Analisis Keamanan Jaringan dari Serangan DoS dengan Metode LOIC pada SIMPTT Mahasiswa UNISA Yogyakarta

Hanafi fajar*, Tikaridha Hardiani, Danur Wijayanto
Program Studi Teknologi Informasi, Fakultas Sains dan Teknologi, Universitas Aisyiyah Yogyakarta
*Email: hanafifajar98@gmail.com, tikaridha@unisayogya.ac.id, danurwijayanto@unisayogya.ac.id

Abstrak

Teknologi saat ini berkembang sangat cepat, teknologi saat ini dimanfaatkan untuk mengakses informasi, mencari hiburan, sebagai alat untuk mendapatkan penghasilan, menambah ilmu pengetahuan, serta sistem integrasi untuk sumber data. Pesatnya teknologi ini juga sebanding dengan kejahatan-kejatan siber yang ada saat ini, kejahatan ini dilakukan oleh penyerang atau hacker. SIMPTT (Sistem Informasi Manajemen Perguruan Tinggi Terpadu) Mahasiswa merupakan sistem yang digunakan untuk mengelola data pendidikan di Universitas Aisyiyah Yogyakarta (UNISA Yogya) dan pernah mendapatkan serangan jenis DoS (Denial of Service). Tujuan dari penelitian ini guna mengetahui tingkat keamanan jaringan terhadap serangan DoS dengan alat bantu LOIC untuk meluncurkan serangan DoS. Penyerangan dilakukan dengan 2 skenario yakni dari jaringan luar internet UNISA Yogya dan internet UNISA Yogya, metode yang digunakan untuk melakukan serangan TCP, UDP dan HTTP. Hasil dari serangan yang diluncurkan pada SIMPTT Mahasiswa dibuktikan dari kecepatan akses sistem yang melambat dibandingkan sebelum serangan, penggunaan memori dan CPU server sistem yang bertambah besar dibandingkan dengan sebelum dilakukan serangan pada sistem.

Kata kunci: Denial of Service; LOIC; Keamanan Jaringan; SIMPTT Mahasiswa

Network Security Analysis of DoS Attacks with LOIC Method on SIMPTT UNISA Yogyakarta Students

Abstract

Technology is advancing rapidly, and it is now utilized for accessing information, seeking entertainment, earning income, expanding knowledge, and integrating systems for data sources. However, the rapid growth of technology is paralleled by an increase in cybercrimes, which are carried out by attackers or hackers. The Integrated Higher Education Management Information System (SIMPTT) at Universitas Aisyiyah Yogyakarta (UNISA Yogya) is used to manage educational data and has experienced a type of attack known as a DoS (Denial of Service) attack. The aim of this study is to assess the network security level against DoS attacks using the LOIC tool to launch the attacks. The attack was conducted under two scenarios: from an external network and from within the UNISA Yogya network, using TCP, UDP, and HTTP methods. The results showed that the SIMPTT system experienced slower access speeds, increased memory usage, and higher CPU usage on the server after the attack.

Keywords: *Denial of Service; LOIC; SIMPTT Student Network Security*

1. Pendahuluan

Teknologi saat ini digunakan untuk mengakses informasi, mencari hiburan, sebagai alat untuk mendapatkan penghasilan, menambah ilmu pengetahuan, serta sistem integrasi untuk sumber data (Sutarman n.d, 2022). Pesatnya dunia digital saat ini tentu saja tidak terlepas dari resiko yang akan

diperoleh terlebih untuk pengelola suatu sistem. Serangan terhadap layanan sistem belakangan ini kerap terjadi, serangan yang dilakukan biasanya untuk melumpuhkan sistem sehingga pengguna tidak dapat mengakses layanan dari sistem/*web server* (Sutarman n.d, 2022) . Serangan yang biasa digunakan peretas untuk melumpuhkan layanan yakni serangan DoS (*Denial Of Service*).

Kasus terkait serangan DoS (*Denial of Service*) juga terjadi di salah satu kampus di Yogyakarta, salah satunya di Universitas Aisyiyah Yogyakarta (UNISA Yogya). Kasus terkait keamanan di UNISA Yogya pada SIMPTT (Sistem Informasi Manajemen Perguruan Tinggi Terpadu) terjadi pada Februari 2023 SIMPTT mengalami lambat akses saat pengguna ingin mengakses sistem saat akan melakukan KRS (Kartu Rencana Studi). Pemeriksaan terkait *log* dan aktivitas yang terjadi pada server menunjukkan hasil *traffic* yang masuk ke *web server* mengalami *overload* sehingga menyebabkan memori dan CPU penuh. Hasil pemeriksaan tersebut terdapat indikasi serangan DoS pada SIMPTT. Keamanan SIMPTT semenjak itu mulai diperbaiki namun belum ada lagi pengujian untuk menguji apakah sistem tersebut sudah aman apabila mendapatkan serangan serupa atau yang lainnya.

Penelitian ini berfokus pada pengujian keamanan pada SIMPTT Mahasiswa, dengan menggunakan serangan DoS. Alat bantu yang akan digunakan adalah aplikasi LOIC (*Low Orbit Ion Cannon*). LOIC merupakan aplikasi untuk menguji jaringan sumber terbuka, melumpuhkan web server dengan cara mengirimkan paket-paket serangan sebanyak mungkin. Jenis seragan yang akan dilakukan yakni jenis DoS, alat ini memiliki kelebihan dapat melakukan pengiriman paket *request* berdasarkan protokol *TCP* (*Transmission Control Protocol*), HTTP (*Protokol Transfer Hiperteks*) maupun *UDP* (*User Datagram Protocol*) juga target *port* yang akan dikirim dapat ditentukan oleh penyerang. TCP merupakan protokol yang digunakan untuk menghubungkan komputer satu dengan komputer yang lainnya melalui internet agar dapat saling berkomunikasi (Mitro et al., n.d, 2023) . HTTP merupakan protokol jaringan (*application layer*) yang dikembangkan dengan tujuan untuk memudahkan proses transfer antar komputer, sedangan UDP merupakan salah satu jenis protokol dari internet yang memungkinkan sebuah perangkat lunak pada komputer bisa mengirimkan pesan ke komputer lain melalui jaringan tanpa perlu ada komunikasi awal (Sugiyono, 2016).

2. Metode

Metode penelitian yang digunakan dalam penelitian kali ini yakni:

2.1. Studi Pustaka

Tahap penelitian ini melakukan pencarian informasi melalui buku, jurnal, website universitas, maupun artikel yang akan dijadikan acuan analisis penelitian dan proses pengujian (Hamdani et al., 2023).

2.2. Pengumpulan Data

Tahap penelitian ini mengelompokan data dan informasi yang telah diperoleh pada tahap studi pustaka. Informasi yang dikumpulkan terkait teori dan juga data-data untuk proses pengujian penelitian.

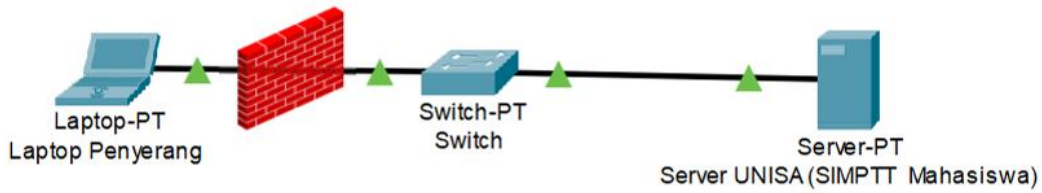
2.3. Persiapan dan Perancangan Pengujian

Tahap penelitian ini melakukan persiapan dan perancangan proses pengujian, hal yang harus dipersiapan sebelum melakukan pengujian yakni installasi alat bantu LOIC yang digunakan untuk melalukan serangan DoS (Dasmen et al., 2022).

2.4. Melakukan Serangan

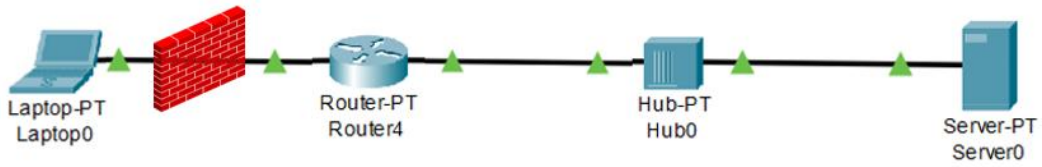
Tahap ini melakukan serangan dengan LOIC jenis serangan yang digunakan yakni DoS, serangan dilakukan dengan mengirimkan paket TCP, UDP, atau HTTP untuk mengganggu layanan web server dari SIMPTT Mahasiswa Universitas Aisyiyah Yogyakarta (Chandra, n.d. 2022).

Percobaan yang akan dilakukan sebanyak 3 kali, waktu setiap kali melakukan percobaan serangan 5 menit dengan jumlah *packet* data menyesuaikan jumlah waktu serangan. Serangan ini dilakukan menggunakan jaringan dari dalam UNISA Yogyakarta dan percobaan dari dalam dan luar jaringan UNISA Yogya. Gambaran dari serangan yang akan dilakukan seperti ditunjukkan pada Gambar 2.1.



Gambar 2.1 Topologi Serangan DoS Jaringan UNISA Yogya

Gambaran dari serangan yang akan dilakukan seperti ditunjukkan pada Gambar 2.2.



Gambar 2.2 Topologi Serangan DoS Jaringan Luar UNISA Yogya
(Wijaya et al., 2020).

2.5. Analisis Serangan

Tahap penelitian ini melakukan analisis dari hasil penelitian yang telah dilakukan. Keberhasilan dari serangan dibuktikan dengan uji manual yang dilakukan dengan mengakses SIMPTT Mahasiswa secara langsung, juga dibuktikan dengan mengukur kecepatan website speed test dengan Pingdom yang merupakan alat untuk uji coba aplikasi situs web. Perbandingan juga dilaakukan untuk mengetahui kecepatan untuk mengakses situs sebelum dan sesudah dilakukan serangan DoS pada SIMPTT Mahasiswa (Akbar.nd, 2018).

Sisi Server dilakukan pengecekan dengan mengecek sistem log atau monitoring penggunaan memori dan prosesor yang akan dilakukan pengecekan secara langsung di server (Sidaputar, n.d, 2020) . Analisis ini yang akan dijadikan bahan untuk mendapatkan kesimpulan dari penelitian yang telah dilakukan.

3. Hasil dan Pembahasan

Hasil dan pembahasan merupakan tahap pemaparan hasil dari serangan pada SIMPTT (Sistem Informasi Manajemen Perguruan Tinggi Terpadu) Mahasiswa. Tahapan yang akan dilakukan untuk melakukan serangan yakni mengumpulkan informasi, installasi serta konfigurasi LOIC, melakukan serangan DoS dan deteksi terhadap serangan yang telah dilakukan dijelaskan sebagai berikut:

3.1. Mengumpulkan Informasi

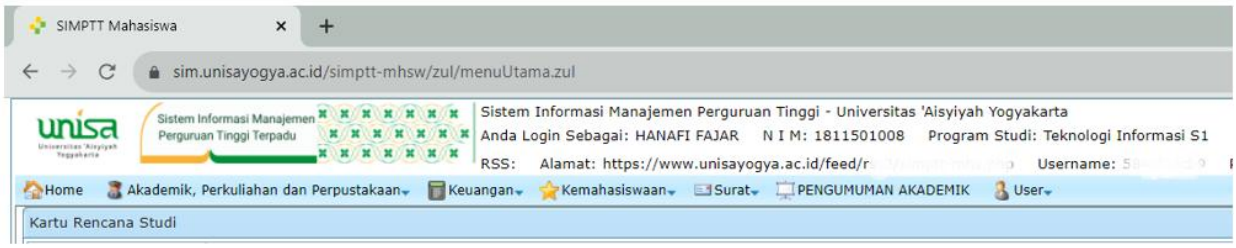
Tahap awal yang dilakukan untuk melakukan penelitian ini guna mendapatkan informasi terkait SIMPTT Mahasiswa yakni melakukan akses sistem yang akan dijadikan sebagai target serangan DoS. Sistem yang akan dilakukan serangan yakni SIMPTT Mahasiswa dengan link https://sim.unisayogya.ac.id/simptt-mahasiswa/ dari UNISA Yogyakarta dengan IP server 49.128.176.211, tampilan ini merupakan salah satu sisi keamanan yang diterapkan oleh pihak IT yakni redirect ke halaman akses aplikasi (Mahajan et al., 2013). Tampilan akses aplikasi ditunjukkan pada Gambar 3.1.

Gambar 3.1 Tampilan Akses SIMPTT Mahasiswa

Akses berhasil dilakukan dengan link https://sim.unisayogya.ac.id/simptt-mhsw/. Tampilan awal untuk akses akan muncul pada aplikasi ditunjukkan pada Gambar 3.2.

Gambar 3.2 Tampilan *Login* Awal Sistem

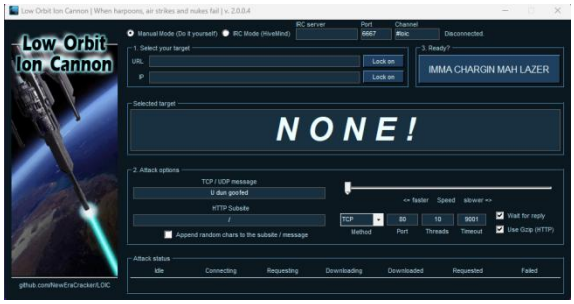
Tampilan sistem pada apabila sudah berhasil *login* pada link https://sim.unisayogya.ac.id/simptt-mhsw/zul/menuUtama.zul ditunjukkan pada Gambar 3.3.



Gambar 3.3 Tampilan Menu Fitur Aplikasi

3.2. Installasi dan Konfigurasi LOIC

Aplikasi LOIC pada penelitian ini digunakan sebagai alat untuk melakukan serangan pada keamanan jaringan SIMPTT (Sistem Informasi Manajemen Perguruan Tinggi Terpadu) Mahasiswa dengan jenis serangan DoS, LOIC di pasang pada Laptop (Siregar, n.d, 2022) . LOIC memiliki 3 metode penyerangan yaitu TCP, UDP dan HTTP, untuk langkah-langkah instalasi LOIC dapat dilihat pada halaman lampiran, tampilan LOIC setelah berhasil terpasang ditampilkan pada Gambar 3.4.



Gambar 3.4 Tampilan LOIC

3.3. Serangan DoS pada SIMPTT Mahasiswa

Perobaan serangan DoS pada SIMPTT Mahasiswa dilakukan dengan 2 skenario yakni serangan dari luar jaringan internet Universitas Aisyiyah Yogyakarta dan Jaringan WiFi internet Universitas Aisyiyah Yogyakarta. Serangan dilakukan dengan 1 device (Laptop) dan menyerang 1 sistem. Tabel IP Laptop dan server/sistem yang digunakan ditunjukkan pada tabel 3.1.

Tabel 3.1 Tabel IP Laptop dan Server

Nama Device	IP Address laptop/server	Keterangan
Asus	192.168.100.62 (Privat) 139.194.30.189 (Publik)	Penyerang
Server SIMPTT Mahasiswa	49.128.176.211	Server target yang diserang

Tabel IP Laptop dan sistem/server dengan jaringan dalam yang digunakan ditunjukkan pada tabel 3.3.

Tabel 3.3 Tabel IP Laptop dan Server Jaringan UNISA

Nama Device	IP Address laptop/server	Keterangan
Asus	192.168.200.225 (privat) 49.128.176.221 (publik)	Penyerang
Server SIMPTT Mahasiswa	49.128.176.211	Server target yang diserang

Metode yang akan dilakuan pada serangan dengan alat bantu LOIC yaitu TCP, UDP dan HTTP, identitas dari skenario yang akan dilakukan ditunjukkan pada tabel 3.4.

Tabel 3.4 Identitas Serangan 3 Metode Jaringan Dalam dan Luar UNISA Yogyakarta

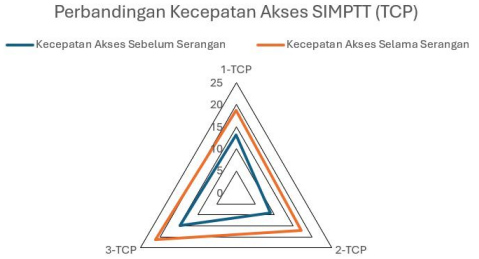
Serangan Ke-	IP Penyerang	IP Public	IP Target	Metode	Port	Threads	Timeout
1	192.168.1.6	139.194.30.82	49.128.176.211	TCP	80	99	9001

Serangan Ke-	IP Penyerang	IP Public	IP Target	Metode	Port	Threads	Timeout
				UDP	80	99	9001
				HTTP	80	99	9001
				TCP	80	99	9001
2				UDP	80	99	9001
				HTTP	80	99	9001
				TCP	80	99	9001
3				UDP	80	99	9001
				HTTP	80	99	9001

3.4. Deteksi Serangan

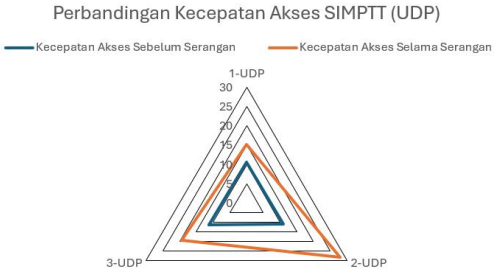
Deteksi terhadap serangan ditinjau dari 2 hal yakni pengecekan secara manual terhadap tingkat kecepatan mengakses aplikasi dengan melakukan pengecekan manual serta memanfaatkan *speed test website* (Mitro et al., n.d, 2023) . Cara lain yang digunakan untuk mendeteksi seraangan dengan melakukan pengecekan *traffic* dan *log* di server (Anif et al., 2015) (Mahendra. n.d, 2020).

Grafik perbandingan kecepatan akses yang dilakukan dengan Pingdom *speed test* dengan Metode TCP pada SIMPTT Mahasiswa sebelum dan selama serangan ditunjukkan pada gambar 3.5.



Gambar 3.5 Grafik Perbandingan Kecepatan Akses SIMPTT Mahasiswa Serangan Metode TCP dari jaringan UNISA Yogyakarta

Perbandingan kecepatan akses yang dilakukan dengan Pingdom *speed test* dengan Metode UDP pada SIMPTT Mahasiswa sebelum dan selama serangan ditunjukkan pada gambar 3.6.



Gambar 3.6 Grafik Perbandingan Kecepatan Akses SIMPTT Mahasiswa Serangan Metode UDP dari jaringan UNISA Yogyakarta

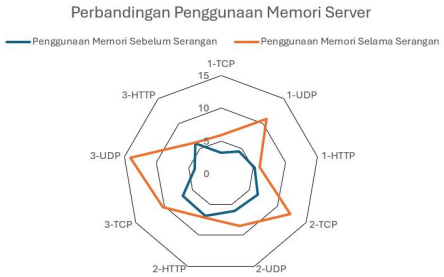
Monitoring server dengan perintah htop dilakukan juga untuk memperoleh rata-rata CPU yang terpakai di server saat sebelum dan selama mengalami serangan (Dody Firmansyah, 2021). Tabel rata-rata penggunaan CPU sebelum dan selama serangan berlangsung yang dilakukan dari jaringan Luar UNISA Yogyakarta ditunjukkan pada Tabel 3.5.

Tabel 3.5 Rata-rata penggunaan CPU sebelum dan selama serangan dari Luar UNISA Yogyakarta

Metode	Rata-rata CPU Server Sebelum Serangan /5 menit	Rata-rata CPU Server Selama Serangan /5 menit	GAP
TCP	0.64	1.92	1,28
UDP	0.61	2.65	2,04
HTTP	0.53	1.12	0,59
TCP	0.62	1.08	0,46
UDP	0.69	1.10	0,41
HTTP	0.67	0.77	0,1
TCP	0.68	1.87	1,19
UDP	0.63	1.20	0,57
HTTP	0.99	1.08	0,09
Rata-Rata	**0,67%**	**1,42%**	**0,74%**

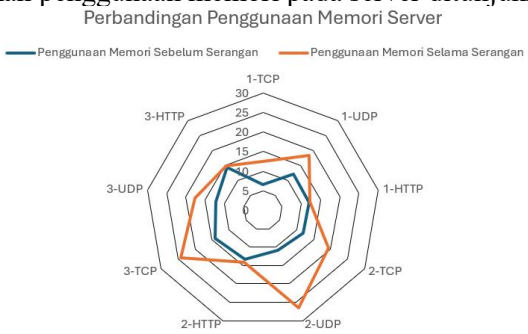
Rata-rata CPU pada server diperoleh berdasarkan waktu rata-rata server saat beroperasi selama interval 5 menit. Data yang diperoleh berdasarkan percobaan yang dilakukan dengan metode TCP, UDP, dan HTTP, Gap yang diperoleh dari penggunaan CPU sebelum serangan dan selama serangan dicatat dengan hasil percobaan pertama Metode TCP sebesar 1.28, UDP sebesar 2,04 dan HTTP sebesar 0.59. Percobaan kedua Metode TCP sebesar 0.46, UDP sebesar 0.41 , dan HTTP sebesar 0.01. Perobaan ketiga Metode TCP sebesar 1.19, UDP sebesar 0.57, dan HTTP sebesar 0,09. Persentase rata-rata CPU yang digunakan saat sebelum serangan dilakukan sebesar 0.67% dan rata-rata CPU yang digunakan selama serangan berlangsung yakni sebesar 1.42%.

Grafik perbandingan penggunaan memori yang didapatkan dari pengecekan penggunaan memori pada server ditunjukkan pada gambar 3.7.



Gambar 3.7 Grafik Penggunaan Memori Server SIMPTT Mahasiswa Jaringan luar UNISA Yogyakarta

Rata-rata persentase keseluruhan 3 kali percobaan dengan 3 metode yang digunakan sebelum serangan 11.94% dan selama serangan sebesar 17.76%. Grafik perbandingan penggunaan memori yang didapatkan dari pengecekan penggunaan memori pada server ditunjukkan pada gambar 3.8.



Gambar 3.8 Grafik Penggunaan Memori Server SIMPTT Mahasiswa Jaringan UNISA Yogyakarta

4. Kesimpulan

Kesimpulan yang didapatkan dari penelitian ini dengan melakukan serangan pada keamanan jaringan pada Sistem Informasi Manajemen Perguruan Tinggi Terpadu (SIMPTT) Mahasiswa, jenis serangan yang diluncurkan yakni DoS menggunakan alat bantu LOIC dengan hasil penelitian yang peroleh berupa bukti serangan berhasil dilakukan. Serangan ini dilakukan dengan 2 skenario dan 3 metode yakni menggunakan jaringan luar UNISA Yogya dan jaringan internet WiFi UNISA Yogya dengan masing-masing menggunakan 3 metode yakni TCP, UDP, dan HTTP. Kecepatan yang diperoleh sebelum serangan yang dilakukan dari jaringan luar UNISA Yogya adalah 12.24% dan selama mendapatkan serangan 20.87%, sedangkan rata-rata kecepatan akses dengan 3 metode yang dilakukan dari jaringan UNISA Yogya sebelum dilakukan serangan adalah 11.94% dan selama mendapatkan serangan 17.76%.

Serangan DoS dari jaringan dalam UNISA Yogya ditunjukkan pada perbandingan hasil kecepatan akses dan penggunaan server SIMPTT Mahasiswa setiap percobaan serangan mendapatkan gap hasil setiap serangannya, berdampak akses sistem menjadi lambat sementara namun tidak *down* atau *trouble*. Hasil yang diperoleh yang dijelaskan menunjukkan bahwa tingkat keamanan jaringan dari SIMPTT Mahasiswa masih perlu ditingkatkan terutama untuk serangan dari Metode TCP dan UDP, karena serangan masih bisa masuk dan tidak ada pembatasan seperti block IP dari sisi server.

5. Ucapan terimakasih

Penulis mengucapkan terima kasih Kepada Program Studi Teknologi Informasi Fakultas Sains dan Teknologi Universitas Aisyiyah Yogyakarta yang telah membantu peneliti selama proses pengumpulan data, penelitian dan pengolaan data.

Daftar Pustaka

Jurnal, Bulletin, dan Majalah Ilmiah

Affandi, M., Program, S., Teknik, S., Stmik, I., Pradnya, P., Malang, P., Laksda, J., Sucipto, A., & 249-A Malang, N. (n.d.). IMPLEMENTASI SNORT SEBAGAI ALAT PENDETEKSI INTRUSI MENGGUNAKAN LINUX. In *Jurnal Teknologi Informasi* (Vol. 4, Issue 2). www.linux.org

Anif, M., Hws, S., & Huri, D. (2015). Penerapan Intrusion Detection System (IDS) dengan metode Deteksi Port Scanning pada Jaringan Komputer di Politeknik Negeri Semarang. In *JURNAL TELE* (Vol. 13).

Chandra, J. C. (n.d.). Analisis Keamanan Layanan E-Learning Terhadap Serangan Dos Dan Implementasi Mitigasi Pada Universitas Budi Luhur. *Jurnal TICOM: Technology of Information and Communication*, *10*(3), 2022. https://elearning.budiluhur.ac.id,

Dasmen, R. N., M. Hendra Firmansyah, M. Khadafi, & Tri Yolanda. (2022). Penerapan Keamanan Jaringan Menggunakan Metode Firewall Security Port. *Decode: Jurnal Pendidikan Teknologi Informasi*, *2*(1), 1–7. https://doi.org/10.51454/decode.v2i1.29

Dody Firmansyah, M. (2021b). Analisa Keamanan Web Server terhadap Serangan Distributed Denial of Service menggunakan Modevasive. *TELCOMATICS*, *6*(1), 2541–5867. https://doi.org/10.37253/telcomatics.v6i1.4990

Hamdani, F., Bella Fitriana, Y., & Oper, N. (2023). KLIK: Kajian Ilmiah Informatika dan Komputer Analisis Keamanan Website Terhadap Serangan DDOS Menggunakan Metode National Institute of Standards and Technology (NIST). *Media Online)*, *3*(6), 1296–1302. https://doi.org/10.30865/klik.v3i6.830

Hermawan, R. (n.d.). *ANALISIS KONSEP DAN CARA KERJA SERANGAN KOMPUTER DISTRIBUTED DENIAL OF SERVICE (DDOS)* (Vol. 5, Issue 1).

Mahajan, A., Dahiya, M. S., & Sanghvi, H. P. (2013). Forensic Analysis of Instant Messenger Applications on Android Devices. *International Journal of Computer Applications*, *68*(8), 975–8887.

Prayudi, Y., & Iqbal, M. (2013). *Analisis Forensika Digital Pada Blackberry Untuk Mendukung Penanganan Kasus Cybercrime Menggunakan Smartphone*.

Siregar, J. J. (n.d.). *Analisis Explotasi Keamanan … (Junita Juwita Siregar) ANALISIS EXPLOTASI KEAMANAN WEB DENIAL OF SERVICE ATTACK*.

Sugiyono. (2016). SISTEM KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN METODE WATCHGUARD FIREBOX PADA PT GUNA KARYA INDONESIA. *Jurnal CKI On SPOT*, *9*(1).

Suwaryo[1], N., Nawangsih[2], I., Rejeki[3], S., & Raya, J. (n.d.). *DETEKSI SERANGAN PADA INTRUSION DETECTION SYSTEM (IDS) UNTUK KLASIFIKASI SERANGAN DENGAN ALGORITMA NAÏVE BAYES, C.45 DAN K-NN DALAM MEMINIMALISASI RESIKO TERHADAP PENGGUNA*.

Wijaya, B., & Pratama, A. (n.d.). Deteksi Penyusupan Pada Server Menggunakan Metode Intrusion Detection System (IDS) Berbasis Snort. *Sistem Informasi Dan Komputer)*, *09*, 97–101. https://doi.org/10.32736/sisfokom.v9.i1.770

Tesis, Disertasi

Serangan, D. (n.d.). *ABSTRAK JUANDA SIDABUTAR Analisis Keamanan Server Menggunakan IDS dan Router Firewall Server*.

Risang Mahendra.*T1_672016206 Analisa Keamanan Jaringan yang Menggunakan Firewall Palo Alto dan Non Firewall Palo Alto terhadap Serangan DDoS di UKSW_Full text*. (n.d.).