Jurnal TICOM: Technology of Information and Communication
Volume 11, Nomor 1, September 2022 Hal: 33-38 E-ISSN: 2962-7982

Sistem Monitoring Serangan Ssh Dengan Metode *Intrusion Prevention System (IPS) Fail2ban* Menggunakan *Python* Pada Sistem Operasi Linux

Farhannullah[1*], Mardi Hardjianto[2]

[12]Fakultas Teknologi Informasi, Teknik Informatika, Universitas Budi Luhur, Jakarta, Indonesia
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Email: [1*]1811510443@student.budiluhur.ac.id, [2]Mardi.Hardjianto@budiluhur.ac.id
(* : corresponding author)

Abstrak-**Penelitian ini bertujuan untuk memberikan kemudahan bagi administrator sistem dalam memantau serangan *Bruteforce SSH (Secure Shell)* melalui akses jarak jauh yang terjadi pada server yang memiliki akses jarak jauh ke *Secure Shell (SSH)* dengan *port* 22 yang dapat diakses oleh siapa saja dan menjadi tanggung jawabnya. Karena akan berbahaya jika penyerang bisa masuk ke server sehingga penyerang bisa leluasa menggunakan data informasi yang ada. Untuk mencegah serangan tersebut peneliti menggunakan metode *Intrusion Prevention System (IPS)* dengan *tool Fail2ban* sebagai *firewall* yang dapat memblokir serangan yang terjadi pada server. Dari hasil log yang diperoleh untuk memudahkan dalam memonitor serangan *Bruteforce SSH*, maka dibuatlah sistem *WEB Dashboard* yang dijalankan pada script Python untuk melakukan monitoring secara real-time. Penelitian ini mengimplementasikan *Cloud Virtual Private Server (VPS)* dengan sistem operasi *Linux* Debian 10. Hasil implementasi yang peneliti lakukan monitoring log sebanyak 2.498 log blocking dalam 1 minggu dari berbagai negara dengan target pada login credential *SSH server Debian* 10. Maka dari itu hasil Penelitian ini membuat suatu sistem *monitoring WEB Dashboard* yang dapat diakses dari jarak jauh, yang dapat membantu seorang administrator untuk memantau serangan terhadap server yang menjadi tanggung jawabnya dan dapat mengurangi tingkat kejahatan *cyber* yang terjadi pada jaringan publik di Perusahaan**

Kata Kunci: ***Brute Force, Fail2ban, Intrusin Prevention System (IDS), WEB Dashboard*.**

Abstract- ***This study aims to provide convenience for system administrators in monitoring Bruteforce SSH (Secure Shell) attacks through remote access that occurs on servers that have remote access to Secure Shell (SSH) with port 22 which can be accessed by anyone and be their responsibility. Because it will be dangerous if the attack can enter the server so that the attacker can freely use the existing information data. To prevent this attack, the researcher uses the Intrusion Prevention System (IPS) method with the Fail2ban tool as a firewall that can block attacks that occur on the server. From the log results obtained in order to make it easier to monitor Bruteforce SSH attacks, a WEB Dashboard system was created that was run on Python scripts to perform real-time monitoring. This study implements a Cloud Virtual Private Server (VPS) with the Linux Debian 10 operating system. The results of the implementation that researchers have carried out monitoring logs are 2,498 log blocking in 1 week from various countries with a target on the Debian 10 server SSH login credential. Therefore the results This study makes a WEB Dashboard monitoring system that can be accessed remotely, which can help an administrator to monitor attacks on the servers that are his responsibility and can reduce the level of cyber crime that occurs in the public network at Company.***

Keywords: ***Brute Force, Fail2ban, Intrusin Prevention System (IDS), WEB Dashboard***.

I. PENDAHULUAN

Perkembangan teknologi dan internet yang cukup pesat saat ini membawa perubahan proses bisnis bagi pihak-pihak yang memanfaatkan internet untuk memberikan layanan seperti transaksi *online*, promosi, pertukaran data dan lain-lain. Kebutuhan akan keamanan dan kelancaran dari layanan-layanan tersebut sangat penting, hal ini dikarenakan kemajuan teknologi dan internet berbanding lurus dengan kejahatan yang ada pada internet itu sendiri. Selain perubahan proses bisnis, hal ini juga merubah cara sistem administrator dalam melakukan manajemen server. Dimana manajemen *server* saat ini mayoritas dilakukan melalui akses jarak jauh, sehingga tidak memerlukan akses fisik untuk dapat melakukan akses jarak jauh ini. *Secure Shell* (SSH) adalah sebuah protokol administrasi yang memungkinkan user untuk mengakses dan memodifikasi berbagai macam pengaturan maupun file yang ada di dalam *server* [1] Saat ini, Protokol *SSH* menjadi salah satu sasaran tindak kejahatan yaitu pengambil alihan akses server. Sepanjang 2020, Badan Siber dan Sandi Negara mendeteksi adanya serangan SSH di Indonesia melalui 71 titik *Honeypot* yang dimiliki[2].Menurut Ketua Indonesia *Honeynet* Project Dr Charles, *SSH attack* merupakan serangan pada layanan yang digunakan Administrator, bukan layanan umum biasa. *SSH Atttack* sudah lama popular dikalangan peretas lantaran SSH layaknya pintu gerbang ke semua layanan. Jika penyerang berhasil memasuki SSH, mereka dapat melakukan apapun terhadap sistem yang dimasuki. Mereka bisa meyiapkan perangkat yang terinfeksi untuk dimanfaatkan sendiri atau justru ditawarkan kepada peretas lain [2].

Metode yang sering digunakan untuk melakukan pengambilan alihan *server* melalui protokol SSH adalah dengan metode serangan *brute force*. Serangan ini dilakukan dengan cara menggunakan semua kemungkinan kata sandi yang sudah disediakan dengan masukan dan panjang karakter tertentu. Untuk itu diperlukan satu penanganan yaitu dengan membuat sistem yang bisa membantu memberikan laporan

deteksi adanya ancaman serangan *brute force* tersebut. Salah satu solusi yang dapat melakukan deteksi adanya serangan *brute force* pada protokol SSH adalah *Fail2ban*[3]. *Fail2ban* bekerja dengan cara merubah *konfigurasi firewall* dan mencoba membuat aturan berdasarkan log dari protokol SSH. *Fail2ban* berfungsi untuk melakukan pemantauan pada jumlah kegagalan *login* protokol SSH pada sistem dan melakukan pemblokiran pada IP tertentu yang dianggap melakukan *brute force* [3]. *Fail2ban* menggunakan mode teks untuk melihat daftar IP yang terindikasi melakukan serangan *brute force* sehingga dilakukan pemblokiran pada IP tersebut[4].

Pada penelitian ini dilakukan oleh Syani ini terdapat masalah kerentanan jika penyedia VPS untuk melakukan pengelola server tidak melakukan pengujian terhapat serangan yang terjadi dengan menggunakan *Network Development Life Cycle (*NDLC). dengan salah satu tapahan monitoring dengan menggunakan metode monitoring *Intrusion Detection System (*IDS) dengan tool suricata ini [5]. Penelitian yang dilakukan selanjutnya oleh resevoa, ndriarini dan Iqbal ini melakukan sistem keamanan pada jaringan lokal meggunakan honeypot dengan tools dioneadan dan IDS, dapat melakukan deteksi serangan untuk mengetahui kemampuan IDS dan dapat melakukan analisis mengenai malware yang berhasil dilakukan deteksi [6], Adapun Penelitian yang lakukan oleh fadlin, yamin dan surimi ini bertujuan unutk melakukan pendeteksian menggunakan *Intrusion Detection and Prevention System (IDPS)* dengan menggunakan notifikasi secara realtme yang dapat dilakukan monitoring serangan dengan tool snort sebagai firewall untuk malekukan pemblokiran [7]. Berbeda dari penelitian sebelumnya penelitian ini penulis melakukan monitoring terhadap serangan yang terjadi pada VPS, dan dapat melakukan monitoring serangan melalui WEB Dashboard dan bisa melakukan pencegahan berupa pemblokiran dengan menggunakan Metode *Intrusion Prevention System* (IPS)

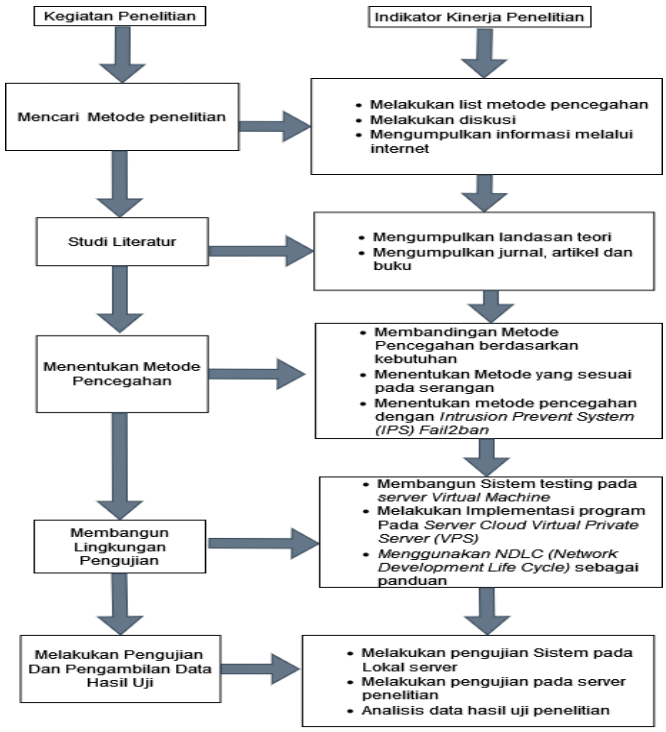
Data dari BSSN yang mengatakan bahwa SSH merupakan salah satu protokol yang sering dijadikan target serangan [2]. Serangan ini perlu dilakukan pencegahan dan penanggulangan dengan cepat untuk menjaga layanan tetap berjalan tetapi untuk membaca log dari protokol SSH harus masuk ke dalam sistem operasi dari *server* sehingga memakan waktu yang lebih lama. untuk itu diperlukan *tools* yang memudahkan dalam membaca log dari SSH tersebut yang tanpa perlu melakukan akses kedalam sistem operasi pada *server*. Tujuan dari penelitian ini yaitu untuk memberikan kemudahan untuk para sistem administrator dalam memonitoring serangan *bruteforce SSH (Secure Shell)* yang terjadi pada *server-server* yang menjadi tanggung jawab mereka. *Intrusion Prevention System* (IPS) merupakan sebuah perangkat lunak (*software*) yang berfungsi untuk memonitoring trafik jaringan, mendeteksi aktivitas yang mencurigakan dan melakukan prncegahan terhadap serangan yang dapat membuat jaringan menjadi berfungsi dengan tidak semestinya [8]. Dengan menggunakan metode *Intrusion Prevent System* (IPS) dengan *tools Fail2ban*. Untuk itu dalam melakukan pemantauan dari hasil *Fail2ban* ini maka perlu dibuat sebuah *tools* yang dapat diakses melalui halaman WEB. Pada *tools* ini akan menampilkan waktu serangan, IP asal yang terindikasi melakukan serangan sampai dengan lokasi dari IP tersebut, sehingga dapat memudahkan sistem administrator untuk dapat memonitor log serangan yang terjadi. Sistem monitoring ini dibangun dengan tujuan untuk membantu pihak – pihak terkait, seperti sistem administrator dalam melakukan pemantauan layanan SSH terkait serangan yang terjadi pada *server – server* yang dimiliki.

II. METODE PENELITIAN

2.1 Penerapan Metode Penelitian

Berisikan tahapan dalam tahap uji coba berupa rangkaian menggunakan *Fail2ban* pada sistem operasi Linux Debian 10 yang dijalankan pada *cloud Virtual Private Servers* (VPS) yang divisualisikan ke dalam WEB *dashboard* yang script-nya dijalankan oleh *Pyhton*. *Python* merupakan salah satu bahasa pemograman yang tinggi dapat menjalankan semantik dinamis untuk memberikan tingkat keterbacaan sintaks dan dapat mengeksekusi sejumlah eksekusi multifungsi secara langsung (*interpretatif*) dengan pendekatan Pemrograman Berorientasi Objek [9]. Berikut tahapan penelitian agar hasil dari penelitian dapat berjalan sesuai yang diinginkan dapat dilihat pada Gambar 1.

Pertama mencari metode penelitian pada metode ini peneliti melakukan list mencari data dari berbagai sumber untuk menentukan metode pencegahan yang nantinya dibutuhkan pada pencegahan serangan *Bruteforce*. Kedua Studi Literatur, pada tahap ini mengumpulkan landasan teori untuk dapat melakukan penelitian, literatur yang digunakan berasal dari Junal, artikel serta buku yang berkaitan dengan serangan *bruteforce* salah satu nya menurut kris prasetyo tahun 2020 [10]. Tahap ketiga menentukan metode, pada tahap ini peneliti menentukan parameter untuk melakukan pencegahan pada serangan *bruteforce*, dengan metode *Intrusion Prevention System* (IPS) berjalan berdasarkan parameter yang telah ditentukan. Peneliti melakukan konfigurasi pada sistem jika ada serangan yang mencoba untuk login pada *Session* SSH sebanyak 5 kali percobaan maka sistem akan memblokir IP tersebut. Tahap selanjutnya membangun lingkungan penelitian dengan komponen-komponen perangkat lunak yang dibutuhkan pada penelitian ini. Dirancang pada tahap ini sebelum melakukan tahap pengujian dengan melakukan Implementasi pada jaringan lokal dan membangun sistem pada *Virtual Private Server* (VPS). Untuk dapat mempermudah dalam membangun lingkungan penelitian, peneliti menggunakan metode *Network Development Life Cycle* (NDLC). Terakhir tahap pengujian dan pengambilan data, Pada tahap ini peneliti melakukan pengujian dengan menggunakan sistem tiga tahap uji coba yaitu melakukan penyerangan terhadap target dengan tidak menggunakan keamanan sistem *Fail2ban*. Selanjutanya melakukan serangan dengan sistem *Fail2ban* yang nanti nya akan diblokir dan dapat divisualisasikan *log IP* yang telah di *banned*. Melakukan pengujian selama satu minggu untuk mendapatkan pengumpulan data dengan hasil serangan *realtime* dari kondisi target penelitian ini dijalankan dengan jaringan publik. Dengan begitu maka pengujian dapat berjalan untuk mengetahui tindak kejahatan yang ada dijaringan publik.



Gambar 1. Metode penelitian

2.3 Rancangan Pengujian

Rancangan pengujian ini dilakukan dengan teknik pengujian *testing* melalui jaringan *local* dengan Teknik *bruteforce attack* menggunakan *script pyhton*. Teknik pengujian ini merupakan pengujian program langsung melihat pada *tools Fail2ban* dapat melakukan *blocking* saat pengujian. Setelah dapat melakukan *blocking logs* yang didapatkan *WEB Dashboard* dapat menampilkan hasil logs yang diterima dari *Fail2ban*. Berikut adalah perincian dari rancangan pengujian pada Tabel 1.

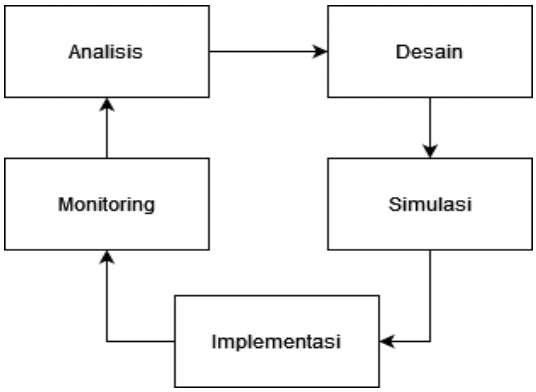
Tabel 1. Perincian dari Rancangan Pengujian

No	Komponen	Rencana Pengujian	Hasil
1	*Tools Nmap*	Melakukan pengujian untuk mengetahui *port ssh* 22 terlah terbuka pada *Server* Debian 10	Dapat hasil dari *Scanning* untuk mengetahui *port* 22 terbuka
2	Melakukan Uji login ke *SSH*	Melakukan uji coba serangan *Bruteforce* ketarget *server* penelitian	Ujin login *SSH* terblokir dan tercatat di log
3	*Script* Program *WEB Dashboard*	Dapat menampilkan *logs* yang di-*Parsing* oleh *script python flask* ke dalam *WEB dashboard*	Mampu menampilkan *logs* ke *WEB Dashboard*

III. HASIL DAN PEMBAHASAN

2.2 Implementasi Metode

Pada tahap ini peneliti melakukan implentasi metode dengan menggunakan *Network Development Life Cycle* (NDLC) sebagai panduan untuk melakukan pengembangan sistem berikut pada Gambar 2 alur jalan kerja.



Gambar 2. *Network Development Life Cycle* (NDLC)

a. Analisis
Pada Tahap ini peneliti melakukan analisis dari sistem yang ada pada Perusahaan seperti menggunakan sistem operasi apa kebutuhan akan hal dari sistem, permasalahan yang muncul dari dunia luar, dan juga analisis topologi dari sistem *Cloud* yang digunakan.

b. Desain
Dari hasil analisis didapat peneliti melakukan desain dari t*opologi* yang akan dibangun untuk melakukan penelitian, seperti pemasangan sistem *firewall* yang akan diimplementasikan, desain sistem *WEB Dashboard* akan dirancangn seperti apa.

c. Simulasi
Untuk melakukan simulasi dari rancangan ini peneliti melakukan analisis pada *sistem Virual Machine* untuk mengetahui kekurangan sistem yang telah dilakukand rancangan sebelum berjalan pada tahap implementasi melakukan pengujian sistem yang telah dilakukan.

d. Pada tahap ini implementasi difokuskan untuk melakukan penginstalan sistem *WEB Dashboard* dan sistem *tools Fail2ban* yang dikonfigurasi berdasarkan kebutuhan dari penelitian. Penerapan *Intrusion Prevention System* (IPS) ini dapat berjalan jika terjadinya penyerangan dan Sistem *WEB Dashboard monitoring* dapat berjalan sesuai rancangan penelitian.

e. Monitoring
Tahap monitoring pelaksanaan melalui pemantauan dan pengamatan selama percobaan sistem dilakukan berdasarkan skenario pengujian pada tahap ini dapat mengetahui sistem berjalan sesuai rencana dan dapat menentukan bahwa metode *Intrusion Prevention System* (IPS) dapat berjalan dengan baik.

2.3 Algoritme

Algoritma ini menjelaskan proses untuk akses server jika kurang dari lima kali maka dapat mengakses ke server dan lebih dari lima kali pemblokiran terhadap serangan *Bruteforce* yang ingin mencoba akses ke *SSH* jika sudah terjadi pemblokiran akan ter-*banned* lalu tercatat log ke *WEB Dashboard* dapat dilihat pada Algoritme 1.

Algoritme 1 Algoritme Sistem *Fail2ban*

1	Jika ada seranganSerangan *bruteforce*
2	*If Login* kurang dari 5 kali *then*
3	*Login* Ke *server*
4	
5	*Else If* Lebih dari 5 kali *then*
6	IP serangan ter-*Banned* dan tercatat di *log*
	EndIf

Pada Algoritme ini menjelaskan proses *Menu Config* untuk melakukan *Enable/Disable service* itu sendiri dan terdapat alur akses menu yang terdapat pada *WEB Dashboard* yang di jelaskan pada Algoritma 2.

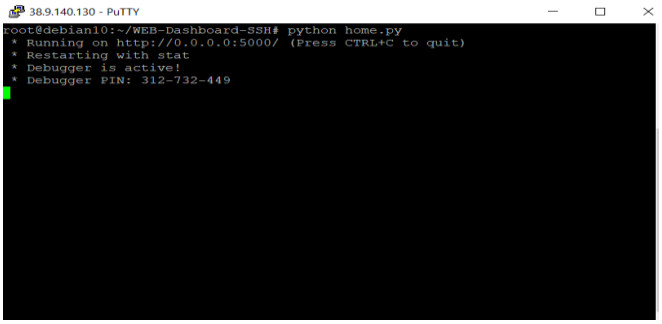
Algoritme 2 Algoritme Menu *Config*

1	Tampilan *Form* Menu *Config*
2	Pilih aksi
3	
4	*If* aksi = *Enable Service* SSH *Then*
5	SSH *Service* Berjalan
6	*End If*
7	
8	*Else If* aksi = *Disable Service* SSH *Then*
9	SSH *service* tidak berjalan
10	*End if*
11	
12	*Else If* aksi = Menu Home *Then*
13	Menampilkan Menu Home
14	*End If*
15	
16	*Else If* aksi = Menu Banned IP *Then*
17	Menampilkan Menu Banned IP
18	*End If*
19	
20	*Else If* aksi = Menu Successful Login *Then*
21	Menampilkan Menu Successful Login
22	*End If*
23	
24	*Else If* aksi = Logout
25	Menampilkan Halaman Utama
26	*End if*
27	
28	*End If*

2.4 Tahap Pengujian

a. Menjalankan *Service Home.py*

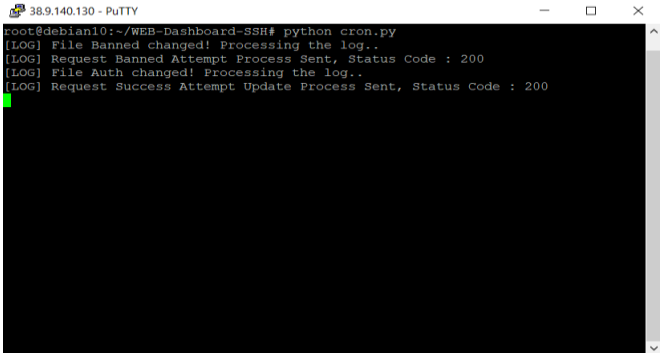
Pada tahap ini peneliti menjalankan *Service Home.py* untuk melakukan akses *WEB Dashboard* dari hasil *script* yang ada di dalam *python* itu dapat menjalankan html untuk mendapatkan visualisasi Sistem ini dijalankan dengan *Script Python* yang di jalankan dengan bahasa pemograman HTML untuk dapat di visualisasikan dilihat pada Gambar 3.



Gambar 3. *Service Home.py*

b. Menjalankan *Service Cron.py*

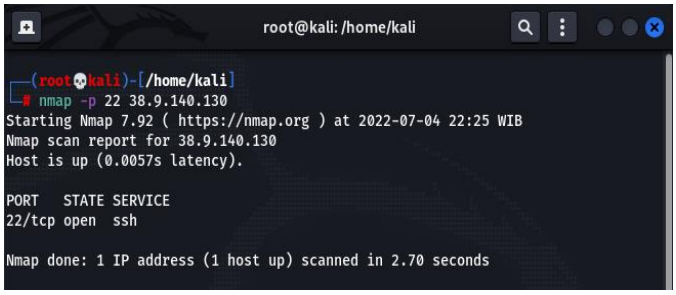
Pada tahap ini peneliti menjalankan *Service Cron.py* untuk melakukan *parsing log* dari *banned IP* secara berkala untuk menentukan data *realtime* yang berasal dari *Fail2ban.log* untuk diolah data nya ke dalam JSON untuk dapat dilakukan visualisasi ke dalam *WEB Dashboard* dapat dilihat pada Gambar 4.



Gambar 4. *Service Cron.py*

c. Pengujian *Scanning*

Pada tahap ini peneliti melakukan pengujian pada sistem *server* yang ada pada *cloud* memastikan bahwa port 22 untuk melakukan *bruteforce* telah dibuka dengan menggunakan teknik *information gathering tools* dari *Nmap* dengan *command nmap -p* 22 38.9.140.130 script ini dapat mengetahui status port yang terbuka yang dapat dilihat pada Gambar 5.

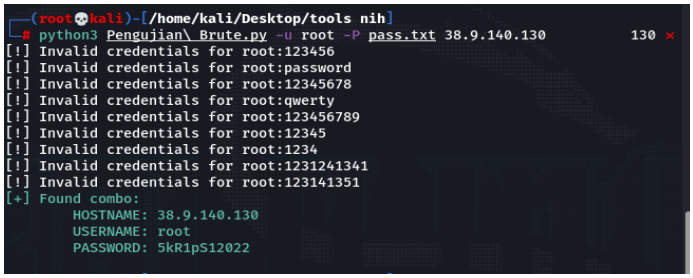


Gambar 5. Pengujian *Bruteforce*

d. Uji Serangan *Bruteforce*

Pada Gambar 6 peneliti melakukan *Bruteforce* dengan metode *Intrusion Prevention System* (IPS) tidak diaktifkan maka *tools script python bruteforce* ini dapat melakukan percobaan sampai dia menemukan *password* yang benar script

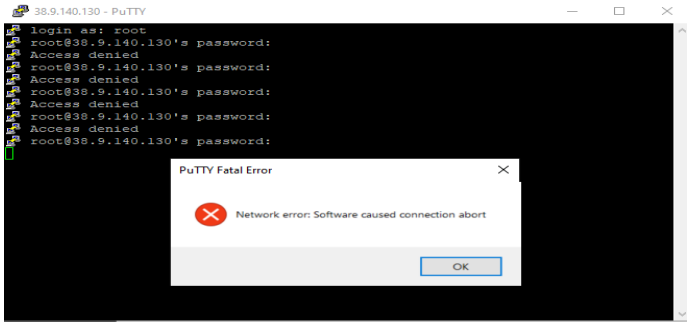
ini melakukan perulangan kata sandi yang sudah dibuat oleh peneliti dengan yang terdapat isi pada pass.txt dapat dilihat pada Gambar 6.



Gambar 6. Serangan *Bruteforce* uji coba

e. Pengujian *Bruteforce* dengan *enable server ssh Fail2ban bruteforce.*

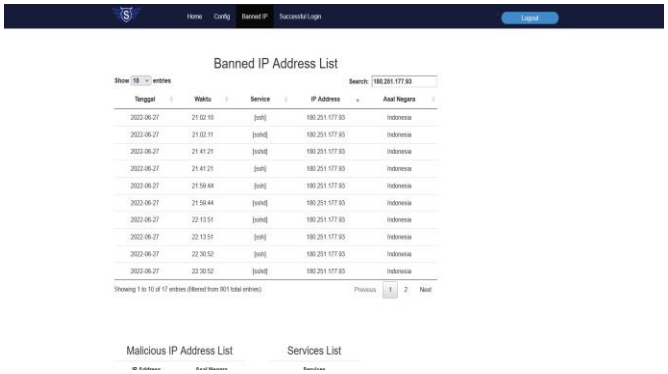
Pada Gambar 7 dilakukan *banned* jika percoba 5 kali berulang dengan 1 jam *blocking*, pengujian ini dengan tujuan apakah jika *fail2ban* ini bekerja sesuai yang sudah di konfigurasi yang dapat di lakukan *Intrusion Prevention System (IPS).* Metode ini menggunakan sistem pencegahan dan deteksi untuk mencegah serangan dapat dilihat pada Gambar 7.



Gambar 7. Uji coba *Login*

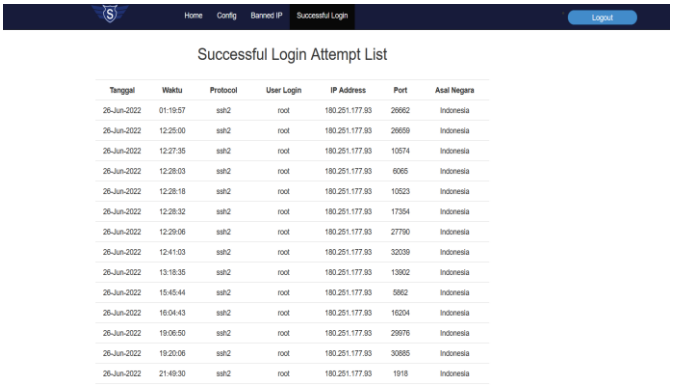
3.3 Hasil Pengujian

Pada pengujian yang dilakukan melalui jaringan lokal terdapat IP peneliti yang terblokir oleh *Fail2ban* karena melakukan percobaan *bruteforce* yang di visualisasikan ke *WEB Dashboard* dan juga ada serangan dari luar jaringan dari berbagai macam negara bisa dilihat pada Gambar 8.



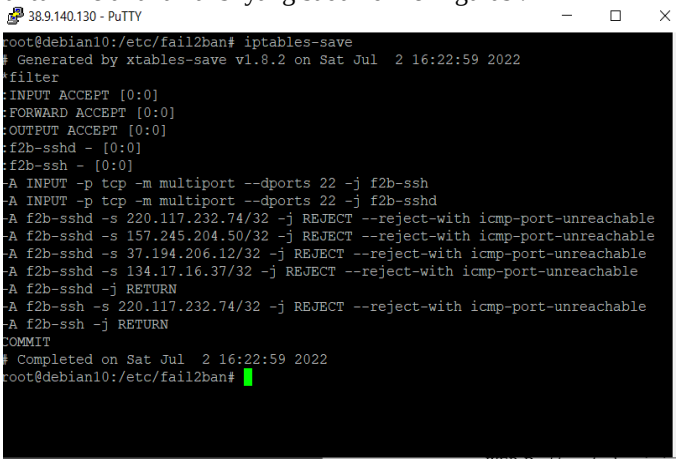
Gambar 8. Hasil *Banned* ditampilkan di *WEB Dashboard*

Hasil penelitan pada bagian ini merupakan list-list dari user yang telah berhasil login pada server dapat dikonfirmasi juga dari hasil login tersebut yang di tampilkan pada WEB Dashboard yang dapat dilihat pada Gambar 9.



Gambar 9. Hasil *Login* ke *Server* pada *WEB Dashboard*

Pada Gambar 10 menampilkan hasil Kerja dari Iptables untuk melakukan blokir yang diperintah kan oleh *Fail2ban* untuk melakukan aksi yang sudah di konfigurasi.

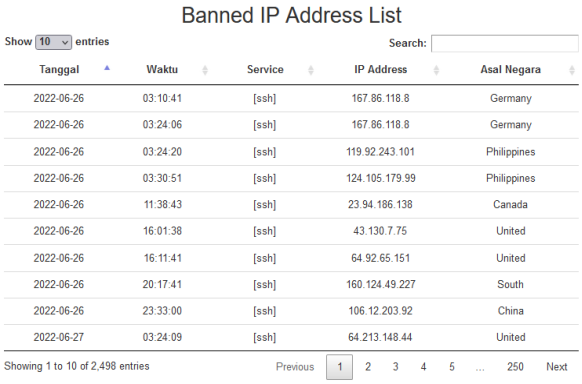


Gambar 10. Hasil blokir *Iptables* yang diperintahkan *Fail2ban*

3.4 Analisis Pengujian

Pada Analisis dari hasil pengujian ini, peneliti mendeteksi bahwa jika dari hasil serangan yang bertujuan pada *server Debian* 10 dengan *service Fail2ban* tidak aktif maka penyerang mendapatkan *password* karena tidak ada pemblokiran pada *server* tersebut. Pada tahap selanjutnya sistem *Fail2ban* diaktifkan maka penyerangan dapat dicegah dan sistem akan melakukan pemblokiran pada IP penyerang, yang dilakukan *parsing log* menggunakan *Python Cronjob* yang sudah dilakukan *filter* data *log* yang nantinya akan dilakukan visualisasi ke *WEB Dashboard*.

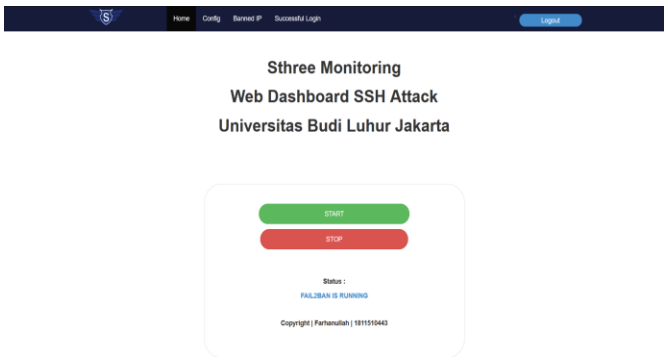
Tahap Implementasi pada *server cloud Virutal Private Server* (VPN) ini peneliti melakukan *monitoring* pada sistem yang sudah dilakukan tahap penelitian. Dari hasil yang sudah di jalankan pada kurang lebih satu minggu monitoring ada sekitar 2.498 log yang telah ter-*banned* yang dapat dilihat pada gambar 11.



Gambar 11. Visualisasi *log* serangan yang sudah di Analisis

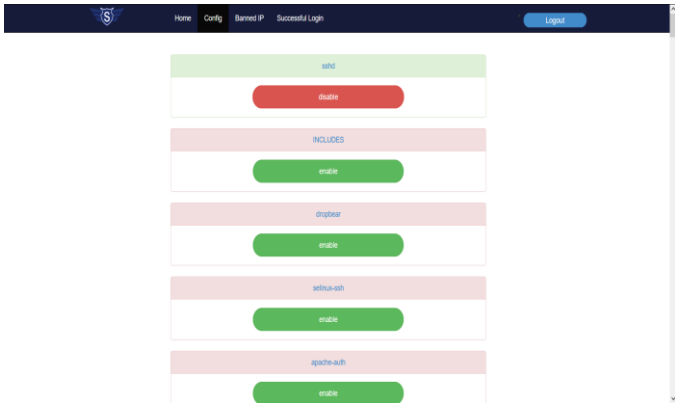
3.5 Rancangan Antarmuka

Rancangan layar ini adalah rancangan yang ditampilkan pada WEB Dashboard yang sudah dilakukan *Implement Program*.



Gambar 12. Tampilan Menu *Home*

Pada Gambar 12 Menu *home* ini tampilan *layar* akan menunjukan nama program peneliti dan *service* untuk menjalankan *service* untuk *fail2ban* dan ada info status kalau *service* sedang running atau tidak.



Gambar 13. Tampilan Menu *Config*

Pada Gambar 13 tampilan layar *config* untuk melakukan *enable service* fitur yang ada pada *Fail2ban* untuk penelitian ini peneliti melakukan *enable* pada fitur SSH untuk melakukan pencegahan pada *Bruteforce SSH.*

IV. PENUTUP

Berdasarkan penelitian yang telah dilakukan maka dapat disimpulkan bahwa pengamanan pada *Cloud Virtual Private Server* (VPS) dengan Sistem Operasi Debian 10 Pada Perusahaan dapat berjalan dengan baik. Dan berhasil melakukan sebuah pencegahan serangan menggunakan metode *Intrusion Prevention System* (IPS) *tools Fail2ban* yang dapat menjalankan pemblokiran serangan SSH pada *server* dalam *monitoring* kurang lebih satu minggu terdapat 2.498 *banned IP*. Dengan membangun *WEB Dashboard* dapat membantu seorang administrator untuk melakukan *monitoring* serangan pada *server* Debian 10 yang dimanfaatkan dengan baik untuk melakukan monitoring serangan. Hasil *parsing log* yang didapatkan dari *fail2ban.log* dan *Auth.log* dapat berjalan dengan baik sesuai rencana yang merupakan log yang akan di visualisasikan di dalam *WEB Dashboard.*

REFERENSI

[1] J. Park, J. Kim, B. B. Gupta, and N. Park, “Network Log-Based SSH Brute-Force Attack Detection Model,” *Comput. Mater. \& Contin.*, vol. 68, no. 1, pp. 887–901, 2021, doi: 10.32604/cmc.2021.015172.

[2] T. Gobel, “BSSN Sebut Sebanyak 71 SSH Attack Terjadi di Indonesia, Serangan Apa Itu?,” *cyberthreat.id*. Mar. 2021. Accessed: May 12, 2022. [Online]. Available: https://cyberthreat.id/read/11054/BSSN-Sebut-Sebanyak-71-SSH-Attack-Terjadi-di-Indonesia-Serangan-Apa-Itu

[3] T. Mulyana, “Mengamankan SSH dengan Fail2ban,” *Nothinux*. Aug. 2016. Accessed: May 12, 2022. [Online]. Available: https://nothinux.id/mengamankan-ssh-dengan-fail2ban/

[4] F. Indyawan, “Pengertian Fail2ban dan Cara Kerjanya.” Jun. 2019. Accessed: Jun. 03, 2022. [Online]. Available: https://www.kitaadmin.com/2019/03/pengertian-fail2ban-dan-cara-kerjanya.html

[5] M. Syani, “Implementasi Intrusion Detection System (IDS) Menggunakan Suricata Pada Linux Debian 9 Berbasis Cloud Virtual Private Servers (VPS),” *JurnalInkofar*, vol. 1, no. 1, Aug. 2020, doi: 10.46846/jurnalinkofar.v1i1.155.

[6] R. M. Muhammad, I. D. Irawati, and M. Iqbal, “Implementasi Sistem Keamanan Jaringan Lokal Menggunakan Honeypot Dionaea , Dan IDS,” *J. Elektro Telekomun. Terap.*, pp. 1–7, 2020.

[7] F. Arsin, M. Yamin, L. Surimi, J. T. Informatika, F. Teknik, and U. H. Oleo, “Implementasi Security System Menggunakan Metode IDPS (Intrusion Detection And Prevention System) Dengan Layanan Realtime Notification,” in *semanTIK*, 2017, vol. 3, no. 2, pp. 39–48.

[8] Y. W. Pradipta and Asmunin, “Implementasi Intrusion Prevention System (IPS) Menggunakan Snort dan IP Tables Berbasis Linux,” *Manaj. Inform.*, vol. 7, pp. 21–28, 2017.

[9] P. Pendidikanmu, “Pengertian SSH: Fungsi, Cara Kerja, Manfaat, Kelebihan, Kekurangan.” 2022. Accessed: Jun. 10, 2022. [Online]. Available: https://pendidikanmu.com/2022/03/materi-ssh.html

[10] K. A. Prasetyo, M. Idhom, and H. E. Wahanani, “Sistem Pencegahan Serangan Bruteforce Pada Multiple Server Dengan Menggunakan FAIL2BAN,” . *Novemb.*, vol. 01, no. 3, p. 7, 2020.