# Implementasi Sistem Monitoring Jaringan Menggunakan Zabbix dan Web Web Application Firewall di PT PLN (Persero) Transmisi Jawa Bagian Tengah

**Achmad Hamzah [1], Setia Juli Irzal Ismail, S.T., M.T. [2], Lisda Meisaroh, S.Si., M.Si. [3]**
**[1, 2, 3]Prodi D3 Teknologi Komputer, Fakultas Ilmu Terapan, Universitas Telkom**
[1]hamzbond@gmail.com, [2]jul@tass.telkomuniversity.ac.id, [3]lisda@tass.telkomuniversity.ac.id

**Abstrak-** PT PLN (Persero) Transmisi Jawa Bagian Tengah-Area Pelaksana Pemelihara Bandung memiliki jaringan internet yang besar. Untuk itu diperlukan sebuah sistem untuk melakukan pengawasan dan perawatan. Sistem monitoring jaringan yang ada saat ini memiliki keterbatasan akses, yaitu pada komputer yang terinstall sistem monitoring saja. Maka dari itu diajukan sebuah sistem monitoring jaringan yang dapat diakses dari mana saja dalam area jaringan dengan tambahan sistem keamanan jaringan. Sistem monitoring ini bekerja dengan mengirimkan Ping kepada klien untuk memastikan klien sedang terhubung ke dalam jaringan yang sama dengan sistem monitoring. Sistem monitoring dapat mengirimkan notifikasi kepada user apabila ada klien yang tidak terhubung dengan server melalui email dan Telegram. Sedangkan keamanan jaringan yang diberikan mampu mencegah terjadinya serangan DDoS Attack.

Kata Kunci: Monitoring, Zabbix, ModSecurity, Notifikasi, DDoS Attack.

***Abstract***- *PT PLN (Persero) Transmisi Jawa Bagian Tengah - Area Pelaksana Pemelihara Bandung has a large internet network. For this reason, a system for monitoring and maintenance is needed. The current network monitoring system has limited access only on the computer which the monitoring system is installed. Therefore a network monitoring system can be accessed from anywhere in the network area with an additional network security system is proposed. The monitoring system works by sending Ping to the clients to ensure they are connected to the same network with monitoring system. The monitoring system can send notification to users by email and Telegram if there are clients who are not connected to the server. While the network security provided is able to prevent DDoS Attack.*

*Keyword: Monitoring, Zabbix, ModSecurity, Notifikasi, DDoS Attack.*

## 1. Pendahuluan

### 1.1 Latar Belakang

Jaringan komputer adalah salah satu sarana komunikasi yang sangat dibutuhkan dan banyak digunakan saat ini. Melalui jaringan komputer pengguna dapat melakukan pertukaran informasi dari jarak jauh sekalipun. Jaringan komputer dapat dibangun menggunakan kabel maupun tanpa menggunakan kabel (nirkabel)[1].

Untuk memastikan stabilitas jaringan komputer, diperlukan sebuah sistem untuk melakukan pengawasan terhadap jaringan komputer yang disebut sistem *monitoring* jaringan. Sistem *monitoring* jaringan melakukan pemeriksaan kepada setiap klien yang terhubung dengan Server untuk memantau aktifitas klien dan memastikan apakah klien terhubung dengan Server. Sistem ini kemudian memberikan laporan *monitoring* kepada admin secara aktual.

PT PLN (Persero) Area Pelaksana Pemelihara Bandung sudah memiliki sistem *monitoring* jaringan menggunakan WhatsUp Gold, yaitu aplikasi berbasis Flash untuk membuat sistem *monitoring* jaringan. Aplikasi ini bersifat *user-friendly* dengan prosedur instalasi dan konfigurasi yang mudah, serta tampilan yang mudah dimengerti. Namun aplikasi ini memiliki kekurangan, yaitu tidak mendukung *platform* berbasis web, sehingga akses terhadap sistem terbatas pada komputer yang terinstall WhatsUp Gold saja.

Berdasarkan permasalahan di atas, diangkat judul Implementasi Sistem Monitoring Jaringan menggunakan Zabbix dan Web Application Firewall di PT PLN (Persero) Transmisi Jawa Bagian Tengah. Sistem monitoring Zabbix memanfaatkan fitur Ping untuk mengidentifikasi apakah klien terhubung atau tidak dalam jaringan.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diutarakan, maka rumusan masalah dalam proyek akhir ini ialah sebagai berikut.
1.Bagaimana membangun sistem monitoring jaringan yang dapat diakses di dalam area jaringan PT PLN (Persero) TJBT-APP Bandung?
2.Bagaimana menampilkan informasi ketersediaan akses setiap klien yang dimonitoring ke dalam sistem monitoring?
3.Bagaimana mendapatkan notifikasi apabila terdapat klien yang tidak terhubung dengan server?
4.Bagaimana melindungi sistem dari serangan DDoS Attack?

## 1.3 Tujuan

Tujuan dari pembuatan Proyek Akhir ini adalah:
1.Membangun sistem monitoring jaringan menggunakan Zabbix.
2.Melakukan pendataan alamat Ip klien dalam jaringan dan menampilkannya melalui *map* Zabbix.
3.Membuat sistem notifikasi kepada admin apabila terdapat klien yang tidak terhubung dengan server.
4.Melakukan pengamanan sistem terhadap serangan DDoS Attack.

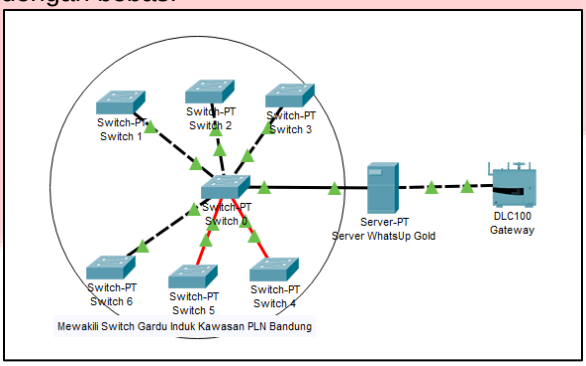
## 1.4 Batasan Masalah

Berdasarkan tujuan yang telah diutarakan sebelumnya maka batasan masalah dalam pengerjaan proyek akhir ini adalah sebagai berikut.
1.Implementasi sistem dilakukan di PT PLN (Persero) Transmisi Jawa Bagian Tengah-Area Pelaksana Pemeliharaan Bandung (PLN TJBT-APP Bandung).
2.Sistem keamanan yang digunakan adalah ModSecurity dan Iptables Persistent.
3.Sistem notifikasi yang dibangun menggunakan *email* dan Telegram.
4.Metode yang digunakan untuk monitoring jaringan adalah metode ICMP Ping.
5.Tidak menyimpan log penyerang dalam pengamanan terhadap DDoS Attack.

# 2. Tinjauan Pustaka

## 2.1 Sistem Saat Ini

Pada sistem yang sudah ada saat ini, sistem monitoring jaringan dibangun menggunakan WhatsUp Gold, yaitu aplikasi berbasis Flash yang berjalan di atas sistem operasi Windows. Cara kerja sistem WhatsUp Gold adalah dengan mengirimkan Ping kepada klien yang terdaftar dan menampilkan informasi ketersediaan akses kepada *user* melalui tampilan desktop. Kekurangan WhatsUp Gold adalah tidak dapat diakses melalui komputer yang tidak terpasang WhatsUp Gold dan tidak dapat dimodifikasi dengan bebas.




**Gambar 2.1. Gambar Sistem Saat Ini**

## 2.2. Teori

### 2.2.1. PT PLN TJBT-APP Bandung

PT PLN TJBT-APP Bandung merupakan salah satu kantor cabang PT PLN. Kantor ini berlokasi di Jl. Moch Toha km 4 Komplek PLN Cigelereng, Bandung[2]. Salah satu divisi kerja di PT PLN TJBT-APP Bandung adalah divisi Teknologi Informasi (TI). Salah satu tugas divisi TI adalah melakukan monitoring jaringan[3].

### 2.2.2. Monitoring Jaringan

Monitoring jaringan adalah kegiatan mengumpulkan data yang berjalan dalam jaringan untuk dipantau dan dianalisa sehingga menghasilkan informasi[4]. Salah satu sistem monitoring jaringan yang ada adalah WhasUp Gold, yaitu sistem monitoring berbasis Flash yang berjalan di atas sistem operasi Windows.

### 2.2.3 Ubuntu

Ubuntu adalah salah satu distribusi Linux berbasis Debian dan memiliki antarmuka desktop[5]. Sistem operasi Ubuntu tersedia secara bebas dan mempunyai banyak pengembang dari seluruh dunia. Kelebihan utama dari sistem operasi Ubuntu adalah sifatnya yang *open source* dan juga kompatibilitas Ubuntu dengan hampir semua perangkat keras terbaru.

### 2.2.4 Zabbix

Zabbix adalah perangkat lunak sistem monitoring jaringan yang bersifat *open source*[6]. Zabbix

terdiri dari Zabbix Server, Zabbix Frontend, dan Zabbix Agent. Zabbix Server berfungsi untuk melakukan tugas-tugas di belakang layar yang tidak diketahui oleh pengguna. Zabbix Frontend adalah tampilan antarmuka yang diakses melalui *web broser* oleh pengguna. Semua perintah yang dimasukkan oleh pengguna melalui Zabbix Frontend akan dikerjakan oleh Zabbix Server. Zabbix Agent adalah sebuah layanan yang berjalan di komputer klien. Zabbix Agent berfungsi untuk mengirimkan data layanan dan aktifitas yang berjalan pada klien kepada server[7].

### 2.2.5 Web Application Firewall (WAF)

WAF adalah aplikasi yang menyaring, memantau, dan memblokir ancaman-ancaman pada *website*. Salah satu aplikasi WAF yang ada adalah ModSecurity. Beberapa serangan yang dapat diatasi oleh ModSecurity adalah SQL Injection dan DDoS Attack.

### 2.2.6 SQL Injection

SQL Injection adalah teknik yang digunakan untuk menyerang *database* sebuah aplikasi *web*. Tujuan utama dari serangan ini adalah mendapatkan informasi dan penggunaan basis data di server aplikasi web[8].

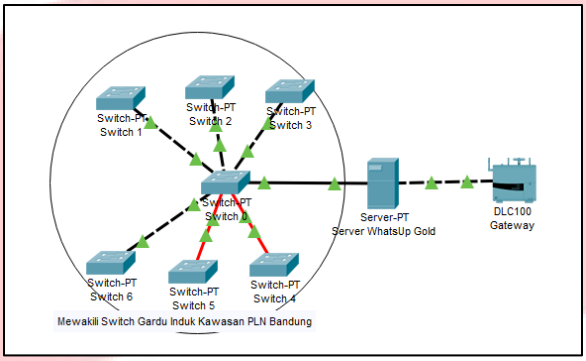
### 2.2.7 DDoS Attack

*Distributed Denial of Service* (DDoS) adalah salah satu metode penyerangan yang digunakan oleh *hacker*. Tujuan dari DDoS Attack adalah untuk membanjiri lalu lintas jaringan pada server, sehingga server terbebani dan tidak bisa memberikan layanan kepada klien. Cara yang paling sederhana untuk melakukan DDoS Attack adalah dengan mengirimkan *request* yang besar secara terus menerus kepada server[9].

## 3. Analisis dan Perancangan

### 3.1 Analisis

### 3.1.1 Gambaran Sistem Saat ini

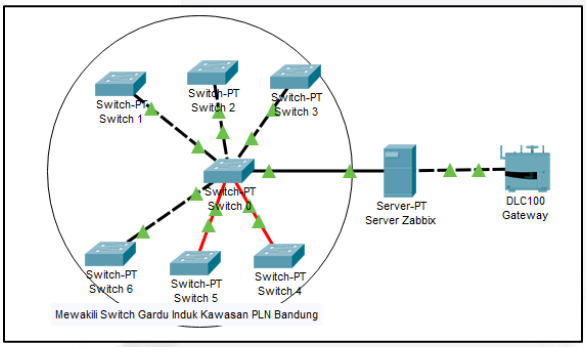



**Gambar 3.1 Gambaran Sistem Saat Ini**

Sistem monitoring yang sudah ada saat ini menggunakan perangkat lunak WhatsUp Gold. Salah satu kelemahan WhatsUp Gold adalah sistemnya yang dibangun menggunakan Flash, sehingga hanya dapat diakses melalui komputer yang sudah terpasang aplikasi WhatsUp Gold. Selain itu WhatsUp Gold juga tidak bersifat *open source* sehingga tidak dapat dimodifikasi secara bebas.

Cara kerja sistem saat ini adalah dengan mengirimkan Ping kepada klien. Apabila ada klien yang tidak berhasil dikirim Ping, makan sistem menganggap klien tidak terhubung dengan server dan menampilkannya melalui antarmuka aplikasi WhatsUp Gold.

### 3.1.2 Gambaran Sistem Usulan



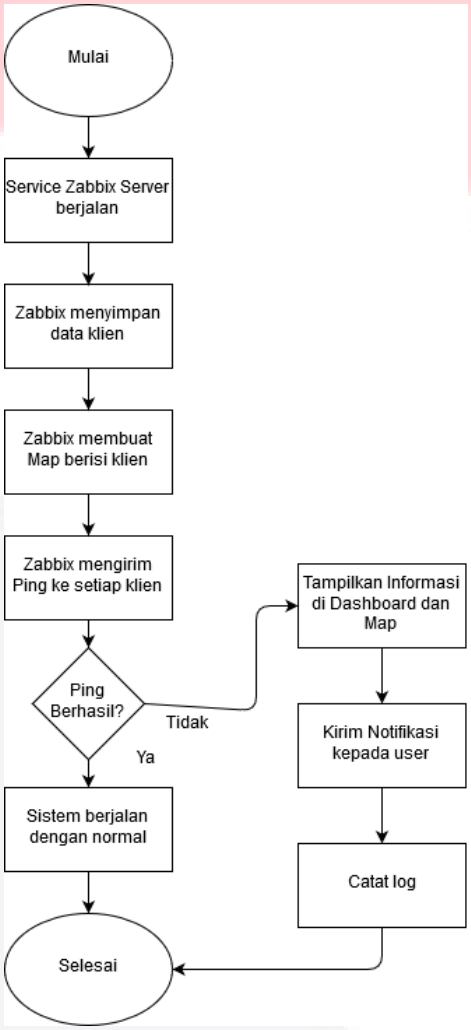

**Gambar 3.2 Gambar Sistem Usulan**

Gambar 3.2 merupakan sistem usulan monitoring jaringan menggunakan Zabbix. Cara kerja sistem usulan tidak jauh berbeda dengan cara kerja sistem yang sudah ada. Hanya saja terdapat penambahan sistem notifikasi menggunakan Telegram pada Zabbix. Zabbix dapat diakses dari *web browser* di klien mana pun yang terhubung dengan server dan bersifat *open source* sehingga dapat dimodifikasi dengan bebas.

### 3.1.3 Flowchart Sistem

Terdapat 2 flowchart sistem, yaitu flowchart Zabbix dan flowchart WAF.

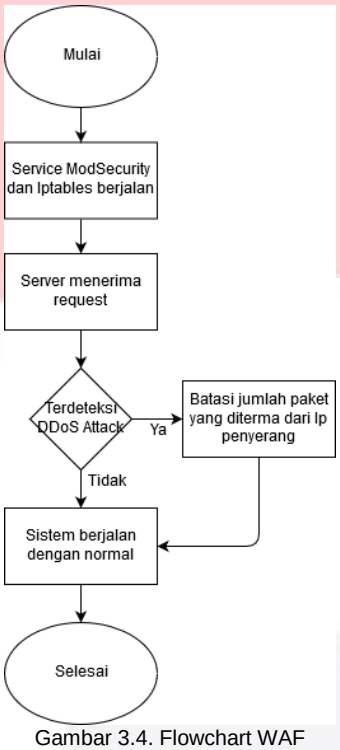
#### 3.1.3.1 Flowchart Zabbix




**Gambar 3.3 Flowchart Sistem**

Sistem dimulai dengan pendataan alamat Ip klien oleh Zabbix. Kemudian dibuat *map* Zabbix untuk mempermudah proses monitoring klien. Selanjutnya Zabbix mengirim Ping secara berkala kepada setiap klien yang terdaftar. Apabila ada klien yang tidak berhasil dikirim Ping, Zabbix memunculkan informasi ini pada *dashboard* dan *map* Zabbix serta mengirim notifikasi kepada *user*. Kegiatan ini kemudian disimpan dalam *log* Zabbix.

#### 3.1.3.2 Flowchart WAF




Gambar 3.4. Flowchart WAF

Sistem WAF dimulai dengan melakukan konfigurasi pada ModSecurity dan Iptables Persistent. Kemudian dimulai penyerangan, apabila server menerima *request* melebihi batas yang ditentukan dalam konfigurasi, maka server membatasi jumlah *request* yang masuk dari Ip penyerang sesuai dengan konfigurasi yang dilakukan sehingga sistem tetap berjalan dengan normal.

### 3.1.4 Analisis Kebutuhan Fungsional dan Non Fungsional

Sistem akan dibuat untuk melakukan kegiatan monitoring jaringan dan menampilkan informasi apabila terdapat klien yang tidak terhubung dengan server melalui antarmuka Zabbix dan media komunikasi *user*.

Kebutuhan Fungsional

1.Mencatat data klien berupa nama klien dan alamat Ip.

2.Membuat *map* yang terdiri dari klien yang dimonitoring.

3.Mengirim Ping kepada setiap klien untuk memastikan klien terhubung dengan server.

4.Mengirim notifikasi kepada *user* apabila terdapat klien yang tidak terhubung dengan server.

5.Menampilkan informasi ketersediaan klie secara *real time* kepada *user*.

Kebutuhan Non Fungsional

1.Dibutuhkan Akses Poin dan Mikrotik untuk menghubungkan klien dan server dalam satu jaringan.

2.Dibutuhkan Virtual Box untuk membuat klien secara virtual.

3.Dibutuhkan sistem operasi Ubuntu untuk menjalankan Zabbix dan WAF.

4.Dibutuhkan sistem operasi Kali Linux untuk menjalankan Http Slowloris dan PyLoris.

## 4. Implementasi dan Pengujian

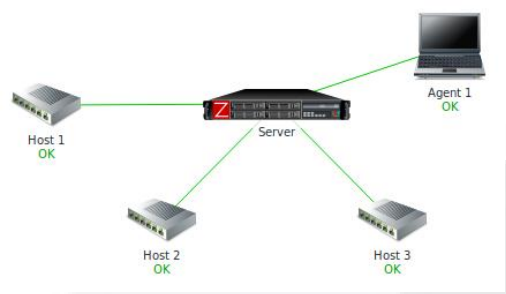
Implementasi sistem dilakukan dengan melakukan instalasi sistem Zabbix dan WAF. Kemudian melakukan konfigurasi *user*, media, *map,* klien dan sistem notifikasi.

### 4.2 Pengujian

Terdapat 3 pengujian yang dilakukan, yaitu pengujian *map* dan *dashboard* Zabbix; pengujian notifikasi Zabbix; dan pengujian WAF.

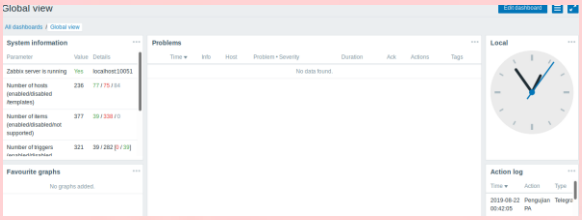
### 4.2.1. Pengujian Map dan Dashboard Zabbix

Tujuan dilakukannya pengujian *map* dan *dashboard* Zabbix adalah untuk mengetahui apakah Zabbix dapat menampilkan informasi ketersediaan akses setiap klien.



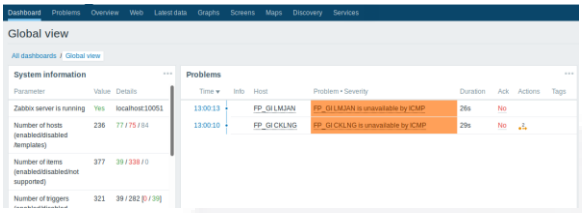

Gambar 4.1. *Map* Zabbix normal

Gambar 4.1. adalah tampilan *map* Zabbix ketika sistem berjalan dengan normal, yaitu tidak ada klien yang tidak terhubung dengan server. Informasi yang ditampilkan adalah ikon klien dan nama klien.



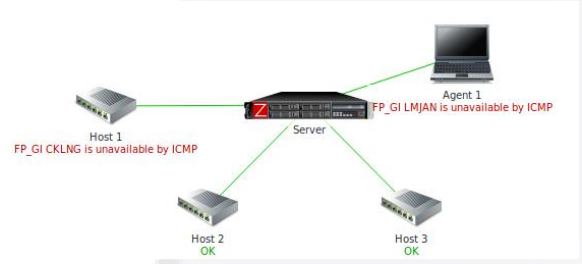

Gambar 4.2. *Dashboard* Zabbix normal

Gambar 4.2 adalah tampilan *dashboard* Zabbix ketika sistem berjalan normal tanpa ada klien yang tidak terhubung dengan server. kolom “Problems” menampilkan informasi klien yang tidak terhubung dengan server.




Gambar 4.3. *Dashboard* Zabbix dengan *problem*

Gambar 4.3. adalah tampilan *dashboard* Zabbix ketika ada klien yang tidak terhubung dengan server. Informasi yang ditampilkan adalah waktu terjadi *problem*, nama *problem*, dan *action* yang dilakukan.



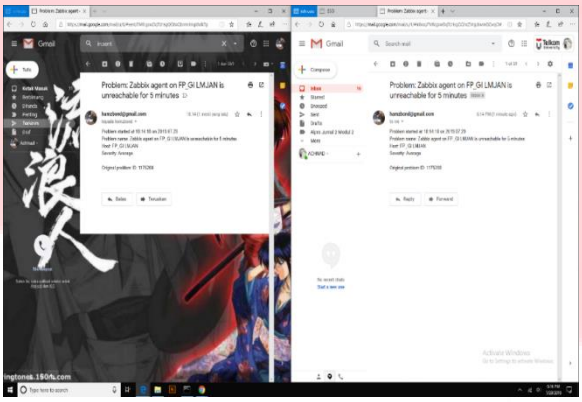

Gambar 4.4. *Map* Zabbix dengan *problem*

Gambar 4.4. adalah tampilan *map* Zabbix ketika terdapat klien yang tidak terhubung dengan server. Perubahan informasi yang ditampilkan adalah nama *problem* dalam teks berwarna merah.

### 4.2.2.Pengujian Notifikasi Zabbix

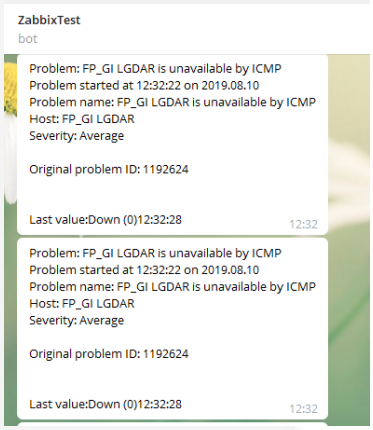
Tujuan dilakukannya pengujian notifikasi Zabbx adalah untuk mengetahui apakah Zabbix berhasil mengirimkan notifikasi kepada *user* apabila

terdapat klien yang tidak terhubung dengan server.



Gambar 4.5. Notifikasi Zabbix melalui *Email*

Gambar 4.6 terdiri dari 2 gambar, di sebelah kiri adalah gambar "Pesan Terkirim" pada *email* server Zabbix dan di sebelah kanan adalah "Pesan Masuk" pada *email user* Zabbix. Informasi yang dikirimkan melalui media *email* adalah nama *problem* dan waktu terjadi *problem*.

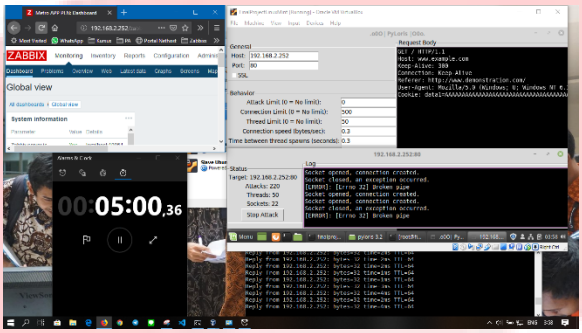



Gambar 4.6. Notifikasi Zabbix melalui Telegram

Gambar 4.6 adalah notifikasi Zabbix yang dikirimkan melalui Telegram. Informasi yang dikirimkan melalui media Telegram adalah nama *problem* dan waktu terjadi *problem*.

### 4.2.3. Pengujian *WAF*

Tujuan dilakukannya pengujian WAF adalah untuk mengetahui apakah ModSecurity dan Iptables Persistent berhasil melindungi server dari serangan DDoS Attack.




Gambar 4.7. Pengujian DDoS Attack dengan PyLoris

Gambar 4.7 adalah pengujian DDoS Attack menggunakan PyLoris. Server diserang menggunakan DDoS Attack selama 5 menit dengan "Attack Limit" dan "Connection Limit" tidak terbatas, namun ping kepada server tetap normal dengan delay 2-5 ms.

## 5. Kesimpulan dan Saran

### 5.1 Kesimpulan

Setelah melakukan pengujian terhadap sistem presensi menggunakan face recognition, maka dapat disimpulkan bahwa:

1.Sistem monitoring jaringan menggunakan Zabbix berhasil dibangun di PT PLN (Persero) TJBT-APP Bandung.

2.Pada pengujian *map* dan *dashboard* Zabbix, informasi klien yang tidak terhubung berhasil ditampilkan pada *map* dan *dashboard* Zabbix dengan selang waktu antara 8-10 detik.

3.Pada pengujian notifikasi Zabbix, informasi klien yang tidak terhubung dengan server berhasil dikirim melalui media *email* dan Telegram secara langsung ketika informasi muncul di *dashboard* Zabbix.

4.Pada pengujian WAF, ModSecurity dan Iptables berhasil melindungi server Zabbix dari serangan DDoS Attack menggunakan Http Slowloris dan PyLoris sehingga sistem Zabbix dapat tetap berjalan dengan normal meskipun mendapat serangan DDoS Attack.

### 5.2 Saran

Sistem monitoring jaringan menggunakan Zabbix dapat dikembangkan lebih lanjut. Disarankan untuk kedepannya server Zabbix diberikan akses Ip public sehingga sistem Zabbix dapat diakses

dari luar area jaringan PT PLN TJBT-APP Bandung. Sistem Zabbix disarankan untuk ditambahkan integrasi dengan sistem *ticketing*.

## 6. Daftar Pustaka

[1] D. Wijonarko, “Zabbix Network Monitoring Sebagai Perangkat Monitoring Jaringan Di,” *J. ELTEK*, 2014.

[2] A. N. S, “Perancangan Alat Monitoring Suhu pada Trafo Tegangan Tinggi dengan Menggunakan Sensor MLX90614 dan SMS Gateway Berbasis Arduino UNO di PT PLN (Persero) Transmisi Jawa Bagian Tengah-Area Pelaksana Pemeliharaan,” 2017.

[3] A. Hamzah, “Monitoring Jaringan Internet Menggunakan Zabbix di PT PLN (PERSERO) Transmisi Jawa Bagian Tengah - Area Pelaksanaan dan Pemeliharaan Bandung,” p. 30, 2018.

[4] W. M. C. Silva, R. M. Medeiros, and R. S. Martins, “ANALYSIS AND NETWORK MANAGEMENT USING A PROACTIVE METHODOLOGY WITH ZABBIX,” *HOLOS*, 2015.

[5] L. Floyd, “Ubuntu,” in *Emergent Possibilities for Global Sustainability: Intersections of Race, Class and Gender*, 2016.

[6] A. D. Vacche and S. K. Lee, *Mastering Zabbix*. 2015.

[7] A. D. Vacche and S. K. Lee, “Zabbix Network Monitoring Essentials,” 感染症誌, vol. 91, pp. 399–404, 2017.

[8] OWASP INJECTION, “SQL Injection Prevention Cheat Sheet,” *2016*, 2016.

[9] S. Karthik, V. . Dr. Arunachalam, and Dr.T.Ravichandran, “An Analysis of DDOS Method, Threats, Tools and Defense Mechanisms,” pp. 1–25.