CESS
(Journal of Computing Engineering, System and Science) 8(1) January 2023 149-161

e-ISSN: 2502-714x
p-ISSN: 2502-7131

Contents list available at www.jurnal.unimed.ac.id

CESS
(Journal of Computing Engineering, System and Science)

journal homepage: https://jurnal.unimed.ac.id/2012/index.php/cess

Implementasi IPS (*Intrusion Prevention System*) *Fail2ban* Pada *Server* Terhadap Serangan DDoS dan *Brute Force*

Implementation of IPS (Intrusion Prevention System) Fail2ban on Server for DDoS and Brute Force Attacks

Fazar Dawamsyach[1*], Ikhwan Ruslianto[2], Uray Ristian[3]

[1,2,3] Program Studi Rekayasa Sistem Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Tanjungpura
Jalan Prof. Dr. H. Hadari Nawawi Pontianak
email: [1] fazeddawms@student.untan.ac.id, [2]ikhwanruslianto@siskom.untan.ac.id [3]eristian@siskom.untan.ac.id

A B S T R A K

Keamanan server merupakan hal penting yang harus diperhatikan agar server dapat bekerja dengan baik dan melayani pengguna. Serangan terhadap server dapat mengancam kinerja server dan keamanan data di dalamnya. Menurut laporan Badan Siber dan Sandi Negara tahun 2020, port 22 dan 80 menjadi port teratas dengan serangan terbanyak. Salah satu serangan pada port 22 adalah brute force dan serangan pada port 80 adalah Distributed Denial of Service (DDoS). Untuk menyelesaikan permasalahan ini, maka dilakukan penelitian implementasi IPS (Intrusion Prevention System) fail2ban untuk meningkatkan keamanan server. Serangan yang diuji terfokus pada serangan brute force pada port 22 dan serangan DDoS pada port 80 menggunakan protokol tcp. Sistem fail2ban dilengkapi dengan antarmuka website dan notifikasi melalui telegram. Hasil pengujian menunjukkan serangan DDoS lebih berdampak pada kinerja CPU dengan kenaikan tertinggi CPU sebesar 92% sedangkan serangan brute force lebih berdampak pada kinerja memory server dengan kenaikan tertinggi memory sebesar 100%. Kenaikan kinerja server mengakibatkan server menjadi lambat. Sistem berhasil mencegah serangan DDoS dengan kecepatan rata-rata 0,5 detik sedangkan serangan brute force 6,1 detik. Sistem berhasil mencegah serangan DDoS dengan total 88 serangan dan brute force dengan total 864 serangan.

Kata Kunci: *Intrusion Prevention System* (IPS), *fail2ban*, *keamanan server*, *Distributed Denial of Service* (DDoS), *brute force.*

A B S T R A C T

Server security is an important thing that must be considered so that the server can work well and serve users. Attacks on servers can threaten server performance and data security in it. According to the National Cyber and Crypto Agency 2020 report, ports 22 and 80 were the top

**Penulis Korespondensi:*
email: fazeddawms@student.untan.ac.id

ports with the most attacks. One of the attacks on port 22 is brute force and an attack on port 80 is Distributed Denial of Service (DDoS). To solve this problem, a study was conducted to implement fail2ban IPS (Intrusion Prevention System) to increase server security. The attacks tested focused on brute force attacks on port 22 and DDoS attacks on port 80 using the TCP protocol. The fail2ban system is equipped with a website interface and notifications via telegram. The test results show that DDoS attacks have more impact on CPU performance with the highest increase in CPU being 92%, while brute force attacks have more impact on server memory performance with the highest increase in memory by 100%. The increase in server performance results in slowed server performance. The system managed to prevent DDoS attacks with an average speed of 0.5 seconds while brute force attacks were 6.1 seconds. The system managed to prevent DDoS attacks with a total of 88 attacks and brute force attacks with a total of 864 attacks.

Keywords: *Intrusion Prevention System* (IPS), *fail2ban*, *server security, Distributed Denial of Service* (DDoS), *brute force.*

1. PENDAHULUAN

Keamanan *server* sangat perlu diperhatikan agar terhindar dari serangan yang dapat mengganggu kinerja *server* dalam melayani pengguna. Serangan yang dapat membahayakan *server* diantaranya adalah *Distributed Denial of Service* (DDoS) *dan brute force*. Berdasarkan laporan Badan Siber dan Sandi Negara tahun 2020 *port* 22 dan *port* 80 termasuk ke dalam *port* teratas dengan jumlah serangan tertinggi dimana *port* 22 dengan total 1,2 juta serangan dan *port* 80 dengan total 10,7 juta serangan [1].

Beberapa penelitian terkait salah satunya adalah penelitian mengenai sistem keamanan dengan judul "*Realtime* Pencegahan Serangan *Brute Force* dan DDoS Pada *Ubuntu Server*". Penelitian ini dilakukan dengan menggunakan *Ubuntu Server* yang terinstall program *OpenSSH* dan *Apache*, sedangkan pada *host* penyerang terinstall sistem operasi *Kali Linux* dan program *hydra, medusa, xerxes* dan *browser*. Tahap pengujian dilakukan dengan penyerangan *brute force* pada SSH, lalu penyerangan DDoS pada SSH dan yang terakhir penyerangan *brute force* pada *Apache*. Sistem keamanan *fail2ban* yang diimplementasikan berhasil mencegah serangan *brute force* dan DDoS dan hasil serangan pada *server* lognya akan dikirim ke *database* [2].

Penelitian terkait lainnya yaitu penelitian mengenai sistem keamanan dengan judul "Implementasi *Intrusion Prevention System* (IPS) Menggunakan *Snort* dan *IPtable* Pada *Monitoring* Jaringan Lokal Berbasis *Website*". Penelitian dilakukan dengan menguji serangan *Ping of Death* dan *Port Scanning* yang terfokus pada *port icmp, tcp,* dan *port udp* terhadap *server* yang memiliki sistem keamanan IPS dan *Iptable*. Hasil dari pengujian yang dilakukan didapat persentase keberhasilan sistem mendeteksi 90% untuk *serangan ping of death* dan 85% pada serangan *port scanning* [3].

Berdasarkan permasalahan yang telah disebutkan maka diharapkan sistem keamanan *Fail2ban* dapat meminimalisir terjadinya serangan terhadap *server* khususnya serangan *Distributed Denial of Service* (DDOS) dan *brute force* dan menjadi tolak ukur sistem keamanan pada *server* lainnya.

2. DASAR/TINJAUAN TEORI

2.1. Intrusion Prevention System (IPS)

Intrusion Prevention System (IPS) adalah sistem keamanan yang digunakan untuk mencegah adanya lalu lintas yang mencurigakan untuk masuk ke dalam jaringan. Sistem keamanan IPS dapat melakukan aksi tambahan dimana memasukkan perangkat penyerang ke dalam *block list* bahkan melakukan *scanning* ke perangkat penyerang [4]. *Intrusion Prevention System* (IPS) adalah sistem keamanan yang umum digunakan untuk meningkatkan keamanan sebuah sistem jaringan yang bekerja dengan memantau aktivitas di dalam jaringan serta mendeteksi dan mencegah serangan. Sistem keamanan IPS digunakan untuk mencegah adanya penyerang yang masuk ke dalam jaringan dengan mencatat dan memeriksa paket yang masuk.

2.2. Fail2ban

Fail2ban adalah sistem keamanan melindungi berbagai macam *server* dan menyediakan hasilnya dalam bentuk *log* data [5]. Sistem *fail2ban* diimplementasikan pada sebuah *server* dengan tujuan dapat meningkatkan keamanan lalu lintas jaringan dari serangan yang dapat membahayakan dan mengganggu layanan pada *server* tersebut. *Fail2ban* bekerja dengan memblokir IP *address* yang berkemungkinan mencoba untuk menyerang dan melanggar keamanan sistem dalam jangka waktu tertentu sehingga akan menghentikan koneksi IP *address* yang melakukan penyerangan. *Sistem Fail2ban* dapat mengirimkan notifikasi adanya serangan kepada seorang administrator sehingga dapat dilakukan tindakan pencegahan yang sesuai dengan *administrator* jaringan inginkan. Notifikasi yang digunakan adalah notifikasi melalui aplikasi *telegram. Fail2ban* digunakan sebagai sistem keamanan untuk serangan *Distributed Denial of Service* (DDoS) dan serangan *brute force*. Sistem *fail2ban* menggunakan aturan parameter serangan yang disebut dengan *jail* yang diatur pada sebuah *file*. Aturan parameter *jail ddos* yang digunakan pada penelitian ini dapat dilihat pada Tabel 1. Lalu untuk aturan parameter *jail sshd* dapat dilihat pada Tabel 2.

Tabel 1. Parameter Jail ddos

Parameter [ddos]	Nilai
enabled	*true* atau *false*
port	80
filter	ddos
logpath	*var/log/nginx/*error.log*
maxretry	satuan angka
findtime	satuan detik
bantime	satuan detik

Tabel 2. Parameter Jail sshd

Parameter [sshd]	Nilai
enabled	*true* atau *false*
port	22
filter	Sshd
logpath	*var/log/auth.log*
maxretry	satuan angka

findtime	satuan detik
bantime	satuan detik

Aturan parameter *jail* yang digunakan adalah *jail DDoS* untuk serangan DDoS dan *jail sshd* untuk serangan *brute force*. Parameter yang umumnya digunakan adalah *maxretry, findtime* dan *bantime*. Parameter *maxretry* menyatakan maksimum percobaan serangan hingga sumber IP dikenakan *ban*. Parameter *findtime* adalah jangka waktu yang diperlukan serangan untuk mencapai *maxretry*. Parameter *bantime* adalah lama waktu *ban* pada IP sumber serangan. Parameter yang digunakan pada penelitian ini adalah *maxretry* dengan nilai 3, *findtime* dengan nilai 120 detik dan *bantime* dengan nilai 600 detik [6].

2.3. Nginx

Nginx adalah sebuah *web server* yang menangani dan melayani permintaan dan tanggapan HTTP dan *logging* informasi. *Nginx* didirikan berdasarkan *event-base architecture* dimana komponen saling berinteraksi dengan menggunakan *event notification* dan tidak menggunakan metode panggilan langsung. *Event notification* kemudian dimasukkan kedalam antrian untuk diproses oleh *event handler* yang berjalan secara berulang. Setelah *event* diproses dan dikeluarkan dari antrian, *event* akan dilanjutkan pada proses selanjutnya [7].

Nginx memiliki kemampuan untuk membatasi frekuensi dari koneksi yang mengakses *web server*. Kemampuan ini digunakan dengan memanfaatkan *limit req module* yang disediakan oleh *nginx*. Parameter yang diatur adalah *zone*, *rate* dan *burst* [8].*Web server Nginx* digunakan untuk target serangan yaitu pada *port* 80 HTTP dan sebagai antarmuka *website* dari sistem keamanan *intrusion prevention system* (IPS) *fail2ban*.

2.4. Distributed Denial of Service (DDoS)

Distributed Denial of Service (DDoS) adalah serangan yang menghabiskan sumber daya dengan mengirimkan paket berbahaya dalam jumlah besar, yang mengakibatkan kegagalan layanan jaringan [9]. Serangan ini memanfaatkan ratusan hingga ribuan komputer untuk menyerang suatu perangkat secara bersamaan. Komputer yang digunakan untuk melakukan serangan DDoS akan mengirimkan paket ke satu perangkat dalam jumlah yang sangat besar sehingga perangkat tersebut tidak dapat bekerja sebagaimana mestinya. Serangan ini juga mengakibatkan pengguna tidak dapat memperoleh informasi dan tanggapan dari perangkat target serangan.

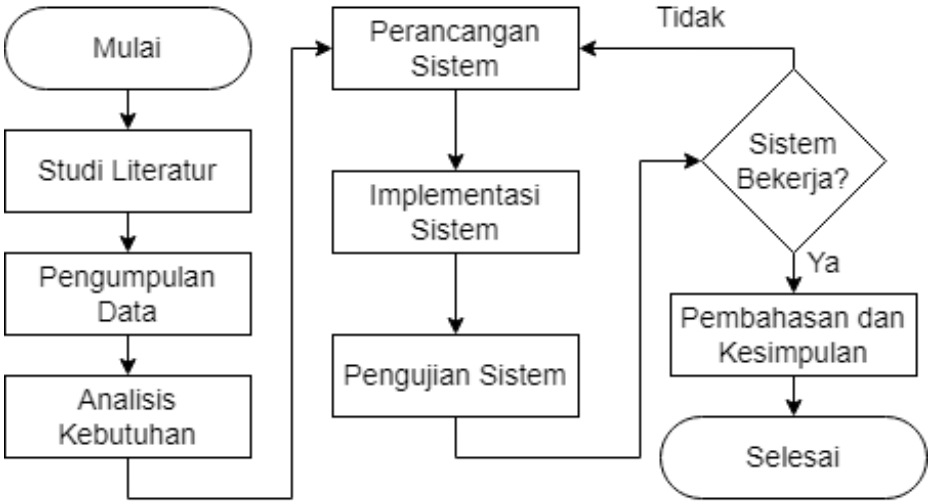
2.5. Brute Force

Brute force adalah teknik serangan terhadap sebuah sistem keamanan dengan menebak atau mencari semua kemungkinan *password* dengan masukan karakter dan panjang *password* tertentu yang tentunya dengan sangat banyak kombinasi *password* [10]. Proses dapat menggunakan menggunakan *software* dan juga cara lain untuk melakukan serangan *brute force.* Beberapa aplikasi yang terdapat dalam sistem operasi *kali linux* biasa digunakan oleh *hacker* untuk melakukan serangan *brute force* [11]. *Brute force* dilakukan dengan cara menebak atau melakukan percobaan terhadap semua kunci *password* dengan harapan dapat memperoleh akses sebuah sistem.

3. METODE

3.1. Metode Penelitian

Metodologi penelitian yang digunakan pada penelitian dapat dilihat pada diagram alir seperti pada Gambar 1.



Gambar 1. Diagram Alir Penelitian.

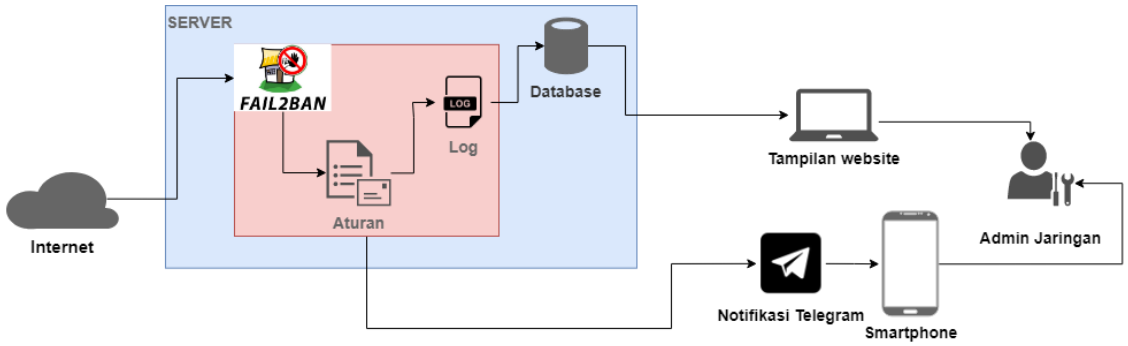
Keterangan:

1. Pada tahap studi literatur, dilakukan pencarian informasi mengenai topik penelitian dari berbagai sumber seperti buku, jurnal ilmiah, blog dan *website*.
2. Pada tahap pengumpulan data, dilakukan pengumpulan *tools* keamanan, perangkat pendukung serta media penelitian seperti *server*.
3. Pada tahap analisis kebutuhan, dilakukan analisis kebutuhan perangkat keras dan perangkat lunak yang diperlukan untuk membangun sistem.
4. Pada tahap perancangan sistem, dilakukan perancangan arsitektur sistem, perancangan sistem deteksi serangan, sistem notifikasi serangan, perancangan basis data, perancangan antarmuka dan perancangan skenario serangan.
5. Pada tahap implementasi sistem, dilakukan implementasi sistem IPS *fail2ban* pada *server* dan antarmuka *website*.
6. Pada tahap pengujian sistem, sistem diuji apakah sistem telah bekerja sesuai dengan yang diinginkan. Pengujian yang dilakukan adalah pengujian sistem *fail2ban,* pengujian fitur dan pengujian serangan. Jika sistem tidak bekerja sesuai dengan yang diinginkan maka kembali ke tahap perancangan sistem, apabila sistem telah bekerja sesuai dengan yang diinginkan maka dilanjutkan ke tahap berikutnya.
7. Pada tahap pembahasan dan kesimpulan, dilakukan pembahasan dari hasil keseluruhan pengujian dan dapat ditarik kesimpulan berdasarkan hasil penelitian yang telah dilakukan.

3.2. Gambaran Umum Sistem

Sistem *fail2ban* dibangun dengan menggunakan *server* sebagai media pengujian dan *website* sebagai antarmuka yang media komunikasi pengguna dan sistem. Antarmuka *website* digunakan untuk memberikan informasi dan beberapa aksi sistem keamanan *fail2ban* tanpa menggunakan input pada *command line server*. Informasi yang ditampilkan adalah kondisi *server* dan *log* hasil serangan. Aksi yang tersedia pada antarmuka *website* diantaranya adalah aksi status *fail2ban*, aksi *ban* atau *unban* dan input konfigurasi parameter serangan.

Antarmuka *website* menggunakan *nginx* sebagai *web server*. Arsitektur sistem *fail2ban* dapat dilihat pada Gambar 2.



Gambar 2. Arsitektur Sistem *Fail2ban*

Sistem keamanan *Intrusion Prevention System* (IPS) *Fail2ban* dibangun dan diimplementasikan pada *Virtual Private Server* (VPS) yang terhubung ke internet. Sistem keamanan *Fail2ban* akan memantau lalu lintas yang masuk ke jaringan *server* melalui internet. Sistem keamanan *Fail2ban* memantau jaringan *server* dengan membaca *log* pada *server* dan membandingkannya dengan aturan *jail* yang telah dibuat sebelumnya. Ketika lalu lintas yang masuk melanggar aturan, sistem keamanan akan bertindak secara otomatis dengan melakukan *ban* pada IP *address* yang melanggar aturan tersebut. Hasil serangan kemudian disimpan pada *database* dan ditampilkan pada *website*. Sistem keamanan juga akan mengirimkan notifikasi aplikasi *telegram* pada *smartphone* agar admin jaringan dapat mengetahui adanya serangan. Setelah hasil ditampilkan pada *website* dan notifikasi dikirimkan pada aplikasi *telegram*, admin jaringan dapat melihat hasil serangan dan dapat bertindak sesuai dengan hasil *log* serangan yang ditampilkan.

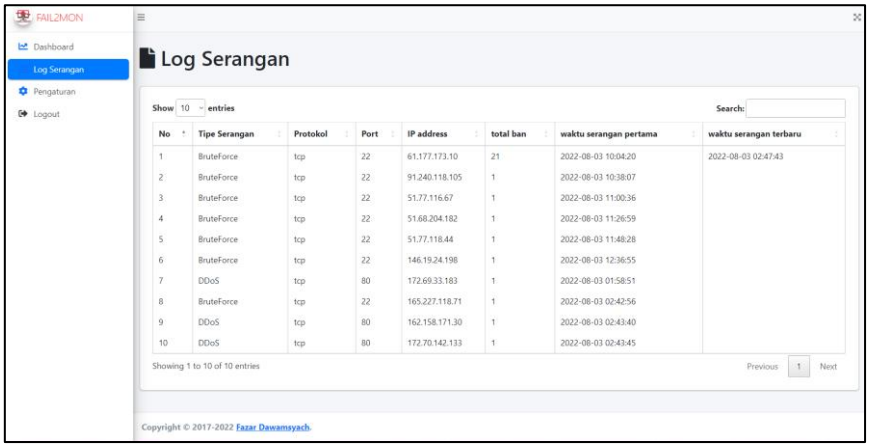
4. HASIL DAN PEMBAHASAN

Sistem keamanan *fail2ban* diuji dalam beberapa tahap yaitu pengujian waktu deteksi serangan untuk mengukur kecepatan sistem dalam mencegah serangan, pengujian notifikasi serangan untuk mengukur kecepatan aksi *ban* dan *unban* sistem *fail2ban*, pengujian kinerja *server* untuk mengukur dampak serangan terhadap kinerja *server* dan pengujian *live attacks* untuk mengukur perubahan pola serangan.

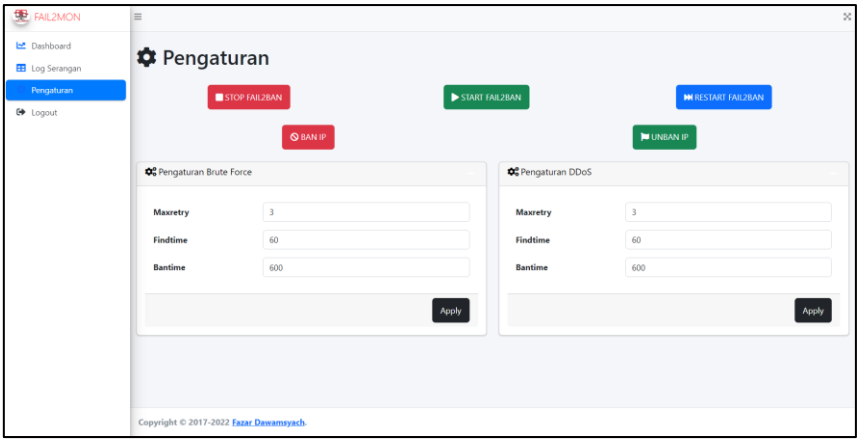
4.1. Implementasi Antarmuka Website

Sistem *fail2ban* dilengkapi dengan antarmuka *website* dan sistem notifikasi untuk membantu pengguna. *Website* digunakan sebagai media pengguna untuk memantau kinerja *server*, hasil *log* serangan dan aksi pencegahan serangan seperti *ban* dan *unban* manual. Tampilan halaman *dashboard* dapat dilihat pada Gambar 3 dan tampilan halaman log serangan dapat dilihat pada Gambar 4 serta tampilan halaman pengaturan dapat dilihat pada Gambar 5.

Gambar 3. Tampilan Halaman Dashboard.



Gambar 4. Tampilan Halaman Log.



Gambar 5. Tampilan Halaman Pengaturan.

4.2. Pengujian Waktu Deteksi Serangan

Pengujian waktu deteksi serangan pada sistem keamanan *fail2ban* terhadap serangan DDoS dilakukan dengan menggunakan *tool Pyflooder*. Jenis DDoS yang di uji adalah HTTP *flood attack* dengan mengirimkan 10000 paket *request* hingga sumber daya *server* tidak dapat melayani pengguna. Hasil pengujian deteksi serangan DDoS dapat dilihat pada Tabel 3.

Tabel 3. Hasil Pengujian Waktu Deteksi Serangan DDoS.

No	IP Sumber	IP Target	*Port*	*Jail*	Selisih waktu deteksi hingga *ban* (detik)
1	180.242.214.242	94.237.3.188	80	*ddos*	0,5
2	180.242.214.242	94.237.3.188	80	*ddos*	0,5
3	180.242.214.242	94.237.3.188	80	*ddos*	0,2
4	180.242.214.242	94.237.3.188	80	*ddos*	0,4
5	180.242.214.242	94.237.3.188	80	*ddos*	0,4
6	180.242.214.242	94.237.3.188	80	*ddos*	0,2
7	180.242.214.242	94.237.3.188	80	*ddos*	0,6
8	180.242.214.242	94.237.3.188	80	*ddos*	0,7
9	180.242.214.242	94.237.3.188	80	*ddos*	0,4
10	180.242.214.242	94.237.3.188	80	*ddos*	0,7
11	180.242.214.242	94.237.3.188	80	*ddos*	0,6
12	180.242.214.242	94.237.3.188	80	*ddos*	0,4
13	180.242.214.242	94.237.3.188	80	*ddos*	0,5
14	180.242.214.242	94.237.3.188	80	*ddos*	0,4
15	180.242.214.242	94.237.3.188	80	*ddos*	0,7
16	180.242.214.242	94.237.3.188	80	*ddos*	0,2
17	180.242.214.242	94.237.3.188	80	*ddos*	0,5
18	180.242.214.242	94.237.3.188	80	*ddos*	0,7
19	180.242.214.242	94.237.3.188	80	*ddos*	0,6
20	180.242.214.242	94.237.3.188	80	*ddos*	0,7
Rata-rata					0,5

Pengujian sistem keamanan *fail2ban* terhadap serangan *brute force* dilakukan dengan *tool medusa*. *Medusa* adalah *tool* yang digunakan untuk melakukan *brute force* dengan memanfaatkan *wordlist* yang berisikan *password*. *Wordlist* yang digunakan adalah *wordlist rockyou.txt* yang tersedia pada sistem operasi *Kali linux*. Hasil pengujian deteksi serangan *brute force* dapat dilihat pada Tabel 4.

Tabel 4. Hasil Pengujian Waktu Deteksi Serangan *Brute Force***.**

No	IP Sumber	IP Target	*Port*	*Jail*	Selisih waktu deteksi hingga *ban* (Detik)
1	180.242.214.242	94.237.3.188	22	*sshd*	7,8
2	180.242.214.242	94.237.3.188	22	*sshd*	6,7
3	180.242.214.242	94.237.3.188	22	*sshd*	8,6
4	180.242.214.242	94.237.3.188	22	*sshd*	7,3
5	180.242.214.242	94.237.3.188	22	*sshd*	3,7
6	180.242.214.242	94.237.3.188	22	*sshd*	4,0
7	180.242.214.242	94.237.3.188	22	*sshd*	7,0
8	180.242.214.242	94.237.3.188	22	*sshd*	5,9
9	180.242.214.242	94.237.3.188	22	*sshd*	4,0

10	180.242.214.242	94.237.3.188	22	*sshd*	5,3
11	180.242.214.242	94.237.3.188	22	*sshd*	4,2
12	180.242.214.242	94.237.3.188	22	*sshd*	7,1
13	180.242.214.242	94.237.3.188	22	*sshd*	6,7
14	180.242.214.242	94.237.3.188	22	*sshd*	7,2
15	180.242.214.242	94.237.3.188	22	*sshd*	6,4
16	180.242.214.242	94.237.3.188	22	*sshd*	6,6
17	180.242.214.242	94.237.3.188	22	*sshd*	5,7
18	180.242.214.242	94.237.3.188	22	*sshd*	6,2
19	180.242.214.242	94.237.3.188	22	*sshd*	6,8
20	180.242.214.242	94.237.3.188	22	*sshd*	5,1
Rata-rata					6,1

4.3. Pengujian Notifikasi Serangan

Pengujian notifikasi serangan adalah pengujian yang dilakukan untuk mengetahui lama waktu yang diperlukan oleh aplikasi *telegram* dalam menerima notifikasi serangan yang dikirimkan oleh sistem keamanan *fail2ban*. Pengujian ini menggunakan fitur *ban* dan *unban* manual pada *website* sistem keamanan *fail2ban* yang menggunakan IP *address dummy* atau buatan dan *jail brute force* sebagai masukan pada *form*.

Sistem notifikasi serangan adalah sistem yang memberitahukan kepada pengguna ketika adanya serangan maupun aksi yang dilakukan oleh sistem *fail2ban*. Sistem notifikasi yang digunakan adalah *telegram bot*. Hasil pengujian notifikasi serangan dapat dilihat pada Tabel5.

Tabel 5. Hasil Pengujian Notifikasi Serangan.

No	IP *address*	Waktu notifikasi *ban* (detik)	Waktu notifikasi *unban* (detik)
1	103.154.110.50	4,4	2,3
2	103.154.110.51	3,0	1,9
3	103.154.110.52	2,4	1,9
4	103.154.110.53	2,2	2,0
5	103.154.110.54	2,3	2,1
6	103.154.110.55	2,1	1,9
7	103.154.110.56	2,1	1,8
8	103.154.110.57	2,4	1,9
9	103.154.110.58	2,2	2,1
10	103.154.110.59	2,1	1,8
11	103.154.110.60	2,2	1,9
12	103.154.110.61	2,2	1,9
13	103.154.110.62	2,4	1,8
14	103.154.110.63	2,6	2,1
15	103.154.110.64	2,2	1,9
16	103.154.110.65	2,2	2,0
17	103.154.110.66	2,4	2,3
18	103.154.110.67	2,2	1,9
19	103.154.110.68	2,0	1,9
20	103.154.110.69	1,9	2,0
Rata-rata		2,4	2,0

4.4. Pengujian Kinerja Server

Pengujian kinerja *server* adalah pengujian yang dilakukan untuk mengetahui kenaikan kinerja CPU dan *memory server* saat serangan terjadi. Pengujian kinerja *server* dilakukan dalam dua tahapan, yaitu pengujian serangan DDoS dan pengujian serangan *brute force.*
Pengujian pada serangan DDoS dilakukan sebanyak 20 kali dalam 60 detik setiap satu pengujian dengan menggunakan *tool Pummel*. Pengujian ini menggunakan parameter *jail* yaitu *maxretry* 3, *findtime* 60 detik dan *bantime* 600 detik. Hasil pengujian skenario serangan DDoS dapat dilihat pada Tabel 6.

Tabel 6. Hasil Pengujian Serangan DDoS Terhadap Kinerja *Server*.

No	IP sumber	IP Target	Waktu (detik)	Kinerja Server (%)	
				CPU	Memory
1	180.242.234.204	94.237.3.188	60	81,8	96,3
2	180.242.234.204	94.237.3.188	60	86,5	97,0
3	180.242.234.204	94.237.3.188	60	86,0	96,1
4	180.242.234.204	94.237.3.188	60	79,3	96,9
5	180.242.234.204	94.237.3.188	60	92,0	97,0
6	180.242.234.204	94.237.3.188	60	83,8	97,0
7	180.242.234.204	94.237.3.188	60	70,8	96,9
8	180.242.234.204	94.237.3.188	60	79,8	96,9
9	180.242.234.204	94.237.3.188	60	82,0	97,0
10	180.242.234.204	94.237.3.188	60	92,0	97,5
11	180.242.234.204	94.237.3.188	60	76,8	97,3
12	180.242.234.204	94.237.3.188	60	88,4	97,2
13	180.242.234.204	94.237.3.188	60	58,9	96,8
14	180.242.234.204	94.237.3.188	60	58.2	96.7
15	180.242.234.204	94.237.3.188	60	61,6	96,6
16	180.242.234.204	94.237.3.188	60	59,7	97,1
17	180.242.234.204	94.237.3.188	60	63,6	96,7
18	180.242.234.204	94.237.3.188	60	89,6	97,2
19	180.242.234.204	94.237.3.188	60	77,6	97,5
20	180.242.234.204	94.237.3.188	60	84,6	97,4
Rata-rata				77,7	97

Pengujian kinerja *server* dengan serangan *brute force* dilakukan sebanyak 20 kali dengan menghitung kinerja *server.* Pengujian dilakukan dengan menggunakan *wordlist* yang memiliki total 100 kata sandi menggunakan *tool ncrack*. Pengujian ini menggunakan parameter *jail* yaitu *maxretry* 100, *findtime* 60 detik dan *bantime* 600 detik. Hasil pengujian skenario serangan *brute force* dapat dilihat pada Tabel 7.

Tabel 7. Hasil Pengujian Serangan *Brute Force* Terhadap Kinerja *Server*.

No	IP sumber	IP Target	Waktu (Detik)	Jumlah Kata Sandi	Kinerja Server (%)	
					CPU	*Memory*
1	180.242.234.204	94.237.3.188	27	100	33,9	99,7
2	180.242.234.204	94.237.3.188	33	100	50,0	98,8

3	180.242.234.204	94.237.3.188	30	100	64,9	99,4
4	180.242.234.204	94.237.3.188	33	100	57,5	98,9
5	180.242.234.204	94.237.3.188	33	100	25,4	98,4
6	180.242.234.204	94.237.3.188	30	100	56,9	99,8
7	180.242.234.204	94.237.3.188	33	100	36,4	98,2
8	180.242.234.204	94.237.3.188	27	100	36,7	97,6
9	180.242.234.204	94.237.3.188	30	100	31,4	97,8
10	180.242.234.204	94.237.3.188	27	100	33,2	98,4
11	180.242.234.204	94.237.3.188	30	100	41,6	97,8
12	180.242.234.204	94.237.3.188	30	100	32,2	97,9
13	180.242.234.204	94.237.3.188	27	100	30,5	97,4
14	180.242.234.204	94.237.3.188	33	100	24,4	97,8
15	180.242.234.204	94.237.3.188	24	100	31,5	97,7
16	180.242.234.204	94.237.3.188	36	100	29,1	97,4
17	180.242.234.204	94.237.3.188	33	100	29,1	97,3
18	180.242.234.204	94.237.3.188	30	100	23,6	97,4
19	180.242.234.204	94.237.3.188	27	100	83,5	100
20	180.242.234.204	94.237.3.188	33	100	66,2	100
Rata-rata					41,5	98,4

4.5. Pengujian Live Attacks

Pengujian *live attacks* dilakukan dengan mengubah parameter *maxretry* pada *jail* DDoS dan *brute force*. Parameter *maxretry* diubah setiap 5 hari sekali. Pengujian dengan parameter *maxretry* bernilai 3 dilakukan dari tanggal 5 Agustus 2022 hingga tanggal 10 Agustus 2022. Pengujian dengan parameter *maxretry* bernilai 4 dilakukan dari tanggal 11 Agustus 2022 hingga tanggal 16 Agustus 2022. Pengujian dengan parameter bernilai 5 dilakukan dari tanggal 16 Agustus 2022 hingga tanggal 21 Agustus 2022. Total serangan DDoS dan *brute force* dicatat setiap pukul 10.00 WIB setiap hari selama 15 hari. Hasil pengujian *live attacks* dapat dilihat pada Tabel 8.

Tabel 8. Hasil Pengujian *Live Attacks.*

Hari	Tanggal Mulai	Tanggal Selesai	Parameter *Jail*			Total Serangan DDoS	Total Serangan *Brute force*
			Maxretry	*Findtime* (Detik)	*Bantime (Detik)*		
1	05-08	06-08	3	60	600	9	50
2	06-08	07-08	3	60	600	2	39
3	07-08	08-08	3	60	600	6	135
4	08-08	09-08	3	60	600	5	114
5	09-08	10-08	3	60	600	7	93
6	11-08	12-08	4	60	600	8	27
7	12-08	13-08	4	60	600	3	28
8	13-08	14-08	4	60	600	6	114
9	14-08	15-08	4	60	600	6	65
10	15-08	16-08	4	60	600	8	47
11	16-08	17-08	5	60	600	5	43
12	17-08	18-08	5	60	600	8	62

13	18-08	19-08	5	60	600	5	19
14	19-08	20-08	5	60	600	1	10
15	20-08	21-08	5	60	600	9	18
			Total			88	864

4.6. Pembahasan

Hasil pengujian waktu deteksi serangan menunjukkan bahwa sistem *fail2ban* lebih andal dalam menangani serangan DDoS daripada serangan *brute force.* Kecepatan waktu rata-rata yang diperlukan sistem *fail2ban* untuk melakukan aksi *ban* saat serangan DDoS adalah 0,5 detik sedangkan pada serangan *brute force* adalah 6,1 detik. Perbedaan waktu ini dikarenakan pada serangan DDoS paket *request* dikirim dengan cepat dan terdeteksi secara langsung sedangkan pada serangan *brute force* sistem autentikasi *server* hanya dapat melakukan 1 kali *login* setiap waktunya dengan memasukkan *password* pada *wordlist*.

Hasil pengujian notifikasi serangan menunjukkan bahwa sistem *fail2ban* lebih cepat dalam melakukan aksi *unban* daripada aksi *ban*. Perbedaan kecepatan pada sistem notifikasi dalam menerima notifikasi serangan dikarenakan pada saat sistem melakukan *ban*, sistem *fail2ban* menuliskan data baru yaitu IP *address* dan tipe serangan pada daftar *banned* dan memasukkan *entry* data baru pada *database* kemudian mengirimkan notifikasi ke aplikasi *telegram*. Sedangkan pada saat sistem melakukan *unban*, sistem hanya mengeluarkan IP *address* dari daftar *banned* dan mengirimkan notifikasi ke aplikasi *telegram*.

Hasil pengujian serangan terhadap kinerja *server* menunjukkan serangan DDoS mengakibatkan kinerja CPU *server* naik lebih tinggi daripada serangan *brute force*, dan serangan *brute force* mengakibatkan kinerja *memory* naik lebih tinggi daripada serangan DDoS. Kenaikan kinerja *server* mengakibatkan *website* sistem *fail2ban* mengalami respon yang lama. Hasil pengujian *live attacks* menunjukkan bahwa perubahan pada parameter *jail maxretry* mengakibatkan perubahan pada pola serangan. Serangan *brute force* yang dicegah oleh sistem mengalami penurunan setiap perubahan nilai *maxretry* yang semakin besar. Perubahan pola serangan diakibatkan oleh sistem *fail2ban* hanya melakukan *ban* pada IP *address* yang mencapai atau melebihi *maxretry*. Sehingga ketika serangan terjadi dan tidak mencapai *maxretry* yang ditentukan, maka sistem tidak melakukan *ban* dan tidak mencatat serangan.

5. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan sistem *fail2ban* berhasil diterapkan dan dapat mencegah adanya serangan DDoS dan *brute force*. Sistem *fail2ban* diuji dalam beberapa tahapan diantaranya pengujian waktu deteksi serangan, pengujian notifikasi serangan, pengujian kinerja *server* dan pengujian *live attacks*. Hasil pengujian menunjukkan bahwa sistem *fail2ban* lebih cepat dalam mendeteksi serangan DDoS daripada serangan *brute force* dan sistem *fail2ban* lebih cepat dalam melakukan aksi *unban* daripada aksi *ban.* Serangan DDoS lebih berdampak pada kenaikan kinerja CPU daripada *brute force* yang lebih berdampak pada kenaikan kinerja *memory* dan perubahan pada parameter *maxretry* mengakibatkan perubahan pada pola serangan. Perubahan nilai parameter *jail maxretry* mengakibatkan perubahan pada pola serangan.

REFERENSI

[1] Badan Siber dan Sandi Negara, "Laporan Tahunan 2020 Honeynet Project BSSN-IHP," 2021.
[2] Syaifuddin, D. Risqiwati, and E. Ari Irawan, "Realtime Pencegahan Serangan Brute Force dan DDOS Pada Ubuntu Server," *Techno.COM*, vol. 17, no. 4, pp. 347–354, 2018.
[3] R. Suwanto, I. Ruslianto, and M. Diponegoro, "Implementasi Intrusion Prevention System (IPS) Menggunakan Snort dan IPTable pada Monitoring Jaringan Lokal Berbasis Website," *Jurnal Komputer dan Aplikasi*, vol. 7, no. 1, pp. 97–107, 2019.
[4] R. Alder, "Snort IDS and IPS Toolkit," pp. 25–26, 2007.
[5] I. Muakhori, Sunardi, and A. Fadlil, "Security of Dynamic Domain Name System Servers Against DDOS Attacks Using Iptable and Fail2ba," *Jurnal Mantik*, vol. 4, no. 1, pp. 41–49, 2020.
[6] K. Hess, "Linux Security: Protect Your Systems with Fail2ban," Jun. 04, 2020. www.redhat.com/sysadmin/protect-systems-fail2ban (accessed Sep. 21, 2022).
[7] I. F. Irza, Zulhendra, and Efrizon, "Analisis Perbandingan Kinerja Web Server Apache dan Nginx Menggunakan Httperf pada Portal Berita (Studi Kasus beritalinux.com)," *Teknik Elektronika & Informatika*, vol. 5, no. 2, pp. 75–82, 2017.
[8] Martin. Fjordvald, *Instant Nginx Starter : Implement the Nifty Features of Nginx with This Focused Guide*. Packt Publishing, 2013.
[9] R. Zhong and G. Yue, "DDoS Detection System Based On Data Mining," *Proceedings of the Second International Symposium on Networking and Network Security*, pp. 62–65, 2010.
[10] K. E. Pramudita, *Brute Force Attack dan Penerapannya pada Password Cracking*. 2010.
[11] H. S. Pratita, "Analisa Brute Force Attack Menggunakan Scanning Aplikasi pada HTTP Attack," 2016.