



Journal of Internet and Software Engineering Vol: 1, No 3, 2024, Page: 1-17

Analisis Log Server untuk mendeteksi Serang DDoS pada Keamaan Jaringan di Website

Afifah Rodhiyatun Nisa*, Ananditto Daffa Wijayanto, Arya Prabudi Jaya Priana, Aep Setiawan

Sekolah Vokasi, Insitut Pertanian Bogor

Abstrak: Serangan *Distributed Denial of Service* (DDoS) telah muncul sebagai ancaman besar terhadap keamanan jaringan di era digital yang berkembang pesat dan canggih, khususnya pada situs web. Serangan DDoS dapat menyebabkan ganggguan layanan dengan membanjiri server target menggunakan lalu lintas jaringan yang sangat besar, berpotensi merugikan bisnis dan pengguna. Karena alasan ini, sebuah penelitian dilakukan dengan tujuan untuk mendeteksi serangan *Distributed Denial of Serviced* (DdoS) pada keamanan jaringan situs web dengan menggunakan Wireshark, yaitu sebuah alat analisis log server yang canggih. Dengan mengimplementasikan Wireshark maka dapat menganalisis data log server untuk mengidentifikasi pola-pola yang mencurigakan dan anomali yang menunjukkan aktivitas DdoS. Metode yang digunakan melibatkan pengumpulan data log, kemudian menganalisis pola-pola yang mengindikasi adanya serangan DDoS, selanjutnya dicari sebuah solusi dalam mengatasi adanya serangan tersebut dengan menggunakan *firewall*, diharapkan dapat meningkatkan ketahanan dan keamanan jaringan *website* terhadap serangan DDoS.

Kata kunci: Analisis Log Server, Firewall, Serangan DDoS, Wireshark

DOI:

https://doi.org/10.47134/pjise.v1i3.2612 *Correspondence: Afifah Rodhiyatun Nisa Email: <u>afifahrnisa@apps.ipb.ac.id</u>

Received: 15-05-2024 Accepted: 30-06-2024 Published: 31-07-2024



Copyright: © 2024 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution-ShareAlike (CC BY SA) license (http://creativecommons.org/licenses/by-sa/4.0/). Abstract: In an increasingly advanced and developing digital era, Distributed Denial of Service (DDoS) attacks have become a very serious threat to network security, especially on Websites. DDoS attacks can cause service disruptions by overwhelming target servers with huge amounts of network traffic, potentially harming businesses and users. Therefore, a study was carried out aimed at detecting Distributed Denial of Service (DdoS) attacks on website network security using Wireshark, a sophisticated server log analysis tool. By implementing Wireshark, you can analyze server log data to identify suspicious patterns and anomalies that indicate DDoS activity. The method used involves collecting log data, then analyzing patterns that indicate a DDoS attack, then finding a solution to overcome the attack by using a firewall. By implementing a combination strategy between server log analysis and the use of firewalls, it is hoped that it can increase the resilience and security of the website network against DDoS attacks.

Keywords: DDoS Attack, Firewall, Server Log Analysis, Wireshark

Pendahuluan

Perkembangan teknologi informasi, khususnya dalam konteks infrastruktur jaringan seperti *website*, telah memberikan kemudahan akses informasi dan layanan kepada pengguna secara global. Situs web adalah platform digital yang terdiri dari beberapa halaman dengan konten yang dapat dilihat secara global melalui internet. *Website* adalah sekumpulan halaman yang menampilkan informasi digital yang dapat dilihat oleh siapa saja di dunia melalui koneksi internet. Informasi ini dapat berbentuk teks, foto, animasi, suara, video, atau kombinasi dari semuanya. Halaman di *website* dibuat dengan bahasa HTML standar, yang kemudian diubah oleh browser web menjadi data yang dapat dibaca. (Susilawati *et al.* 2020).

Hypertext adalah istilah untuk hubungan yang terjalin antara dua halaman web; *hyperlink* adalah hubungan antar halaman web (Wibisono dan Susanto 2015). Halamanhalaman dalam sebuah *website* bisa diakses melalui URL, yang umumnya mengarah ke halaman utama yang dikenal sebagai *Homepage*. URL ini mengorganisasi halaman-halaman situs dalam sebuah struktur hierarkis. Meskipun demikian, *hyperlink* di halaman-halaman tersebut membantu mengarahkan pembaca dan menjelaskan susunan serta aliran informasi secara keseluruhan. Beberapa *website* memerlukan langganan atau pendaftaran dari pengguna untuk mengakses sebagian atau keseluruhan konten situs web tersebut (Trimarsiah dan Arafat 2017).

Namun, seiring dengan kemajuan tersebut, ancaman terhadap keamanan jaringan juga semakin meningkat. Keamanan siber adalah tindakan melindungi sistem komputer, perangkat lunak, dan data dari akses, pengungkapan, transfer, perubahan, atau kerusakan yang tidak sah, baik yang terjadi secara tidak sengaja maupun sengaja (Annef 2021).

Keamanan siber menjadi sangat penting bagi suatu negara karena melibatkan berbagai aspek yang dapat mempengaruhi stabilitas dan keselamatan negara tersebut. Di Indonesia, tingginya angka kejahatan siber dipicu oleh jumlah pengguna internet yang terus bertambah. *Cybersecurity* diperlukan untuk mengantisipasi ancaman kejahatan teknologi informasi ini. Keamanan siber adalah langkah-langkah yang diambil untuk melindungi pengguna ruang siber dari berbagai ancaman dan serangan yang mungkin terjadi di dunia maya (Haryanto dan Sutra 2023).

Keamanan siber dapat diartikan sebagai berbagai tindakan yang diambil oleh individu atau kelompok, baik secara mandiri maupun bersama-sama, untuk melindungi, menjaga, mengantisipasi, atau mengurangi dampak yang berhubungan dengan dunia maya (Primawanti dan Pangestu 2020).

Salah satu ancaman yang paling umum dan merusak adalah serangan *Distribute Denial* of Service (DDoS). Serangan ini dapat mengakibatkan gangguan serius pada ketersediaan layanan, menimbulkan kerugian finansial, serta merusak reputasi sebuah platform online. Serangan *Distributed Denial-of-Service* (DDoS) merupakan jenis serangan yang bertujuan untuk mengganggu kinerja server atau sistem dalam jaringan sehingga tidak berfungsi dengan optimal. Serangan ini dilakukan dengan cara membanjiri server atau sistem target dengan jumlah besar paket data atau permintaan, sehingga menyebabkan kelebihan beban (*overload*) pada server tersebut. Akibatnya, server menjadi tidak responsif atau bahkan mengalami kegagalan (*crash*). Serangan DDoS bekerja dengan memanfaatkan sumber daya

dari banyak komputer yang tersebar di berbagai lokasi, yang dikendalikan oleh penyerang untuk mengirimkan serangan ke target secara bersamaan. Tujuan dari serangan ini adalah untuk mengganggu layanan yang disediakan oleh server target kepada pengguna yang sah (Zidane 2022). Umumnya, serangan DDoS dapat dibagi ke dalam beberapa jenis sebagai

berikut:

1. Serangan dengan basis *bandwidth*

Serangan DDoS jenis ini melibatkan pengiriman pesan data sampah secara besarbesaran untuk menciptakan *overload*, mengakibatkan berkurangnya ketersediaan *bandwidth* jaringan atau sumber daya perangkat jaringan. Perangkat seperti *router*, server, dan *firewall* yang menjadi target serangan seringkali memiliki sumber daya terbatas. Kelebihan beban ini menyebabkan peralatan jaringan menjadi tidak mampu mengelola lalu lintas reguler, yang dapat menyebabkan penurunan kualitas layanan atau bahkan kegagalan sistem (DoS) secara keseluruhan. Pengguna tidak dapat mengakses sistem yang mereka perlukan dalam kedua skenario.

2. Serangan berbasis lalu lintas jaringan

Serangan banjir lalu lintas jaringan adalah salah satu jenis serangan yang paling umum. Mengirimkan paket TCP, UDP, atau ICMP dalam jumlah besar ke *host* atau *server* target yang tampak asli adalah cara serangan ini dilakukan. Dengan menggunakan teknologi penyamaran alamat asal, serangan tertentu berdasarkan teknologi ini juga dapat menghindari deteksi oleh sistem. Karena banyaknya paket serangan yang beredar di jaringan, permintaan asli tidak dapat diproses. Jika eksploitasi *malware* digunakan bersamaan dengan tindakan terlarang lainnya, seperti kebocoran informasi atau pencurian informasi pribadi dari mesin target, kerusakan akibat serangan ini dapat meningkat.

3. Serangan berbasis aplikasi

Serangan semacam ini biasanya menggunakan operasi yang tampak autentik dan fungsional, termasuk akses *database*, untuk menyampaikan pesan data pada lapisan aplikasi sesuai dengan aspek bisnis tertentu. Akibatnya, sumber daya lapisan aplikasi tertentu—seperti jumlah maksimum pengguna dan koneksi aktif yang diizinkan—menjadi semakin langka, sehingga menyebabkan tidak tersedianya layanan sistem. Serangan-serangan ini seringkali tidak dilakukan dalam jumlah besar; bahkan lalu lintas yang sepi dapat mengganggu sistem secara serius atau bahkan mengakibatkan kinerja sistem komersial menjadi sangat terganggu (Geges dan Wibisono 2015). DDoS merupakan salah satu bentuk serangan yang terjadi dalam lingkungan maya, di mana pelaku berupaya membuat perangkat, server, atau jaringan menjadi tidak dapat diakses oleh pengguna. Umumnya, serangan ini dilakukan dengan cara membanjiri perangkat atau server target dengan lalu lintas yang sangat tinggi (Dody Firmansyah 2021).

Gunakan alat jaringan HPING3 untuk meluncurkan serangan DDoS. Sebuah aplikasi untuk jaringan bernama Hping3 memungkinkan pengiriman paket TCP/IP yang dipersonalisasi dan melihat balasan target. Alat ini sudah terpasang secara *pre-installed* di Kali Linux. Hping3 dapat digunakan untuk berbagai keperluan seperti menguji aturan *firewall*, melakukan *port scanning*, dan menguji performa jaringan. Selain itu, hping3 juga dapat mengirim paket dengan kecepatan maksimal menggunakan opsi *flood* (Nida dan Adrian 2023). Hping3 memiliki fitur utama yang meliputi kemampuan untuk mendeteksi host yang sedang aktif di jaringan serta melakukan serangan DDoS (*Distributed Denial of Service*) menggunakan metode SYN *flood* (Listyawati *et al.* 2022). Berbeda dengan perintah ping yang hanya bisa mengirim permintaan echo ICMP, Hping3 mampu mengirim paket TCP, UDP, dan ICMP (Sinambela 2020).

Untuk menangani dan mengatasi serang DDoS tersebut maka dapat di deteksi melalui analisis log server. Log server merupakan *file* yang mencatat kejadian-kejadian spesifik pada server web. Namun, *file* ini umumnya hanya diperiksa saat terjadi masalah atau kesalahan pada server web (Yogi *et al.* 2019). Teknologi log server adalah sebuah fitur yang seringkali ada dalam sistem operasi. Fitur ini dapat memberikan informasi mengenai catatan akses pengguna terhadap server. Dalam konteks penelitian, teknologi log server dimanfaatkan untuk melacak data akses pengguna pada situs web.

Data yang dihasilkan oleh layanan log server berbentuk file teks. Isi dari file log tersebut dapat diubah menjadi format data MySQL, sehingga mempermudah proses pengolahan dan analisis (Wagito dan Librado 2022). Server syslog adalah suatu server yang berperan menyimpan data syslog dari beragam perangkat komputer dan jaringan secara terpusat. Ketersediaan tinggi sangat penting bagi server syslog agar dapat mengelola penyimpanan syslog dari setiap perangkat komputer dan jaringan dengan efektif (Ditanaya *et al.* 2016). Kemudian untuk membaca server log tersebut menggunakan sebuah *software* Wireshark dan menggunakan sistem operasi windows 10.

Perangkat lunak yang disebut Wireshark, terkadang disebut sebagai penganalisis paket jaringan, digunakan untuk memeriksa paket data dalam jaringan. Tugasnya adalah mencatat setiap paket yang mengalir melalui jaringan dan menampilkan setiap detail dari setiap paket data (Hasbi dan Saputra 2021). Dengan Wireshark, pengguna dapat memeriksa dan mengatur data yang dikumpulkan secara langsung, serta melihat data dari jaringan langsung atau data yang disimpan di *disk*. Pengguna dapat memperoleh rincian yang komprehensif dan ringkas tentang setiap paket, mencakup semua *header* dan bagian data. (Mahmud *et al.* 2020).

Tujuan dan Manfaat Wireshark Manfaat dari penggunaan aplikasi Wireshark adalah sebagai berikut:

- 1. Menangkap data paket atau informasi yang akan dikirim dan diterima dalam jaringan komputer.
- 2. Memantau aktivitas yang terjadi dalam jaringan komputer.
- 3. Memeriksa dan menganalisis kinerja jaringan komputer, seperti kecepatan akses atau berbagi data dan koneksi jaringan ke internet.
- 4. Mengawasi keamanan jaringan komputer.

termasuk Ethernet, FDDI, Token Ring, serial (PPP dan SLIP), jaringan nirkabel LAN 802.11, serta konektivitas ATM. (Farhan *et al.* 2023). Wireshark adalah alat yang fleksibel karena mampu memeriksa data pada jaringan internet kabel maupun nirkabel (Luthfansa dan Rosiani 2021).

Pada dasarnya, semua perangkat dilengkapi dengan sistem operasi untuk mengatur fungsinya. Ada berbagai macam alat yang memanfaatkan sistem operasi dalam aktivitas sehari-hari. Sistem operasi bertindak sebagai penghubung antara pengguna perangkat dan perangkat keras yang digunakan pada perangkat tersebut (Supriyono 2018). Sistem operasi pada sebuah komputer memiliki peranan yang sangat penting karena tugasnya adalah mengelola semua perangkat keras yang terdapat dalam komputer tersebut (Dalimunthe *et al.* 2020).

Microsoft menciptakan Windows 10, sistem operasi komputer pribadi yang merupakan anggota keluarga Windows NT. Windows 10 pertama kali diluncurkan pada tanggal 30 September 2014, dan secara resmi tersedia pada tanggal 29 Juli 2015 (Mulawarman 2017). Sistem operasi ini juga memiliki kemampuan pembaruan otomatis yang memperbarui sistem dengan tampilan yang lebih modern dan menarik. Windows 10 tersedia dalam beberapa edisi: Rumah dirancang untuk pengguna rumahan, Pro ditujukan untuk pengguna bisnis kecil dan menengah, Perusahaan ditujukan untuk perusahaan, dan Pendidikan ditujukan untuk pelajar.

Beberapa fitur yang ada pada Windows 10, Yaitu:

- 1. Windows Hello: Fitur ini menggantikan penggunaan kata sandi dengan sistem identifikasi wajah atau sidik jari untuk mengautentikasi dengan tingkat keamanan yang lebih tinggi dan berkesinambungan.
- 2. Microsoft Edge: Browser modern yang didesain untuk pengalaman penjelajahan yang lebih individual dan responsif.
- 3. Windows Ink: Fitur ini memperbolehkan pengguna menuliskan ide-ide secara langsung dengan menggunakan pena spesial, yang kemudian dapat diabadikan dalam bentuk gambar dan diolah lebih lanjut.
- 4. Cortana: Cortana adalah asisten pribadi yang membantu pengguna mengatur pekerjaan mereka, membuat pengingat, dan memaksimalkan efisiensi perangkat mereka.
- 5. Xbox Play Anywhere: Dengan fitur ini*, gamer* dapat memainkan *game* sebaik mungkin dan berinteraksi dengan komunitas *game* dari mana saja.
- 6. Continuum: Fitur ini memungkinkan perangkat beradaptasi menjadi mode 2 in 1 sesuai dengan preferensi pengguna, sehingga dapat digunakan dengan fleksibilitas dalam berbagai situasi (Gayatrie *et al.* 2017).

Metode

A. Teknik dan Pengumpulan Data

Teknik pengumpulan data yang digunakan pada proposal ini yaitu menggunakan metode penelitian kuantitatif dan kualitatif. Pada penelitian kualitatif menggunakan studi pustaka untuk memahami mengenai server log dan juga bagaimana solusi yang dapat dilakukan apabila terdapat *website* yang diserang oleh DDoS. Kemudian pada penelitian kuantitatif menggunakan eksperimen pada sebuah *website* yang telah dibuat kemudian diimplementasikan dengan menggunakan server log untuk membaca aktivitas yang terjadi pada server dan mengidentifikasi pola-pola yang mencurigakan seperti serangan pada DDoS kemudian serangan tersebut dapat diatasi dengan berbagai solusi.

B. Analisis Data

Setelah dilakukan Studi pustaka dan juga Eksperimen maka dapat dilakukan analisis data dari proyek yang telah kami buat, yaitu:

1. Analisis Implementasi Server Log Pada Website

Implementasi server log pada sebuah *website* memungkinkan untuk merekam dan menganalisis berbagai aktivitas yang terjadi pada server, termasuk permintaan dari pengguna, tanggapan server, dan kejadian lain yang terjadi selama operasi normal maupun saat terjadi serangan.

2. Pendeteksi Serangan DDoS Pada Server Log

Server log mencatat semua aktivitas yang terjadi pada server, termasuk permintaan dan tanggapan yang dilakukan oleh pengguna atau sistem lainnya. Dengan memantau log ini secara kontinu, dapat diidentifikasi peningkatan tiba-tiba dalam volume permintaan yang mungkin menandakan adanya serangan DDoS. Kemudian pola-pola seperti peningkatan aktivitas dari alamat IP yang terdaftar dalam daftar hitam atau identifikasi pola perilaku yang konsisten dengan bot dapat menjadi tanda-tanda serangan DDoS.

3. Solusi Serangan DDoS

Untuk mengatasi serangan DDoS tersebut maka terdapat beberapa solusi yang diperlukan seperti penggunaan *Firewall* dan teknik *filltering* untuk membantu dalam mengidentifikasi dan memblokir lalu lintas yang mencurigakan.

Hasil dan Pembahasan

A. SetUp Web Server pada Windows Share

📾 Server Manager		- a ×
Server M	anager • IIS	• 🕄 🚩 Manage Tools View Help
III Dashboard	SERVERS Al severs 1 total	TASKS V
Local Server All Servers	Filter P (B) •	۲
III File and Storage Services ▷	Server Name IPv4 Address Manageability Last Update Windows Activation	
to IIS	WN-02887MUK2M4 192.166.1.7 Online \$/20/7024 63332 PM Not activated	
	EVENTS	
	All events 16 total	TASKS 💌
	Filter D (B) V (R) V	•
	anter name a arenny aduce ug useran me	
	Win-Q287MLCM4 521 Information Microsoft-Window-Wo-System 5/20/224 63311 PM	
	WIN-Q2R87MLK2M4 1007 Error Nicrosoft-Windows-IIS-W3SVC System 5/20/2024 621/23 PM	
	WIN-Q2R87MLK2M4 5211 Information Microsoft-Windows-WAS System 5/20/2024 621:22 PM	
	WIN-Q2887MJK2XM 1007 Error Microsoft-Windows-IIS-WISXVC System 5/20/2024.432.22 PM	v
	cepuires	
	SERVICE 3 total	TASKS 🔻
	Filter P (II) • (R) •	\odot
	Server Name Display Name Service Name Statu Stat True	
	WN-02887M K7M4 World Wide Web Publishing Service WSSVC Bunning Automatic	
	WIN-Q2R87MUK2M4 Application Host Helper Service AppHostSvc Running Automatic	
	WIN-Q2887/MJK2M4 Windows Process Activation Service WAS Running Manual	
		638 PM
P Type here to search		^ ™ ₩ 4s 5/20/2024

Gambar 1. Web Server pada Windows Share

Hal pertama yang harus disiapkan untuk membuat simulasi *website* dengan menerapkan serangan DDoS yaitu dengan membuat dan menyiapkan *website* terlebih dahulu. Pada hal ini *website* juga sudah dapat diakses pada *localhost*.



Gambar 2. Akses Web Server dengan Localhost

B. Simulasi Penyerangan DDoS Attack

Menyimulasikan serangan DDoS menggunakan Kali Linux melibatkan langkahlangkah serupa, tetapi memanfaatkan alat yang tersedia secara khusus dalam distribusi Kali Linux, yang sering digunakan untuk pengujian penetrasi dan penelitian keamanan. Berikut adalah beberapa langkah dan alat untuk menyimulasikan lalu lintas tinggi di *server web localhost* Anda menggunakan Kali Linux.

1. Siapkan Server Web Localhost

Pastikan Anda memiliki server web yang berjalan di komputer lokal Anda. Anda dapat menggunakan pengaturan server sederhana dengan alat seperti Apache atau Nginx. Misalnya, untuk menyiapkan server Apache:

```
pembaruan sudo apt
```

```
sudo apt menginstal apache2
sudo systemtarget mulai apache2
sudo systemctl mengaktifkan apache2
```

2. Pilih Alat Untuk Simulasi

Kali Linux hadir dengan berbagai alat yang dapat digunakan untuk mensimulasikan lalu lintas tinggi. Berikut adalah beberapa alat yang tersedia di Kali Linux:

- Menggunakan Apache Benchmark

a. Install Apache Benchmark

Apache Benchmark biasanya disertakan secara *default* di Kali Linux. Jika tidak, instal: sudo apt-get install apache2-utils

b. Jalankan Apache Benchmark ab -n 10000 -c 100 http:// 192.168.1.7/

└─ # ab -n 10000 -c 500 h	ittp://192.168.1.17/
This is ApacheBench, Vei	rsion 2.3 <\$Revision: 19139
2 \$>	
Copyright 1996 Adam Twis	ss, Zeus Technology Ltd, ht
p://www.zeustech.net/	
Licensed to The Apache S	Software Foundation, http://
www.apache.org/	
Benchmarking 192.168.1.1	(be patient)
completed 1000 requests	
Completed 2000 requests	
Completed 3000 requests	
Completed 4000 requests	
Completed 5000 requests	
Completed 8000 requests	
AvassCompleted 8000 requests	locto
Completed 0000 requ	lesus
Completed 9000 requests	
Einishod 10000 requests	,
Finished 10000 lequests	
Server Software:	Microsoft-TIS/10.0
Server Hostname:	192.168.1.17
Server Port:	80
Document Path:	
Document Length:	30896 bytes
Concurrency Level:	500
Time taken for tests:	4.098 seconds
Complete requests:	10000
Failed requests:	0
Total transferred:	311420000 bytes
HTML transferred:	308960000 bytes
Requests per second:	2440.29 [#/sec] (mean)
Time per request:	204.893 [ms] (mean)
Time per request:	0.410 [ms] (mean, across a
concurrent requests)	

Gambar 3. Serangan Menggunakan Apache Benchmark

```
Keterangan :
```

'**-n 10000**' : Jumlah total permintaan untuk melakukan.

'**-c 100**' : Jumlah beberapa permintaan untuk dilakukan pada satu waktu (tingkat konkurensi).

- Menggunakan Hping3
 hping3 adalah alat jaringan yang dapat menghasilkan paket TCP, UDP, ICMP, dan RAW-IP untuk menguji kinerja dan keamanan jaringan.
- a. Install Hping3

hping3 biasanya disertakan secara *default* di Kali Linux. Jika tidak, instal: sudo apt-get install hping3

b. Simulasikan Lalu Lintas Dengan Hping3

Lakukan *command* di bawah untuk menghasilkan banjir paket SYN untuk menyimulasikan serangan DDoS:

```
sudo hping3 -S -p 80 --flood 192.168.1.7
```



Gambar 4. Serangan Menggunakan Hping3

Ketika perintah tersebut dijalankan maka langsung berdampak pada web server sehingga server tidak dapat diakses karena *traffic request* terlalu banyak.



Gambar 5. Webiste down

3. Pantau Dampak Pada Website

Saat menjalankan pengujian ini, pantau kinerja server web Anda. Cari metrik seperti penggunaan CPU, penggunaan memori, waktu respons, dan tingkat kesalahan. Akan membantu dalam memahami bagaimana server menangani volume lalu lintas tinggi dan mengidentifikasi potensi kemacetan atau kelemahan.

- *Capture Windump* kemudian gunakan wireshark untuk melihat trafik yang masuk



Gambar 6. Capture Windump

 Windump digunakan untuk memantau secara *real time log* yang masuk pada koneksi web server yang lalu akan di-*capture* menggunakan win pcap.

ing Mar	nager																					
ptions		capture	.pcap														_	0		×		
ancing (File	Edit	View	60	Canture	Analyze	Statistics	Telenho	nv Win	loce	Tool	н	eln									-
	a l			1 17%		O G	statistics	л	= A	A	a 10		cip								mode	
				010		1 ~ ~	/ ¥ 1		- 4	4	ч ш								_	_	_	
		pply a	display f	ilter	<ctrl-></ctrl->													_	-	• +	_K	
	No.		Time		Sourc	e		Destinatio	n		Pro	tocol	Leng	tł Ini	fo						^	
	1	L189	36.180	522	192.3	168.1.7		192.168.	1.4		TCF	•	5	8 80) →	52409	9 [SY	Ν, /	ACK			
	1	L189	36.180	530	192.1	168.1.7		192.168.	1.4		TCF		5	8 80) →	52410	9 [SY	Ν, /	ACK			
		189	36.180	538	192.			192.168.	1.4		TCF		-		СР	ACKed	1 uns	een	se			
		1189	36.180	553	192.1	168.1.7		192.168.	1.4		TCF			58 80	, <i>→</i>	5241	2 [31 3 [SY	N. /				
		L189	36.180	587	192.1	168.1.7		192.168.	1.4		TCF			58 80) ->	52414	1 [SY	N, /	АСК	_		
	1	L189	36.180	596	192.3	168.1.7		192.168.	1.4		TCF		5	8 80) →	5241	5 ESY	Ν, /	АСК_			
	1	L189	36.180	506	192.3	168.1.7		192.168.	1.4		TCF		5	58 80) →	52417	7 [SY	Ν, /	ACK			
	1	1189	36.180	614	192.	168.1.7		192.168.	1.4		TCF	•	5	58 [T	СР	ACKee	d uns	een	se			
		L189	36.180	522	192.1	168.1.7		192.168.	1.4		TCF		-	58 80 	→	52419	9 [SY	N, /				
		1189	36 180	538	192	168 1 7		192.100.	1.4		тся		-	00 00	-	52420	9 [51 1 [SV	N, / N /			~	
	<																		>			
	> F	rame :	1: 121	byte	s on wir	e (968 b	its), 96	bytes c	a 0000	c8	94 0	df	d8 4	o c4	27	28	c4 f4	7b	08	00 4	5	
	> E	therne	et II,	Snc:	zte_c4:	f4:7b (c	4:27:28:	c4:f4:7b	0010	00	6b 00	00	40 0	37	11	6e	f4 4a	7d	c8	5f c	0	
	> 1	nterne	et Prot	ocol	Version	4, Src:	74.125.	200.95,	0020	01 52	a0 do	1 4 f	ed 9 Øa fi	9 00 9 88	57 2d	C6 88	da 45 d0 7e	5C	46 33	79 4 1c 3	a	
		ser Da	atagran	1 Pro	tocol, S	rc Port:	443, Ds	t Port:	0040	79	b5 14	↓ b1	b7 30	ð d3	e7	1a	b4 a2	4f	17	81 9	d	
	1 P	ata (:	54 Dyte	:5)					0050	b6	ab 65	5 f5	a8 a:	L 83	07	0f	b8 da	87	db	b8 9	b	_
Time																						
11:22:52																						
	<							>	<												>	
	0	7 .	apture.p	cap					Packe	ts: 26	10998	Displ	ayed:	26109	98 (1	100.0%	5) P	rofile	e: Def	ault		
										_	_		·	_		-		-	_	-		

Gambar 7. *Capture.pcap*

Setelah itu file akan tersimpan pada direktori yang ditentukan, kemudian file tersebut dapat dibuka dengan menggunakan Wireshark untuk dianalisa traffic yang masuk seperti dari mana asal dan seberapa banyak paket tersebut masuk. Dalam kasus DDoS Attack traffic masuk dalam jumlah yang tidak wajar atau sangat banyak menjadi suatu pola serangan tersebut.

4. Menguji Kinerja Server Dengan Siege.

Siege adalah alat populer lainnya untuk menguji kinerja server web Anda di bawah beban berat.

```
sock.c:384: Connection timed out
[alert] socket: read check timed out(30) sock.c:273
: Connection timed out
[alert] socket: select and discovered it's not read
y sock.c:384: Connection timed out
[alert] socket: read check timed out(30) sock.c:273
: Connection timed out
[alert] socket: select and discovered it's not read
y sock.c:384: Connection timed out
[alert] socket: read check timed out(30) sock.c:273
: Connection timed out
[alert] socket: select and discovered it's not read
y sock.c:384: Connection timed out
[alert] socket: read check timed out(30) sock.c:273
: Connection timed out
[alert] socket: select and discovered it's not read
y sock.c:384: Connection timed out
[alert] socket: read check timed out(30) sock.c:273
: Connection timed out
[alert] socket: select and discovered it's not read
y sock.c:384: Connection timed out
[alert] socket: read check timed out(30) sock.c:273
 Connection timed out
[alert] socket: select and discovered it's not read
y sock.c:384: Connection timed out
[alert] socket: read check timed out(30) sock.c:273
: Connection timed out
[alert] socket: select and discovered it's not read
y sock.c:384: Connection timed out
[alert] socket: read check timed out(30) sock.c:273
  Connection timed out
             Gambar 9. Output Siege
```

-c 100: Simulasikan 100 pengguna bersamaan.

-t 1M: Jalankan pengujian selama 1 menit.

C. Pencegahan Serangan DDoS

1. Mengidentifikasi Serangan DDoS

Sebelum mengatasi serangan, Pengguna perlu mengidentifikasi bahwa serangan DdoS sedang terjadi. Beberapa tanda umum serangan DDoS meliputi:

- Lonjakan lalu lintas yang tiba-tiba.
- Kinerja server yang lambat atau tidak responsif.
- Meningkatnya jumlah koneksi TCP/IP.
- Peningkatan penggunaan CPU dan memori.
- 2. Mengonfigurasi Firewall Untuk Solusi Penyerangan Website

a) Menggunakan Windows Firewall

1. Buka Windows Firewall

Tekan Win + R, ketik wf.msc, dan tekan Enter untuk membuka "Windows Defender Firewall with Advanced Security".



Gambar 10. Win+R

2. Buat Aturan Baru

Klik "Inbound Rules" di panel kiri, lalu klik "New Rule" di panel kanan.

ws Defender Firewall with Inbou	nd Rules			Actions
ound Rules Name		Group	Profile ^	Inbound Rules
bound Rules Paria Rule Type Select the type of frewal rule Steps: a Rule Type B Rule Type a Rule Type b Rule Type b Rule Type b Rule Company b Rule	o create. What type of rule wou Program Rule that controls - Prod That Controls - Prodemost Alloyn Rocter	Unoup Id you like to create? connections for a program.	Prone	X .
	Rule that controls . (e) Custom nule. Custom nule.	connections for a Windows experience	re sck Next >	Cancel

Gambar 11. Inbound Rules

- 3. Konfigurasi Aturan
 - Pilih "Custom" dan klik "Next".
 - Pilih "All programs" dan klik "Next".
 - Pilih protokol yang sesuai (contohnya, TCP) dan klik "Next".
 - Masukkan port yang ingin dibatasi (contohnya, 80 untuk HTTP atau 443 untuk HTTPS) dan klik "Next".
 - Pilih "Any IP address" untuk Source dan Destination, lalu klik "Next".

	🔗 New Inbound Rule Wizard		
	Scope		
	Specify the local and remote IP add	resses to which this rule applies.	
	Steps:		
	Rule Type		
	Program	Which local IP addresses does this rule apply to?	
	Protocol and Ports	○ Any IP address	
IP Address		X These IP addresses:	
Seccify the IP a	uddraaaaa ta matah :		Add
Specify the frie	duresses to match.		Edit
This IP add	ress or subnet:		lemove
192.168.1.	7		
Examples:	192.168.0.12 192.168.1.0/24	stomize the interface types to which this rule applies: Cus	tomize
	2002:9d3b:1a31:4:208:74ff.fe39:6c43 2002:9d3b:1a31:4:208:74ff.fe39:0/112	hich remote IP addresses does this rule apply to?	
O This IP add	ress range:	Any IP address	
From:	-	These IP addresses:	
To			Add
			Edit
			lomovo
			iomovo

Gambar 12. Konfigurasi Aturan

- 4. Konfigurasi Rate Limiting
 - Pada bagian "Action", pilih "Block the connection" dan klik "Next".
 - Beri nama aturan ini (contoh: "Rate Limit HTTP") dan klik "Finish".

b) Menggunakan Load Balancer Mengonfigurasi IIS Untuk Rate Limiting

- 1. Install IIS
 - Buka "Server Manager", pilih "Add roles and features"

IICK START	2	Add	roles and features		
	3	Add	other servers to manage	🛼 Add Roles and Features Wizard	- 0
LAT'S NEW	4	Creat	e a server group	Before you begin	DESTRUKTION SERVES WHI-Q2837MLK2M4
ARN MORE	5	Conn	ect this server to cloud :	Before You Begin This Installation Type hosti	vizard helps you install roles, role services, or features. You determine which roles, role services, o res to install based on the computing needs of your organization, such as sharing documents, or ng a website.
LES AND SERVER GF s:2 Server groups: 1	tOUPS	total: 1		Server Selection To re Server Roles Start Features Befor	move roles, role services, or features: the Remove Roles and Features Witand e you continue, verify that the following tasks have been completed:
LES AND SERVER GF s:2 Server groups: 1 File and Storag Services	tOUPS Servers e	total: 1 1	to IIS	Server Selection To re Server Roles Start Features Befor Confirmation • The Results • Net	move roles, role services, or features: the Remove Roles and Features Wood er you continue, verify that the following tasks have been completed Administrate recount has a strong parsword word settings, such as static IP addresses, are configured most current scurely lighters from Widdow Lighter are initiated
LES AND SERVER GF sc 2 Server groups: 1 File and Storag Services Manageability Events	tOUPS Servers e	total: 1	IIS Manageability Events	Server Selection To re Server Roles Seart Features Beford Confirmation The Results Net Hypo comp	more roles, nois services, or features: the femous Notas and Features Water e you continue, welly that the following tasks have been completed -Administrator account has a strong parsened round current security updates from Windows Update are installed - most current security updates from Windows Update are installed - most welly that any of the spreeding prerequides have been completed, close the wizard, - whet he steps, and ther unit her work galaxy.
LES AND SERVER GF s:2 Server groups: 1 File and Storag Services Manageability Events Performance	toups Servers le	total: 1	IIS Manageability Events Services	Server Selection To re Server Roles Seat Factors Beter Confirmation • Th Results • Ne Hype Confirmation • Th Results • The To co	more only, so due structure, or features: the more volume and relationship stacks have been completed: Administration excerpt the a strong parsenal in more strong the structure of the structure of the structure more structure structure of the parsenaling parsenalistic have been completed, close the viscand, refune, clock here.

Gambar 13. Roles and Features IIS

- Pilih "Network Load Balancing" dan ikuti Wizard Instalasi.



Gambar 14. Select Features "Network Load Balancing"

- 2. Konfigurasi NLB
 - Buka "Network Load Balancing Manager"



Gambar 15. Network Load Balancing Manager

- Pilih "Cluster" > "New" dan ikuti Wizard untuk membuat cluster

±-2	New			Cluster configuration for a	I known NLB clusters
	Connect to Existing			Cluster name	Cluster IP addres
	Add Host Delete				
	Properties				
	Refresh				
	Remove From View				
	Control Hosts Control Ports	>			
Les fe	Data Taur	Chastra	11-1		

Gambar 16. Membuat Cluster

- Tambahkan host ke cluster dan konfigurasikan parameter sesuai kebutuhan

Host: 192.168.1.7		Connect
Connection status		
Connected		
Interfaces available for co	onfiguring a new cluster	
Interface name	Interface IP	
Ethernet	192.168.1.7	
Ethemet	192.168.1.7	
Ethernet	192.168.1.7	

Gambar 17. Menambahkan host ke Cluster

- 3. Menggunakan IP Security Policies (IPSec)
 - a) Langkah 1:
 - Buka IP Security Policies, tekan "WIN + R", dan ketik **secpol.msc** lalu tekan **enter**
 - Navigasikan ke IP Security Policies on Local Computer
 - b) Langkah 2 Membuat Kebijakan IPSec Baru
 - Klik kanan pada "IP Security Policies on Local Computer" dan pilih "Create IP Security Policy"
 - Ikuti wizard untuk membuat kebijakan baru dan beri nama kebijakan tersebut.
 - c) Langkah 3 Tambahkan Filter dan Aturan
 - Dalam wizard, tambahkan filter IP untuk memblokir Alamat IP atau rentang IP tertentu.
 - Buat aturan tindakan untuk menetapkan tindakan blokir atau mengamankan koneksi.

- 4. Pemulihan dan Pencegahan Lanjutan **Backup dan Disaster Recovery**
 - a) Rencana Backup:
 - Pastikan Anda memiliki rencana backup yang teratur untuk memastikan data dan konfigurasi dapat dipulihkan dengan cepat jika terjadi serangan.
 - Gunakan alat backup bawaan Windows Server atau solusi pihak ketiga.
 - b) Disaster Recovery Plan:
 - Miliki rencana pemulihan bencana yang mencakup prosedur untuk mengatasi serangan DDoS.
 - Lakukan uji coba pemulihan secara berkala untuk memastikan bahwa semua proses berjalan dengan baik.

Simpulan

Berdasarkan latar belakang dan tujuan penelitian maka dapat disimpulkan bahwa kami dapat mengidentifikasi pola-pola yang mencurigakan dari aktifitas pada log server yang mungkin merupakan tanda dari serangan DdoS yang sedang terjadi, kemudian dapat mengembangkan sistem deteksi dini serangan DdoS melalui analisis log server. Dari serangan tersebut juga dapat menyajikan berbagai solusi pencegahan dan penanggulangan serangan DdoS yang efektif untuk meminimalkan dampaknya pada sistem website dengan menggunakan Firewall.

Daftar Pustaka

- Annef AB. 2021. Ancaman Siber Di Tengah Pandemi Covid-19: Tinjauan Terhadap Keamanan Non-Tradisional Dan Keamanan Siber Di Indonesia. *Sriwij. J. Int. Relations*. 1(1):18–33.doi:10.47753/sjir.v1i1.3.
- Dalimunthe RA, Yusda RA, Ramdhan W. 2020. Instalasi Sistem Operasi Berbasis Windows 10 Pada Sekolah Man Kisaran. *Jurdimas (Jurnal Pengabdi. Kpd. Masyarakat) R.* 3(2):163– 168.doi:10.33330/jurdimas.v3i2.499.
- Ditanaya TH, Ijtihadie RM, Husni M. 2016. Rancang Bangun Sistem Log Server Berbasis Syslog dan Cassandra untuk Monitoring Pengelolaan Jaringan di ITS. *J. Tek. ITS*. 5(2).doi:10.12962/j23373539.v5i2.18815.
- Farhan RM, Hendita G, Kusuma A. 2023. Teknik Sniffing Jaringan Menggunakan Wireshark. J. Informatics Adv. Comput. 4(1).
- Gayatrie MS, Kusyanti A, Saputra MC. 2017. Analisis Penerimaan Os Windows 10 Dengan Unified Theory of Acceptance and Use of Technology (UTAUT2). *J. Pengemb. Teknol. Inf. dan Ilmu Komput.* 1(6):514–523.
- Haryanto A, Sutra SM. 2023. Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020. *Glob. Polit. Stud. J.* 7(1):56– 69.doi:10.34010/gpsjournal.v7i1.8141.
- Hasbi M, Saputra NR. 2021. Analisis Quality of Service (Qos) Jaringan Internet Kantor Pusat King Bukopin Dengan Menggunakan Wireshark. *Univ. Muhammadiyah Jakarta*.

12(1):1–7.

- Listyawati NMM, Widjajarto A, Kurniawan MT. 2022. Implementasi dan Analisis Profil Sistem Pada Virtualisasi Paloalto Firewall Berdasarkan Metrik Sumber Daya Komputasi. J. Sist. Komput. dan Inform. 4(1):112.doi:10.30865/json.v4i1.4780.
- Luthfansa ZM, Rosiani UD. 2021. Pemanfaatan Wireshark untuk Sniffing Komunikasi Data Berprotokol HTTP pada Jaringan Internet. *J. Inf. Eng. Educ. Technol.* 5(1):34– 39.doi:10.26740/jieet.v5n1.p34-39.
- Mahmud PT, Arafi MT, Destianti LL, Cahyani I, Cantika I, Huda FN, Saputra DM, Anggraeni D, Putrie AA, Maharani A. 2020. Sniffing Jaringan Menggunakan Wireshark. J. Jar. Komput.:5–8.
- Mulawarman U. 2017. Analisis usabilitas sistem operasi windows 10 pada pengguna expert dan novice (studi kasus : mahasiswa fakultas teknik universitas mulawarman). *Manaj. dan Tek. Ind.*(September 2014):16–23.
- Nida H, Adrian R. 2023. Analisis Perbedaan Pengaruh Penggunaan Iptables Chains dalam Mencegah Denial of Service (DoS) pada Jaringan IoT. J. Internet Softw. Eng. 4(1):12– 17.doi:10.22146/jise.v4i1.5192.
- Primawanti H, Pangestu S. 2020. Diplomasi Siber Indonesia Dalam Meningkatkan Keamanan Siber Melalui Association of South East Asian Nation (Asean) Regional Forum. *Glob. Mind.* 2(2):1–15.doi:10.53675/jgm.v2i2.89.
- Sinambela ES. 2020. Evaluasi Performansi Deteksi Serangan Pada Hids Ossec. J. Ilm. Kohesi. 4(1):30–43.
- Supriyono S. 2018. Membangun Server Repository Di Windows Guna Mempermudah Pemasangan Aplikasi Pada Sistem Operasi Windows Di Laboratorium Informatika S-1 Itn Malang. *Ind. Fak. Teknol.* 2(1):199–205.
- Susilawati T, Yuliansyah F, Romzi M, Aryani R. 2020. Membangun Website Toko Online Pempek Nthree Menggunakan Php Dan Mysql. *J. Tek. Inform. Mahakarya*. 3, No.1(1):35– 44.
- Trimarsiah Y, Arafat M. 2017. Analisis dan Perancangan Website sebagai Sarana Informasi Pada Lembaga Bahasa Kewirausahaan dan Komputer AKMI Baturaja. *J. Ilm. MATRIK*. 19:1–10.
- Wagito, Librado D. 2022. ANALISIS DATA AKSES SITUS BERDASAR TEKNOLOGI LOG SERVER Wagito 1), Dison Librado 2). *Technologia*. 13(1):22–29.
- Wibisono G, Susanto WE. 2015. Perancangan Website Sebagai Media Informasi dan Promosi Batik Khas Kabupaten Kulonprogo. J. Evolusi. 6(2):46–55.
- Yogi, Ruslianto I, Bahri S. 2019. Analisa Log Web Server Untuk Mengetahui Pola Perilaku Pengunjung Website Menggunakan Teknik Regular Expressions. *Coding J. Komput. dan Apl.* 07(01):120–130.
- Zidane M. 2022. Klasifikasi Serangan Distributed Denial-of-Service (DDoS) menggunakan Metode Data Mining Naïve Bayes. J. Pengemb. Teknol. Inf. dan Ilmu Komput. 6(1):172– 180.