INFOTECH journal
ISSN : 2460-1861 (Print), 2615-4250 (Online)
Vol. 10 No. 1, pp. 64-73

ANALISIS KEAMANAN JARINGAN SERVER TERHADAP SERANGAN DICTIONARY MENGGUNAKAN TOOLS FAIL2BAN DENGAN NOTIFIKASI TELEGRAM

Arthur Dida Batistuta[1], Ade Hendri Hendrawan[2], Ritzkal[3]
Teknik Informatika, Fakultas Teknik dan Sains, Universitas Ibn Khaldun Bogor
Jl. KH Sholeh Iskandar Km 2 Kota Bogor
Email: didabatistuta08@gmail.com

ABSTRACT
DOS (Denial of Service) attacks aim to deplete server resources to the point where the server is unable to perform its function as a provider of access to its services, such as flooding the server with a variety of password combinations to discover the true password for the targeted company's servers. Based on this information, the researchers recommend that the fail2ban program be evaluated. This program will operate on a server that will monitor for unusual outside activity before blocking the originating IP address. This study attempts to protect the server from malicious intruders by applying the fail2ban program and the basic approach of scanning and blocking the attacker's IP address.

Keywords: Denial of Service, Linux Server Security, Intrusion Detection System.

ABSTRAK

Serangan DOS (Denial of Service) bertujuan untuk menguras sumber daya server hingga server tidak mampu menjalankan fungsinya sebagai penyedia akses layanannya, seperti membanjiri server dengan berbagai kombinasi password untuk mengetahui password sebenarnya untuk server perusahaan yang ditargetkan. Berdasarkan informasi tersebut, peneliti merekomendasikan agar program fail2ban dievaluasi. Program ini akan beroperasi pada server yang akan memantau aktivitas luar yang tidak biasa sebelum memblokir alamat IP asal. Penelitian ini mencoba melindungi server dari penyusup jahat dengan menerapkan program fail2ban dan pendekatan dasar memindai dan memblokir alamat IP penyerang.

Kata kunci : *Penolakan Layanan, Keamanan Server Linux, Sistem Deteksi Intrusi.*

Riwayat Artikel :

Tanggal diterima : 11-02-2024

Tanggal revisi : 24-02-2024

Tanggal terbit : 26-02-2024

DOI :

https://doi.org/10.31949/infotech.v10i1.8730

INFOTECH journal by Informatika UNMA is licensed under CC BY-SA 4.0

Copyright © 2024 By Author

1. PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi yang pesat tentu akan membawa dampak pada seluruh aspek kehidupan. Di sisi positifnya, hal ini mendorong pertukaran dan akumulasi informasi, namun di sisi negatifnya, hal ini harus dihindari [1]. Jaringan yang terhubung ke internet perlu ekstra hati-hati karena lebih rentan terhadap aktivitas terlarang oleh pihak-pihak yang tidak waspada [17].

Seorang administrator mungkin tidak menyadari atau tidak dapat memprediksi kemungkinan serangan, pencurian data, dan kehilangan data pada jaringan. Jika data penting perusahaan dicuri atau dirusak, reputasi bisnis pasti terancam karena konsumen dan klien mungkin kehilangan kepercayaan terhadap perusahaan. pada bisnis dan memiliki kekhawatiran tentang keamanan data mereka [2]. Dengan pemindaian menyeluruh dan pemblokiran alamat IP, penelitian ini berupaya mempertahankan server dari serangan pihak luar yang tidak bertanggung jawab dalam memanfaatkan perangkat aplikasi.

Sistem operasi, yaitu sekelompok program komputer, terletak di antara perangkat lunak aplikasi dan perangkat keras [27]. Sistem operasi Linux biasanya digunakan pada server bisnis. Hal ini disebabkan oleh sifat Linux yang bebas atau open source dan kemampuannya untuk berjalan pada berbagai platform perangkat keras, termasuk Intel [28].

Ancaman serangan biasanya merupakan hasil dari perilaku yang disengaja, yang dimulai dengan melakukan sesuatu yang tidak diinginkan dan akhirnya mengarah pada suatu kejadian yang dapat merugikan orang lain [11]. Serangan denial-of-service (DOS) adalah serangan yang membombardir target dengan banyak data dengan tujuan menurunkan kinerja target. Serangan kamus adalah contoh serangan DOS [14]. Serangan kamus bekerja dengan mengeksploitasi penggunaan istilah-istilah pendek dan terkenal dari kamus oleh pengguna sebagai semacam kata sandi. Serangan ini akan mencoba semua kombinasi kata menggunakan teknik hashing kata demi kata dan menebak mana yang benar [3]. Perangkat lunak cracking login dan pengujian penetrasi open source yang disebut Hydra mendukung protokol serangan numeros. Pakar keamanan bisa mendapatkan akses ilegal ke jaringan jarak jauh menggunakan teknologi ini. Alat ini cepat dan mudah beradaptasi. tersedia dalam bentuk grafis atau berbasis perintah [9].

Jika Anda ingin mengurangi kemungkinan terjadinya peristiwa apa pun di jaringan komputer saat terhubung ke internet, ada banyak arsitektur yang dapat meningkatkan keamanan jaringan secara signifikan untuk memerangi serangan kamus [4]. Menurut Vijayarani, sangat penting untuk mengawasi aktivitas jaringan dan mengidentifikasi perintah sistem [29]. Dan salah satu teknik untuk menjaga jaringan adalah dengan menggunakan perangkat lunak dari sistem deteksi intrusi (IDS) [10].

Odon (2005: 565) mengutip Arus lalu lintas jaringan dapat diperiksa untuk paket data yang berpotensi membahayakan menggunakan perangkat yang disebut Instrument Detection System (IDS), yang kemudian dapat menghasilkan laporan aktivitas jaringan [30]. Selain berfungsi sebagai pengawas dan mengeluarkan peringatan ketika aktivitas yang tidak biasa terjadi, IDS dapat merespons secara bebas dalam menanggapi serangan pada sistem jaringan dan server [22]. Untuk keamanan total, sistem deteksi intrusi diperlukan [25].

Firewall dan sistem deteksi intrusi (IDS), dua komponen penting dari keamanan jaringan, dapat melindungi server dan jaringan internal dan menggagalkan intrusi [5]. Namun, aplikasi IDS tidak diragukan lagi memiliki kelebihan dan kekurangan [18].

Salah satu perangkat lunak IDS, Fail2ban, akan digunakan dalam penyelidikan ini. Sekelompok perangkat lunak yang disebut Fail2ban dapat mengenali upaya login yang gagal dan kemudian memblokir alamat IP sumber serangan [6]. Fail2ban saat ini tersedia di hampir setiap repositori distribusi [13].

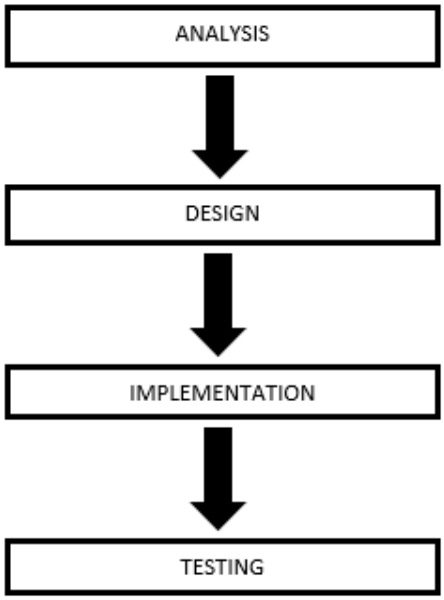
Secara desain, fail2ban hanya dapat digunakan pada satu server dan tidak dapat bergabung dengan jaringan server [16].

Sebuah aplikasi berbasis cloud bernama Telegram dapat memudahkan admin untuk mengambil informasi yang diberikan oleh server dari perangkat yang berbeda dengan mentransfer hasil dari seluruh aktivitas keamanan server yang dilakukan kepada admin dalam bentuk data teks [12].

Berdasarkan permasalahan yang ada yaitu mudahnya alat Hydra digunakan untuk memecahkan password suatu server sehingga mengakibatkan resiko data-data penting tercuri, akhirnya peneliti ingin mencari solusi server yang dapat melindungi data-data penting di suatu server. server dengan alat fail2ban yang akan bertindak sebagai pelindung. server dari serangan kamus eksperimental [7]. Tujuan dari penelitian ini adalah untuk membatasi kemungkinan serangan mencapai server dengan memanfaatkan alat IDS fail2ban untuk memindai port yang mungkin digunakan untuk melancarkan serangan, mencuri data, atau menghancurkan data oleh oknum yang tidak bertanggung jawab [16].

2. METODOLOGI PENELITIAN

Pendekatan studi yang biasa diterapkan, seperti dapat dilihat di bawah.



Gambar 1. Metode penelitian

3.1 Analisis(*Analysis*)

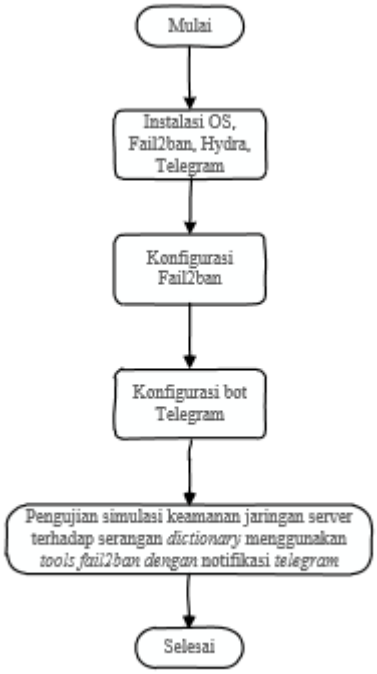
Kemampuan untuk memecah masalah atau informasi yang kompleks menjadi bagian-bagian kecil yang dapat dikelola untuk meningkatkan pemahaman dikenal sebagai analisis [19]. Peneliti mengkaji peralatan dan perlengkapan yang dibutuhkan untuk penelitian serta kebutuhan aplikasi IDS untuk menjaga server dari upaya pencurian dan penghancuran data oleh pihak yang ceroboh dengan menggunakan langkah-langkah keamanan seperti memindai dan memblokir alamat IP penyerang. keseluruhan.

3.2 Desain(Design)

Meliputi topologi jaringan dan arsitektur infrastruktur sebagai gambaran lingkungan jaringan penelitian sebenarnya [20]. Topologi jaringan menurut Aldo dalam bukunya Pengantar Teknologi Informasi adalah suatu metode menghubungkan beberapa komputer, baik dengan kabel maupun tanpa kabel [23].

3.3 Penerapan(Implementation)

Seluruh prosedur yang telah dibuat, termasuk perancangan perangkat lunak dan perangkat keras, proses pengaturan alamat IP, dan konfigurasi aplikasi yang akan digunakan dalam penelitian ini, akan digunakan dalam tahap aplikasi ini [26].



Gambar2. Alur Pembuatan Sistem.

1. Pengaturan Sistem Operasi

   Sistem operasi untuk proses penelitian dipasang oleh peneliti. Sistem operasi Linux Ubuntu versi 20.04.3 digunakan oleh para peneliti dalam penelitian ini. Tahapan instalasi sistem operasi Linux Ubuntu adalah sebagai berikut:

   a. Buat instalasi Ubuntu Linux yang dapat di-boot.
   b. Masuk ke mode bios, lalu konfigurasikan komputer untuk booting dari perangkat instalasi (DVD/Flash Disk).
   c. Simpan perubahan dan restart komputer/laptop Anda.
   d. Mulailah instalasi dengan memilih bahasa lalu klik install ubuntu.
   e. Di area tata letak Keyboard, keluar saja dari opsi dan klik Lanjutkan.
   f. Pilih Instalasi Normal dari kotak Pembaruan dan perangkat lunak lainnya, lalu klik Lanjutkan.
   g. Ada dua jenis instalasi yang dapat dipilih di bagian Jenis instalasi. Namun peneliti menyarankan untuk memilih Erase drive dan menginstal Ubuntu, lalu klik Lanjutkan.
   h. Isikan lokasi pada area Where are you. Dalam penyelidikan ini, peneliti memilih Jakarta dan kemudian mengklik Lanjutkan.
   i. Di area Siapa Anda, masukkan informasi yang diperlukan lalu klik Lanjutkan.
   j. Tunggu beberapa detik hingga instalasi selesai.

2. Instalasi Fail2ban

   Program Fail2ban digunakan dalam penelitian ini untuk mendeteksi adanya aktivitas mencurigakan yang berpotensi membahayakan keamanan server Linux. Tahapan instalasi Fail2ban adalah sebagai berikut:

   a. Luncurkan terminal di Ubuntu.
   b. Sebelum melakukan instalasi, lakukan update sistem untuk memastikan tidak ada kesulitan pada saat instalasi.
   c. Untuk menjalankan pembaruan sistem, gunakan perintah "sudo apt update && sudo apt upgrade -y".
   d. Jalankan perintah "sudo apt-get install fail2ban -y" untuk menginstal utilitas Fail2ban.

3. Pemasangan Hidra

   Penelitian ini menggunakan alat Hydra untuk melakukan serangan bruteforce. Prosedur pemasangan Hydra dibagi menjadi beberapa tahapan sebagai berikut:

   a. Jalankan instalasi git.
   b. Selanjutnya, gunakan git clone untuk mengambil kode sumber Hydra dari GitHub.
   c. Terakhir, gunakan perintah "sudo apt-get install hydra" untuk menginstal Hydra.
   d. Tunggu hingga instalasi selesai.

4. Pengaturan Telegram

   Penelitian ini menggunakan aplikasi Telegram untuk menampilkan notifikasi aktivitas serangan yang diterima fail2ban. Tahapan proses instalasi Telegram adalah sebagai berikut:

   a. pertama buka https://desktop.telegram.org/, dan unduh filenya.
   b. Setelah pengunduhan selesai, cari file tersebut dan klik kanan untuk mengekstraknya.
   c. Pindahkan folder ke /opt dan jalankan aplikasi dari /opt/telegram/telegram.

5. Konfigurasi fail2ban dan Telegram

   a. Cari bagian [DEFAULT] di file jail.local dan letakkan aturan di sana.

   "[DEFAULT]
   enabled = false
   ignoreip = 127.0.0.1/8
   ignorecommand =
   bantime = 3600
   findtime = 120
   maxretry = 3
   "

   Nilai bantime menunjukkan berapa lama penyerang akan diblokir melalui fail2ban. maxretry menunjukkan jumlah maksimum upaya serangan gagal yang diizinkan. enabled = false Ini adalah layanan default fail2ban, dan sebaiknya tidak mengubahnya. findtime menampilkan batas waktu upaya serangan yang gagal sebelum dilarang.

   b. Buka aplikasi Telegram dan cari akun botfather; akun ini digunakan untuk membuat bot yang nantinya akan terhubung ke server Linux.
   c. Untuk membuat bot baru, jalankan perintah /newbot diikuti dengan nama bot, yang selanjutnya akan digunakan untuk menerima notifikasi serangan yang masuk dari server Linux. Peneliti disini menggunakan nama akun bot notifcheck.
   d. Jika nama Anda diterima, Anda akan menerima apiToken dan chatID untuk dimasukkan ke dalam file fail2ban-telegram.sh.
   e. Pada file fail2ban-telegram.sh cari baris notifikasi #send, lalu masukkan apiToken dan chatId yang diperoleh dari bot telegram.

6. Simulasi serangan kamus akan berlangsung dalam langkah-langkah berikut:

   a. Aktifkan fail2ban di server.
   b. Buat file berisi kombinasi kata acak yang akan dikirimkan ke server.
   c. Mensimulasikan serangan dengan mendistribusikan file yang dibuat ke server menggunakan alat Hydra.
   d. Fail2ban memindai aktivitas mencurigakan yang mencoba menjangkau server.
   e. Fail2ban melarang alamat IP penyerang.
   f. Fail2ban mengirimkan peringatan serangan masuk ke administrator melalui Telegram.

3.4 Pengujian(Testing)

Untuk mendapatkan temuan yang dapat meningkatkan sistem keamanan server, maka dilakukan pengujian pada penelitian ini sesuai dengan parameter pengujian [21].

3. HASIL DAN PEMBAHASAN

Mengacu pada hasil dari semua fase sebelumnya yang telah diselesaikan. Hasil pengujian akan mencakup peringatan serangan pada aplikasi Telegram serta apakah server berhasil mendeteksi dan memblokir IP yang terkait dengan sumber serangan. Temuan penelitian ini menghasilkan keluaran sebagai berikut.

4.1 Analisis

Studi Keamanan Jaringan Server Linux Terhadap Serangan Kamus Menggunakan Alat Fail2ban Dengan Notifikasi Telegram sekarang akan menjalani analisis persyaratan.

Jika memungkinkan, penelitian ini akan membahas isu-isu terkini. Seperti terlihat pada Tabel 1 dan 2, tahap analisis kebutuhan memerlukan alat

pendukung untuk mempelajari permasalahan yang perlu dianalisis:

Tabel 1. Perangkat keras

NO	Perangkat Keras	Fungsi
1.	Laptop	Untuk mempraktikkan proses sistem dan menjalankan pengujian untuk penelitian ini

Tabel 2. Perangkat lunak

NO	Perangkat Lunak	Fungsi
1.	Desktop Linux Ubuntu 20.04.3	Program yang digunakan untuk menjalankan server Linux pada penelitian ini
2.	UbuntuLinux 16.04.6	Sistem operasi yang digunakan dalam penyelidikan ini adalah musuh
3.	File2ban	Alat untuk memantau dan mempertahankan server dari serangan kekerasan
4.	Hydra	Sebuah alat yang pada akhirnya akan membuat server terkena serangan brute force
5.	Telegram	Sebagai perangkat lunak yang akan menerima notifikasi dari server melalui fail2ban

Peneliti akan memeriksa peralatan dan perlengkapan yang diperlukan sebelum mendiskusikan mengapa barang-barang tersebut diperlukan untuk penelitian khusus ini.:

a. Perangkat keras
   1. Laptop
      Laptop diperlukan sebagai alat untuk membuat server dan untuk mensimulasikan serangan..

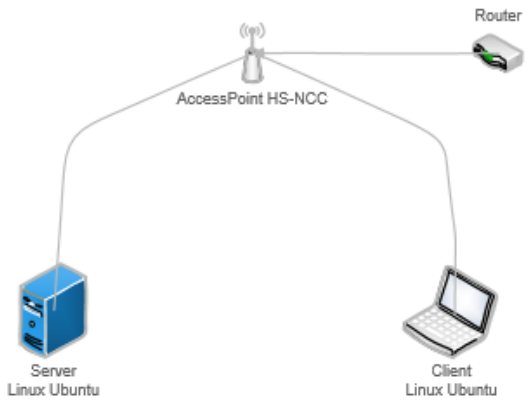
b. Perangkat lunak
   1. Linux
      Linux diperlukan sebagai sistem operasi yang ideal untuk server dan untuk melakukan simulasi serangan secara bersamaan karena dapat mengolah data lebih efektif dibandingkan Windows. Selain itu, Linux dirancang sebagai sistem operasi multi-pengguna, sehingga aman dari virus dan malware serta hanya mengizinkan pengguna dengan akses "root" yang dapat mengakses kernel. Selain itu, Linux adalah sistem operasi sumber terbuka dan gratis.
   2. File2ban
      Peneliti menggunakan program IDS Fail2ban karena membatasi jumlah percobaan dan mencegah akses tidak sah ke server adalah solusi tercepat dan tersukses untuk serangan kamus.
   3. Hydra
      Salah satu alat terbaik untuk melakukan serangan kamus menggunakan kombinasi kata adalah Hydra..
   4. Telegram
      Karena berisi kode API telegram untuk berkomunikasi, Telegram digunakan sebagai aplikasi yang akan mendapatkan informasi dari server tentang ancaman yang akan datang.

4.2 Desain

Suatu metode untuk mempersiapkan lingkungan penelitian untuk mengumpulkan data yang sesuai dengan persyaratan dan kegiatan tahap analisis disebut sebagai tahap desain. Tata letak perancangan menyajikan gambaran perencanaan rangkaian dan komponen-komponen yang dibutuhkan untuk mencapai hasil kerja yang diinginkan.

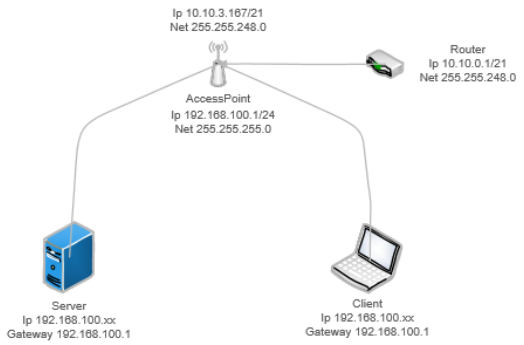
Desain topologi fisik, desain logika, dan desain strategi serangan dimaksudkan untuk diberikan pada tahap desain ini. Hal ini ditunjukkan sebagai berikut:

a. Desain Topologi Fisik
   Peralatan yang digunakan dalam penelitian ini direpresentasikan di bawah ini berupa router, laptop client, server, dan access point.



Gambar3. Desain Topologi Fisik

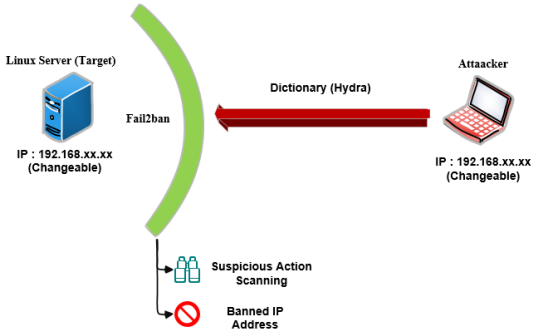
b. Desain Topologi Jaringan
   Setiap perangkat yang terhubung memiliki alamat IP unik. Alamat IP Kelas C digunakan dari Accesspoint ke server Linux dan penyerang, berbeda dengan alamat IP kelas A dari jalur FT Router ke Accesspoint. Perbedaan ini disebabkan oleh penggunaan IP pribadi dalam penelitian, yang memungkinkannya membangun jaringan baru menggunakan IP kelas C.



Gambar4. Desain Topologi Jaringan

c. Desain Skema Serangan

Strategi penyerangan yang digunakan dalam penyelidikan ini digambarkan dalam gambar. Sedangkan server di alamat IP 192.168.10.xx akan memperkirakan upaya serangan masuk menggunakan alat fail2ban, dan penyerang di alamat IP 192.168.100.xx akan menggunakan alat hydra untuk melakukan serangan kamus.



Gambar5. Desain Skema Serangan.

4.3 Penerapan

Kelanjutan dari tahap analisis dan desain adalah tahap implementasi. Langkah ini dibagi menjadi beberapa bagian sebagai berikut:

a. Di bawah direktori /etc/fail2ban. Selanjutnya, cari file jail.conf, yang merupakan file default fail2ban, di dalam direktori. Salin lalu ke file jail.local baru. ubah file jail.local setelah itu. Menyalin memastikan bahwa file asli jail.conf tidak diubah dan memfasilitasi pembaruan.

```
root@server-VirtualBox:/home/server# cd /etc/fail2ban/
root@server-VirtualBox:/etc/fail2ban# ls
action.d                        jail.conf.save     jail.local.save.3
fail2ban.conf                   jail.d             paths-arch.conf
fail2ban.d                      jail.local         paths-common.conf
fail2ban-telegram-notification  jail.local.save    paths-debian.conf
filter.d                        jail.local.save.1  paths-opensuse.conf
jail.conf                       jail.local.save.2  scripts
root@server-VirtualBox:/etc/fail2ban# nano jail.local
```

Gambar6. Lokasi file jail.local

b. Selanjutnya, cari bagian [DEFAULT] di file jail.local dan tambahkan panduan di bawahnya.

```
[DEFAULT]
#enabled = true
#ignoreip = 127.0.0.1
#ignorecommand =
#backend = systemd
#mode = normal
#filter = %(__name__)s[mode=%(mode)s]
#findtime = 600
```

Gambar7. Aturan Awal Default.

```
[DEFAULT]
enabled = false
ignoreip = 127.0.0.1/8
ignorecommand =
bantime = 3600
findtime = 120
maxretry = 3
```

Gambar8. Menambahkan Aturan Default

c. Kemudian, temukan bagian [sshd] dan masukkan aturan berikut di sana untuk mengamankan layanan ssh sebelum menyimpannya.

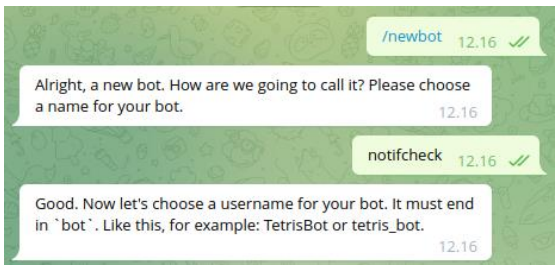
```
[sshd]

# To use more aggressive sshd modes set filter parameter "mode" in jail.local:
# normal (default), ddos, extra or aggressive (combines all).
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and de>
#mode   = normal
#port    = ssh
#logpath = %(sshd_log)s
#backend = %(sshd_backend)s
```

Gambar9. Aturan Awal SSHD

```
[sshd]

# To use more aggressive sshd modes set filter parameter "mode" in jail.local:
# normal (default), ddos, extra or aggressive (combines all).
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and de>
#mode   = normal
enabled  = true
port     = ssh
filter   = sshd
maxretry = 3
logpath  = /var/log/auth.log
action   = iptables[name=SSH, PORT=22, protocol=tcp]
           telegram
backend  = %(sshd_backend)s
```

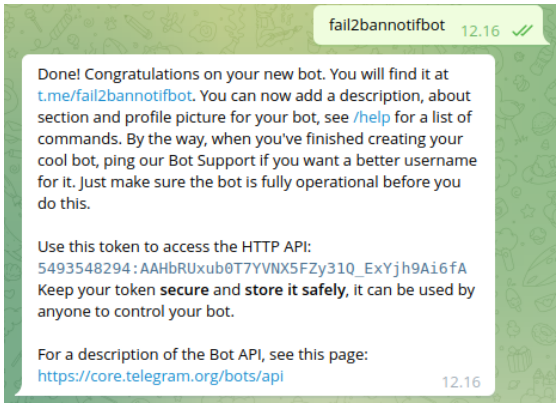
Gambar10. Menambahkan Aturan SSHD

d. Dapatkan akun botfather dengan membuka aplikasi Telegram lalu mencarinya. Akun ini digunakan untuk membangun bot yang nantinya akan dihubungkan ke server Linux. Saat menggunakan perintah /newbot untuk membuat bot baru, berikan nama bot yang akan digunakan untuk menerima peringatan tentang serangan masuk dari server Linux. Peneliti dalam hal ini login ke bot notifcheck.



Gambar11. Membuat Bot Telegram

e. Anda akan menerima apiToken dan chatID untuk ditambahkan ke file fail2ban-telegram.sh jika nama tersebut diotorisasi.



Gambar12. apitokens dan chatid

f. Selanjutnya masuk ke direktori fail2ban-telegram-notification, lalu cari bagian #send notifikasi di file fail2ban-telegram.sh. Area ini harus diisi dengan chatId dan apiToken yang berhasil dibuat.

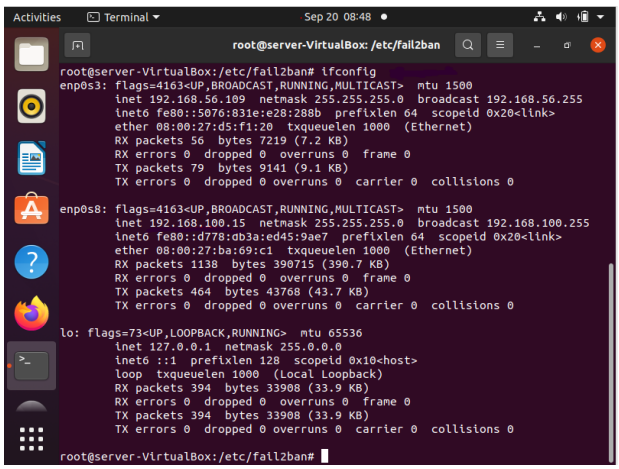
```
# Send notification
function send_msg {
  apiToken=5493548294:AAHbRUxub0T7YVNX5FZy31Q_ExYjh9Ai6fA
  chatId=1102934119
  url="https://api.telegram.org/bot$apiToken/sendMessage"

  curl -s -X POST $url -d chat_id=$chatId -d text="$1"
  exit
}
```

Gambar13. Lengkapi bidang Apitoken dan chatid

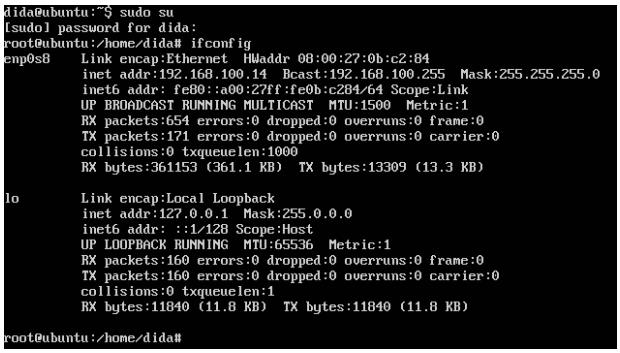
4.4 Pengujian

Pada titik ini, gunakan alat Hydra untuk mereplikasi pengujian serangan Kamus di server Linux.

a. Memeriksa alamat ip server dan penyerang.



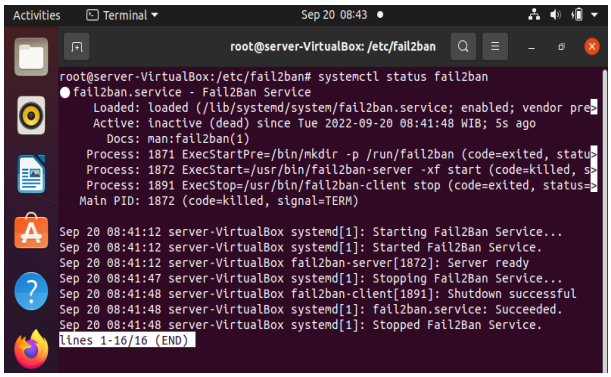
Gambar14. Periksa IP Server



Gambar15. Periksa IP Penyerang

Hal ini dilakukan agar penyerang dapat mengidentifikasi korban yang dituju.

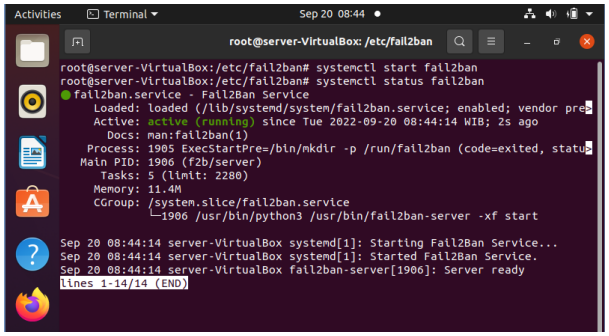
b. Kondisi penjaga server, utilitas fail2ban. Dan sesuai penjelasan Gambar 16, status fail2ban masih inaktif.



Gambar16. Periksa Status Fail2ban

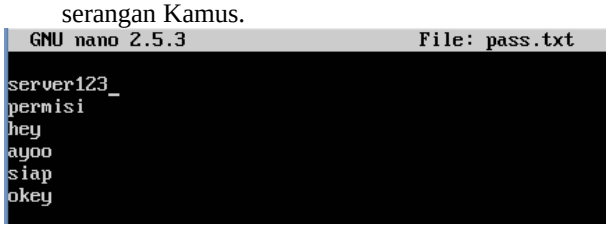
Kondisi ini memperjelas bahwa server tidak terlindung oleh program IDS jika fail2ban tidak berjalan.

c. Gambar 17 menggambarkan layar setelah aktivasi fail2ban berhasil.



Gambar17. Periksa Status Fail2ban

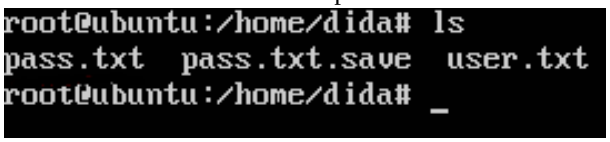
d. Kombinasi kata sandi acak yang telah disiapkan penyerang untuk meluncurkan serangan Kamus.



Gambar18. Kombinasi Kata Sandi

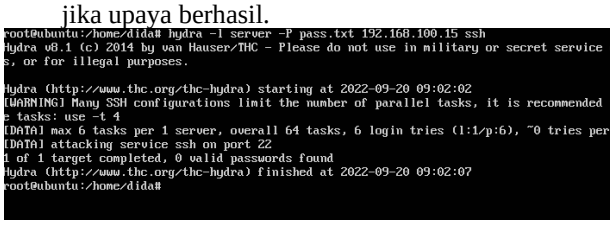
Dokumen ini mencakup berbagai jenis kata sandi umum yang digunakan orang.

e. File tersebut diberi nama pass.txt.



Gambar19. Lokasi file pass.txt

f. Untuk mendapatkan password server yang sebenarnya, penyerang melancarkan serangan dengan membanjirinya dengan berbagai frase yang telah disiapkan ke dalam satu file. kalimat "kata sandi berhasil diperoleh" akan muncul jika upaya berhasil.

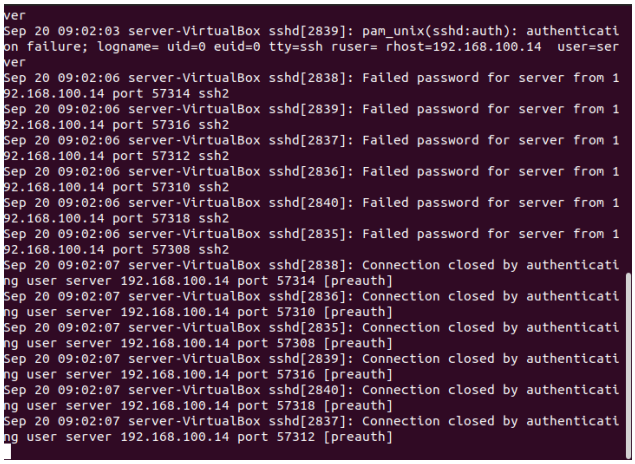


Gambar20. File Serangan Spam

g. Kemudian, scan server dengan tools fail2ban untuk mencari aktivitas tidak biasa yang mencoba masuk ke server.

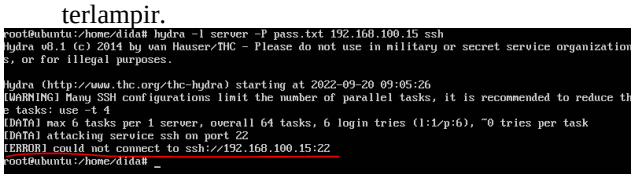
Gambar21. Pindai di Fail2ban

h. Pemindaian berhasil dilakukan. alamat IP sumber serangan dicantumkan, bersama dengan informasi mengapa serangan itu tidak berhasil.



Gambar22. Hasil Pemindaian Serangan Berhasil

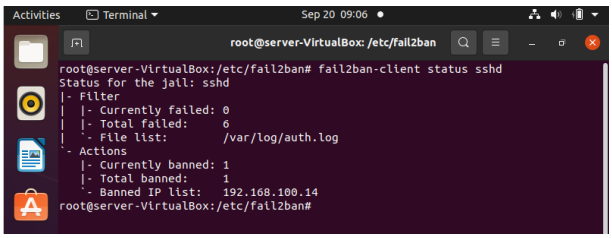
i. Hasil penyerangan akan dikomunikasikan kepada penyerang. Selain itu, kegagalan penyerang untuk menyelesaikan penyerangannya ditunjukkan pada gambar terlampir.



Gambar23. Serangan Gagal

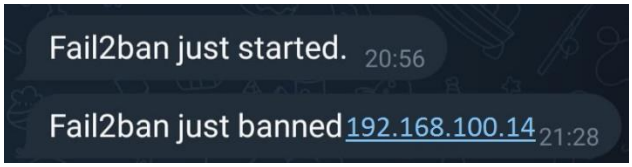
Gambar 23 memiliki "kesalahan", yang menunjukkan bahwa penyerang tidak dapat melakukan serangan kedua karena alamat IP penyerang telah diblokir oleh server (fail2ban).

j. Selain itu, informasi hasil scan yang dihasilkan oleh program fail2ban dapat dilihat pada gambar di bawah ini.



Gambar24. Daftar Hasil Pemindaian

k. Aplikasi Telegram akan menerima pemberitahuan seperti yang terlihat di bawah ini.



Gambar25. Pemberitahuan Telegram

Berdasarkan hasil pengujian di atas, software IDS Fail2ban efektif dalam mendeteksi serangan yang masuk di server, memblokir IP dari sumber serangan, dan kemudian menginformasikan administrator serangan tersebut melalui aplikasi Telegram.

5. KESIMPULAN

Beberapa kesimpulan yang dapat diambil dari penelitian ini antara lain sebagai berikut: 1) Diperlukan lebih banyak file dengan kombinasi kata sandi acak yang lebih beragam, dan serangan kamus akan lebih berhasil seiring dengan bertambahnya jumlah kombinasi kata. 2) Fail2ban dapat dengan cepat menemukan alamat IP dari mana penyerang dan file spam dikirimkan. Seperti yang diilustrasikan pada Gambar 22, server mencari port yang dianggap rentan terhadap serangan. 3) Gambar 24 menunjukkan bagaimana fail2ban secara efektif memblokir dan memasukkan alamat IP penyerang ke daftar hitam. 4) Fail2ban dapat memberi tahu Telegram tentang penyerangan tersebut, sehingga administrator dapat mempelajarinya lebih lanjut kapan pun dan di mana pun mereka berada, seperti terlihat pada Gambar 25. 5) Dengan menggunakan fail2ban dan Telegram yang terhubung, administrator dapat lebih mudah memantau server dari jarak jauh menggunakan personal perangkat yang dimiliki oleh administrator.

DAFTAR PUSTAKA

[1] oleh S. Dian dan C. Cendikia, “Volume.8 Nomor 2 Tahun 2020,” 2020.

[2] oleh M. Iqbal, A.- Arini, dan HB Suseno, “Analisis dan Simulasi Keamanan Jaringan Server Ubuntu dengan Port Knocking, Honeypot, Iptables, Icmp,” Cyber Secur. dan Tokoh Forensik., vol. 3, tidak. 1, hal. 27–32, 2020, doi: 10.14421/csecurity.2020.3.1.1933.

[3] V. Singh, K Bhatia, dan SK Pandey, “Meninjau Kembali Ancaman Keamanan Cloud Serangan Man-in-the-Middle,” Int. J.Komputer. dan Sains. Bahasa Inggris, jilid. 7, tidak. 2, hal. 342–348, 2019, doi: 10.26438/ijcse/v7i2.342348.

[4] oleh N. Fitriana dan FN Secara khusus, “Honeypot Menggunakan Honeyd sebagai Solusi Keamanan Jaringan dari Aktivitas Serangan,” Build Insa. Ict J., Jil. 5, No. 2, hal. 143–152, 2018

[5] oleh RR oleh Adha, M F. Rizal, dan SJI Isma, “Membangun sistem keamanan jaringan berbasis firewall dan ID menggunakanAlat Opnsense,” eProceedings..., vol. 2846–2856, 2021, [Online] Tersedia: https://openlibrarypublications.telkomuniversity.ac.id/index.php/appliedscience/article/view/17034%0Ahttps://openilibrary publikasi. telkomuniversitas. ac

[6] - Shayfuddin D. Risqiwati, dan EA Irawan, "Pencegahan Serangan Brute Force dan DDOS Real-time di Server Ubuntu," Techno.Com, vol. 17,Tidak. 4, hal. 347–354, 2018, doi: 10.33633/tc.v17i4.1766.

[7] Saya dan Saya Kurniawan, “Sistem Pencegahan Serangan Bruteforce di Server Ubuntu Menggunakan Fail2Ban,” Infomatek, vol. 18, tidak. 2, hal. 89, 2017, doi: 10.23969/infomatek.v18i2.496.

[8] SayedAchmady, “Kamus Analisis Serangan dan Modifikasi Password Cracking dan Strategi Antisipatif,”bisnis大学อีสเทิร์นเอเชีย, vol. 88–100 dan 2557.

[9] oleh M. Shruti, “Menyerang Layanan Ssh, Telnet, Vnc dengan Metasploit dan Thc-Hydra,” no. 16, hal. 4408–4416, 2019

[10] Emil Salim, “Analisis dan Implementasi Honeypot Menggunakan Honeyd pada Jaringan Nirkabel Sebagai Penilaian Keamanan Jaringan”, Vol. Februari, hlm. 1–6, 2017

[11] oleh AOD oleh Aritonang, T Ilmu Komputer v. Box, dan I Protokol, “Jurnal Informatika Armada Volume 1 No. 2 Desember 2020 KEAMANAN JARINGAN TERPUSAT GUNAKAN INTRUSION DETETION SYSTEM (IDS) IN,” vol. 1 hingga 11, 2020.

[12] oleh G. Nugraha, T A. Purnama dan AA Rizky, “Rencana Pembuatan Alat Gosok Tangan Otomatis dan Pengecekan Suhu Tubuh Yang Terkoneksi Telegram Di Puskesmas Sawahlega,” JIPI (Jurnal Sains. Peneliti dan Informasi Pembelajaran., vol. 7, no.1, hal.10–21, 2022, doi: 10.29100/jipi.v7i1.2167.

[13] oleh A. Aryapranata, “Web Application Firewall pada Website Institut Bisnis Nusantara www. ibn. AC. id,” Menghitung Esensi, Vol. 55–59, 2020, [Online] Tersedia: https://ibn.e-journal.id/index.php/COMPUTER/article/view/321.

[14] oleh AH Ditandai dengan, s Come dan M.Kom, “Analisis Serangan Banjir Data

pada Router Mikrotik," Krea-TIF, hal. 12–20, 2016

[15] W adalah W. Old dan R. Efendi, "Perancangan dan Analisis Sistem Keamanan Jaringan Komputer Menggunakan SNORT," Aiti, vol. 17, tidak. 2, hal. 143–158, 2021, doi: 10.24246/aiti.v17i2.143-158.

[16] K is A. oleh Prasetyo, M Idhom, dan HE Wahanani, "Di Banyak Server Dengan Menggunakan," Vol. 1, No.3, hal. 789 menjadi 796 pada tahun 2020.

17 dan Y. Hae, "Analisis Keamanan Jaringan pada Web dari Serangan Sniffing dengan Metode Eksperimental," JATISI (Jurnal Tek. Informasi dan terakhir. Informasi), vol. 8, tidak. 4, hal. 2095–2105, 2021, doi: 10.35957/jatisi.v8i4.1196.

[18] oleh L. Lukman dan M. Sacred, "Analisis perbandingan kinerja snort dan Suricata sebagai sistem deteksi intrusi dalam mendeteksi serangan synflood pada web server Apache," Respati, vol. 6–15, 2020, [Online] Tersedia: http://jti.respati.ac.id/index.php/jurnaljti/article/view/343.

[19] dan Y. oleh Mulyanto, H Herfandi, dan R. Candra Kirana, "ANALISIS KEAMANAN WIRELESS LOCAL AREA NETWORK (WLAN) DARI BRUTE FORCE ATTACK MENGGUNAKAN METODE PENETRATION TESTING (STUDI KASUS : RS H.LMANAMBAI ABDULKADIR)," menginformasikan. Teknologi. dan Sains, jilid. 4, tidak. 1, hal. 26–35, 2022, doi: 10.51401/jinteks.v4i1.1528.

[20] J adalah D. Santoso, "Keamanan Jaringan Nirkabel Menggunakan Sistem Deteksi Intrusi Nirkabel," Infos, vol. 44–50, 2019

[21] Ayah Pertama, M.Dr.Ir. Randy Munadi, dan M. Arif Indra Irawan, ST, "Implementasi Sistem Keamanan Jaringan Menggunakan Suricata dan Ntopng," e-Proceeding Eng., vol. 4076, pada tahun 2019.

[22] dan OW Nugroho, "Implementasi Sistem Keamanan Jaringan Intrusion Prevention System (Ips) Menggunakan Iptables Dengan Notifikasi Berbasis Telegram Di SMA Siang Surabaya," J. by Chem. inf. Model., Jil. 110, tidak. 9, hal. 1689–1699, 2017[23] Y. Mulyanto dan A. Algi Fahri, "ANALISIS KEAMANAN LOGIN MICROTIC ROUTER DARI SERANGAN BRUTEFORCE MENGGUNAKAN METODE PENETRATION TESTING," vol. 4, tidak. 3, hal. 145–155, 2022, [Online]. Tersedia: http://www.jurnal.uts.ac.id/index.php/JINTEKS/article/view/1897.

[24] oleh S. Susanto, B A. Pramono, dan S. Handayani, "Analisis Sniffing Password Menggunakan Aplikasi Cain and Abel Pada Jaringan Wifi Universitas Semarang," J. Transform., vol. 16, tidak. 1, hal. 67, 2018, doi: 10.26623/transformatika.v16i1.787.

[25] D adalah R. Arrasy dan A. Noertjahyana, "Analisis perbandingan akurasi deteksi serangan dan efisiensi pemanfaatan sumber daya CPU dari alat pendeteksi serangan Snort dan Suricata yang diinstal pada server web." Infra, jilid. 10, tidak. 1 tahun 2022.

[26] oleh MF oleh Syarif, R Ritzkal, dan AH Hendrawan, "Analisis dan Implementasi Virtual Local Area Network (Vlan) di Laboratorium Program Studi Teknik Komputer Universitas Ibnu Khaldun Bogor," Inova-Tif, vol. 3, tidak. 1, hal.

[27] D adalah Kado, "Penggunaan Bettercap Sebagai Teknik Sniffing Pada Paket Lalu Lintas Jaringan Wifi," Semin. oleh Nas. oleh Teknologi. UISU, Jil. 2, No. 1, hal. 83–85, 2019, [Online] Tersedia di www.olx.co.

[28] oleh MA Ridho dan M. Arman, "Analisis Serangan DDoS Menggunakan Metode Fake Neural Network," J. Sisfokom (Sistem Informasi dan Komputer), vol. 9, tidak. 3, hal. 373–379, 2020, doi: 10.32736/sisfokom.v9i3.945.

[29] S adalah Alviana dan ID Sumitra, "Analisis Pengukuran Penggunaan Sumber Daya Komputer pada Sistem Deteksi Intrusi dalam Meminimalkan Serangan Jaringan," Computer J. by Ilm. Komputer. dan Informasikan., vol. 7, tidak. 1, hal. 27–34, 2018, doi: 10.34010/computa.v7i1.2533.

[30] Suhartono dan Abd.Rahman Patta, "dosen Pendidikan Teknik Informatika dan Komputer, Pendidikan Teknik Elektro Universitas Negeri Makassar (UNM) 145," hal. 145–155, 2017.