Jurnal TICOM: *Technology of Information and Communication*
Volume 10, Nomor 3, Mei 2022 Hal: 197-203 E-ISSN: 2962-7982

Analisis Keamanan Layanan E-Learning Terhadap Serangan Dos Dan Implementasi Mitigasi Pada Universitas Budi Luhur

Joko Christian Chandra

[1]Fakultas Teknologi Informasi, Manajemen Informatika, Universitas Budi Luhur, Jakarta, Indonesia
Jalan Raya Ciledug, Petukangan Utara, Jakarta Selatan 12260
E-mail: joko.christian@budiluhur.ac.id

Abstrak—**Universitas Budi Luhur di Jakarta memiliki layanan pembelajaran berbasis elektronik (E-Learning). Layanan ini berperan penting dalam pelaksanaan kegiatan belajar mengajar, khususnya selama masa pembelajaran daring, sehingga kegagalan layanan dalam bentuk apa pun akan berdampak besar. Layanan E-learning yang dimaksud berbasis web dengan pendekatan komunikasi *client-server*. Layanan ini menggunakan server tunggal, sehingga rentan terhadap serangan keamanan jenis *Denial of Service* (DoS) dan *Distributed Denial of Service* (DDoS). Serangan DoS berupaya untuk menghabiskan sumber daya server yang ada, sehingga layanan kepada pengguna valid menjadi terganggu atau terputus. Data kuantitatif dari tingkat kerentanan layanan belum diukur dan penerapan langkah mitigasi masih rendah. Berdasarkan keadaan tersebut, penelitian ini mengkaji komponen sistem yang terkait, menggunakan metode model *workflow* analisis keamanan sistem berbasis web untuk melakukan pengukuran tingkat keamanan server, memformulasi rancangan mitigasi, dan menerapkan mitigasi yang diperlukan. Hasil dari penelitian ini adalah peningkatan keamanan terhadap sebagian jenis serangan DoS dan DDoS, sehingga layanan E-learning memiliki peningkatan rata-rata 3 kali kapabilitas untuk menangani serangan DDoS dari *Application layer attack*.**

Kata Kunci— keamanan sistem, Denial of Service, e-learning, layanan berbasis web.

Abstract—**Budi Luhur University in Jakarta has Electronic Learning (E-Learning) services. This service is very crucial in carrying out teaching and learning activities, especially during the online learning period, so that any service failure in any form will have a major impact. The e-learning service in question is web-based with a client-server communication approach. This service uses a single server, thus susceptible to security attacks, especially Denial of Service (DoS) and Distributed Denial of Service (DDoS) types. DoS attacks are a form of attack that consumes existing server resources, so that services to valid users are interrupted or disconnected. Quantitative data for service vulnerability has not been measured and the implementation of mitigation measures is still low. Based on these circumstances, this study examines the related system components, using method of web security analysis workflow to measure server security levels, formulate mitigation plans, and implement the necessary mitigations. The result of this research is an increase in security against certain types of DoS and DDoS attacks, so that E-learning services have 3-fold capability to withstand DDoS Application layer attacks.**

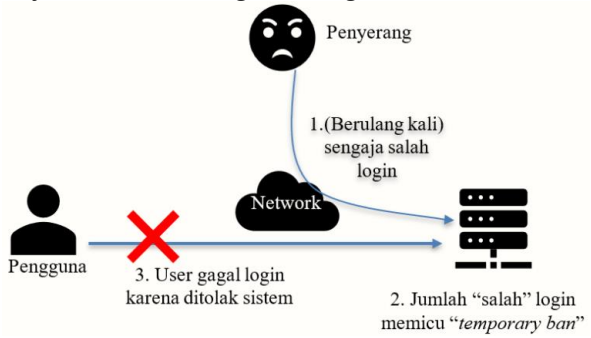
Keywords— *system security, Denial of Service, e-learning, web-based services.*

I. PENDAHULUAN

Universitas Budi Luhur memanfaatkan *Learning Management System* (LMS) berbasis moodle untuk memberikan layanan e-learning. Layanan ini harus tersedia 24/7 hampir tanpa *down time* untuk melayani proses belajar mengajar daring. Dengan jumlah pengguna yang lebih dari 10000 pengguna, jika terjadi kegagalan layanan, maka kerugian yang muncul akibat terhambatnya proses bisnis pendidikan berpotensi untuk merugikan semua pihak terkait. Kegagalan layanan bisa muncul dalam berbagai bentuk, sisi teknis, sisi manusia, sisi administrasi, sisi keamanan, dan *force majeure*. Dalam penelitian ini, diangkat sisi keamanan sistem komputer yang dapat dilihat sebagai kumpulan dari mekanisme yang melindungi sistem tersebut dari akses yang tidak di ijin kan, pencurian, dan gangguan dari layanan yang diberikan [1]. Seiring dengan meningkatnya kompleksitas sistem TI yang memiliki banyak komponen, hal ini meningkatkan kerentanan terhadap kondisi kejahatan [2]. Keadaan ini diperparah bahwa banyak sistem yang dikembangkan menggunakan referensi buku analisis sistem yang mengabaikan atau tidak memperhatikan aspek keamanan. Sehingga untuk melakukan penilaian keamanan sistem [3], organisasi harus menyiapkan kebijakan penilaian, mengimplementasikan metodologi yang terdokumentasi, menentukan objektif setiap penilaian keamanan, hingga melakukan analisis temuan untuk mengembangkan rencana, dan teknik mitigasi yang menjawab permasalahan.

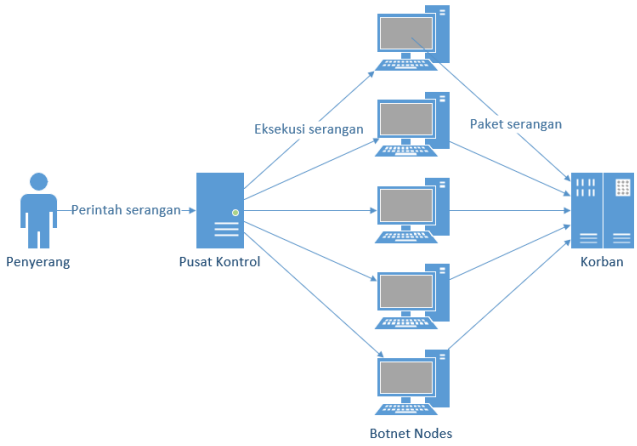
Keamanan layanan web sangat dipengaruhi oleh protokol yang bekerja menyusunnya, karena mekanisme kerjanya yang kompleks dan menyimpan banyak celah keamanan, sebuah layanan berbasis web dapat digunakan untuk menyerang infrastruktur jaringan lain, khususnya jika terbuka bagi akses publik. Ancaman dari sisi integritas, kerahasiaan, ketersediaan dan autentikasi dapat di mitigasi hanya dengan langkah-langkah yang spesifik untuk setiap jenisnya [4]. Layanan web yang dijalankan oleh web server dapat menggunakan berbagai aplikasi, dua aplikasi besar pemimpin pasar adalah Apache Web server dan Nginx [5]. Karena sifat kerjanya yang berbasis web, keamanan layanan e-learning rentan terhadap serangan eksternal. Serangan eksternal yang bisa dialami oleh sebuah

layanan IT cukup beragam, namun penelitian ini membahas *Denial of Service*. *Denial of Service* (DoS) merupakan jenis serangan yang melumpuhkan kapabilitas sistem untuk memberikan layanan kepada pengguna yang semestinya. Serangan DoS dianggap sebagai salah satu serangan yang paling signifikan beberapa tahun terakhir, sangat sulit untuk melindungi sistem dari jenis serangan ini [6]. Gambar 1 menunjukkan ilustrasi singkat serangan DoS.



Gambar 1.Ilustrasi DoS pada proses login sistem [7]

Distributed DoS (DDoS) adalah versi yang lebih agresif dari DoS. *Application Layer* DDoS, sebagai salah satu variannya adalah yang paling sulit dideteksi, karena tidak seperti serangan layer network, serangan AL-DDoS dapat dijalankan dengan sumber daya yang rendah, dan memanfaatkan *request* yang resmi[8]. Serangan AL-DDoS terlihat "resmi" pada layer OSI 1,2,3 dan berusaha untuk mengeksploitasi protokol HTTP ketimbang mengirimkan lalu lintas yang tinggi[9]. Penyerangan dengan mekanisme *botnet* adalah yang paling umum. *Botnet* memanfaatkan banyak komputer *zombie*, penyerang dapat melumpuhkan server dan layanan target menggunakan penyerang dari penjuru dunia. Gambar 2 menunjukkan ilustrasi penyerangan DDoS secara umum.



Gambar 2. Ilustrasi Penyerangan DDoS

Kelemahan yang meningkatkan kemungkinan serangan DoS adalah konfigurasi TCP/IP *stack* yang kurang baik dan sistem operasi yang tidak di *patch*.

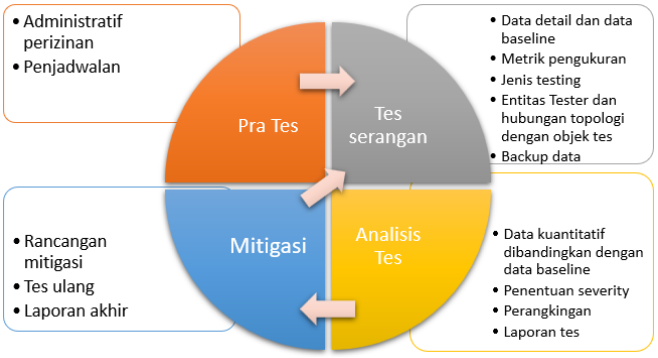
Layanan e-learning yang digunakan Universitas Budi Luhur pernah mengalami *down time* sebagai imbas dari serangan *Distributed DoS* (DDoS). Jenis serangan ini memang tidak bisa dihentikan, tetapi bisa dikurangi dampaknya terhadap layanan yang diserang. Memahami bahwa diperlukan sebuah model *framework* pengujian, penulis telah menyusun *framework* untuk melaksanakan proses analisis keamanan. Setelah tata cara dan pola analisis berhasil dikembangkan, maka diperlukan tindakan lanjutan berupa pelaksanaan teknis pengukuran dan implementasi. Penelitian ini melakukan pengukuran kuantitatif dari kapabilitas sistem e-learning, memformulasikan langkah mitigasi yang dimungkinkan, mengimplementasikan, untuk kemudian diukur kembali tingkat efektivitas mitigasi secara teoritis dan uji sintetis. Berdasarkan latar belakang di atas, dapat disusun sebuah rumusan masalah sebagai berikut :
"Bagaimana melaksanakan analisis keamanan kuantitatif terhadap serangan *Denial of Service* pada sistem E-learning Universitas Budi Luhur"; "Bagaimana menyusun langkah mitigasi yang dapat diterapkan dan mengimplementasikannya pada sistem E-Learning Universitas Budi Luhur"; dan "Perubahan apa yang terjadi setelah implementasi mitigasi diterapkan?".

Agar lebih tepat sasaran, batasan masalah dari penelitian ini pada layanan e-learning https://elearning.budiluhur.ac.id, dengan pengujian spesifik untuk serangan DoS dan DDoS, mencakup OSI layer 3, 4, 5, 6, dan 7. Data yang dianggap terlalu sensitif, dirahasiakan, atau dapat membocorkan mekanisme keamanan lain tidak disajikan. Penelitian ini tidak ditujukan untuk membuat *early warning system* serangan DoS. Berbeda dengan [10] yang menggunakan *machine learning*, atau [11] yang menggunakan *genetic algorithm*, pengukuran pada penelitian ini menggunakan uji sintetis sesuai dengan *best practices* yang valid saat pengujian dan memanfaatkan model *framework* [7]. Implementasi mitigasi yang dilakukan hanya dalam ruang lingkup memperbaiki / menambah konfigurasi layanan *software* yang digunakan. Penambahan perangkat fisik dan atau peningkatan level layanan pada ISP tidak termasuk dalam mitigasi yang dilaporkan pada penelitian ini.

Tujuan dari penelitian ini adalah melakukan pengukuran dan analisis terhadap kapabilitas layanan e-learning menghadapi serangan DoS dan DDoS. Kemudian mengimplementasikan model *framework* analisis keamanan dalam pengukuran teknis yang kuantitatif. Luaran berupa informasi kuantitatif yang dijadikan dasar analisis dan perancangan mitigasi. Implementasi mitigasi dapat kembali diuji secara iterasi untuk peningkatan berkesinambungan. Manfaat dari penelitian ini menghasilkan layanan e-learning Universitas Budi Luhur yang memiliki daya tahan lebih baik terhadap serangan DoS, dan *DDoS*.

II. METODE PENELITIAN

Sebuah model *workflow* digunakan untuk melakukan proses analisis keamanan pada sistem layanan berbasis web akan memiliki 4 grup proses utama, yaitu : pra-tes, tes serangan, analisis tes, dan mitigasi [7]. Gambar 3 menunjukkan grup proses dalam model analisis keamanan.



Gambar 3. *Process Group* Analisis Keamanan Sistem Berbasis Web [7].

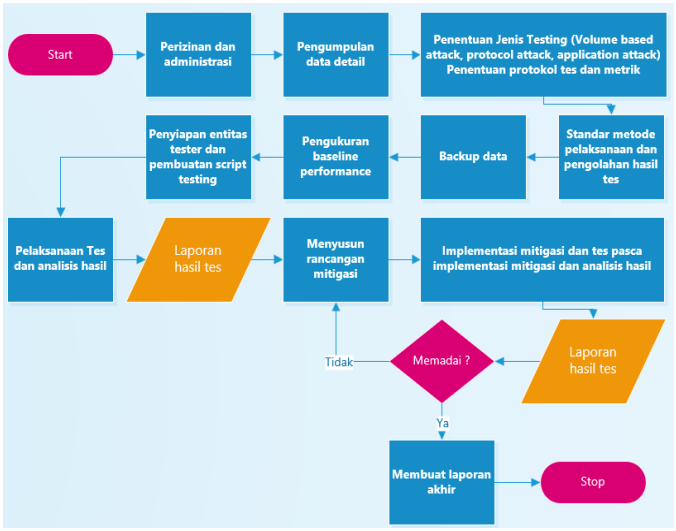
Data penelitian didapatkan dari berbagai sumber, manusia maupun sistem. Data administratif dan kebijakan digunakan sebagai acuan, seperti : standar layanan, standar operasi, standar penanggulangan bencana, dan standar kebijakan layanan, baik dari unit pengelola layanan, maupun lembaga yang menaunginya.

Data teknis dan kuantitatif didapatkan dari proses pengukuran *baseline performance*, di antaranya : *bandwidth*, *throughput*, rerata *user*, *latency*, rerata koneksi, jenis dan konfigurasi protokol, jenis dan konfigurasi aplikasi layanan web. Data teknis penting lain adalah log dari operasional sistem yang berjalan, mencakup : *access log, bandwidth usage log, violation log*.

Untuk melaksanakan penelitian ini digunakan kerangka kerja dan *workflow* urutan proses pelaksanaan analisis keamanan sistem berbasis web. Adapun urutannya adalah :

1. Diawali dari proses perizinan & administrasi.
   Karena sistem dan data yang akan dianalisis bersifat *business critical* dan sebagian rahasia.
2. Pengumpulan data detail.
   Data yang dimaksud adalah spesifikasi teknis *hardware* dan *software* semua komponen terkait layanan, semua dokumen kebijakan, standar operasi dan dokumentasi jaringan IT.
3. Penentuan jenis testing, protokol, metrik pengukuran, dan metode teknis testing.
   Berdasarkan data detail yang dikumpulkan, ditentukan parameter pengujian sesuai standar HTTP yang terbaru RFC 9113 [12].
4. Penentuan standar metode pelaksanaan dan pengolahan tes.
   Berdasarkan data detail yang dikumpulkan, ditentukan parameter pengolahan data yang dihasilkan.
5. *Backup* data.
   Sebelum pelaksanaan, seluruh data pada layanan perlu di *backup* pada server dan atau media berbeda, dengan kapabilitas restorasi 100% kembali ke kondisi sebelum pengujian.
6. Pengukuran *baseline performance*.
   Dilakukan pengukuran *performance* teknis secara sehari-hari, dapat juga di inferensi dari data log dan dokumen administratif yang sudah dikumpulkan.
7. Persiapan entitas tester dan *script testing*.
   Untuk melakukan pengujian diperlukan satu atau lebih entitas (server lain) yang mampu menyamai atau melebihi kapabilitas dari server yang diuji. *Script command* pengujian berbasis teks juga disiapkan.
8. Pelaksanaan testing.
   Dilakukan pada kondisi *off-hours* atau setidaknya pada beban rendah, disarankan menginformasikan dulu pada pengguna bahwa masuk ke periode *maintenance*.
9. Analisis hasil testing dan pembuatan laporan.
   Hasil pengujian pertama dianalisis dan dibuat laporan versi awal.
10. Perancangan mitigasi.
    Berdasarkan hasil pengujian pertama, mempertimbangkan *best practices*, kapabilitas sistem, dan kebijakan / kemampuan / komitmen organisasi, disusun bentuk mitigasi yang dapat dilakukan.
11. Implementasi dan testing rancangan mitigasi.
    Rancangan mitigasi hasil proses sebelumnya di konfigurasikan / ditambahkan / diganti ke sistem target dan dilakukan testing ulang.
12. Pembuatan laporan hasil tes dan analisis hasil mitigasi.
    Hasil pengujian kedua dianalisis dan dibuat laporan pembanding. Kemudian dibandingkan hasil sebelum dan sesudah implementasi mitigasi.
13. Pengulangan dari langkah 10 jika hasil tidak memuaskan.
    Penentuan keputusan melanjutkan usaha mitigasi atau menghentikan. Keputusan diambil bersama oleh pihak yang relevan mencakup tapi tidak terbatas pada *stake holder* langsung sistem (dengan mengecualikan pengguna umum).
14. Pembuatan laporan akhir.
    Jika implementasi hasil mitigasi dirasakan sudah mencukupi, maka dibuat laporan akhir.

Gambar 4 menunjukkan urutan tahapan pelaksanaan penelitian dalam bentuk *flowchart*.



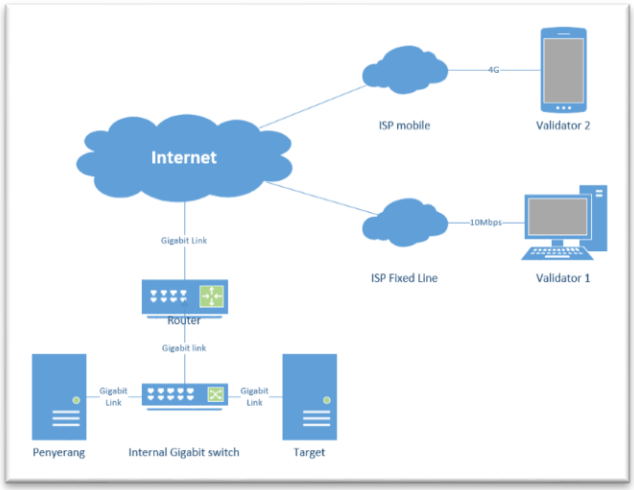
Gambar 4. *Workflow* Proses Analisis Keamanan Sistem E-Learning [7]

III. HASIL DAN PEMBAHASAN

Proses pelaksanaan teknis dari keseluruhan pengujian cukup ekstensif. Bagian perizinan, administratif, hingga *backup* data sengaja dihilangkan karena tidak dapat disajikan sepenuhnya dalam artikel jurnal ini. Secara umum dapat dilaporkan sebagai berikut:

A. *Topologi Jaringan pengujian*

Untuk melakukan pengujian yang efektif pada mayoritas jenis pengujian, server tester (penguji) harus memiliki koneksi jaringan yang tinggi dan sebaiknya berdekatan dengan server target. Digunakan topologi jaringan seperti pada Gambar 5. Terlihat bahwa server penyerang memiliki koneksi *gigabit* penuh untuk men-saturasi *bandwidth* yang tersedia. Penggunaan topologi ini juga untuk menghindari gangguan layanan bagi ISP yang memberikan layanan ke lebih dari satu penyewa di bawah "*Router*".



Gambar 5. Topologi jaringan pengujian

B. Baseline performance

Tabel 1 adalah beberapa metrik *baseline performance* yang diukur pada server target pada penggunaan jam operasional normal (jam 06:00-22:00).

TABEL 1. KUTIPAN METRIK *BASE PERFORMANCE*

Jenis	Nilai	pengujian
Bandwidth	1000 Mbps	#ethTool em1 | grep -i speed
Pengolahan Packet per Second	67.67 Kilo Packet per second	#time hping3 {target} -q -i u{durasi} –ICMP | tail -n10
Port terbuka	4 buah (detail dirahasiakan)	Nmap -sS -sU -T4 -A -v elearning.budiluhur.ac.id
Rerata penggunaan *bandwidth* pada kondisi normal	Rx:68.51 kbps Tx: 990.82 kbps Rx: 71pps Tx: 102 pps	/sys/class/net/{nama *interface*}/statistics/ #vnstat -i {nama interface} -tr {durasi}
Established connection	15 *concurrent*	Pada moodle sekitar 75-105 *user online*.

C. *Kategori Testing*

Ada 3 kategori testing serangan yang akan dilakukan:

1. *Volume Based Attack*. Tujuan dari serangan ini adalah menghabiskan *bandwidth* (saturasi atau memenuhi kapasitas *bandwidth*). Contoh serangan adalah DNS *amplification*, UDP *flood*, ICMP (ping) *flood*.
2. *Protocol attack*. Disebut juga *state-exhaustion attack* bertujuan menghabiskan sumber daya perangkat *intermediate*, atau sistem operasi, atau perangkat *firewall* dan *load balancer*. Contoh adalah SYN *flood*, Ping *of Death*, *fragmented packet attack*.
3. *Application layer attack*. Serangan ini melumpuhkan aplikasi atau *services* yang bertugas memberikan layanan dengan memanfaatkan cara kerja *native* dari layanan tersebut. Pengukuran menggunakan *request per second* (rps). Termasuk dalam serangan ini adalah Slowloris, HTTP *Flood*.

D. *Jenis serangan testing*

Menimbang bahwa server target berfungsi memberikan layanan web saja, berikut adalah jenis serangan yang akan di test:

1. UDP *flood* (dengan hping3) --> volume.
2. DNS *Amplification* (dengan *script* saddamnew) --> volume.
3. ICMP (ping) *flood* (dengan hping3) -->volume /*protocol*.
4. SYN *flood* (dengan hping3) --> volume/*protocol*.
5. Land *Attack* (dengan hping3) --> volume/*protocol.*
6. Slowloris (dengan slowhttptest) --> *application*.
7. HTTP *Flood* (dengan *script* HULK) --> *application*.

E. *Hasil testing pertama dan analisis*

Berdasarkan 7 tes utama yang telah dilakukan, Tabel 2 menunjukkan hasil pengujian dan analisis secara keseluruhan :

TABEL 2. PROFIL HASIL UJI PERTAMA

Jenis Tes	Gangguan serangan DoS (tunggal)	Probabi-litas serangan	Tingkat kerenta-nan	Jumlah DDoS agar serangan efektif/tipe serangan *)
UDP flood	Tidak ada	Sedang	Rendah	35211 *node*/1
DNS amplification attack	Tidak ada	Rendah	Sedang	25906 *node*/1
ICMP Ping flood	Tidak ada	Sedang	Sedang	19293 *node*/1 112 *node*/2
SYN attack	Sedang	Tinggi	Tinggi	193 *node*/1 120 *node*/2
Land attack	Sedang	Tinggi	Tinggi	111 *node*/1 57 *node*/2
Slow loris :	rendah	Sedang	Rendah	Kapasitas koneksi *concurrent*

Slow Header				Apache (rahasia)/3
Slow loris : *Slow Read*	Sedang	Sedang	Sedang	Kapasitas koneksi *concurrent* Apache (rahasia)/3
Slow loris : *Slow Body*	Tinggi	Sedang	Tinggi	Kapasitas koneksi *concurrent* Apache (rahasia)/3
Http Unbearable Load King(HULK)	Rendah	Sedang	Sedang	61795 *concurrent request*/3

*) Keterangan
1. *Bandwidth saturation bit per second (bps) (Volume Based attack)*
2. *Packet per second (pps) (Protocol attack)*
3. *Request per second (rps) (Application layer attack)*

F. *Rancangan dan Implementasi Mitigasi*

Berdasarkan data dari hasil testing pertama, dilakukan *Focus Group Discussion* (FGD) dengan melibatkan *stake holder* khususnya adalah pihak administrasi dan operasi layanan e-learning Universitas Budi Luhur. Langkah selanjutnya adalah menggunakan kaidah *best practices* yang dianut pakar sistem operasi dan jaringan, untuk menyusun beberapa masukan perbaikan yang dapat dilakukan secara *software*. Untuk mitigasi beberapa jenis serangan perlu dilakukan dengan melibatkan pihak ISP, misalnya pada serangan DNS *Amplification attack*. Juga perlu menambah perangkat firewall fisik untuk secara efektif mengatasi serangan ICMP ping di *volume based attack*. Konfigurasi perbaikan yang dapat dilakukan secara *software* lebih efektif untuk jenis serangan *application layer attack*.

Beberapa langkah mitigasi yang dikonfigurasikan ulang pada server e-learning adalah :

1. Konfigurasi kernel linux di optimasi untuk menangani DDoS, khususnya untuk serangan dengan protokol TCP, paling efektif untuk SlowLoris.
2. Penambahan *access list* yang menolak paket karakteristik DoS. Dilakukan pada *routing* tabel sistem operasi yang mencakup :
   a. Buang paket invalid.
   b. Buang paket TCP yang bukan permintaan baru dan bukan SYN.
   c. Buang paket SYN dengan nilai MSS yang mencurigakan.
   d. Blok paket dengan *flag* TCP yang tidak benar.
   e. Blok paket hasil *spoof*.
   f. Buang ICMP (tidak dipasang, karena kebijakan organisasi mengizinkan ping ke server).
   g. Batasi koneksi per sumber IP (tidak dipasang).
   h. Batasi jumlah TCP *connection* per detik.
   i. Tambahan : pelindungan terhadap SSH *brute force* dan port *scanning*.
3. Konfigurasi ulang web server, dalam hal ini adalah Apache, mencakup:
   a. *Request RequestReadTimeout directive* dapat digunakan untuk membatasi waktu sebuah *client* mencoba mengirim permintaan.
   b. *TimeOut directive* harus direndahkan, nilai beberapa detik masih masuk bisa dicoba asalkan tidak menyebabkan permasalahan pada CGI *script* yang panjang.
   c. *KeepAliveTimeout directive* juga dapat direndahkan, atau bahkan dimatikan keseluruhan melalui *KeepAlive*, tetapi ini dapat mengakibatkan penurunan performa pada kondisi normal.
   d. Sesuaikan nilai *timeout* yang terkait pada modul-modul Apache.
      <IfModule mod_reqtimeout.c>
      RequestReadTimeout header={detik min}-{detik max},MinRate={Bytes per second} body= {detik min}-{detik max},MinRate={Bytes per second}
      </IfModule>
   e. *LimitRequestBody, LimitRequestFields, LimitRequestFieldSize, LimitRequestLine, dan LimitXMLRequestBody* harus dikonfigurasi secara hati-hati untuk membatasi jumlah konsumsi sumber daya oleh client input.
   f. Jika didukung OS, pastikan *AcceptFilter directive* digunakan untuk memindahkan beban proses permintaan ke OS (default aktif), tetapi mungkin memerlukan konfigurasi ulang kernel.
   g. Atur nilai *MaxRequestWorkers directive* untuk mengizinkan server menangani jumlah koneksi secara bersamaan tanpa kehabisan sumber daya.
   h. *Tuning* performansi untuk meningkatkan kapabilitas layanan berbasiskan kondisi *hardware* dan konfigurasi sistem operasi yang digunakan.

G. *Hasil testing kedua dan analisis*

Setelah konfigurasi terkait dilakukan pada server e-learning. Maka dilakukan pengujian ulang yang hasilnya ditunjukkan dalam Tabel 3.

TABEL 3. PROFIL HASIL UJI KEDUA

Jenis Tes	Gangguan serangan DoS (tunggal)	Probabi-litas serangan	Tingkat kerenta-nan	Jumlah DDoS agar serangan efektif/tipe serangan *)
UDP *flood*	Tidak ada	Sedang	Rendah	35309 *node*/1
DNS *amplification attack*	Tidak ada	Rendah	Sedang	24773 *node*/1
ICMP Ping *flood*	Tidak ada	Sedang	Sedang	18931 *node*/1 110 *node*/2

SYN *attack*	Sedang	Tinggi	Sedang	452 *node*/1 353 *node*/2
Land *attack*	Sedang	Tinggi	Tinggi	320 *node*/1 143 *node*/2
Slow loris : *Slow Header*	rendah	Sedang	Rendah	~3 kali dari Kapasitas koneksi *concurrent* Apache sebelumnya(rahasia)/3
Slow loris : *Slow Read*	Sedang	Sedang	Sedang	~3 kali dari Kapasitas koneksi *concurrent* Apache sebelumnya(rahasia)/3
Slow loris : *Slow Body*	Tinggi	Sedang	Tinggi	~3 kali dari Kapasitas koneksi *concurrent* Apache sebelumnya(rahasia)/3
Http Unbearable Load King(HULK)	Rendah	Sedang	Sedang	61538 *concurrent request*/3

Tabel 3 menunjukkan bahwa terjadi peningkatan kapabilitas sistem untuk mengatasi serangan DDoS kategori *application layer attack* (*Syn Attack, Land Attack, Slow Loris)* sebesar kurang lebih 3 kali lipat dibandingkan profil hasil uji pertama pada Tabel 2.

H. *Penilaian hasil*

Tabel 3 menunjukkan bahwa terjadi peningkatan kapabilitas sistem untuk mengatasi serangan DDoS kategori *application layer attack* (*Syn Attack, Land Attack, Slow Loris)* sebesar kurang lebih 3 kali lipat dibandingkan profil hasil uji pertama pada Tabel 2. Hasil dari pengujian kedua ini dianggap sudah memuaskan untuk mitigasi awal sistem dari serangan DDoS. Mitigasi lebih lanjut memerlukan penambahan *hardware* dan *software* dengan pembiayaan di luar dari penelitian ini, sehingga tidak dilakukan iterasi peningkatan kedua. Proses penelitian dilanjutkan dengan pembuatan laporan.

IV. KESIMPULAN

Analisis keamanan kuantitatif terhadap serangan DoS pada sistem e-learning Universitas Budi Luhur dapat dilakukan mengikuti kaidah *workflow* analisis keamanan sistem berbasis web, proses ini melibatkan tim operasional layanan, pakar sistem operasi dan jaringan. Implementasi dilakukan dengan memperbaiki / menambah konfigurasi *software* dari sistem operasi dan aplikasi. Setelah implementasi mitigasi yang disusun, pengujian ulang menunjukkan peningkatan rata-rata 3 kali kapabilitas untuk menangani serangan DDoS dari *Application layer attack*. Sedangkan serangan dari *Volume based attack* memerlukan implementasi perangkat fisik dan atau tambahan layanan dari ISP.

Beberapa saran yang dapat diberikan terkait kelanjutan penelitian ini:

1. Pengujian dalam penelitian ini harus dilakukan secara periodik setiap tahun. Perubahan *software* seperti *update* sistem operasi dan aplikasi, serta *patch* yang dikeluarkan oleh developer mungkin mengubah karakteristik kapabilitas mitigasi serangan DDoS.
2. Berlangganan dengan ISP yang mendukung *filtering traffic* seperti Cloudflare. Sehingga serangan berbasiskan *Volume based attack* dapat dimitigasi lebih efektif.
3. Penambahan server dan penggunaan layanan *load balance* atau *clustering* untuk membagi beban layanan ke lebih dari satu server.
4. Riset lanjutan untuk early warning system serangan DoS menggunakan *real time* log memanfaatkan *machine learning* atau ke arah penggunaan kombinasi *genetic algorithm* dan FSM untuk mengklasifikasikan serangan DoS yang di desain khusus untuk sistem ini.

UCAPAN TERIMA KASIH

Terima kasih kepada unit Direktorat Digitalisasi Pembelajaran Universitas Budi Luhur yang memungkinkan penelitian ini terlaksana.

REFERENSI

[1] J. L. Duffanny, “Computer Security,” in *Computer and Network Security Essentials*, 1st ed., K. Daimi, Ed. Cham: Springer International Publishing, 2018, pp. 3–20.

[2] P. M. Beach, L. O. Mailloux, B. T. Langhals, and R. F. Mills, “Analysis of Systems Security Engineering Design Principles for the Development of Secure and Resilient Systems,” *IEEE Access*, vol. 7, pp. 101741–101757, 2019.

[3] K. Scarfone, S. Murugiah, A. Cody, and A. Orebaugh, “Technical Guide to Information Security Testing and Assessment.” National Institute of Standards and Technology USA, Gaithersburg, MD, p. 80, 2008.

[4] W. Stallings, *Cryptography And Network Security Principles And Practice Seventh Edition Global Edition British Library Cataloguing-in-Publication Data*, 7th ed. Essex: Pearson Education Limited, 2017.

[5] D. Kunda, S. Chihana, and M. Sinyinda, “Web Server Performance of Apache and Nginx: A Systematic Literature Review,” *Computer Engineering and Intelligent Systems*, vol. 8, no. 2, pp. 43-52, 2017.

[6] T. Hamed, J. B. Ernst, and S. C. Kremer, “A Survey and Taxonomy of Classifiers of Intrusion Detection Systems,” in *Computer and Network Security Essentials*, 1st ed., K. Daimi, Ed. Cham: Springer International Publishing, 2018, pp. 21–39

[7] J. C. Chandra, “Model Framework Untuk Analisis Keamanan Dari Serangan Denial Of Service Pada Sistem E-Learning Universitas Budi Luhur,” in *Spirit Adaptasi Normal Baru dalam Perspektif Ekonomi, Pariwisata, Hukum dan Teknologi Informasi untuk Mencapai Keunggulan Bersaing*, 2021, pp. 371–378.

[8] A. Praseed and P. S. Thilagam, “DDoS attacks at the application layer: Challenges and research perspectives for safeguarding web applications,” *IEEE Commun. Surv. Tutor.*, vol. 21, no. 1, pp. 661–685, 2019.

[9] S. Black and Y. Kim, “An Overview on Detection and Prevention of Application Layer DDoS Attacks,” in *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, Jan. 2022, pp. 0791–0800.

[10] M. Abushwereb, M. Mustafa, M. Al-kasassbeh, and M. Qasaimeh, "Attack based DoS attack detection using multiple classifier," *arXiv.org*, Jan. 2020, doi: 10.48550/arXiv.2001.05707.

[11] M. S. Nafie, K. Adel, H. Abounaser, and A. Badr, "Hybrid Genetic-FSM Technique for Detection of High-Volume DoS Attack," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 4, pp. 500–509, 2019

[12] RFC-IETF, "RFC 9113: HTTP/2," 2022. https://datatracker.ietf.org/doc/rfc9113/