu kebijakan melarang akses tertentu dari jaringan telekomunikasi ke internet.
2. *Permitted*, yaitu kebijakan mengijinkan jaringan telekomunikasi untuk mengakses internet.

Secara konseptual terdapat 2 macam *firewall*:

1. *Network Firewall*
   Keputusan mengijinkan atau melarang akses ke internet berdasarkan pada alamat sumber, alamat tujuan dan *port* yang terdapat dalam setiap paket IP.
2. *Application Firewall*
   Keputusan mengijinkan atau melarang akses ke internet berdasarkan pada *host* yang berjalan sebagai *proxy server*,

BAB IX
SISTEM PENGAMANAN JARINGAN

9.1. Intrusion Detection System (IDS)

Intrusion Detection System (IDS) adalah suatu perangkat lunak berbasis *host* pada jaringan telekomunikasi yang mendeteksi adanya percobaan penyusupan data oleh pihak asing (yang tidak disahkan oleh sistem *authentification* jaringan telekomunikasi). IDS menerima salinan paket data yang bertujuan pada suatu *server* untuk kemudian memeriksa paket-paket data tersebut. Apabila ditemukan adanya paket data yang dideteksi sebagai suatu ancaman terhadap keamanan jaringan telekomunikasi maka IDS memberi peringatan pada administrator jaringan telekomunikasi. Karena IDS hanya memeriksa dan mendeteksi salinan paket data, sekalipun ditemukan adanya paket data yang terdeteksi sebagai ancaman terhadap keamanan jaringan telekomunikasi, paket data tersebut tetap sampai ke *server* tujuan. Dalam hal ini, IDS bersifat pasif.

Metode yang digunakan dalam IDS adalah:

1. *Signature based Intrusion Detection System*
   Dalam metode ini, terdapat daftar tandatangan (*signature*) yang dapat digunakan untuk menilai apakah paket data dapat menjadi ancaman terhadap keamanan jaringan telekomunikasi, dengan mencocokkan tandatangan pada paket data tersebut dengan daftar paket data yang sudah ada, yang diperbarui secara periodik.Metode ini melindungi sistem dari jenis-jenis seragangan yang sudah

BAB X
VIRUS, WORM, TROJAN

10.1. Virus

Virus adalah suatu program perangkat yang dapat menyebar pada perangkat atau jaringan telekomunikasi dengan cara membuat salinan dari dirinya sendiri tanpa sepengetahuan dari pengguna perangkat tersebut.

Suatu virus pertamakali harus dijalankan sebelum mampu untuk menginfeksi suatu perangkat. Berbagai macam cara agar virus ini dijalankan oleh sasaran, menempelkan dirinya pada suatu program yang lain. Terdapat juga virus yang jalan ketika dibuka suatu jenis *file* tertentu yang memanfaatkan celah keamanan jaringan telekomunikasi yang terdapat pada perangkat (baik sistem operasi atau aplikasi). Suatu *file* yang sudah terinfeksi virus dalam *attachment* e-mail. Begitu *file* tersebut dijalankan, maka kode virus akan berjalan dan mulai menginfeksi perangkat dan dapat menyebar pula ke semua *file* yang terdapat di jaringan telekomunikasi.

Virus dapat memperlambat *email* yaitu dengan membuat trafik *email* yang sangat besar yang akan membuat *server* menjadi lambat atau bahkan menjadi *crash*. Virus dapat mencuri informasi dan mampu merekam *key*stroke *keyboard*. Virus dapat menggunakan perangkat lain untuk menyerang suatu situs (*MyDoom*), merusak informasi (*Virus Compatable*), menghapus informasi (Virus Sircam), men-*disable hardware* (Virus CIH atau Chernobyl), menimbulkan hal-hal yang aneh dan mengganggu (Virus Netsky-D) dan menampilkan

BAB XI
SPYWARE, KEYLOGGER, ADWARE, SPAM

11.1. Spyware

Spyware adalah perangkat lunak yang melacak penggunaan internet dan melaporkannya ke pihak lain, dimana proses pelacakan tidak diketahui oleh pengguna perangkat lunak tersebut. Saat ini *spyware* sudah dijadikan alat untuk mencari informasi pribadi pada suatu perangkat dan menjadikan perangkat sasaran sebagai mata-mata tanpa diketahui pengelolanya.

Ciri khas adanya *spyware* adalah:

1. Perangkat menjadi lambat, bahkan jika dijalankan tanpa menggunakan banyak program.
2. Perubahan *setting browser* dimana pengguna merasa tidak pernah mengubah atau memasangnya. Banyak kasus *start page browser* berubah tanpa sebab yang jelas dan bahkan tidak dapat diubah meskipun secara manual.
3. Gejala lain munculnya *toolbar* yang menyatu dengan komponen *toolbar browser*.
4. Kegiatan mencurigakan. Banyak pengguna melaporkan perangkat mengakses *harddisk* tanpa campur tangan pengguna. Hubungan internet menunjukkan kegiatan, meskipun pengguna tidak menggunakannya. Munculnya *icon-icon* baru yang tidak jelas pada *tray icon*. Semuanya ini menandakan adanya kegiatan *background* yang sedang bekerja pada perangkat pengguna.
5. Muncul iklan pop up setiap kali pengguna terhubungan

BAB XII
KEAMANAN KOMUNIKASI BERBASIS WEB

12.1. World Wide Web (WWW)

World Wide Web (WWW) dikembangkan oleh Tim Berners-Lee ketika bekerja di CERN (Swiss). Untuk membaca atau melihat sistem WWW digunakan tools yang dikenal dengan istilah *browser.*

Browser awal adalah NeXT. Selain NeXT, saat itu terdapat *browser* yang berbentuk text seperti "*line mode*" *browser*. Kemudian terdapat Mosaic yang *multi-platform* (Unix/Xwindow, Mac, Windows) dikembangkan oleh Marc Andreesen dkk ketika sedang magang di NCSA.Arsitektur sistem Web terdiri dari dua sisi: s*erver* dan *client*.

Selain menyajikan informasi-informasi dalam bentuk statis, sistem Web dapat menyajikan informasi dalam bentuk dinamis dengan menjalankan program. Program ini dapat dijalankan di *server* (misal dengan CGI, servlet) dan di *client* (applet, Javascript). *Server* WWW menyediakan fasilitas agar *client* dari tempat lain dapat mengambil informasi dalam bentuk berkas (*file*), atau mengeksekusi perintah (menjalankan program) di *server*. Fasilitas pengambilan berkas dilakukan dengan perintah "GET".

Pembatasan akses dapat dilakukan dengan membatasi domain atau nomor IP yang dapat mengakses; (konfigurasi Web *Server* atau *Firewall*, menggunakan pasangan *userid* dan *password*; mengenkripsi informasi sehingga hanya dapat dibuka (dekripsi) oleh orang yang memiliki kunci pembuka.

BAB XIII
KEAMANAN JARINGAN LOKAL NIRKABEL

13.1. Pengenalan Jaringan Lokal Nirkabel (WLAN)

Jaringan Lokal Nirkabel/*Wireless Local Area Network* (WLAN) adalah suatu teknologi yang memungkinkan pengiriman informasi dengan kecepatan antara 11-54 *Megabyte persecond*. Teknologi ini dikenal dengan sebutan *Wireless Fidelity (Wi-Fi)* yang membuat pengguna internet berkomunikasi informasi secara nirkabel. WLAN sebenarnya hampir sama dengan jaringan LAN, akan tetapi setiap *node* pada WLAN menggunakan *wireless device* untuk berhubungan dengan jaringan telekomunikasi. *Node* pada WLAN menggunakan *channel* frekuensi yang sama dan SSID yang menunjukkan identitas *wireless device*.

WLAN memiliki dua mode yang dapat digunakan, yaitu: Infastruktur dan Ad-Hoc. Konfigurasi Infrastruktur adalah komunikasi antara masing-masing PC melalui suatu *Access Point* pada WLAN atau LAN. Komunikasi *Ad-Hoc* adalah komunikasi secara langsung antara masing-masing perangkat dengan menggunakan kartu antarmuka jaringan nirkabel (*wireless network interface card).*

Umumnya, komponen WLAN terdiri atas:

1. *Access Point*, berfungsi untuk mengkonversikan sinyal frekuensi radio (RF) menjadi sinyal digital yang akan disalurkan melalui kabel, atau disalurkan ke perangkat WLAN yang lain dengan dikonversi ulang menjadi sinyal frekuensi radio.

BAB XIV
KEAMANAN WIDE AREA NETWORK (WAN)

14.1. DMZ

Pembagian kelompok jaringan telekomunikasi perlu dilakukan untuk mengatasi kemungkinan terjadinya gangguan keamanan pada suatu kelompok jaringan telekomunikasi. Suatu jaringan telekomunikasi dapat dibedakan antara jaringan lokal (*local area network*) dan jaringan luar (jaringan telekomunikasi pihak luar) dengan menggunakan *Demilitarized Zone (DMZ*). Perangkat-perangkat DMZ adalah perangkat-perangkat yang perlu dihubungi secara langsung oleh pihak luar. Contohnya adalah *web-server*, *mail-exchange*, *server* dan *name server*. Perangkat-perangkat pada DMZ perlu disiapkan secara khusus karena terbuka ke luar (dapat diakses dari pihak luar). Aplikasi-aplikasi yang digunakan pada *host-host* dalam DMZ harus merupakan aplikasi-aplikasi yang aman, terus menerus dipantau dan diperbarui secara periodic.

Aturan-aturan yang berlaku dalam DMZ adalah:

1. Pihak luar hanya dapat berhubungan dengan *host-host* dalam DMZ sesuai dengan kebutuhan yang ada. Secara *default*, pihak luar tidak dapat melakukan hubungan dengan *host-host* di jaringan lokal setelah DMZ.
2. *Host-host* pada DMZ secara *default* tidak dapat melakukan hubungan dengan *host-host* pada jaringan lokal, hubungan secara terbatas dapat dilakukan sesuai dengan kebutuhan.
3. *Host-host* pada jaringan lokal dapat melakukan hubungan secara bebas baik ke *host* maupun ke DMZ. Pada beberapa

DAFTAR PUSTAKA

[1] C. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners. Springer Berlin Heidelberg, 2011, isbn: 9783642041006.[Online]. https://books.google.com.eg/books?id=N_e4NAEACAAJ

[2] Budi Rahardjo, "Keamanan Sistem Informasi Berbasis Internet", Penerbit. PT. Insan Indonesia, Bandung, 2005.

[3] Richardus Eko Indrajit, "Peranan Teknologi Informasi dan Internet", Penerbit. Andi Offset, Yogyakarta, 2011.

[4] Sri Hartanto, "Pencegahan dan Pendeteksian Serangan Penolakan Layanan (Denial of Service Attack) Dalam Jaringan komunikasi", Jurnal Ilmiah Elektrokrisna, Vol. 1, No. 3, pp.133-144, 2013.

[5] Luo, Xiapu., W.W.Chan, Edmond., and K.C. Chang, Rocky, "Detecting Pulsing Denial-of-Service Attacks with Nondeterministic Attack Intervals", EURASIP Journal on Advances in Signal Processing, Vol. 2009, No. 1, pp. 1-13, 2009, DOI:10.1155/2009/256821.

[6] Meenakshi, S and S.K Srivatsa, "A Distributed Framework with less False Positive Ratio Against Distributed Denial of Service Attack", Information Technology Journal, Vol. 6, No. 8, pp. 1139-1145, 2007, DOI:10.3923/itj.2007.1139.1145.

[7] S. H. C. Haris, "Anomaly Detection of IP Header Threats", International Journal of Advanced Computer Science and Applications, Vol. 4, No. 5, pp. 497–504, 2011.

BUKU AJAR TEKNIK ELEKTRO

KEAMANAN DAN KEHANDALAN JARINGAN

SRI HARTANTO

Buku Ajar Keamanan dan Kehandalan Jaringan ini disusun sebagai bahan pembelajaran bagi mahasiswa yang mengikuti perkuliahan Keamanan dan Kehandalan Jaringan. Buku Ajar Keamanan dan Kehandalan Jaringan ini berisikan pengenalan keamanan dan kehandalan jaringan, seperti kriptografi dan steganografi, kunci enkripsi dan dekripsi, evaluasi keamanan jaringan, keamanan jaringan berbasis sistem server, ancaman terhadap keamanan jaringan, keamanan jaringan berbasis protokol komunikasi, firewall, IDS dan IPS, virus, worm, trojan, spyware, keylogger, adware, spam, keamanan jaringan berbasis web, keamanan jaringan lokal nirkabel dan keamanan jaringan wide area network. Buku Ajar Keamanan dan Kehandalan Jaringan bertujuan untuk memperkaya pemahaman tentang pentingnya keamanan suatu jaringan telekomunikasi, dan mengenali potensi atau bahaya yang mengancam jaringan telekomunikasi.

ISBN: 978-623-145-089-0

9 786231 450890

PENERBIT CV. MITRA ILMU

IKAPI