DESAIN DAN ANALISIS *BEST PRACTICE PHYSICAL SECURITY* DAN *LOGICAL SECURITY* PADA *DATA CENTER* FAKULTAS REKAYASA INDUSTRI UNIVERSITAS TELKOM MENGGUNAKAN STANDAR TIA-942 DAN *OPEN ENTERPRISE SECURITY ARCHITECTURE*

DESIGN AND ANALYSIS OF BEST PRACTICE PHYSICAL SECURITY AND LOGICAL SECURITY IN DATA CENTER OF SCHOOL OF INDUSTRIAL AND SYSTEM ENGINEERING TELKOM UNIVERSITY BASED ON TIA-942 AND OPEN ENTERPRISE SECURITY ARCHITECTURE STANDARD

I Gede Iswara Darmawan[1], Mochamad Teguh Kurniawan[2]

[1,2]Program Studi Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom

[1]iswaradrmwn@students.telkomuniversity.ac.id, [2]teguhkurniawan@telkomuniveristy.ac.id

Abstrak

Data center **telah menjadi suatu hal yang penting dalam organisasi.** ***Data center*** **menyimpan semua data yang dibutuhkan oleh organisasi. Data organisasi ini selanjutnya akan diambil, diolah dan disimpan kembali pada** ***data center*****. Pengelolaan** ***server*** **pada** ***data center*** **harus sesuai dengan standar atau** ***best practices*** **yang ada. Kenyataannya, pengelolaan** ***server*** **yang ada pada Fakultas Rekayasa Industri Universitas Telkom masih belum sesuai standar sehingga masih banyak yang memiliki kerentanan. Perancangan** ***logical security*** **dan** ***physical security*** **pada** ***data center*** **Fakultas Rekayasa Industri Universitas Telkom menggunkan metode** ***Prepare, Plan, Design, Implement, Operate, Optimize*** **(PPDIOO) dan standar** ***Open Enterprise Security Architecture*** **serta TIA-942 beserta** ***best practices*** **pendukung. Metode PPDIOO yang digunakan bersifat siklus sehingga mendukung** ***continuous improvement*****. Perancangan keamanan** ***data center*** **yang dibahas adalah mengenai penerapan perangkat** ***surveillance*** **untuk keamanan fisik, penerapan VPN dan SSH serta IDS untuk pengamanan akses** ***remote*** **, deteksi penyusupan dan serangan terhadap** ***server*** **pada** ***data center*** **serta penerapan pembaharuan atau** ***update*** **otomatis pada level sistem operasi dan penonaktifan layanan yang tidak digunakan pada** ***server.***

Kata Kunci: ***Data Center,*** **Keamanan Fisik** ***Data Center,*** **Keamanan Logik** ***Data Center***

Abstract

The data center has become an important issue in the organization. The data center stores all the data required by the organization. This organization of data will then be captured, processed and stored back in the data center. Management of servers in the data center must be in accordance with the standards or best practices that exist. In fact, the existing server management at the School of Industrial and System Engineering Telkom University is still not standardized so there is still has a lot of vulnerabilities. Design of logical security and physical security at data centers Telkom University Faculty of Industrial Engineering and using the Prepare, Plan, Design, Implement, Operate, Optimize (PPDIOO) method, Open Enterprise Security Architecture and TIA-942 standard along with supporting best practices. PPDIOO method used is thus supporting continuous improvement cycle. The design of data center security that discussed is the application of surveillance devices for physical security, VPN and SSH as well as the application of IDS for securing remote access, intrusion detection on the servers in the data center, automatic updates on the operating system level and disabling unused services on the server.

Keywords: Data Center, Data Center Physical Security, Data Center Logical Security

1. Pendahuluan

Data center dewasa ini telah menjadi hal penting dalam organisasi. *Data center* menyimpan semua data dan informasi yang dibutuhkan organisasi. Demikian pentingnya informasi yang tersimpan di dalam *data center* menyebabkan keamanan *data center* harus diperhatikan dengan baik.

Fakultas Rekayasa Industri (FRI) Universitas Telkom merupakan salah satu fakultas yang berada di Universitas Telkom. FRI membutuhkan *data center* untuk menunjang kegiatan akademik fakultas, khususnya untuk menempatkan *server* aplikasi milik dosen maupun mahasiswa FRI dan juga sebagai *server* penyimpanan

data fakultas (*data storage*).

Berdasarkan hasil pengamatan, didapatkan bahwa *server – server* pemrosesan informasi dan jaringan yang berada di lingkungan FRI memiliki kerentanan-kerentanan baik secara fisik maupun logik. Kerentanan ini berupa *server* yang beroperasi tanpa pengawasan, *server* yang berjalan dengan sistem operasi maupun layanan yang versinya belum diperbaharui, maupun jaringan yang tidak memiliki layanan pendeteksian penyusupan dan serangan. Ini terjadi karena pengelolaan *server* belum terstandarisasi. Hal ini dapat dijadikan catatan atau landasan pembangunan desain keamanan *data center* dimana nantinya *server – server* inilah yang akan berada di dalam *data center* ini.

Analisis dan desain rancangan keamanan *data center* menggunakan metode *Prepare, Plan, Design, Operate, Optimize* (PPDIOO) dan menggunakan standar *Open Enterprise Security Architecture* (O-ESA) dan TIA-942. Metode PPDIOO adalah metodologi pengembangan jaringan yang mendefinisikan siklus hidup berkelanjutan mengenai layanan yang ada pada jaringan komputer, termasuk di dalamnya keamanan jaringan dan *server*.

2. Dasar Teori

2.1. Definisi *Data Center*

Data center menurut Arregoces & Portolani pada buku *Data Center Fundamentals* adalah suatu tempat yang memuat sumber daya komputasi kritikal yang terletak pada lingkungan terkontrol dan di bawah kendali yang tersentralisasi yang memungkinan organisasi menggunakannya sebagai pendukung kelangsungan bisnis [1].

2.2. Serangan Logikal pada Data Center

Menurut Arregoces dan Portolani pada buku *Data Center Fundamentals*, serangan pada sisi logikal yang umum terjadi adalah sebagai berikut [1]:

1. *Scanning* / *Probing*
2. *Denial of Service* (DoS)
3. Akses yang tidak terotorisasi
4. Penyadapan
5. *Malware*

2.3. Serangan Fisikal pada Data Center

Serangan fisikal yang biasa terjadi pada *data center* adalah:

1. Pencurian perangkat
2. Masuknya orang yang tidak bertanggungjawab ke dalam *data center*

2.4. *Open Enterprise Security Architecture* (O-ESA)

O-ESA adalah sebuah *framework* untuk *merancang Enterprise Information Security Architecture* yang dikembangkan oleh The Open Group. O-ESA adalah *framework* yang menggunakan metode *policy-driven architecture*, yaitu membangun arsitektur keamanan dengan berbasiskan kebijakan [2].

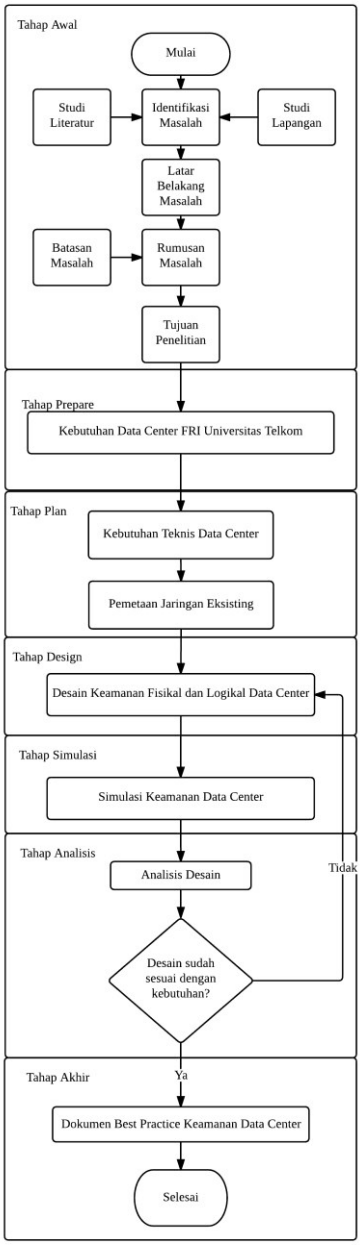
2.5. *Telecommunication Association Industry* (TIA) – 942

TIA-942 adalah standar untuk *Data Center*. TIA-942 digunakan untuk menentukan persyaratan minimum untuk infrastruktur telekomunikasi dari *data center* dan ruang-ruangnya. Topologi yang disiapkan dalam standar ini adalah dimaksudkan agar bisa diterapkan di semua tipe *data center*. [3]

3. Metodologi Penelitian

3.1. Sistematika Penelitian

Dalam penelitian ini digunakan metode PPDIOO *Network Life-Cycle Approach*. Pada sistematika penelitian menjelaskan tahapan-tahapan pada penelitian. Mulai dari tahap awal hingga tahap akhir. Adapun sistematika penelitiannya adalah seperti pada Gambar 1.



Gambar 1 Sistematika Penelitian

Terdapat lima tahapan utama yang dilakukan yaitu tahap persiapan (*Prepare*), tahap perencanaan (*Plan*), tahap desain (*Design*), tahap simulasi *prototyping*, dan tahap analisa. Berdasarkan batasan masalah yang telah ditentukan, penggunaan metode PPDIOO hanya digunakan sampai tahap simulasi *prototyping*. Penjelasan dari setiap tahapan adalah sebagai berikut [4]:

1. Tahap Awal

   Tahap awal dimulai dengan mengidentifikasi masalah dan dibantu dengan latar belakang masalah yang akan digunakan untuk membantu merancangan perumusan masalah. Selanjutnya adalah menentukan batasan masalah dan tujuan penelitian agar penelitian yang dilakukan menjadi jelas arah dan tujuannya.
2. Tahap *Prepare*

   Tahapan ini adalah tahapan persiapan penelitian. Pada tahap ini didefinisikan visi yang jelas bagaimana perancangan keamanan *data center*, kebutuhan penggunaan dan teknologi yang akan digunakan.
3. Tahap *Plan*

   Pada tahap ini dilakukan perencanaan perancangan keamanan *data center* berdasarkan kebutuhan teknis dan jaringan eksisting dari lokasi implementasi *data center*.
4. Tahap *Design*

Tahap ini adalah tahap dimana desain keamanan *data center* dilakukan berdasarkan studi literatur dan kebutuhan FRI.

5. Tahap Simulasi

   Pada tahap ini simulasi terhadap desain yang dirancang dilakukan. Tahap ini mencakup skema penyerangan yang dialamatkan terhadap *server* yang terdapat dalam *data center*.

6. Tahap Analisa

   Tahap ini merupakan tahap terakhir dimana desain yang sudah dibuat dianalisa apakah sudah sesuai dengan kebutuhan atau tidak.

4. Analisa Eksisting

Analisa kondisi eksisting dibagi kedalam empat bagian, yaitu : (1) Daftar *Server*, (2) Identifikasi Keamanan Jaringan Eksisting, (3) Identifikasi Keamanan Logik *Server* Eksisting, (4) Identifikasi Keamanan Fisik *Server* Eksisting, (5) Identifikasi Gap Keamanan Jaringan Eksisting, (6) Identifikasi Gap Keamanan Logik *Server* Eksisting dan (7) Identifikasi Gap Keamanan Fisik *Server* Eksisting.

4.1. Daftar Server

Daftar server di Fakultas Rekayasa Industri yang berhasil terobservasi adalah seperti pada Tabel 1.

Tabel 1 Daftar *Server* di Fakultas Rekayasa Industri

No	IP	Fungsi	Pemilik	Lokasi	Aplikasi
1	10.3.248.93	Pembangunan Aplikasi	BPAD *Laboratory*	C 222	Apache, MySQL
2	10.3.23.199	*Server* Praktikum Basis Data	Prodase *Laboratory*	C 105	DB2 *Server*, OpenSSH *Server*
3	10.3.121.4	Portal Registrasi Praktikum	PFT *Laboratory*	C 313	Apache, MySQL
4	10.3.23.20	*Private Cloud* FRI	FRI	C 105	Apache, MySQL, OpenSSH *Server*, OpenStack
5	10.3.71.71	*Sharing* Data	Sisjar *Laboratory*	C 205	Apache, OpenSSH *Server*

4.2. Identifikasi Keamanan Jaringan Eksisting

Berdasarkan hasil observasi pada jaringan Gedung Karang (Gedung C) selama 1 bulan, terhitung mulai dari Maret 2015 hingga April 2015 menggunakan perangkat *Network Intrusion Detection System* (NIDS), didapatkan hasil seperti pada Tabel 2.

Tabel 2 Hasil Pengamatan Perangkat NIDS

No.	*Signature*	Tingkat Ancaman	Persentase
1	ET DROP Spamhaus DROP Listed Traffic Inbound	*Medium*	24,59 %
2	GPL ICMP_INFO PING *NIX	*Informational*	4,31 %
3	ET POLICY GNU/Linux APT User-Agent Outbound	*Informational*	70,37%

Berdasarkan hasil pengamatan NIDS, didapatkan temuan bahwa telah terjadi serangan DDoS kepada *server* yang berada dalam jaringan FRI. Hal ini dibuktikan dari adanya hasil pengamatan NIDS dengan *signature* ET DROP Spamhaus DROP *Listed Traffic Inbound* [5]. *Server* yang terkena DDoS adalah *server* dengan alamat IP 10.3.23.20 dengan presentase 24,59%. Selain signature ET DROP Spamhaus DROP *Listed Traffic Inbound* adalah *signature* yang sifatnya tidak berbahaya karena tingkat ancamannya hanya *informational*.

4.3. Identifikasi Keamanan Logik *Server* Eksisting

Berdasarkan hasil pengamatan kepada sistem operasi dan layanan yang berjalan pada *server*, didapatkan hasil bahwa terdapat kerenatanan pada layanan yang dijalankan pada *server*. Kerentanan

tersebut adalah pada layanan SSL POODLE yang menyerang fungsi SSL [6].

Temuan lain juga didapatkan saat melakukan pengamatan terhadap penugasan *server*. *Server* seharusnya hanya digunakan untuk melakukan fungsi utamanya, yaitu sebagai tempat terpasangnya aplikasi seperti *web server*, *database server* maupun *file sharing*. Kenyataannya, pada *server* juga terpasang aplikasi lain yang tidak seharusnya terpasang, seperti contoh *video game*.

4.4. Identifikasi Kemanan Fisik *Server* Eksisting

Temuan yang didapatkan pada keamanan fisik *server* adalah penempatan *server* pada kondisi tidak terawasi. *Server* yang tidak dalam kondisi terawasi adalah *server* milik Lab. BPAD, Lab. Sisjar dan Lab. PFT. Selain itu, tidak adanya mekanisme pengawasan yang diterapkan menyebabkan tidak teramatinya aktivitas yang terjadi dalam ruang *server* tersebut.

4.5. Identifikasi *Gap* Keamanan Jaringan Eksisting

Identifikasi *gap* keamanan jaringan eksisting dilakukan dengan membandingkan keadaan eksisting dengan standar O-ESA dan Cisco SAFE. Perbandingan di sini dilakukan pada aspek kecukupan. Alasan pemilihan *best practice* ini adalah karena pembahasannya sesuai dengan standar yang digunakan sebagai acuan. *Gap* yang terjadi adalah seperti pada Tabel 3.

Tabel 3 Gap antara Standar O-ESA dan *Best Practice* Cisco SAFE dengan Keadaan Jaringan Eksisting

No.	*Checklist*	O-ESA / Cisco SAFE	Keadaan Eksisting (Sudah / Belum)
1	Penerapan IDS untuk pencegahan DDoS	Ya	Belum
2	Penerapan IDS untuk pencegahan serangan terhadap aplikasi *web*	Ya	Belum

Seperti terlihat pada Tabel 3, jaringan Gedung Karang (Gedung C) belum memiliki layanan deteksi penyerangan sehingga lalu-lintas data tidak terawasi.

4.6. Identifikasi Gap Keamanan Logik Server Eksisting

Identifikasi *gap* dilakukan dengan membandingkan keadaan eksisting dengan standar O-ESA dan *best practice* NIST SP800-44 v2. Alasan pemilihan *best practice* ini adalah karena *best practice* ini sangat cocok diterapkan untuk *server* yang menjalankan aplikasi *web* dan dapat digunakan juga sebagai *checklist server* secara umum.

Gap yang terjadi adalah seperti pada Tabel 4.

Tabel 4 Analisis Gap antara Keamanan Logik Server Eksisting dengan Standar O-ESA dan NIST SP800-44 v2

No	*Checklist*	O-ESA / NIST SP800-44 v2	Keadaan Eksisting (Sudah / Belum)
1	Pemasangan perangkat *firewall*	Ya	Sudah
2	*Update* sistem operasi *server* secara terjadwal	Ya	Belum
3	Nonaktifkan semua layanan yang tidak diperlukan	Ya	Belum
4	Perangkat *server* hanya digunakan untuk layanan *server*	Ya	Belum

Dari Tabel 4 terlihat bahwa dari sisi kecukupan, pengelola *server* sudah memasang perangkat *firewall*, namun dari sisi ketaatan, pengelola *server* belum mengelola *server*nya dengan baik. Hal ini terlihat dari sistem operasi yang tidak di*update* secara terjadwal, pengelolaan layanan yang berjalan pada sistem operasi dan penggunaan *server* yang di luar peruntukkannya (temuan di lapangan adalah penggunaan komputer *server* untuk bermain *video game*).

4.7. Identifikasi Gap Keamanan Fisik *Server* Eksisting

Identifikasi *gap* keamanan fisik *server* eksisting adalah dibandingkan dengan standar TIA-942 Tier III. *Gap* yang terjadi adalah seperti pada Tabel 5.

Tabel 5 Analisis Gap antara Keamanan Fisik Eksisting dengan Standar TIA-942 Tier III

No	*Checklist*	Standar TIA-942 (Ya / Tidak)	Keadaan Eksisting
	CCTV Monitoring		
1	Perimeter Bangunan	Ya	Tidak
2	Generator	Ya	Tidak
3	Pintu	Ya	Tidak
4	UPS, Telepon	Ya	Tidak
5	Ruangan Komputer	Ya	Tidak
	CCTV		
1	CCTV merekam semua aktivitas	Ya	Tidak
2	Bitrate perekaman (fps)	Ya ; 20 fps	Tidak

Seperti terlihat pada Tabel 5, pengelola *server* tidak memasang perangkat *surveillance* dalam bentuk CCTV yang digunakan untuk mengawasi ruang *server*. Hal ini berbahaya karena resiko perusakan *server* akan semakin besar.

5. Perancangan Usulan

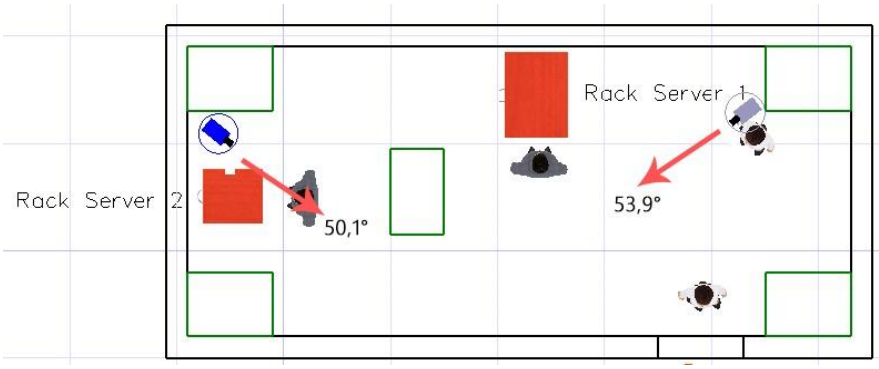
5.1. Simulasi dan Analisis Usulan Keamanan Fisik

Rancangan keamanan fisik untuk *data center* Fakultas Rekayasa Industri (FRI) adalah menggunakan perangkat *surveillance* yang berupa kamera CCTV. Perancangan peletakan kamera CCTV ini sesuai dengan standar TIA-942. Spesifikasi kamera yang digunakan adalah seperti pada Tabel 6.

Tabel 6 Spesifikasi Kamera

Spesifikasi	Detail
IP / Analog	IP
Berat	5,89 kg
Dimensi (PxLxT)	11,5” x 21,5” x 11,5”
Kebutuhan *Power*	AC 24V
Temperatur Pengoperasian	-28° C – 50° C
Kompresi yang Didukung	H-264, MPEG4, JPEG
FPS	*Variable*, Max 30 FPS
Resolusi	*Full High Definition*

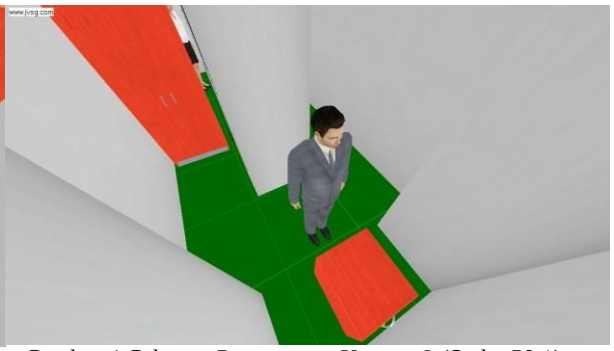
Posisi peletakan kamera terdapat pada Gambar 2.



Gambar 2 Posisi Peletakan Kamera

Dengan peletakan kamera seperti pada Gambar 2, maka cakupan pengamatan dari kamera tersebut adalah seperti pada Gambar 3 dan Gambar 4.

Gambar 3 Cakupan Pengamatan Kamera 1 (Sudut 53,9)



Gambar 4 Cakupan Pengamatan Kamera 2 (Sudut 50,1)

Berdasarkan hasil di atas, pengelola *data center* akan mempunyai cakupan pandangan yang hampir menyeluruh, Hanya ada sedikit *blankspot* pada cakupan pengamatan.Sementara untuk perhitungan *bandwidth* dan ruang *harddisk* yang digunakan untuk menyimpan hasil pantauan CCTV per hari adalah seperti pada Tabel 7.

Tabel 7 Bandwidth dan Ruang Harddisk yang DIgunakan untuk Dua Kamera per Hari

Resolusi (pixel)	**Tipe Kompresi**	**FPS**	***Frame Size* (kB)**	***Bandwidth* (Mbit/s)**	**Disk Space (GB)**	***Bitrate* Perekaman(kbit/s)**
640x480	H-264	20	3,8	1,25	13,4	623

Kebutuhan ruang *harddisk* dan *bandwidth* untuk menyimpan hasil pantauan selama 1 hari adalah 13,4 GB dan 1,25 Mbit/s.

5.2. Simulasi dan Analisis Usulan Keamanan Logik

Pada perancangan usulan keamanan logik, akan dibahas rancangan pengamanan *server* dalam bentuk pengamanan lalu-lintas data dari dalam dan ke luar *server* (*Border Protection*), deteksi ancaman terhadap *server* (*Detection*), menonaktifkan layanan yang tidak perlu pada sistem operasi dan melakukan konfigurasi *update* otomatis pada sistem operasi.

5.2.1. *Border Protection Service*

Menurut standar *Open Enterprise Security Architecture* (O-ESA), *border protection service* adalah layanan yang digunakan untuk mengontrol koneksi dar *server*. Layanan yang diterapkan pada *border protection service* menurut O-ESA adalah *Virtual Private Network* (VPN), *Secure Shell* (SSH), *Packet Filtering Service*, dan *Proxy*.

Usulan yang akan diakukan pada layanan ini adalah penerapan VPN dan SSH untuk keamanan transmisi data. Alasan penerapan VPN dan SSH adalah karena hanya dengan VPN dan SSH sudah dapat mengamankan *data center* dengan baik dari sisi *layer* 2 dan *layer* 3 OSI.

Hasil dari simulasi usulan ini adalah seperti pada Tabel 7.

Tabel 8 Hasil Simulasi Usulan Koneksi VPN dan SSH

No	Kondisi Koneksi VPN	Kondisi Koneksi SSH
1	Terkoneksi	Terkoneksi
2	Tidak Terkoneksi	Tidak Terkoneksi

Berdasarkan hasil simulasi pada Tabel 7 didapatkan bahwa saat *client* terkoneksi ke dalam VPN maka *client* bisa mengakses *server* secara *remote* menggunakan SSH. Saat *client* tidak terkoneksi ke dalam VPN, maka *client* tidak bisa mengakses *server* secara *remote* melalui SSH.

5.2.2. *Detection Service*

Menurut standar O-ESA, *detection service* adalah layanan untuk mencatat dan mendeteksi ancaman keamanan yang terjadi ke dalam sistem. Layanan yang diterapkan pada *detection service* menurut O-ESA adalah *Intrusion Detection Services* , *Anomaly Detection Services*, *Logging Services* dan *Vulnerability Assessment Services*.

Usulan yang akan diterapkan pada penelitian ini adalah penerapan *Intrusion Detection System* (IDS) untuk deteksi serangan pada aplikasi *web* (*Cross Site Scripting, SQL injection*) dan untuk deteksi pada serangan DDoS. Alasan pemilihan usulan menggunakan IDS adalah karena merupakan solusi termudah untuk diterapkan dalam jaringan dibandingkan dengan layanan lain pada *detection service*.

Hasil simulasi IDS untuk deteksi serangan adalah seperti pada Tabel 8.

Tabel 9 Hasil Pengujian IDS

No	Serangan	Serangan Terdeteksi atau Tidak Terdeteksi
1	DDoS	Terdeteksi
2	SQL *Injection*	Terdeteksi
3	*Cross Site Scripting*	Terdeteksi

Berdasarkan hasil simulasi IDS pada Tabel 8, IDS mampu mendeteksi 100% serangan yang diujikan.

5.2.3. Menonaktifkan Layanan yang Tidak Diperlukan pada Sistem Operasi

Menurut *best practice* NIST SP800-442 v2, untuk menciptakan *web server* yang aman salah satu langkah yang dilakukan adalah menonaktifkan layanan yang tidak diperlukan [7]. Hal ini bertujuan untuk mengamankan *server* dari serangan terhadap layanan yang sebenarnya tidak perlu diaktifkan.

Pada kondisi eksisting, terdapat satu *server* yang rentan terhadap serangan SSL POODLE. Menonaktifkan SSL versi 3 yang menjadi sumber masalah adalah solusi [6].

5.2.4. Konfigurasi *Update* Otomatis

Menurut *best practice* NIST SP800-442 v2 [7], untuk menciptakan *web server* yang aman salah satu langkah yang dilakukan adalah melakukan *update* sistem operasi secara terjadwal. Hal ini dilakukan agar sistem operasi mendapatkan versi terbaru dan terhindar dari kerentanan yang terjadi karena versi sistem operasi atau komponen sistem operasi yang belum ter*update* ternyata memiliki celah keamanan.

Sebagai referensi, pada sistem operasi Linux distribusi Debian dan Ubuntu, terdapat fitur yang bernama *Unattended Upgrades* [8] . Fitur ini berfungsi untuk melakukan update sistem operasi secara otomatis. Pada sistem operasi Windows dapat menggunaan fitur *Windows Update* [9].

6. Kesimpulan dan Saran

6.1. Kesimpulan

Pada penelitian ini dapat ditarik kesimpulan, sebagai berikut:

Pada tahap identifikasi keamanan eksisting didapat hasil sebagai berikut.

a. Jaringan Gedung Karang (Gedung C) FRI belum menerapkan layanan keamanan berupa *Intrusion Detection System* (IDS) sehingga tidak bisa mendeteksi serangan yang datang ke dalam jaringan. Contoh serangan yang masuk adalah DDoS.

b. *Server* yang terletak pada Gedung Karang FRI masih belum baik dalam hal pengoperasian. Hal ini dapat dibuktikan dari penggunaan server yang seharusnya hanya digunakan untuk menjalankan layanan yang diperlukan, namun pada kenyataannya digunakan pula untuk hal lain selain yang diperuntukkan (*video game*).
c. *Server* yang terletak pada Gedung Karang FRI belum terkelola dengan baik di sisi keamanan fisik. Peletakkan *server* yang tidak terlindungi dan terawasi dengan baik menyebabkan resiko kerusakan dan kehilangan data secara fisik.

Perancangan *logical security* dan *physical security* yang diusulkan adalah sebagai berikut.

a. *Data center* FRI diberikan layanan yang dapat mendeteksi serangan yang dialamatkan pada *server* yang terletak di dalam *data center*. Layanan yang diusulkan adalah pemasangan perangkat IDS.
b. Pengamanan akses ke dalam *server* pada *data center* dilakukan dengan cara pemasangan VPN *server* untuk mengamankan akses SSH ke dalam *server*. Pada pengujian usulan terlihat bahwa *client* tidak bisa mengakses *server* apabila belum terkoneksi kedalam jaringan VPN.
c. Keamanan fisik yang diusulkan adalah dengan pemasangan perangkat *surveillance* berupa CCTV. Hasil pengujian menunjukkan bahwa dengan penggunaan CCTV, ruangan *data center* dapat dipantau secara menyeluruh. Hal ini meningkatkan keamanan dari sisi fisik *data center*.

6.2. Saran

Saran untuk penelitian selanjutnya:

a. Edukasi kepada pengelola *server* tentang tata cara pengelolaan *server* sesuai standar ataupun *best practice* agar tidak terjadi kerentanan karena pengelolaan menyalahi prosedur pada standar atau *best practice*. Contohnya adalah penggunaan SOP *incident management* dari pihak terkait, seperti ID-SIRTII atau CSIRT BPPT.
b. Dilakukan prosedur *vulnerability assessment* yang lebih dalam agar mengetahui lebih detail mengenai kerentanan yang ada.

Daftar Pustaka:

[1] M. Arregoces and M. Portolani, Data Center Fundamentals, Indianapolis: Cisco Press, 2004.

[2] The Open Group, Open Enterprise Security Architecture (O-ESA) : A Framework and Template for Policy-Driven Security, Zaltbommel: Van Haren Publishing, 2011.

[3] ADC Krone, "TIA-942 : Data Center Standards Overview," ADC Telecommunications, Berlin, 2008.

[4] D. Teare, Designing for Cisco Internetwork Solutions (DESGN), Indianapolis: Cisco Press, 2007.

[5] Spamhaus, "DROP and EDROP. Don't Route Peer List," 2015. [Online]. Available: https://www.spamhaus.org/drop/. [Accessed 20 March 2015].

[6] US-CERT, "SSL 3.0 Protocol Vulnerability and POODLE Attack," 17 10 2014. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA14-290A.

[7] National Institute of Standard and Technology, "Guidelines on Securing Public Web Server," National Institute of Standard and Technology, Gaithersburg, 2007.

[8] Canonical Software, "Automatic Updates," 2015. [Online]. Available: https://help.ubuntu.com/12.04/serverguide/automatic-updates.html. [Accessed 26 May 2015].

[9] Microsoft, "How To Configure Automatic Updates with Group Policy," 12 July 2013. [Online]. Available: https://support.microsoft.com/en-us/kb/328010. [Accessed 27 May 2015].

[10] M. Williams, "First Sites Admit Data Loss through Heartbleed Attacks," 14 April 2014. [Online]. Available: http://www.itworld.com/article/2697949/security/first-sites-admit-data-loss-through-heartbleed-attacks.html.

[11] Wikipedia, "TIA942," November 2014. [Online]. Available: http://en.wikipedia.org/wiki/TIA-942.

[12] A. S. Tannebaum, Computer Networks, 4th Edition, New Jersey: Pearson Education, 2003.

[13] W. Stallings, Cryptography and Network Security Principles and Practice, 5th Edition, Pearson Education, 2011.

[14] R. T. Prabowo, "Analisis dan Desain Keamanan Jaringan Komputer dengan Metode Network Development Life Cycle (Studi Kasus : Universitas Telkom)," Bandung, 2014.

[15] E. Maiwald, Network Security: A Beginner's Guide, New York: McGraw-Hill, 2001.

[16] S. Y. Lelono, N. Anharito, E. Ainun Najib F. and G. I.P., Makalah Rekayasa Sistem Jaringan Komputer, Kudus: Universitas Muria Kudus, 2011.

[17] E. Dulaney, CompTIA Security+ Study Guide Exam SY0-301, 5th Edition, Wiley & Sons, 2011.

[18] CiscoZine, "The PPDIO Network Lifecycle," 29 January 2009. [Online]. Available: http://www.ciscozine.com/wp-content/uploads/ppdioo.png.

[19] U. Chidiebele and O. Kennedy, "Effective Security Architecture for Virtualized Data," *International Journal of Advanced Computer Science and Applications,* vol. Volume 3, pp. 196-200, 2012.

[20] SoftEther, "VPN Communication Protocol," 2015. [Online]. Available: https://www.softether.org/4-docs/1-manual/2._SoftEther_VPN_Essential_Architecture/2.1_VPN_Communication_Protocol. [Accessed 26 May 2015].

[21] Digital Attack Map, "Understanding DDoS," 2013. [Online]. Available: http://www.digitalattackmap.com/understanding-ddos/.

[22] Debian, "UnattendedUpgrades," 4 May 2015. [Online]. Available: https://wiki.debian.org/UnattendedUpgrades. [Accessed 26 May 2015].

[23] Fakultas Rekayasa Industri, Rencana Strategis Fakultas Rekayasa Industri Universitas Telkom, Bandung: Fakultas Rekayasa Industri Universitas Telkom, 2014.

[24] Fakultas Rekayasa Industri Telkom University, Rencana Strategis Fakultas Rekayasa Industri, Bandung: Fakultas Rekayasa Industri Telkom University, 2014.

[25] Real World Studios, "Real World Studios," 06 May 2008. [Online]. Available: http://realworldstudios.com/news/article/1320/well-be-back-soon-apologies-for-the-lack-of-service/. [Accessed 26 November 2014].

[26] Open Web Application Security Project, "OWASP Top 10 Project," 17 April 2015. [Online]. Available: https://www.owasp.org/index.php/Top10#tab=OWASP_Top_10_for_2010. [Accessed 26 May 2015].

[27] OWASP, "Cross-site Scripting (XSS)," 22 04 2014. [Online]. Available: https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29.

[28] Cisco Systems, Cisco SAFE Reference Guide, San Jose: Cisco, 2010.

[29] JVSG, "CCTV Bandwidth and Storage Space Calculation," 2015. [Online]. Available: http://www.jvsg.com/bandwidth-storage-space-calculation/. [Accessed 26 May 2015].

[30] Data Center Journal, "Basics of a UPS System," 7 February 2012. [Online]. Available: http://www.datacenterjournal.com/facilities/basics-of-a-ups-system/.