MODEL *FRAMEWORK* UNTUK ANALISIS KEAMANAN DARI SERANGAN *DENIAL OF SERVICE* PADA SISTEM *E-LEARNING* UNIVERSITAS BUDI LUHUR

***Joko Christian Chandra*[1]**
[1]Program Studi Manajemen Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
e-mail: [1]joko.christian@budiluhur.ac.id

ABSTRAK

Universitas Budi Luhur menggunakan layanan pembelajaran Electronic Learning (E-Learning) berbasis web. Layanan ini sangat krusial dalam melaksanakan kegiatan belajar mengajar, sehingga tidak boleh ada kegagalan layanan dalam bentuk apa pun. Layaknya layanan berbasis web pada umumnya, sistem ini berpotensi memiliki kerentanan terhadap gangguan serangan keamanan, khususnya jenis Denial of Service (DoS) dan turunannya seperti Distributed Denial of Service (DDoS). Saat ini belum ada pengukuran kuantitatif dari tingkat kerentanan layanan tersebut, dan belum ada kaidah langkah pengamanan untuk menangani serangan DoS. Sebelum pengukuran tersebut dapat dilakukan, diperlukan sebuah model / kerangka kerja untuk melaksanakan proses analisis keamanan sistem yang berjalan. Menggunakan model tersebut, barulah proses analisis kuantitatif dapat dilakukan untuk memformulasikan mitigasi yang diperlukan. Berdasarkan kondisi tersebut, dalam penelitian kualitatif ini akan dilakukan pengkajian menggunakan metodologi tradisional waterfall untuk memformulasi model analisis yang dapat digunakan. Hasil penelitian ini akan menjadi salah satu pilar untuk menyiapkan layanan E-learning yang lebih resistan terhadap gangguan keamanan jenis DoS, yang secara langsung meningkatkan kualitas layanan bagi pengguna. Hasil dari penelitian ini adalah sebuah model analisis dalam bentuk kerangka kerja untuk melaksanakan analisis keamanan kuantitatif pada sistem e-learning. Hasil penelitian ini juga dapat menjadi template untuk melakukan pengujian sejenis bagi layanan web lain.

***Kata Kunci**: model analisis, keamanan, Denial of Service, e-learning, web*

1. PENDAHULUAN

1.1. Latar Belakang

Universitas Budi Luhur merupakan salah satu perguruan tinggi di Jakarta yang melaksanakan pola pembelajaran *blended learning* dengan memanfaatkan pembelajaran elektronik (e-learning). Untuk memberikan layanan tersebut diperlukan sebuah *Learning Management System* (LMS) yang fungsional dan operasional terus-menerus (24/7). Saat ini layanan e-learning yang dimaksud menggunakan LMS *open source* Moodle yang berada di bawah manajemen langsung dari salah satu direktorat. LMS Moodle menggunakan pola interaksi berbasis jaringan internet, bisa berupa web, *mobile application* atau *web service*. Namun memiliki layanan yang operasional saja tidak cukup, seiring dengan meningkatnya ketergantungan sivitas akademik terhadap layanan e-learning, jika terjadi kegagalan layanan, maka potensi kerugian yang dialami oleh pengguna menjadi makin besar. Kegagalan layanan e-learning akan menjadi hambatan besar dalam melaksanakan proses pembelajaran.

Salah satu langkah untuk menjamin ketersediaan layanan secara berkelanjutan adalah menyiapkan keamanan sistem tersebut. Dengan keamanan yang baik, salah satu faktor kegagalan layanan dapat dikurangi. Keamanan sistem sendiri memiliki cakupan yang luas, untuk riset ini difokuskan pada keamanan terhadap serangan *Denial of Service* (DoS), dan turunannya seperti *Distributed Denial of Service* (DDoS) karena pernah terjadi serangan *Denial of Service* (DoS) terhadap layanan ini. Perlu dipahami bahwa tidak ada mekanisme yang dapat dilakukan untuk menghalangi secara menyeluruh sebuah serangan DoS, namun sistem yang sudah dipersiapkan akan memiliki kemungkinan *down time* yang lebih kecil dan kesempatan perbaikan lebih baik.

Sebuah sistem yang tidak diamankan ibarat sebuah gudang penuh barang yang tidak dijaga. Jika sampai gudang tersebut rusak, atau barangnya mengalami kehilangan atau kerusakan, maka dapat melumpuhkan proses bisnis yang normal. Oleh karena itu lebih baik sedia payung sebelum hujan. Diperlukan sebuah pengukuran dasar kapabilitas sistem dan menemukan celah keamanan yang ada. Sayangnya belum ada model *framework* (kerangka kerja) yang tersedia sebagai panduan dalam pelaksanaan analisis keamanan sistem e-learning agar langkah mitigasi yang tepat dapat dilakukan.

Diperlukan sebuah model *framework* yang menjabarkan kerangka kerja dan langkah-langkah yang perlu dilakukan agar proses analisis dan hasil rancangan mitigasi yang dilakukan optimal dan sesuai dengan kondisi organisasi.

1.2. Identifikasi dan rumusan masalah

Berdasarkan pada latar belakang penelitian, berikut adalah identifikasi masalah yang didapat : "Sistem E-learning Universitas Budi Luhur belum memiliki panduan kerangka kerja untuk melaksanakan analisis keamanan sistem dari serangan *Denial of Service*". Sehingga menghasilkan rumusan masalah sebagai berikut:

"Bagaimana mengembangkan model *framework* analisis keamanan sistem E-learning Universitas Budi Luhur terhadap jenis serangan DoS, agar analisis kuantitatif dapat dilaksanakan dengan terstruktur?"

1.3. Batasan Masalah

Adapun batasan masalah yang digunakan dalam penelitian ini sebagai berikut:

1. Sistem E-learning yang dimaksud adalah https://elearning.budiluhur.ac.id yang memberikan layanan berbasis koneksi internet dengan antar muka web, dan *web service* (*mobile*).
2. Pengujian yang dilakukan adalah untuk kesiapan sistem dari serangan DoS dan turunannya menggunakan sudut pandang layer OSI 3-7.
3. Model analisis yang dimaksud berupa *framework* (kerangka kerja) dalam melakukan proses pengujian.
4. Langkah-langkah mitigasi yang dimaksud berupa solusi untuk meningkatkan daya tahan sistem terhadap serangan, berdasarkan hasil analisis dan *best practices*, terlepas dari kondisi kesiapan *stakeholder* mengimplementasikannya.
5. Sebagian data yang dianggap terlalu sensitif dan tidak cocok untuk dipublikasikan dalam laporan terbuka akan digantikan dengan data substitusi, atau interpolasi dari kondisi yang sebenarnya tanpa mengubah efek atau sebab-akibat yang ditimbulkan.
6. Penelitian ini tidak melakukan pengumpulan data kuantitatif, analisis yang muncul dari data tersebut, dan langkah mitigasi yang diperlukan, karena proses tersebut termasuk bagian dari penelitian lanjutan.

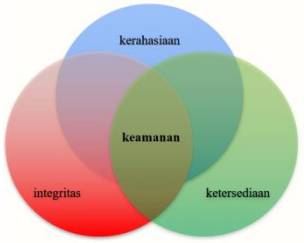
1.4 Tujuan dan manfaat penelitian

Tujuan utama adalah menghasilkan model (*framework*) analisis keamanan sistem E-learning Universitas Budi Luhur untuk mitigasi serangan DoS dan turunannya. Sedangkan manfaat utama dari hasil penelitian ini memungkinkan proses penelitian kuantitatif lanjutan dilaksanakan dengan terstruktur yang menghasilkan profil keamanan sistem dan langkah mitigasi terkait.

2. TINJAUAN PUSTAKA

2.1. Konsep Dasar Keamanan Sistem

Keamanan sistem komputer dapat dilihat sebagai kumpulan dari mekanisme yang melindungi sistem tersebut dari akses yang tidak di ijin kan, pencurian, kerusakan, dan gangguan dari layanan yang diberikan. Mekanisme untuk mencapai hal tersebut adalah menjamin kerahasiaan, integritas dan ketersediaan dari sistem dan data [1]. Gambar 1 menunjukkan hubungan ketiga komponen tersebut.



Gambar 1. Komponen Keamanan Sistem

2.2. Konsep Analisis Keamanan Sistem

Sistem informasi modern semakin kompleks, terdiri dari sistem elemen, sub-sistem, prasyarat, dan infrastruktur yang ekstensif. Hampir seluruhnya menghasilkan interaksi yang rumit dan karena sifatnya yang saling berhubungan: sangat rentan terhadap kondisi kejahatan [2]. Hal ini diperparah bahwa pada saat desain sistem, yang selalu diutamakan adalah sisi fungsionalitas dan operasional, tanpa mempertimbangkan aspek keamanan yang cukup mendalam. Sebagian besar sistem yang digunakan saat ini adalah hasil pengembangan analis yang menggunakan referensi buku-buku analisis sistem dan desain yang mengabaikan atau sangat minim memperhatikan aspek keamanan. Adapun urutan untuk melakukan penilaian keamanan sistem [3], organisasi harus :

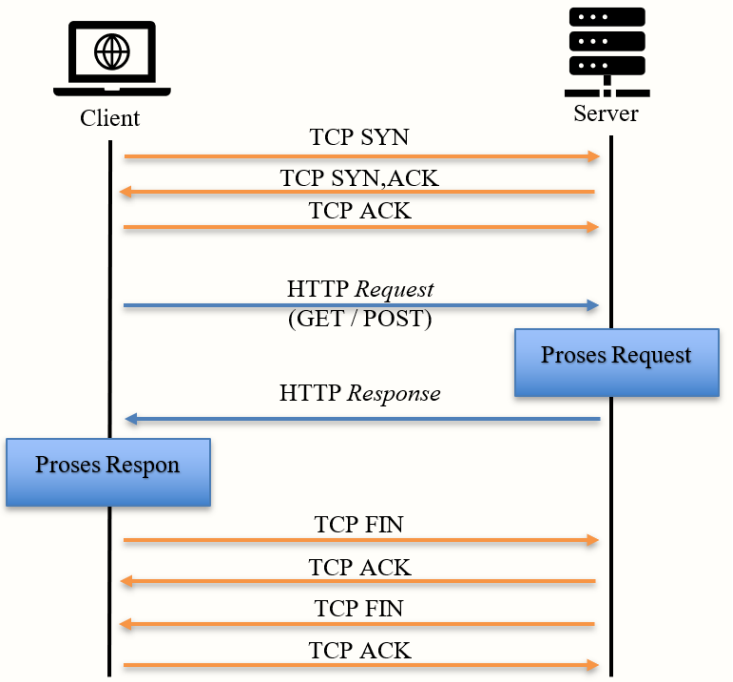
1. Menyiapkan kebijakan penilaian keamanan sistem / data.
2. Implementasi metodologi yang terdokumentasi dan dapat diulang.
3. Menentukan objektif dari setiap penilaian keamanan.

4. Analisis temuan, dan mengembangkan rencana, model atau teknik untuk melakukan mitigasi yang memecahkan permasalahan keamanan.

2.3. Konsep Dasar Layanan Web

Layanan web adalah salah satu layanan yang sudah menjadi standar dalam sistem informasi saat ini. Berawal dari protokol HTTP yang dikembangkan bersamaan dengan *protocol stack* TCP/IP, HTTP mengalami evolusi yang cukup banyak. Secara resmi HTTP versi 1.0 didokumentasikan pada *Request For Comment* (RFC) nomor 1945 dari draf bulan November 1994, hingga *update* terakhir pada Februari 2016 (RFC-IETF). Konsep kerja HTTP berdasarkan koneksi *client-server* dengan memanfaatkan *Hyper Text Markup Language* (HTML) sebagai data *encoding* dan penggunaan *Universal Resource Identifier* (URI).

Dalam praktiknya, protokol HTTP tidak dapat berdiri sendiri, melainkan sebagai komponen dari keseluruhan *protocol stack* TCP/IP. HTTP sendiri sebagai protokol dari layer aplikasi (model TCP/IP dan model OSI nomor 7), menggunakan protokol TCP pada layer Transport (model TCP/IP dan model OSI nomor 4). Sehingga sebelum komunikasi HTTP dapat dilakukan, protokol TCP harus membuka sesi koneksi. Selama komunikasi berlangsung, harus tunduk pada mekanisme TCP, dan setelah komunikasi selesai, protokol TCP menutup sesi koneksi. Gambar 2 menunjukkan ilustrasi kerja protokol HTTP dan TCP.



Gambar 2. Ilustrasi Kerja Protokol HTTP dan TCP

2.4. Konsep Keamanan pada Layanan *Web*

Layanan *web* pada dasarnya adalah aplikasi klien / server yang berjalan dengan konektivitas internet memanfaatkan konsep TCP/IP. Sehingga layanan web mendapatkan sifat turunan kelebihan dan kelemahan dan celah keamanan dari *protocol stack* TCP/IP. Cakupan kelemahan dan celah keamanan yang ada tidak dibahas satu-persatu di sini, namun akan disampaikan beberapa karakteristik dasar *web* yang membutuhkan pendekatan khusus pada analisis dan pengamanan.

Meskipun layanan web umum sangat mudah dikonfigurasi dan di manajemen secara dasar, sebenarnya *software* yang melandasi fungsionalitasnya sangat kompleks dan menyimpan banyak potensi celah keamanan. Sebuah layanan *web*, dalam hal ini web server dapat dieksploitasi sebagai landasan untuk menyerang infrastruktur jaringan organisasi lebih lanjut, hal ini dimungkinkan karena sifat layanan *web* yang terbuka pada publik di satu sisi, dan umumnya terhubung pada infrastruktur organisasi di sisi yang lain. Beberapa ancaman yang dapat muncul pada layanan web [4] disajikan dalam Tabel 1.

Tabel 1. Perbandingan Beberapa Ancaman pada Layanan *Web*.

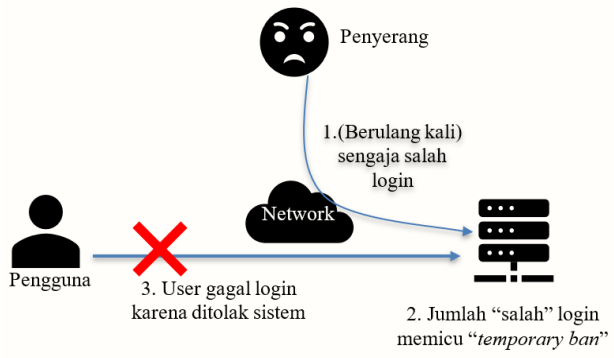
	Ancaman	Akibat	Pencegahan
Integritas	Modifikasi data pengguna *Trojan horse* browser Modifikasi memori Modifikasi lalu lintas pesan	Hilangnya informasi Membuka jalan ke ancaman lain	*Cryptographic checksums*
Kerahasiaan	"Penguping" di network Pencurian informasi dari server Pencurian informasi dari *client* Informasi konfigurasi jaringan Informasi *client* yang aktif	Kehilangan informasi Kehilangan privasi	Enkripsi dan penggunaan *web proxy*
Denial of Service (ketersediaan)	Mematikan *thread* dari *user* "Banjir" permintaan "aspal" Memenuhi disk atau memori Mengisolasi mesin dengan serangan DNS	Menghabiskan sumber daya sistem Mencegah pengguna mengakses layanan	Sulit untuk dicegah
Autentikasi	Peniruan *user* yang sah Pemalsuan data	Salah interpretasi oleh *user* Mempercayai informasi yang salah	Teknik kriptografi

2.5. Konsep Dasar Serangan *Denial of Service* dan Turunannya

Serangan *Denial of Service* (selanjutnya dituliskan DoS) adalah salah satu jenis serangan untuk melumpuhkan kapabilitas sistem memberikan layanan kepada penggunanya. Berbeda dengan jenis serangan lain yang umumnya berusaha untuk masuk ke dalam sistem (*gain entry*) atau mencuri data (*information stealing*), jenis serangan ini menggunakan permintaan sumber daya melalui prosedur yang valid.

Serangan DoS sering dianggap sebagai salah satu serangan yang paling signifikan terhadap jaringan komputer pada beberapa tahun terakhir. Serangan ini bisa mengakibatkan kekacauan besar pada fungsi jaringan, dan sangat sulit untuk melindungi sistem dari jenis serangan ini [5].

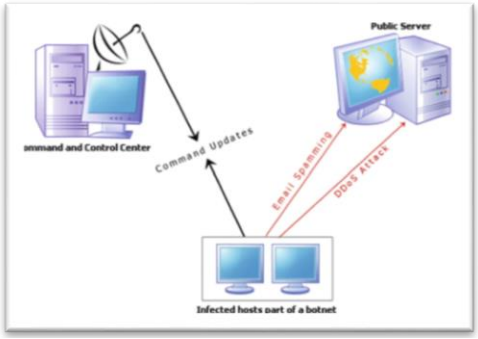
Contoh serangan yang paling mudah adalah pihak ketiga mencoba menghambat seorang user *login* ke dalam sistem dengan berulang kali mencoba *login* ke sistem tersebut (dengan kredensial yang tidak perlu valid) agar mengaktifkan mekanisme pertahanan sistem terhadap kegagalan log in. Gambar 3 menunjukkan ilustrasi serangan DoS tersebut.



Gambar 3. Ilustrasi DoS untuk *Login System*

Bentuk serangan lain adalah dengan meminta sumber daya dari server target hingga memicu "*overload*" atau kelebihan beban. Efek yang dihasilkan adalah server target tidak bisa memberikan layanan kepada pengguna yang membutuhkan. Serangan tunggal dari sebuah *IP address* tunggal cukup mudah untuk ditangani dengan menambahkan baris firewall, namun saat serangan datang dari banyak titik disebut dengan *Distributed Denial of Service* (DDoS), mempertahankan layanan akan sulit dilakukan.

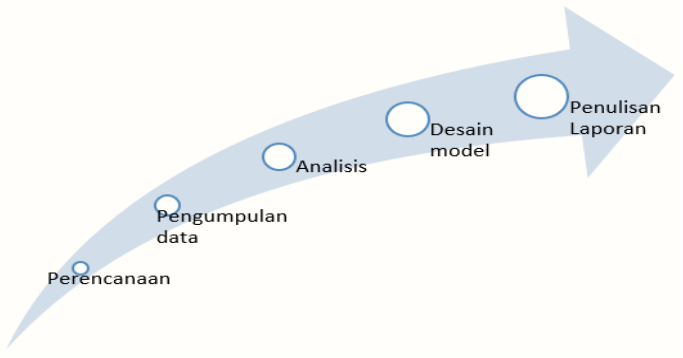
Serangan DDoS dapat berasal dari komputer *zombie* (bagian dari *botnet*) tapi ada banyak teknik lain seperti *reflection* dan *amplification attack* yang menyebabkan sistem pihak ketiga lain "dikelabui" untuk mengirimkan lalu lintas pada server target. Gambar 4 memberikan ilustrasi serangan DDoS.



Gambar 4. Ilustrasi Anatomi Penyerangan DDoS[1]

3. METODE PENELITIAN

Penelitian ini merupakan penelitian kualitatif yang menggunakan kerangka umum SDLC *Waterfall*. Gambar 5 menunjukkan tahapan penelitian yang dilakukan :



Gambar 5. Tahapan Penelitian

3.1. Perencanaan

Langkah awal ini bertujuan untuk mendapatkan persetujuan administratif, penentuan ruang lingkup, perumusan masalah dan penentuan tujuan. Juga untuk membuat daftar *stakeholder* terkait yang perlu dihubungi dalam pelaksanaan penelitian dengan objek penelitian sistem e-learning Universitas Budi Luhur. Termasuk di dalam perencanaan ini adalah pengumpulan data karakteristik awal sistem yang akan mempengaruhi proses pengumpulan data yang lebih detail.

3.2. Pengumpulan Data

Ada dua bagian utama dari pengumpulan data :

1. Studi pustaka.
   Studi pustaka dilakukan untuk mengetahui keilmuan (teori), dan hasil penelitian yang terkait dengan komponen atau kerja sistem sejenis dari objek penelitian.
2. Observasi dan wawancara.
   Data ini dikumpulkan dari proses observasi periset yang berinteraksi langsung dengan sistem, dan dengan wawancara / diskusi grup bersama *stakeholder* objek penelitian. Dalam konteks penelitian ini utamanya adalah pihak manajemen dan administrasi dari sistem e-learning.
3. Analisis dokumentasi.
   Data dokumentasi sistem dasar di kumpulkan dan dipelajari, kemudian diverifikasi dengan *stakeholder* terkait.

3.3. Analisis

Berdasarkan data yang dikumpulkan dan hasil diskusi grup, dilakukan analisis terhadap data yang tersedia dan *best-practices* yang dilakukan dan dipublikasikan oleh para profesional keamanan sistem. Proses ini mempertimbangkan faktor internal : (spesifikasi *hardware* dan *software*), kondisi yang unik dari objek penelitian utamanya dari sudut pandang standar pelayanan, *quality of service*, dan ketersediaan layanan bagi penggunanya,

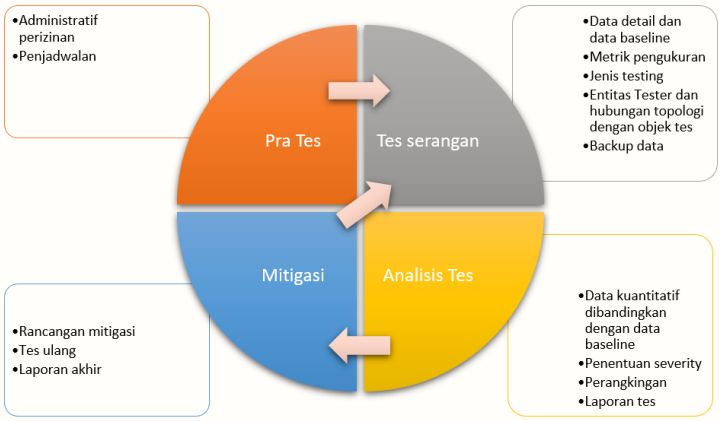
serta ketersediaan sumber daya (dana dan SDM). Dari sisi faktor eksternal mempertimbangkan : standar keamanan umum internasional, konektivitas dan mitra penyedia, sejarah serangan.

3.4. Desain Model

Pada langkah ini dikembangkan rancangan metode pengujian yang spesifik terhadap sistem tersebut. Hal ini diperlukan karena tidak ada sistem yang sama persis dari sudut pandang kapabilitas, kondisi keamanan, jenis layanan, jumlah layanan, jumlah pengguna layanan, target kenyamanan dan target keamanan yang mau dicapai. Dengan memformulasikan metode testing, didapatkan urutan yang sistematis dalam melakukan proses testing untuk menghasilkan data yang valid. Pada tahap ini pula dihasilkan kebijakan penilaian, metrik dan asumsi yang digunakan pada proses testing. Hasil dari langkah ini adalah sebuah model *framework*. Model ini yang akan menjadi hasil dari penelitian yang kemudian diuji silang dengan *stakeholder* terkait untuk validasi.

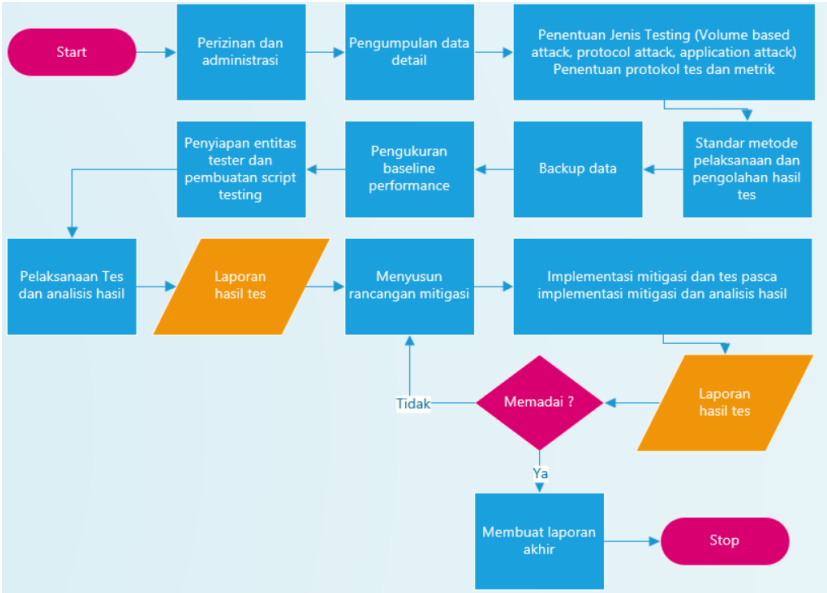
4. HASIL DAN PEMBAHASAN

Setelah pelaksanaan tahapan penelitian, dihasilkan kesimpulan terkait faktor dan entitas yang mempengaruhi analisis keamanan dan model (*framework*) untuk melakukan analisis keamanan sistem e-learning. Gambar 6 menunjukkan model dasar komponen yang terkait dalam ranah grup proses utama sebanyak 4.



Gambar 6. Grup Proses Model Analisis Keamanan Sistem *Elearning*

Sedangkan gambar 7 menunjukkan *workflow* urutan proses yang harus dilakukan dalam melaksanakan analisis keamanan.



Gambar 7. *Workflow* Proses Analisis Keamanan

4.1. Perizinan dan Administrasi

Sebuah proses analisis keamanan sistem memerlukan testing yang *intrusive* dan dapat mengakibatkan kerusakan pada sistem jika tidak dilakukan dengan benar. Hal ini juga terkait dengan keamanan data yang disimpan pada *objek testing*. Oleh karena itu sebelum proses analisis keamanan dilakukan, perlu didapatkan dulu perijinan yang terkait dan koordinasi dengan pihak administrasi terkait jadwal.

4.2. Pengumpulan Data Detail

1. Data *server* :
   a. *Hardware*: spesifikasi *hardware*, dan karakteristik merek/model *hardware* yang digunakan,
   b. *Software*: spesifikasi *software*, utamanya adalah server web *engine* yang digunakan, bahasa pemrograman yang digunakan pada sistem, server *database* yang digunakan.
2. Data jaringan dan konektivitas : topologi, *bandwidth*, *delay*, *jitter*, *latency*, jenis dan kapasitas perangkat *intermediate* terdekat dengan server, karakteristik dan jenis langganan koneksi internet.

4.3. Penentuan Protokol, Metrik Pengukuran, dan Metode Teknis *Testing* (dan Metode Pengolahan Data)

Tentukan jenis protokol yang mau diuji coba berkaitan dengan metrik yang mau diukur. Untuk menentukan kerawanan sistem dari serangan DDos, langkah awal dapat dilakukan testing serangan DoS. Ada banyak jenis serangan yang bisa dilakukan, tetapi secara umum masuk dalam 3 kategori besar yaitu :

1. *Volume based attack*: bertujuan untuk menghabiskan *bandwidth* (saturasi *bandwidth*) melebihi kapasitas fisik dari kartu jaringan target. Hal ini mengakibatkan permintaan layanan yang valid tidak bisa diterima. Pengukuran menggunakan *bit per second* (bps).Termasuk dalam serangan ini adalah UDP *flood*, DNS *amplification*, ICMP (*ping*) *flood*.
2. *Protocol attack*: juga disebut sebagai *state-exhaustion attack*, jenis serangan ini berusaha menggunakan sumber daya server (dari sisi sistem operasi), atau perangkat *intermediate* seperti firewall dan *load balancer*. Pengukuran menggunakan *packet per second* (pps). Termasuk dalam serangan ini adalah SYN *flood*, *Ping of Death*, *fragmented packet attack*, dan sejenisnya.
3. *Application layer attack:* bertujuan untuk melumpuhkan aplikasi yang memberikan layanan dengan memanfaatkan cara kerja *native* dari layanan tersebut, misalnya GET / POST *flood*s, serangan spesifik ke *webserver*, *database* server, OS, dll. Pengukuran menggunakan *request per second* (rps). Juga serangan yang menggunakan celah keamanan yang sudah ditemukan pada versi aplikasi spesifik. Termasuk dalam serangan ini adalah Slowloris, HTTP *Flood*, dan sejenisnya.

4.4. Penentuan Standar Metode Pelaksanaan dan Pengolahan Hasil Tes

Diperlukan sebuah standar untuk mekanisme pelaksanaan khususnya jumlah iterasi tes, dan bagaimana mengolah hasil tes (cara menghitung atau menentukan hasil tes yang digunakan, apakah rata-rata, tertinggi, terendah, atau bentuk lainnya).

4.5. *Backup* Data

Banyak dari proses testing yang dilakukan akan "memaksa" sistem di luar dari batas normal yang mungkin mengakibatkan kerusakan sebagian atau keseluruhan data yang berjalan. Oleh karena itu, proses *backup* data (dan konfigurasi terkait) wajib dilakukan untuk mencegah kehilangan data.

4.6. Pengukuran Baseline Performance

Menggunakan metrik yang sudah ditentukan pada tahap sebelumnya, dilakukan pengukuran kondisi keseharian (*baseline performance*). Pengukuran ini dapat dilaksanakan dalam rentang (durasi) yang disesuaikan dengan objek testing.

4.7. Persiapan Entitas Tester dan Pembuatan Script

Pengujian keamanan untuk DoS (dan DDoS) memerlukan entitas tester (mesin yang menyerang), sehingga perlu disiapkan sesuai dengan jenis testing yang direncanakan. Hubungan topologi antara entitas tester dengan objek tes juga perlu didesain agar mengakibatkan dampak serangan maksimal dengan menggunakan jumlah tester minimal. Testing yang mau dilaksanakan disusun dalam bentuk *script* yang dapat mudah digunakan untuk memulai, menghentikan, dan menghasilkan *output* testing dalam format yang mudah untuk diolah. Dalam penelitian ini disarankan menggunakan *script* linux karena obyek riset menggunakan sistem operasi linux.

4.8. Pelaksanaan Testing dan Analisis Hasil Testing

Adalah pelaksanaan dari testing yang sudah ditentukan pada objek tes. Dilakukan sebanyak n kali (sesuai dengan kesepakatan pada proses perizinan dan administrasi). Data hasil tes dikumpulkan dan kategorikan. Data hasil tes dari tiap kategori kemudian diolah dengan metode yang sudah ditetapkan untuk kemudian disajikan secara kuantitatif dan dibandingkan dengan data *baseline*, kemudian diukur tingkat kerentanannya (*severity*) dengan mempertimbangkan aspek probabilitas. Setelah itu dilakukan pemeringkatan dari tingkat kerentanan tertinggi hingga terendah.

4.9 Pembuatan Laporan Hasil Tes, dan Rancangan Mitigasi

Berdasarkan analisis hasil testing, disajikan informasi kondisi sistem yang berjalan (as-is).

4.10. Pembuatan Rancangan Mitigasi

Berdasarkan hasil tes, dan dengan menyertakan *stakeholder* terkait, disusun rancangan mitigasi yang perlu dilakukan untuk mengurangi dampak serangan yang dapat terjadi.

4.11. Implementasi dan *Testing* Rancangan Mitigasi

Jika disetujui, maka rancangan mitigasi di implementasikan pada sistem dan proses diulangi dari langkah 6. Pengulangan dapat dilakukan sesuai kebutuhan dan kondisi kesanggupan organisasi, hingga kondisi saat pihak administratif merasa hasil sudah memadai (atau tidak bisa dilanjutkan karena keterbatasan SDM dan dana).

4.12. Pembuatan Laporan Akhir

Setelah keseluruhan proses dilakukan, maka perlu disusun laporan akhir yang menunjukkan informasi komprehensif dari sistem e-learning objek tes, kondisi sebelum, dan kondisi sesudah, dan perubahan nilai -nilai metrik terkait.

5. KESIMPULAN

Berdasarkan hasil dari penelitian ini, dihasilkan sebuah model *framework* yang dapat digunakan sebagai acuan dalam pelaksanaan proses analisis keamanan sistem e-learning Universitas Budi Luhur dari serangan *Denial of Service* (DoS). Model ini juga dapat digunakan untuk melakukan proses analisis keamanan pada sistem lain.

6. SARAN

Hasil penelitian ini digunakan untuk pelaksanaan proses analisis kuantitatif, yang kemudian dianalisis dan dilanjutkan dengan implementasi mitigasi agar keamanan dari sistem e-learning yang menjadi objek riset dapat ditingkatkan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Direktorat Digitalisasi Pembelajaran Universitas Budi Luhur yang telah memberikan dukungan ijin dan pelaksanaan riset ini.

DAFTAR PUSTAKA

[1] Duffanny, J. L., 2018, *Computer Security*, Daimi, K. (ed.)., *Computer and Network Security Essentials*, Ed. 1, Springer International Publishing, Cham-Switzerland, pp. 3–20. doi: 10.1007/978-3-319-58424-9.

[2] Beach, P. M. et al., 2019, Analysis of Systems Security Engineering Design Principles for the Development of Secure and Resilient Systems, *IEEE Access*, Volume 7, pp. 101741–101757. doi: 10.1109/access.2019.2930718.

[3] Scarfone, K. et al., 2008, Technical Guide to Information Security Testing and Assessment- Gaithersburg, MD: National Institute of Standards and Technology USA, https://www.govinfo.gov/content/pkg/GOVPUB-C13-894df23cbad6ad74af7d49c17b081dd1/pdf/GOVPUB-C13-894df23cbad6ad74af7d49c17b081dd1.pdf., diakses tanggal 13 Oktober 2020.

[4] Stallings, W. ,2017, *Cryptography And Network Security Principles And Practice*, Global Ed. 7, Pearson Education Limited, Essex-England.

[5] Hamed, T., Ernst, J. B. and Kremer, S. C., 2018, *A Survey and Taxonomy of Classifiers of Intrusion Detection Systems*, Daimi, K. (ed.)., *Computer and Network Security Essentials*, Ed. 1, Springer International Publishing, Cham-Switzerland, pp. 21–39. doi: 10.1007/978-3-319-58424-9.