Implementasi Fail2ban untuk Melindungi Sistem Keamanan pada *Cloud*

Nurani Harum Fardaniah[1*], Anwar[2], Guntur Syahputra[3]

[1,2,3] *Jurusan Teknologi Informasi dan Komputer Politeknik Negeri Lhokseumawe*
Jln. B.Aceh Medan Km.280 Buketrata 24301 INDONESIA
[1*]harumfardaniah96@gmail.com (penulis korespondensi)
[2]anwarsy@pnl.ac.id
[3]guntursyahputra@pnl.ac.id

***Abstrak*—Dalam era dimana komputasi awan *(cloud computing)* menjadi pondasi utama untuk menyimpan dan mengelola data, keamanan informasi menjadi aspek yang harus diperhatikan. Ancaman keamanan yang terus berkembang, seperti serangan *brute-force* dan DDoS. Penelitian ini menginvestigasi dan implementasi Fail2ban sebagai bentuk solusi untuk melindungi sistem keamanan pada lingkungan *cloud* . Penelitian ini mencakup analisis kelemahan keamanan umum yang dihadapi oleh sistem *cloud* dan merinci bagaimana serangan *brute-force* dan DDoS dapat mempengaruhi kestabilan dan kerahasiaan data. Penelitian ini mengevaluasi implementasi Fail2ban dalam melindungi keamanan sistem pada *Cloud* dan *server Ubuntu.* Setelah diimplementasikan Fail2ban, percobaan *login* pada SSH *Cloud* dan Ubuntu *Server* berhasil diblokir setelah maksimal 5 kali percobaan sampai akhirnya diberhentikan oleh Fail2ban.. Rata-rata waktu yang diperlukan Fail2ban untuk memblokir serangan *brute force* adalah 0,4 detik pada *Cloud* dan 1,9 detik pada Ubuntu *Server*. Pengujian serangan DDoS dengan 10000 paket menunjukkan bahwa Fail2ban dapat mengurangi dampak serangan DDoS, CPU Ubuntu *Server* yang mulanya 100% turun menjadi 25%. Namun pada *Cloud Server*, telah memiliki layanan anti DDoS sendiri. Meskipun demikian, dari seluruh hasil pengujian dan monitoring, dapat disimpulkan bahwa fail2ban berhasil menghentikan adanya serangan *brute force* namun pada serangan DDoS, fail2ban tidak dapat menghentikan serangan tersebut seperti pada serangan *brute force*.*

Kata kunci*— *Cloud,* Ubuntu *Server,* Fail2ban, Keamanan Sistem*, Brute-Force, Distributed Denial of Service

Abstract*—In an era where cloud computing is the main foundation for storing and managing data, information security is an aspect that must be considered. Continuously evolving security threats, such as brute-force and DDoS attacks. This research investigates and implements Fail2ban as a solution to protect security systems in cloud environments. This research includes an analysis of common security weaknesses faced by cloud systems and details how brute-force and DDoS attacks can affect the stability and confidentiality of data. This research evaluates the implementation of Fail2ban in protecting system security on the Cloud and Ubuntu servers. After implementing Fail2ban, login attempts on SSH Cloud and Ubuntu Server were successfully blocked after a maximum of 5 attempts until finally being stopped by Fail2ban. The average time required for Fail2ban to block a brute force attack was 0.4 seconds on the Cloud and 1.9 seconds on Ubuntu Server. Testing DDoS attacks with 10,000 packets shows that Fail2ban can reduce the impact of DDoS attacks, the Ubuntu Server CPU which was initially 100% down to 25%. However, Cloud Server has its own anti-DDoS service. However, from all the testing and monitoring results, it can be concluded that fail2ban was successful in stopping brute force attacks, but in DDoS attacks, fail2ban was not able to stop the attack like brute force attacks

Keywords*— *Cloud, Ubuntu Server, Fail2ban, System Security, Brute-Force, Distributed Denial of Service

I. PENDAHULUAN

Di era transformasi digital, penggunaan teknologi *cloud* menjadi hal yang penting bagi organisasi dalam menjalankan operasional dan menyimpan data. Sistem yang ada di lingkungan *cloud* menawarkan fleksibilitas, skalabilitas, dan efisiensi yang menarik, namun tantangan keamanan menjadi semakin kompleks. Mengamankan sistem keamanan di lingkungan *cloud* sangat penting untuk menjaga integritas data dan ketersediaan layanan. Banyaknya komunitas kelompok *hacking* dan *cracking* yang saat ini terbentuk menimbulkan ancaman aktivitas kriminal pada sistem informasi [1].

Serangan siber, terutama serangan *Brute-Force*, menjadi ancaman serius terhadap keamanan sistem di *cloud*. Serangan *Brute-Force* melibatkan upaya penyerang untuk menebak kombinasi penggunaan dan kata sandi dengan cara yang berulang, dengan tujuan mendapatkan akses yang tidak sah [2]. Kemudian serangan *Distributed Denial of Service* (DDOS) adalah salah satu serangan yang paling sering ditemui. Serangan *Distributed Denial of Service* (DDoS) merupakan upaya untuk membuat layanan *online* tidak tersedia dengan mengirimkan sangat banyak *traffic* atau paket data dalam jumlah yang sangat besar dari berbagai sumber yang bertujuan untuk melumpuhkan jaringan [3]. Oleh karena itu, dibutuhkan langkah-langkah proaktif dalam mendeteksi dan mengatasi ancaman ini.

Ada berbagai jenis strategi yang dapat dipakai untuk menghadapi serangan siber. Beberapa strategi yang umum digunakan untuk meningkatkan keamanan dan melindungi sistem dari ancaman siber diantaranya adalah dengan menginstal Firewall, menggunakan *Antivirus, Antimalware*, dan melakukan enkripsi data [4].

Pada penelitian ini, saya akan meneliti penerapan Fail2ban pada *cloud* , karena *cloud* bekerja secara *online*, sehingga lebih banyak mengundang para *hacker* dan *cracker*

untuk mencoba sistem tersebut. Fail2Ban adalah perangkat lunak yang dirancang untuk memantau *log file system* dan mengidentifikasi pola perilaku mencurigakan, termasuk percobaan *login* yang berulang. Dengan kemampuannya, secara otomatis memblokir alamat IP yang terlibat dalam serangan [5].

Oleh karena itu, penelitian ini bertujuan untuk menginvestigasi dan menerapkan Fail2Ban sebagai solusi yang efektif untuk melindungi sistem keamanan pada lingkungan *cloud*. Dengan pemahaman yang mendalam tentang implementasi Fail2Ban di *cloud*, diharapkan dapat memberikan kontribusi signifikan dalam menghadapi ancaman keamanan yang terus berkembang di dunia teknologi informasi.

A. *Keamanan Jaringan*

Keamanan jaringan adalah praktik dan prosedur yang digunakan untuk melindungi jaringan dari ancaman dan serangan yang merusak seperti *virus, malware*, peretas, dan peretasan data. Tujuan utama keamanan jaringan komputer adalah untuk melindungi data dan informasi rahasia dari kehilangan dan akses yang tidak sah. Keamanan jaringan komputer mencakup berbagai tindakan dan teknologi untuk mencegah, mengidentifikasi, dan merespons ancaman keamanan.

Konsep dasar dari Keamanan Jaringan ada 3 berdasarkan konsep "CIA Triad" yang terdiri atas *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Availability* (ketersediaan). *Confidentiality* atau kerahasiaan merupakan aturan yang membatasi akses informasi dengan konsep ini juga merupakan dasar dari model standar dalam keamanan informasi [6].

B. *Cloud Computing*

Cloud Computing merupakan wadah penyimpanan dan mengakses data program melalui internet dari tempat yang berbeda. Cloud computing merupakan layanan komputasi teknologi informasi yang mencakup layanan hardware, software dan aplikasi yang dapat diperoleh melalui internet [7].

Konsep Cloud computing biasanya dianggap sebagai internet. Karena internet sendiri digambarkan sebagai awan (Cloud) besar (biasanya dalam skema jaringan, internet dilambangkan sebagai awan) yang berisi sekumpulan komputer yang saling terhubung [8].

C. *Virtual Private Server* (VPS)

Virtual Private Server (VPS) adalah jenis layanan hosting yang menggunakan teknologi virtualisasi untuk menyediakan sumber daya khusus pada *server* fisik yang dibagi menjadi beberapa *server* virtual. Setiap VPS berjalan sebagai sistem independen dengan sistem operasi, penyimpanan, dan sumber daya jaringan sendiri, seolah-olah merupakan *server* fisik yang berdiri sendiri. VPS sering digunakan oleh pengguna yang membutuhkan kontrol lebih besar dibandingkan dengan *shared hosting,* tetapi tidak memerlukan seluruh sumber daya dari *server* fisik seperti pada dedicated *server*. VPS memiliki *process, user, files* dan menyediakan full root access. Setiap VPS mempunyai alamat IP, *port number, tables, filtering* dan *routing rules* sendiri. Setiap VPS dapat *delete, add, modify file* apa saja, termasuk *file* yang ada di dalam *root*, dan *install software* aplikasi sendiri atau konfigurasi *root application software*-nya [9].

D. *Fail2ban*

Fail2ban merupakan paket program untuk mendeteksi usaha *login* yang gagal dan kemudian memblokir alamat IP host asal, Fail2ban bekerja dengan cara merubah aturan konfigurasi *firewall* dengan konfigurasi yang berada di Fail2ban itu sendiri, ketika Fail2ban berjalan, ia akan mengambil alih fungsi *firewall* yang berada di *server* fungsi fail2ban itu sendiri untuk monitor jumlah kegagalan *login* ssh di *server*, yang selanjutnya ip akan diblokir sehingga mempermudah kinerja administrator, Fail2ban dapat mengamankan berbagai *server* dan kemudian memberikan hasil serangan berupa data log [10]. Aturan parameter jail sshd dapat dilihat pada Tabel I.

TABEL I
PARAMETER JAIL SSHD

Parameter [sshd]	Nilai
enabled	true atau false
port	ssh
filter	sshd
logpath	var/log/fail2ban.log

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.

E. *Putty*

PuTTY *(Phonetic Transcription)* adalah emulator terminal xterm *open source, consol serial,* dan aplikasi transfer file jaringan. Putty merupakan aplikasi yang biasa digunakan untuk *remote access* seperti SSH atau Telnet. Putty dapat mengakses *server* dari jarak jauh dan merupakan aplikasi *Open Source* yang dapat digunakan secara gratis. PuTTY tidak memiliki antarmuka grafis (GUI), yang berarti setelah terhubung, hanya akan ada tampilan baris perintah *(command line)* yang tersedia [11].

F. *Bpytop*

Bpytop adalah alat pemantauan sumber daya sistem berbasis terminal yang ditulis dalam Python. Alat ini memungkinkan pengguna untuk memantau penggunaan CPU, RAM, disk, dan jaringan dalam antarmuka yang interaktif dan ramah pengguna. Bpytop menawarkan grafik yang intuitif dan informasi rinci mengenai proses yang berjalan, membuatnya sangat berguna untuk pemantauan kinerja sistem secara real time.

G. *Brute Force*

Serangan *Brute-Force* adalah sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin. *Brute force attack* digunakan untuk menjebol akses ke suatu host *(server/workstation/network)* atau kepada data yang terenkripsi. Metode ini dipakai para cracker untuk mendapatkan account secara tidak sah, dan sangat berguna untuk memecahkan enkripsi. Enkripsi macam apapun, seperti Blowfish, AES, DES, Triple DES dsb secara teoritis dapat dipecahkan dengan *Brute-Force attack.* Pemakaian *password* sembarangan, memakai *password* yang cuma sepanjang 3 karakter, menggunakan kata kunci yang mudah ditebak, menggunakan *password* yang sama, menggunakan nama, memakai nomor telepon, sudah pasti sangat tidak aman [12].

H. *Distributed Denial of Service (DDoS)*

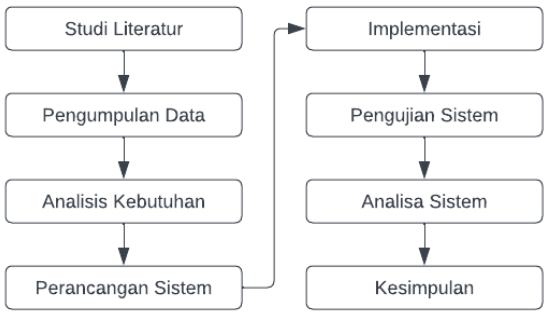
Serangan DDoS menargetkan situs *web* dan *server* dengan mengganggu layanan jaringan yang bertujuan untuk menghabiskan sumber daya aplikasi. Pelaku di balik serangan ini membanjiri situs dengan lalu lintas yang salah, sehingga fungsionalitas *situs web* menjadi buruk atau membuatnya *offline* sama sekali. Serangan DDoS memiliki jangkauan yang luas, yang menargetkan semua jenis industri dan perusahaan dengan semua ukuran di seluruh dunia. Industri tertentu, seperti permainan, e-niaga, dan telekomunikasi, lebih ditargetkan daripada yang lain. Serangan DDoS adalah beberapa ancaman *cyber* yang paling umum, dan dapat berpotensi membahayakan bisnis, keamanan *online*, penjualan, dan reputasi [13].

II. METODOLOGI PENELITIAN

Pada metodologi penelitian akan dibahas mengenai perancangan sistem dan teknik pengujian c*loud.*

A. *Metode Penelitian*

Untuk melaksanakan Implementasi Fail2ban pada *cloud ,* diperlukan susunan kerangka kerja *(frame work)* yang merupakan tahapan-tahapan penyelesaian yang dibahas. Kerangka kerja dalam penelitian dapat dilihat pada gambar 1.

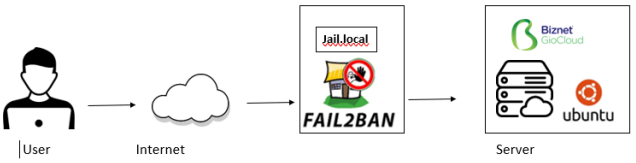


Gambar 1. Metodologi Penelitian

1) Studi Literatur, pencarian informasi mengenai topik penelitian yang akan dilakukan dari berbagai sumber seperti buku, jurnal ilmiah, *blog* dan *webiste*.
2) Pengumpulan Data, pengumpulan *tools* keamanan, jenis serangan, tools serangan, perangkat pendukung serta media penelitian seperti *cloud* .
3) Analisis Kebutuhan, dilakukan analisis kebutuhan perangkat keras dan perangkat lunak.
4) Perancangan Sistem, dilakukan perancangan arsitektur sistem, perancangan sistem deteksi serangan, perancangan skenario serangan
5) Implementasi, dilakukan implementasi fail2ban pada *cloud*
6) Pengujian Sistem, sistem diuji apakah sistem bekerja sesuai dengan yang diinginkan. Pengujian sistem fail2ban meliputi pengujian fitur dan pengujian serangan *Brute-Force* dan DDoS.
7) Analisa Sistem, jika sistem tidak bekerja sesuai dengan yang diinginkan maka kembali ke tahap perancangan sistem, namun apabila sistem telah bekerja sesuai dengan yang diinginkan maka dilanjutkan ke tahap selanjutnya.
8) Kesimpulan, langkah terakhir adalah kesimpulan berdasarkan hasil penelitian yang telah dilakukan.

B. *Rancangan Sistem*

Rancangan sistem dilakukan untuk membuat desain perencanaan arsitektur sistem yang akan dibangun dapat berjalan sesuai dengan tujuan penelitian. Rancangan sistem dapat dilihat pada Gambar 1 di bawah ini.



Gambar 2. Rancangan Sistem

Sistem keamanan Fail2ban dibangun dan diimplementasikan pada *Virtual Private Server* (VPS) dan *Ubuntu Server* yang terhubung ke internet. Penggunaan jail.local untuk melindungi atau memproteksi layanan SSH dari serangan *brute-force* dan serangan ddos dengan menetapkan aturan yang memonitor dan memblokir aktivitas mencurigakan.

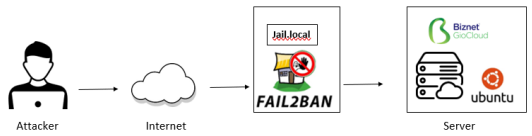
Sistem keamanan Fail2ban akan memantau lalu lintas yang masuk ke jaringan *cloud* dengan membaca *log* pada *cloud*. Ketika lalu lintas yang masuk melanggar aturan, sistem keamanan akan bertindak secara otomatis dengan melakukan ban pada IP *address* yang melanggar aturan tersebut.

Mekanisme Fail2ban yang diterapkan dalam penelitian ini melibatkan penggunaan berbagai fitur dan konfigurasi untuk mendeteksi dan merespons terhadap serangan keamanan secara otomatis. Fail2ban dikonfigurasi untuk memantau jumlah percobaan gagal dari IP dalam rentang waktu tertentu. Ketika jumlah kegagalan ini melewati batas yang ditetapkan, Fail2ban akan langsung merespon, seperti memblokir IP tersebut secara otomatis.

Fail2ban menggunakan konfigurasi jail untuk mengelola aturan dan parameter perlindungan untuk sistem. Setelah

Fail2ban mendeteksi aktivitas yang mencurigakan, IP yang terdeteksi akan diblokir dalam jangka waktu yang telah ditentukan. Dengan menerapkan mekanisme ini, penelitian ini bertujuan untuk mengetahui efektivitas dan responsivitas Fail2ban dalam melindungi sistem keamanan pada lingkungan *cloud* dari berbagai serangan keamanan yang mungkin terjadi.

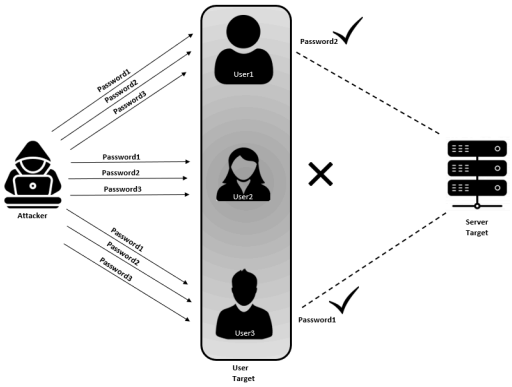
C. Teknik Pengujian



Gambar 3. Teknik Pengujian

Teknik pengujian yang digunakan dalam penelitian "Implementasi Fail2ban untuk melindungi sistem keamanan pada *Cloud*" dilakukan berbagai teknik pengujian untuk memastikan keefektifan alat tersebut dalam menghadapi ancaman keamanan. Teknik pengujian yang digunakan meliputi *Brute force*, dan serangan DDoS *(Distributed Denial of Service).*

Brute force testing dilakukan dengan mencoba berbagai kombinasi *username* dan *password* secara berulang kali untuk mendapatkan akses ke sistem. Metode yang digunakan untuk pengujian *brute force* adalah metode *Dictionary Attack.*



Gambar 4. *Brute force Dictionary Attack*

Brute force dengan metode *dictionary attack* dimulai dengan penyerang menyiapkan daftar *password* umum *(dictionary).* Metasploit kemudian mencoba setiap kata dari daftar *password* untuk dipasangkan dengan *username*. Proses ini terus berulang hingga ditemukan kombinasi yang cocok.

Dalam skenario ini, serangkaian percobaan *login* yang gagal dilakukan untuk menguji apakah Fail2ban dapat mendeteksi dan memblokir upaya *brute force* tersebut. Keberhasilan pengujian ini ditandai dengan blokir otomatis pada IP yang melakukan serangan setelah jumlah percobaan *login* yang gagal mencapai batas yang telah ditetapkan.

Pengujian DDoS melibatkan simulasi serangan yang bertujuan untuk membanjiri sistem dengan lalu lintas yang sangat tinggi, sehingga menyebabkan layanan menjadi tidak dapat digunakan. Metode yang digunakan untuk pengujian DDoS adalah metode SYN Flood.

Dengan melakukan *Brute force Testing,* dan *DDoS Testing*, penelitian ini dapat mengevaluasi sejauh mana Fail2bn dapat memberikan perlindungan terhadap berbagai jenis ancaman keamanan yang mungkin dihadapi oleh lingkungan *Cloud* dan local *server*. Pengujian serangan pada penelitian ini adalah *Brute force* dan *DDoS* dengan menggunakan *tools Metasploit* dan *SlowHttptest.*

III. HASIL DAN PEMBAHASAN

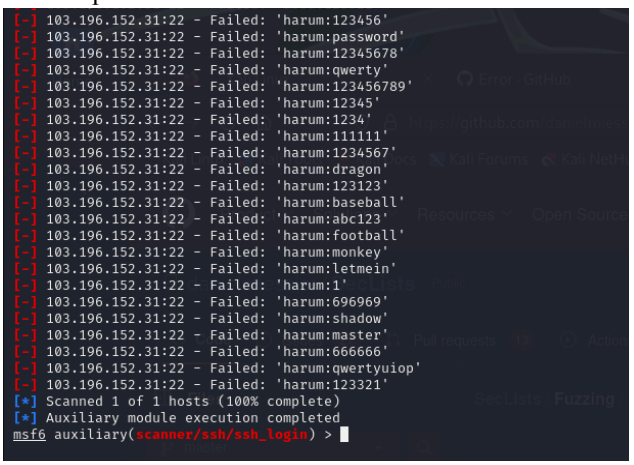
Setelah dilakukan implementasi fail2ban maka didapatkan hasil berupa tampilan *Interface* Putty dan Ubuntu *Server* dengan fail2ban yang aktif. Selanjutnya, dilakukan proses pengujian untuk mengetahui fail2ban mampu menghenttikan serangan *brute force* dan DdoS atau tidak.

A. Hasil Pengujian serangan Brute force

Pengujian serangan *Brute force* ke layanan SSH pada *Cloud* dan Ubuntu *Server* dengan melakukan dua kali pengujian, yaitu Pengujian serangan *Brute force* sebelum sistem terimplementasi Fail2ban dan Pengujian serangan *Brute force* setelah sistem terimplementasi Fail2ban.

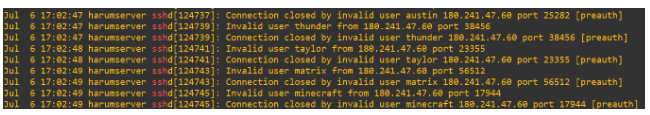
1) Hasil Pengujian serangan Brute force pada Cloud

Pengujian ini menggunakan *tools* Metasploit pada *software* pada kali *linux*. Pengujian *Brute force* menggunakan Metasploit dengan metode *dictionary attack*, metode ini memanfaatkan daftar *username* dan *password* yang telah dibuatkan pada txt.



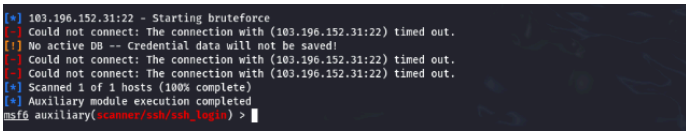
Gambar 5. Monitoring *Brute force* pada *Cloud* sebelum Fail2ban

Terlihat pada Gambar 5, Serangan *brute force* yang dilakukan oleh Metasploit dapat melakukan percobaan kombinasi kata sandi dan nama pengguna tanpa terhenti. *Brute force* berhasil dilakukan, namun Metasploit belum dapat menemukan nama pengguna dan kata sandi yang digunakan pada *cloud server.*.



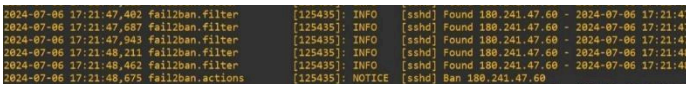
Gambar 6. auth.log pada *cloud*

Pada Gambar 6, Terlihat ada sebuah percobaan *login* yang dilakukan oleh *attacker* atau *client. Client* melakukan percobaan kombinasi nama pengguna dan kata sandi berkali-kali tanpa terhenti.



Gambar 7. *Brute force* pada *Cloud* setelah Fail2ban

Setelah *Cloud* di implementasikan fail2ban, *t*erlihat pada Gambar 7 bahwa *attacker* atau *client* tidak berhasil melakukan percobaan kombinasi nama pengguna dan kata sandi, dimana target otomatis memutuskan koneksi antara *user* dan *attacker*. Pemutusan ini dilakukan oleh fail2ban, dimana *attacker* hanya bisa melakukan percobaan *login* sebanyak 5 kali percobaan kemudian otomatis fail2ban akan memberhentikan adanya serangan *brute force.*

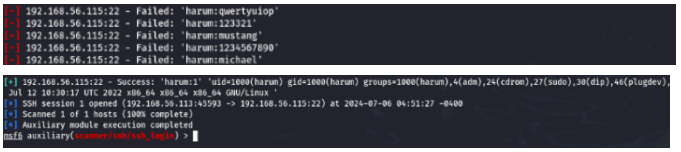


Gambar 8. fail2ban.log pada *cloud*

Pada Gambar 8, terlihat sebuah percobaan kombinasi nama pengguna dan kata sandi yang dilakukan oleh alamat IP 180.241.47.60 dimana alamat IP tersebut merupakan alamat IP *attacker* dan terlihat bahwa *attacker* melakukan percobaan kombinasi nama pengguna dan kata sandi sebanyak 5 kali yang dinyatakan gagal sebelum akhirnya terhentikan oleh fail2ban

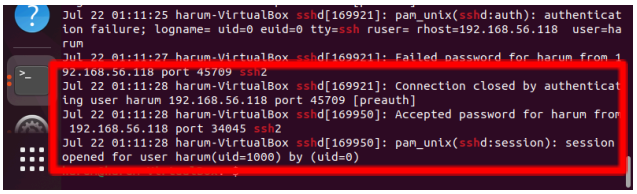
2) Hasil Pengujian serangan Brute force pada Ubuntu Server

Pada pengujian ini sama seperti sebelumnya, menggunakan *tools* Metasploit juga pada *software* pada kali linux. *Brute force* menggunakan Metasploit dengan metode *dictionary attack*, metode ini memanfaatkan daftar *password* yang telah dibuatkan pada txt.



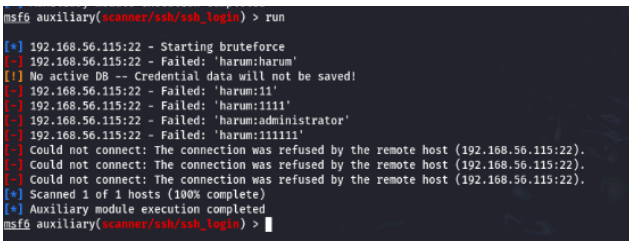
Gambar 9. Monitoring *Brute force* pada *Ubuntu* sebelum Fail2ban

Terlihat pada Gambar 9, Setelah beberapa kali gagal *login*, telihat **entri [+]192.168.56.115:22 -Success: 'harum:1'.** Baris ini menunjukan bahwa ada nama pengguna ***harum*** yang berhasil dengan kombinasi kata sandi ***1***. Kemudian Metasploit akan otomatis memberhentikan serangan saat kombinasi nama pengguna dan kata sandi berhasil didapatkan.



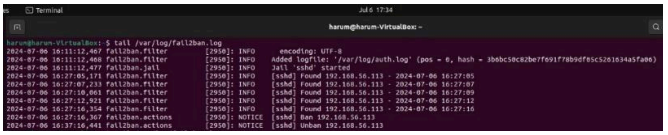
Gambar 10. auth.log pada Ubuntu *Server*

Pada Gambar 10, Terlihat ada sebuah percobaan *login* yang dilakukan oleh *attacker*. *Attacker* melakukan percobaan kombinasi nama pengguna dan kata sandi berkali-kali tanpa terhenti. Kemudian terlihat **Accepted *password* for harum from 192.168.56.118** yang menandakan bahwasanya *Attacker* berhasil mendapatkan *password* dari Ubuntu *Server*.



Gambar 11. Monitoring Brute force pada Ubuntu setelah Fail2ban

Terlihat pada Gambar 11, bahwa *attacker* atau *client* tidak berhasil melakukan percobaan kombinasi nama pengguna dan kata sandi, dimana target otomatis memutuskan koneksi antara *user* dan *attacker*. Pemutusan ini dilakukan oleh fail2ban, dimana *attacker* hanya bisa melakukan percobaan *login* sebanyak 5 kali percobaan kemudian otomatis fail2ban akan memberhentikan adanya serangan *brute force*.



Gambar 12. fail2ban.log pada Ubuntu *Server*

Pada Gambar 12 Terlihat sebuah percobaan kombinasi nama pengguna dan kata sandi yang dilakukan oleh alamat IP 192.168.56.113 dimana alamat IP tersebut merupakan alamat IP *attacker* dan terlihat bahwa *attacker* melakukan percobaan kombinasi nama pengguna dan kata sandi sebanyak 5 kali yang dinyatakan gagal sebelum akhirnya terhentikan oleh fail2ban.

B. Hasil Waktu Pengujian Deteksi Serangan Brute Force

TABEL II
WAKTU DETEKSI SERANGAN BRUTE FORCE PADA *CLOUD SERVER*

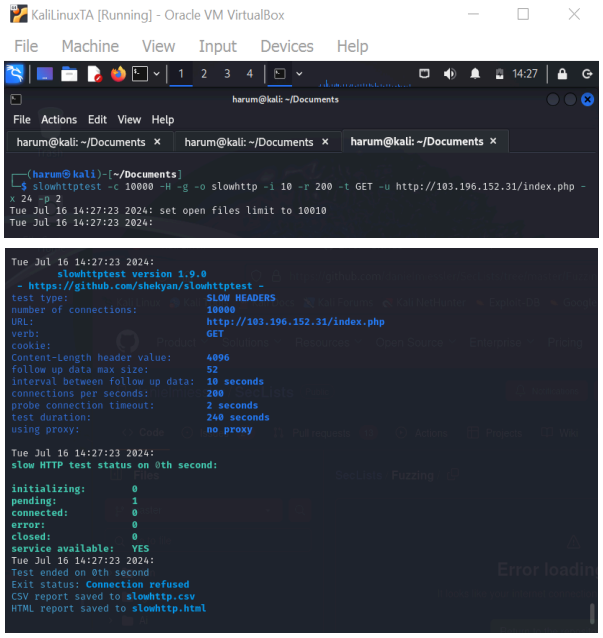
IP Sumber	IP Target	*Port*	Jail	Selisih waktu deteksi hingga ban (Detik)
180.241.47.60	103.192.168.31	22	sshd	0,3
180.241.47.60	103.192.168.31	22	sshd	0,2
180.241.47.60	103.192.168.31	22	sshd	0,7
180.241.47.60	103.192.168.31	22	sshd	1
180.241.47.60	103.192.168.31	22	sshd	0.2
180.241.47.60	103.192.168.31	22	sshd	0.2
Rata - rata				0,4

TABEL III
WAKTU DETEKSI SERANGAN BRUTE FORCE PADA UBUNTU *SERVER*

IP Sumber	IP Target	*Port*	Jail	Selisih waktu deteksi hingga ban (Detik)
192.168.56.113	192.168.56.115	22	sshd	2,0
192.168.56.113	192.168.56.115	22	sshd	2,8
192.168.56.113	192.168.56.115	22	sshd	2,9
192.168.56.113	192.168.56.115	22	sshd	3,4
192.168.56.113	192.168.56.115	22	sshd	0,3
192.168.56.113	192.168.56.115	22	sshd	0.0
	Rata - rata			1,9

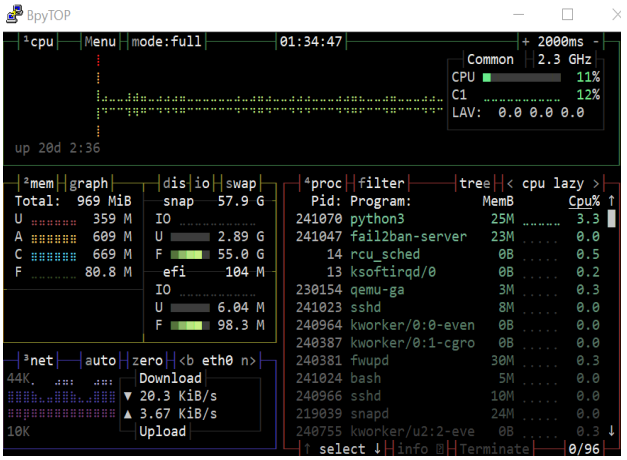
C. Hasil Pengujian serangan DDoS

1) Hasil Pengujian serangan DdoS pada Cloud



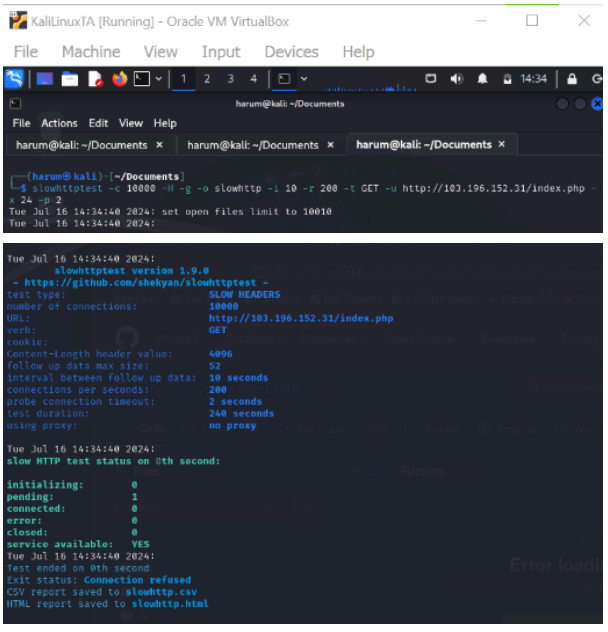
Gambar 13. Pengujian DDoS pada *Cloud* sebelum Fail2ban

Pada gambar 13 Terlihat bahwa *attacker* melakukan serangan DDoS menggunakan *tools slowhttptest.* Ada 10000 paket yang dikirim dengan durasi serangannya adalah 240 *seconds.* Namun *slowhttptest* tidak mampu membuat kinerja *server down*, ditandai dengan **Service available : YES** yang berarti *Server* tetap dapat berjalan dan tidak terganggu meskipun adanya serangan DDoS



Gambar 14. Monitoring kinerja server *cloud* sebelum fail2ban

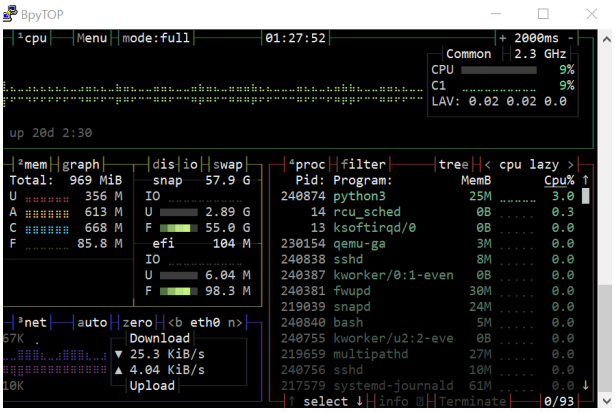
Kinerja *server* dapat dilihat pada monitoring BpyTOP seperti pada gambar 14, dari monitoring terlihat bahwa penggunaan kapasitas cpu *server* selama serangan DDOS adalah 11%. Jumlah penggunaan tersebut masih jauh dari 100% sehingga dapat dikatakan bahwa kinerja *server* seperti CPU, Memori dan Internet masih stabil saat serangan DDoS terjadi atau dengan kata lain serangan DDoS tidak mampu membuat kinerja *Cloud Server down.* Hal ini bisa terjadi karena layanan *cloud* yang digunakan telah memiliki pengamanan tersendiri untuk mencegahnya dari serangan DDoS.



Gambar 15. Pengujian DDoS pada *Cloud* setelah Fail2ban

Pada gambar 15, Setelah diimplementasikan Fail2ban pada *Cloud Server*, *attacker* melakukan serangan DDoS kembali menggunakan *tools* slowhttptest. Ada 10000 paket yang dikirim dengan durasi serangannya adalah 240 *seconds.* Namun *slowhttptest* tidak mampu membuat kinerja *server down*, ditandai dengan **Service available : YES** yang

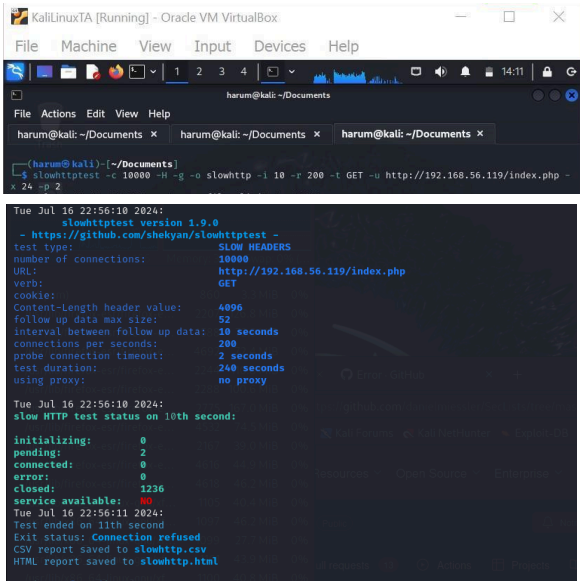
berarti *Server* tetap dapat berjalan dan tidak terganggu meskipun adanya serangan DDoS.



Gambar 16. Monitoring kinerja server *cloud server* setelah fail2ban

Terlihat pada gambar 16, bahwasanya kinerja *server* seperti CPU lebih rendah dibandingkan penggunaan CPU Ketika fail2ban belum diimplementasi. Ketika fail2ban belum diimplementasi menggunakan CPU adalah sebesar 11% namun saat setelah diimplementasi penggunaan CPU turun menjadi 9%. Hal ini berarti implementasi fail2ban dapat mengurangi dampak dari serangan DDoS walaupun efeknya minim karena *cloud* yang telah memiliki sistem keamanan tersendiri untuk mencegah serangan DDoS. Dari hasil tersebut dapat dikatakan bahwa implementasi fail2ban hanya memberikan sedikit pengaruh dan tidak terlalu efektif dalam mencegah DDoS.

2) Hasil Pengujian serangan DdoS pada Ubuntu Server

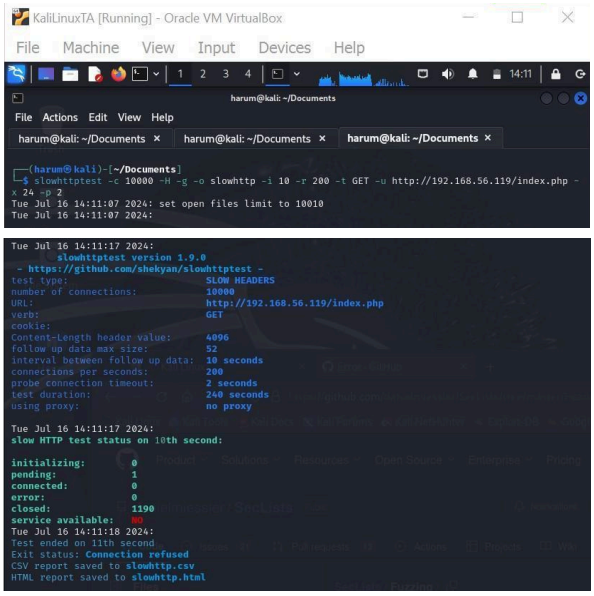


Gambar 17. Pengujian DDoS pada Ubuntu *server* sebelum Fail2ban

Pada gambar 17, A*ttacker* melakukan serangan DDoS menggunakan *tools slowhttptest.* Ada 10000 paket yang dikirim dengan durasi serangannya adalah 240 *seconds.* Terlihat *slowhttptest* mampu membuat kinerja *server down*, ditandai dengan **Service available : NO** yang berarti *Server* terganggu kinerjanya dengan adanya serangan DDoS.

Gambar 18. Monitoring kinerja Ubuntu *server* sebelum fail2ban

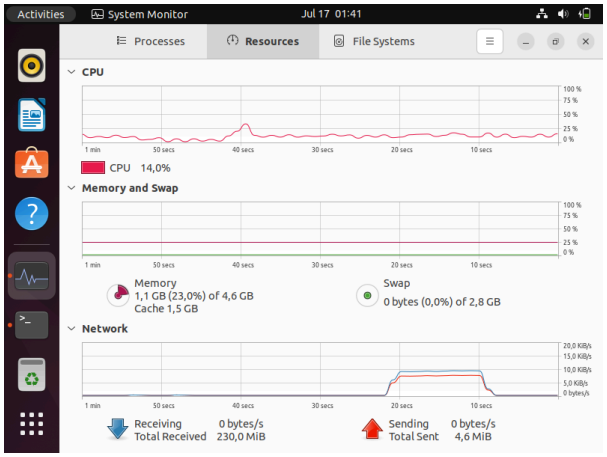
Kinerja *server* dapat dilihat pada monitoring *System Monitor* seperti pada gambar 18, dari monitoring terlihat bahwa penggunaan kapasitas cpu *server* selama serangan DDOS adalah 100%. Jumlah penggunaan tersebut mencapai hasil maksimal sehingga dapat dikatakan bahwa kinerja *server* seperti CPU, Memori dan Internet *down* saat serangan DDoS terjadi. Serangan DDoS mampu membuat kinerja *Ubuntu Server down.*



Gambar 19. Pengujian DDoS pada Ubuntu *server* setelah Fail2ban

Pada gambar 19, setelah diimplementasikan Fail2ban pada *Ubuntu Server, attacker* melakukan serangan DDoS kembali menggunakan *tools slowhttptest.* Ada 10000 paket yang dikirim dengan durasi serangannya adalah 240 *seconds.* Terlihat *slowhttptest* mampu membuat kinerja *server down*, ditandai dengan **Service available : NO** yang berarti *Server* terganggu kinerjanya dengan adanya serangan DDoS. Terlihat meskipun sudah diimplementasikan Fail2ban, Fail2ban tidak

dapat menghentikan adanya serangan DDoS pada *Ubuntu Server*.



Gambar 20. Monitoring kinerja Ubuntu *Server* setelah fail2ban

IV. KESIMPULAN

Setelah melakukan pengujian dan analisis pada penelitian ini disimpulkan bahwa hasil pengujian yang dilakukan dengan menggunakan Serangan *brute force*, Fail2ban mampu memblokir adanya percobaan login pada SSH *Cloud* dan Ubuntu *Server* dengan maksimal percobaan *login* sebanyak 5 kali sampai akhirnya diberhentikan oleh Fail2ban dengan Rata-rata waktu yang diperlukan Fail2ban untuk memblokir adanya serangan *brute force* pada *Cloud* adalah 0,4 detik. Sedangkan pada Ubuntu *Server*, rata-rata waktu yang diperlukan fail2ban untuk memblokir adanya serangan *brute force* adalah 1,9 detik.

Hasil pengujian serangan DDoS dengan 10000 paket setelah diimplementasikan fail2ban didapatkan hasil kinerja Ubuntu *Server* bahwa Fail2ban dapat mengurangi dampak serangan DDoS, CPU Ubuntu *Server* yang mulanya 100% turun menjadi 25%. Namun pada *Cloud Server*, telah memiliki layanan anti DDoS sendiri. Dari seluruh hasil pengujian yang dilakukan dan dengan hasil monitoring dapat disimpulkan bahwa fail2ban berhasil menghentikan adanya serangan *brute force* namun pada serangan DDoS, fail2ban tidak dapat menghentikan serangan tersebut seperti pada serangan *brute force*.

Terlihat pada gambar 20 bahwasanya kinerja *server* seperti CPU lebih rendah dibandingkan penggunaan CPU Ketika fail2ban belum diimplementasi. Ketika fail2ban belum diimplementasi menggunakan CPU adalah sebesar 100% namun saat setelah diimplementasi penggunaan CPU turun menjadi 25%. Hal ini berarti implementasi fail2ban dapat mengurangi dampak dari serangan DDoS walaupun efeknya minim. Dari hasil tersebut dapat dikatakan bahwa implementasi fail2ban hanya memberikan sedikit pengaruh dan tidak terlalu efektif dalam mencegah DDoS.

REFERENSI

[1] S. och D. Irawan, ”Perbandingan Intrusion Prevention System (IPS) pada Linux Ubuntu dan Linux Centos,” *Jurnal Teknologi Informasi Mura,* vol. Vol.12, nr No 02, 2020.

[2] Pratita och H. Sidiq, ”Analisa Brute Force Attack Menggunakan Scanning Aplikasi pada HTTP Attack,” Februari 2016. [Online]. Available: http://repository.uksw.edu/handle/123456789/11304.

[3] S. Khadafi, B. D. Melani och S. Arifin, ”Sistem Keamanan Open Cloud Computing Menggunakan Ids (Intrusion Detection System) Dan Ips (Intrusion Prevention System),” *Jurnal IPTEK,* vol. Vol 21, nr No 2, 2017.

[4] U. A. Ata, ”FIKES,” 24 Maret 2023. [Online]. Available: https://fikes.almaata.ac.id/23-jenis-serangan-cybersecurity/. [Använd 6 Desember 2023].

[5] M. Siahaan, ”Mencegah Serangan DDoS (Distributed Denial of Service)Terhadap Email Server,” *SCIENCE TECH: Jurnal Ilmu Pengetahuan dan Teknologi,* vol. Vol 7, nr No 2, pp. hal 13-21, 2021.

[6] P. Winarianto och D. E. Daud, ”CIA TRIAD,” 2022. [Online]. Available: https://student-activity.binus.ac.id/csc/2022/08/cia-triad/.

[7] Sayfnidawaty, ”Cloud Computing,” 2020. [Online]. Available: https://raharja.ac.id/2020/11/27/cloud-computing/.

[8] A. Andriani, ”Pemanfaatan Cloud Computing dalam pengembangan bisnis,” vol. Vol.1, nr No.1, 2013.

[9] M. N. A. Rizqi och K. D. Nuryana, ”Analisis Perbandingan Kinerja Algoritma Weighted Round Robin dan Weighted Least Connection Menggunakan Load Balancing Nginx Pada Virtual Private Server(VPS),” *JINACS,* vol. Vol 4, nr No 1, 2022.

[10] S. D. Risqiawati och E. A. Irawan, ”Realtime Pencegahan Serangan Brute Force dan DDOS Pada Ubuntu Server,” *Techno.COM,* vol. Vol 17, nr No 4, pp. Hal 347-354, 2018.

[11] U. H. Kunia, ”Rumahweb,” 4 Mei 2023. [Online]. Available: https://www.rumahweb.com/journal/putty-adalah/. [Använd 13 Juni 2024].

[12] M. Rifki, ”Brute Force Attack,” 13 Januari 2024. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/brute-force-attack.

[13] Microsoft Security, ”Apa itu serangan DDoS?,” 2020. [Online]. Available: https://www.microsoft.com/id-id/security/business/security-101/what-is-a-ddos-attack.