PERBANDINGAN PENERAPAN METODE PENGAMANAN WEB SERVER MENGGUNAKAN MOD EVASIVE DAN DDOS DEFLATE TERHADAP SERANGAN *SLOW POST*

Budi Hijriyannto[1)], Faruk Ulum[2)]

Informatika, Universitas Teknokrat Indonesia
Jl. H.ZA Pagaralam, No 9-11, Labuhanratu,Bandarlampung
Email: [1]budihiriyanto@gmail.com, [2]faruk.ulum@teknokrat.ac.id

Abstrak

Pembelajaran jarak jauh didefinisikan sebagai pangalaman belajar yang fleksibel yang disampaikan melalui penggunaan teknologi informasi dan komputer agar dapat diakses kapan saja, dimana saja, oleh siapa saja. Penerapan pembelajaran jarak jauh di Indonesia sendiri sudah banyak diterapkan oleh lembaga pendidikan yang ada. Salah satunya seperti yang sudah dilakukan oleh Universitas XYZ. Mengingat pembelajaran jarak jauh dilakuakn secara online, maka penting untuk menjaga keamanan web server dari ganguan yang tidak diinginkan.

Salah satu ancaman yang dapat menggangu kegiatan belajar mengajar dalam pembelajaran jarak jauh yaitu serangan Slow Post. Slow Post termasuk ke dalam jenis serangan DoS. Sehingga dalam penelitian ini akan menggunakan metode pengamanan yang biasanya digunakan untuk menangkal atau mengurangi dampak serangan DoS. Metode yang digunakan dalam penelitian ini adalah Mod Evasive dan DDoS Deflate.

Hasil dari penelitian ini adalah metode pengamanan yang baik dalam menangani serangan Slow Post. Baik disini dalam artian dimana metode tersebut dapat mengurangi atau menangkal serangan Slow Post yang di tujukan kepada web server. Semoga hasil dari penelitian ini dapat membantu pengelola web server dari pembelajaran jarak jauh pada Universitas XYZ dan dapat dapat dijadikan sebagai salah satu pertimbangan dalam melakukan tindak lanjut mengenai pengamanan web server dari website SPADA di Universitas XYZ.

Kata Kunci: *Apache, Web Server, Slow Post, Mod Evasive, DDoS Deflate.*

1. Pendahuluan

Pembelajaran jarak jauh didefinisikan sebagai pangalaman belajar yang fleksibel yang disampaikan melalui penggunaan teknologi informasi dan komputer agar dapat diakses kapan saja, dimana saja, oleh siapa saja (Ristekdikti, 2016). Perbedaan pembelajaran tradisional dengan pembelajaran jarak jauh yaitu pada kelas tradisional, guru dianggap sebagai orang yang serba tahu dan ditugaskan untuk menyalurkan ilmu pengetahuan kepada pelajarnya. Sedangkan di dalam pembelajaran jarak jauh fokus utamanya adalah pelajar. Pelajar dapat belajar secara mandiri pada waktu tertentu dan bertanggung-jawab untuk pembelajarannya. Suasana pembelajaran jarak jauh akan memaksa pelajar memainkan peranan yang lebih aktif dalam pembelajarannya. Pelajar membuat perancangan dan mencari materi dengan usaha, dan inisiatif sendiri (Suyanto, 2005). Penerapan pembelajarn jarak jauh di Indonesia sendiri sudah banyak diterapkan oleh universitas yang ada.

Salah satunya seperti yang sudah dilakukan oleh Universitas XYZ dengan domain spada.xyz.ac.id. *Website* pembelajaran jarak jauh tersebut digunakan sebagai media dan sarana untuk proses belajar dan mengajar antara mahasiswa dan dosen. Mengingat *website* tersebut diakses melalui jarak jauh, maka penting untuk menjaga keamanan website dari ganguan yang tidak diinginkan. Salah satu ancaman yang dapat menggangu komunikasi data yaitu serangan *Slow Post.*

Slow Post adalah salah satu jenis serangan *DoS. Slow Post* tidak melakukan eksploitasi pada lapisan jaringan seperti serangan *DoS / DDoS*, tetapi mengeksploitasi lapisan aplikasi dengan permintaan HTTP tidak lengkap, atau *transfer rate* yang sangat rendah. *Web server* akan menggunakan banyak sumber daya dalam menunggu sisa data. Didasarkan pada fakta di atas jadi ketika *web server* sudah terlalu banyak atau mengalami kekurangan sumber daya, maka akan terjadi penolakan layanan atau *denial of service* pada *server* (Park, 2015).

Dari permasalahan di atas, penting untuk sebuah *web server* menerapkan suatu metode yang dapat digunakan untuk mengamankan *web server* dari ancaman serangan *Slow Post.* Ada beberapa metode pengamanan yang biasanya digunakan untuk menangkal atau mengurangi serangan *DoS*, dan beberapa diantaranya yaitu *DDoS Deflate* dan *Mod Evasive*.

Dari penjelasan di atas disimpulkan bahwa, pentingnya menjaga keamanan dalam suatu *web server*. Merujuk permasalahan tersebut akan dibuat sebuah pengkondisian sistem *web server* yang kemudian akan di terapkan metode pengamanan *Mod Evasive* dan *DDoS Deflate.* Untuk itu peneliti akan melakukan sebuah penelitian mengenai pengujian dan analisa perbandingan dari penerapan metode *Mod Evasive* dan

DDoS Deflate terhadap serangan *Slow Post* pada *web server* yang telah dilakukan pengkondisian. Sehingga perbandingan kedua metode tersebut dapat di ketahui mana yang lebih baik.

2. Landasan Teori

2.1 Apache Web Server

Apache mudah dikelola karena memiliki struktur berbasis modul (Budiman, Sucipto and Dian, 2021). Modul yang memungkinkan administrator *server* untuk mengaktifkan dan menonaktifkan fungsi atau fitur tambahan. *Apache* memiliki modul untuk keamanan, *caching*, URL *rewriting*, otentikasi *password*, dan masih banyak lagi. Anda juga bisa *setup* konfigurasi *server* sendiri melalui *file* yang disebut .htaccess, yang mana merupakan *file* konfigurasi *Apache* yang didukung oleh semua paket *hosting* (Ariata, 2019).

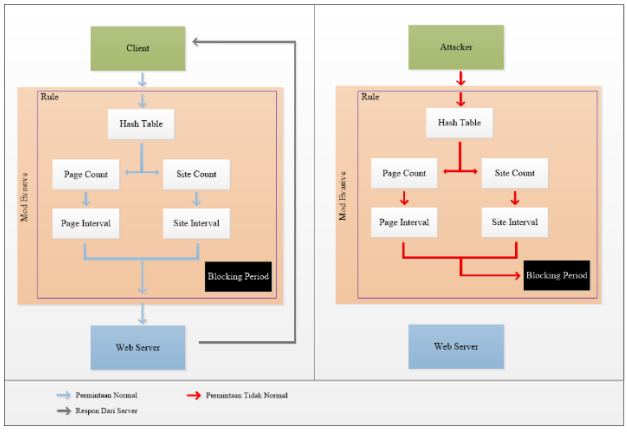
2.2 Denial of Service

Denial of Service (DoS) atau Distributed *Denial of Service* (DDoS) merupakan serangan yang membanjiri server dengan mengirimkan permintaan yang sangat banyak sehingga menghabiskan sumber daya pada *server* tersebut sampai *server* tersebut tidak dapat menjalankan fungsi dan tugasnya dengan benar. Kemudian *server* yang tidak bisa menangani permintaan, maka akan mengalami penolakan layanan (*denial of service*) (Yeasir, Morshed and Fakrul, 2015).

3. Metode Penelitian

3.1 Mod Evasive

Berikut ini adalah cara kerja dari *mod evasive* dalam melakukan tugasnya menjaga web server, pada gambar 1.

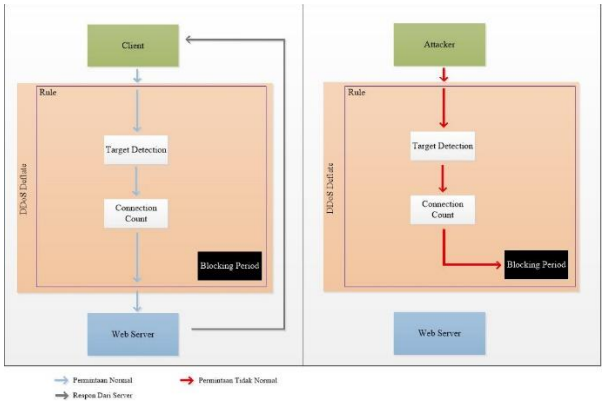


Gambar 1. Cara Kerja *Mod Evasive*.

Dari gambar tersebut menggambarkan mengenai cara kerja *mod evasive*. *Request* yang akan masuk ke *web server*, akan melewati pemeriksaan pada setiap *rule* yang ada pada *mod evasive*. Pada tahap awal akan dibuat *Tabel Hash* dinamis internal dari Alamat IP dan URL sebagai deteksi awal. Kemudian dilakukan perhitungan jumlah permintaan halaman pada bagian *page count* dan permintaan pada situs pada bagian *site count*. Selanjutnya akan di hitung rentang waktu antar permintaan halaman dan situs pada *page interval* dan *site interval*. Apabila jumlah dan waktu permintaan tidak melebihi batas yang sudah ditentukan, maka akan diteruskan ke *web server* dan *web server* akan mengirim respon. Tetapi apabila jumlah permintaan melebihi batas maka permintaan selanjutnya akan ditolak dan dimasukkan dalam daftar hitam sementara atau *blocking period* (Mishra and Sourav, 2012).

3.2 DDoS Deflate

Berikut ini adalah cara kerja dari *DDoS Deflate* dalam melakukan tugasnya menjaga *web server*, pada gambar 2.

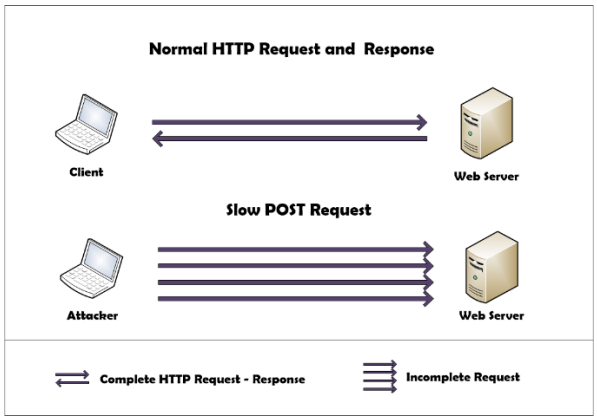


Gambar 2. Cara Kerja DDoS Deflate.

Setelah menetapkan frekuensi target, DDoS Deflate menetapkan kriteria berdasarkan batas untuk jumlah total koneksi, di mana *DDoS Deflate* harus menentukan jumlah maksimum koneksi untuk alamat IP. Jumlah default node diatur ke 200. Jika alamat IP mencapai jumlah maksimum batas *node*, maka *DDoS Deflate* memperlakukan alamat IP sebagai alamat IP yang buruk dan memblokirnya (Sangeetha, 2015).

3.3 Slow Post

Serangan *slow Post* dalam melakukan aksinya akan membanjiri target dengan permintaan yang tidak lengkap atau parsial, seperti yang terlihat pada gambar 3. Pada dasarnya sebelum panjang konten (*content-length)* belum terkirim seluruhnya, maka *web server* akan menunngu isi pesan yang tersisa untuk dikirm. Selama proses menunggu tersebut, *web server* akan membuka koneksi yang lambat. Tidak seperti *slow headers*, karena tidak adanya penundaan dalam pengiriman *HTTP header*, maka akan membatalkan keamanan pada IIS (Internet Information Services) (Chee and Brennan, 2010).

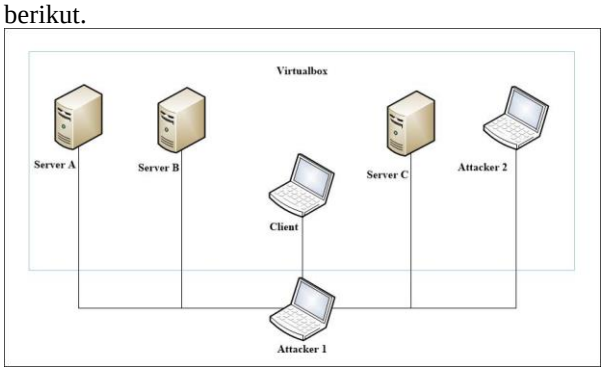


Gambar 3. Cara Kerja Serangan *slow Post.*

Permintaan yang tidak lengkap tersebut akan membuat *web server* menunggu paket tersebut. Sehingga akan terjadinya penumpukan paket yang tidak lengkap. Hal tersebut akan mengakibatkan *web server* menjalankan banyak layanan httpd yang akan menghabiskan banyak sumber daya. Dan ketika *web server* sudah tidak mampu melayani permintaan maka akan terjadi yang namanya *denial of service.*

3.4 Topologi Pengujian

Untuk topologi pengujian, akan menggunakan topologi pengujian yang dapat dilihat pada gambar 4 berikut.

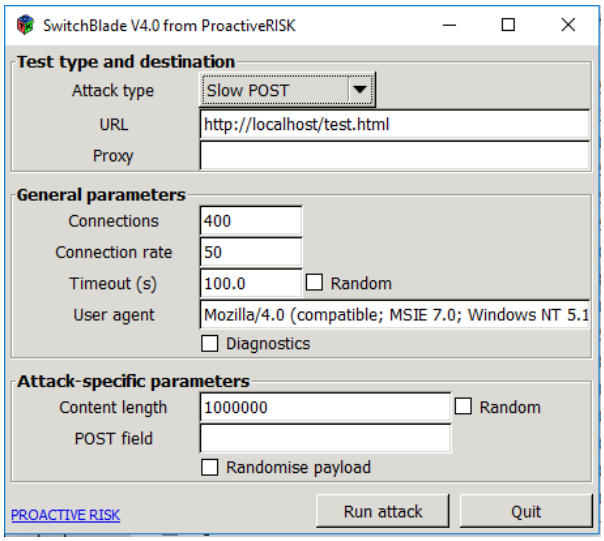


Gambar 4 Topologi *Virtual Web Server*

a. *web server* A yang tidak menggunakan metode pengamanan.
b. *web server* B yang menggunakan *Mod Evasive*.
c. *web server* C yang menggunakan *DDoS Deflate*.

3.5 Parameter Pengujian

Pengujian akan menggunakan aplikasi *Switchblade* untuk melakukan serangan *Slow Post*. Tampilan antarmuka dari aplikasi *Switchblade* dapat dilihat pada gambar 5 berikut.



Gambar 5 Tampilan Antarmuka Switchblade

Kemudian pengujian akan dilakukan dengan beberapa kombinasi pengaturan serangan yang akan terapkan pada *Switchblade*. Kombinasi pengaturan serangan pada *Switchblade* dapat dilihat pada table 1 berikut.

Tabel 1. Kombinasi Serangan

Connections	***Connection Rate***	***Timeout(s)***	***Content Length*** (bytes)
400	50	100	1000000
1000	200	110	8192
20000	50	110	1000

3.6 Waktu Pengujian

Dan lama waktu pengujian yang dilakukan dapat dilihat pada tabel 2 berikut ini:

Tabel 2. Lama Waktu Penngujian

Pengujian	**Lama Waktu**
Pengujian 1	6 Menit
Pengujian 2	8 Menit
Pengujian 3	13 Menit

4. Pengujian

4.1 Pengujian *Web Server* Tanpa Pengamanan

Hasil pengujian terhadap *web server* A yang dilakukan, kemudian dijadikan sebagai acuan dan pembanding terhadap hasil pengujian yang dilakukan terhadap *web server* B dan *web server* C yang diimplementasikan metode pengamanan. Hal ini dilakukan untuk membantu dalam proses analisis. Hasil pengujian yang sudah dilakukan terhadap *web server* A dapat dilihat pada tabel dibawah ini:

Tabel 3 Hasil pengujian pertama *web server* A.

Penyerang	Tujuan	Koneksi				
		Target	Aktif	Terhubung	Terputus	Error
Penyerang 1	192.168.56.2	400	216	216	184	0
Penyerang 2	192.168.56.2	400	82	82	318	0

Tabel 4 Hasil pengujian kedua *web server* A.

Penyerang	Tujuan	Koneksi				
		Target	Aktif	Terhubung	Terputus	Error
Penyerang 1	192.168.56.2	1000	246	246	754	0
Penyerang 2	192.168.56.2	1000	41	41	959	0

Tabel 5 Hasil pengujian ketiga *web server* A.

Penyerang	Tujuan	Koneksi				
		Target	Aktif	Terhubung	Terputus	Error
Penyerang 1	192.168.56.2	20000	217	217	19783	0
Penyerang 2	192.168.56.2	20000	62	62	19938	0

4.2 Pengujian Web Server Mod Evasive

Pada tahap ini dilakukan pengujian yang dilakukan terhadap *web server* B. *Web server* B merupakan *web server* yang diimplementasikan metode pengamanan *Mod Evasive*. *Mod Evasive* merupakan modul tambahan dari *Apache*, sehingga saat *Mod Evasive* dijalankan, masih menggunakan *service Apache.* dalam melakukan tugasnya, *Mod Evasive* memiliki sebuah aturan. Apabila ada yang melanggar aturan tersebut, maka *Mod Evasive* akan melakukan tindakan pemblokiran. Hasil pengujian dari *web server* B dapat dilihat pada tabel di bawah ini:

Tabel 6 Hasil pengujian pertama *web server* B.

Penyerang	Tujuan	Koneksi				
		Target	Aktif	Terhubung	Terputus	Error
Penyerang 1	192.168.56.3	400	159	159	241	0
Penyerang 2	192.168.56.3	400	148	148	252	0

Tabel 7 Hasil pengujian kedua *web server* B.

Penyerang	Tujuan	Koneksi				
		Target	Aktif	Terhubung	Terputus	Error
Penyerang 1	192.168.56.3	1000	258	258	742	0
Penyerang 2	192.168.56.3	1000	71	71	929	0

Tabel 8 Hasil pengujian ketiga *web server* B.

Penyerang	Tujuan	Koneksi				
		Target	Aktif	Terhubung	Terputus	Error
Penyerang 1	192.168.56.3	20000	128	128	19872	0
Penyerang 2	192.168.56.3	20000	151	151	19849	0

4.3 Pengujian Web Server DDoS Deflate

Pengujian ini merupakan pengujian terakhir yang dilakukan pada *web server* C. *web Server* ini menerapkan metode pengamanan *DDoS Deflate*. *DDoS Deflate* dijalankan dalam *service* yang bernama *Cron*. Dalam melakukan tugasnya, *DDoS Deflate* memiliki sebuah aturan. Apabila ada yang melanggar aturan tersebut, maka *DDoS Deflate* akan melakukan tindakan pemblokiran.. Berikut adalah hasil pengujian *DDoS Deflate* terhadap serangan *Slow Post*:

Tabel 9 Hasil pengujian pertama *web server* C.

Penyerang	Tujuan	Koneksi				
		Target	Aktif	Terhubung	Terputus	Error
Penyerang 1	192.168.56.4	400	0	0	400	0
Penyerang 2	192.168.56.4	400	0	0	400	0

Tabel 10 Hasil pengujian kedua *web server* C..

Penyerang	Tujuan	Koneksi				
		Target	Aktif	Terhubung	Terputus	Error
Penyerang 1	192.168.56.4	1000	0	0	1000	0
Penyerang 2	192.168.56.4	1000	0	0	1000	0

Tabel 11 Hasil pengujian ketiga *web server* C.

Penyerang	Tujuan	Koneksi				
		Target	Aktif	Terhubung	Terputus	Error
Penyerang 1	192.168.56.4	20000	0	0	20000	0
Penyerang 2	192.168.56.4	20000	0	0	20000	0

5. Pembahasan

5.1. Pembahasan Web Server A

Efek atau dampak yang terjadi pada *web server* A saat sedang dilakukan penyerangan yaitu, halaman situs dari *web server* A tidak dapat diakses melalui *web browser* pada *virtual client*. Hal ini dikarenakan *web server* A tidak diimplementasikan pengamanan apapun.

5.2. Pembahasan Web Server B

Efek atau dampak yang terjadi pada *web server* B saat sedang dilakukan penyerangan yaitu halaman situs dari *web server* B tidak dapat diakses melalui *web browser* pada *virtual client*. Hal ini dikarenakan pada *Mod Evasive* menggunakan *rule* yang mengatur tentang banyaknya jumlah *page request* maupun *site request* dan juga jarak waktu dari setiap banyaknya jumlah *page request* dan *site request* yang diterima oleh *web server* B. Dimana parameter ini tidak cocok untuk menangkal atau mengurangi serangan *Slow Post*. Karena sejatinya serangan *Slow Post* hanya mengirim sebuah permintaan dari setiap koneksi sampai serangan berakhir. Jadi setelah *web server* B menerima paket tidak lengkap untuk pertama kali, maka paket yang dikirim selanjutnya yaitu untuk melengkapi permintaan sebelumnya, dan akan berlangsung selama paket tersebut belum terlengkapi atau utuh. Dan setelah paket lengkap maka serangan *Slow Post* akan berhenti. Dan hal tersebut hanya terhitung sebagai satu atau sebuah permintaan. Sedangkan nilai terkecil dari parameter yang dapat diatur pada *Mod Evasive* bernilai 1. Sedangkan pada saat sebuah permintaan serangan *Slow Post* telah lengkap, maka serangan akan berhenti. Sehingga *Mod Evasive* tidak sempat untuk melakukan pemblokiran terhadap penyerang yang menggunakan serangan *Slow Post*.

5.3. Pembahasan Web Server C

Pada *web server* C saat sedang dilakukan penyerangan yaitu halaman situs dari *web server* C berhasil diakses melalui *web browser* pada *virtual client*. Dan *web server* C berhasil diakses setelah *DDoS* melakukan tindakan pemblokiran terhadap alamat IP penyerang, karena penyerang mencoba membuat koneksi lebih dari yang sudah ditetapkan pada *rule DDoS Deflate*, yang dimana hal tersebut melanggar *rule* yang ada pada *DDoS Deflate*. Dimana kemudian *DDoS Deflate* mengambil tindakan untuk memutus koneksi dari penyerang yang sudah berhasil terhubung dengan *web server* C. Sehingga penyerang tidak dapat mengirim paket tidak lengkap kepada *web server C*.

6. Kesimpulan

Berdasarkan dari seluruh kegiatan penelitian yang dilakukan maka dapat diambil beberapa kesimpulan yang antara lain sebagai berikut:

1. Metode pengamanan terbaik dari penelitian ini yang digunakan untuk menangkal atau meminimalisir serangan *Slow Post* adalah *DDoS Deflate,* hal ini dapat dilihat pada saat pengujian berlangsung. Hanya metode pengamanan *DDoS Deflate* yang dapat mempertahankan *web server* agar situs tetap dapat diakses oleh *client*. Hal ini dikarenakan *DDoS Deflate* dapat memutus koneksi yang dibuat oleh penyerang ketika jumlah koneksi melebihi *rule* yang telah ditentukan, sehingga penyerang tidak dapat melakukan pengiriman paket yang tidak lengkap kepada *web server*.
2. Jumlah koneksi yang terhubung menjadi faktor terpenting dalam melakukan serangan *Slow Post*, karena jika semakin banyak koneksi yang terhubung kepada *web server*, maka *volume* paket tidak lengkap yang dikirim kepada *web server* akan semakin banyak, sehingga *web serve*r akan semakin cepat mengalami penolakan layanan atau *denial of service*.

7. Saran

Berdasarkan kesimpulan yang telah dijelaskan sebelumnya mengenai hasil dari pengujian pengkondisian dengan menggunakan serangan *Slow Post* dan untuk penelitian, maka beberapa hal yang dapat penulis sarankan adalah sebagai berikut:

1. Pengujian yang penulis lakukan hanya dilakukan dalam skala kecil dan bermanfaat dalam skala kecil, sehingga penulis tidak menyarankan untuk menggunakan hasil penelitian ini dalam orgasnisasi atau instansi yang berskala besar.
2. Jumlah koneksi maksimum yang terhubung dengan *web server* dapat ditingkatkan atau diturunkan pada *file* konfigurasi *DDos Deflate* dapat diatur dan disesuaikan dengan kebutuhan *web server*.
3. *DDoS Deflate* akan lebih efektif jika dikombinasikan dengan modul *Apache* atau metode lain dan juga perangkat keras / *hardware* khusus.
4. Untuk penelitian yang akan datang, dapat dilakukan dengan metode yang sama, akan tetapi dalam skala yang besar, sehingga dapat lebih bermanfaat bagi orgasnisasi atau instansi yang berskala besar.

DAFTAR PUSTAKA

Ariata (2019) *Apa Itu Apache? Pengertian Apache Serta Kelebihan dan Kekurangannya*.

Chee, W. O. and Brennan, T. (2010) 'L7DDOS Atttacks'.

Mishra, D. P. and Sourav, K. (2012) 'DDoS Detection and Defense: Client Termination Approach', pp. 2–6. doi: 10.1145/2381716.2381859.

Park, J. (2015) 'Analysis of Slow Read DoS Attack and Countermeasures on Web servers', *International Journal of Cyber-Security and Digital Forensics*, 4(2), pp. 339–353. doi: 10.17781/p001550.

Ristekdikti (2016) *Kebijakan Pendidikan Jarak Jauh dan E-Learning di Indonesia*.

Sangeetha, D. S. B. (2015) 'DDoS Deflate and APF (Advanced Policy Firewall):A Report', *International Journal of Computer Trends and Technology*, 27(2), pp. 64–69. doi: 10.14445/22312803/ijctt-v27p111.

Suyanto, A. H. (2005) 'Mengenal E-Learning'.

Yeasir, M., Morshed, M. and Fakrul, M. (2015) 'A Practical Approach and Mitigation Techniques on Application Layer DDoS Attack in Web Server', *International Journal of Computer Applications*, 131(1), pp. 13–20. doi: 10.5120/ijca2015907209.

Budiman, A., Sucipto, A. and Dian, A.R. (2021). Analisis Quality of Service Routing MPLS OSPF Terhadap Gangguan Link Failure. Techno.com, 20(1), pp.28–37.

Ahdan, Syaiful. (2015). STRESS TESTING TO THE NETWORK TOPOLOGY USING NS2 MODELING AND SIMULATION OF NETWORK. 10.13140/RG.2.2.16100.58249.