p-ISSN 2086-7395
http://ejournal.unsub.ac.id/index.php/Fasilkom

SISTEM INFORMASI MONITORING SERANGAN KEAMANAN MAIL SERVER DI YAYASAN ASSYIFA AL-KHOERIYYAH

Aldy Kustyandi[1], Sofwandi Noor[2]
Ilmu Komputer Universitas Subang

[1]aldykustyandi@gmail.com

Abstrak

Serangan *brute force* adalah serangan keamanan yang menggunakan algoritma percobaan terhadap seluruh kemungkinan kunci akses sebuah sistem yang biasanya juga di sebut algoritma *brute force*, serangan *brute force* dapat terjadi pada segala aspek sistem komputer baik berupa sistem komputer server maupun komputer client. Serangan *brute force* selain dapat memecahkan sebuah kunci masuk sebuah sistem, serangan *brute force* juga dapat menghabis kan resource sebuah sistem komputer. peneliti membatasi pembahasan pada aspek serangan *brute force* pada layanan SSH (secure shell) sebuah mail server di yayasan asyifa al-khoeriyyah, hal ini di karenakan serangan *brute force* dapat terjadi di segala aspek sistem komputer dari mulai *brute force* pada sistem aplikasi komputer berbasis web hingga serangan *brute force* pemecahan kunci akses sebuah personal komputer oleh program malware sehingga hal ini membutuhkan pembahasan yang lebih luas. Hasil dari penelitian penulis menemukan bahwa penanganan serangan *brute force* yang saat ini berjalan pada mail server di yayasan assyifa al khoeriyyah kurang maksimal dikarenakan informasi serangan hanya dalam bentuk log file dan notifikasi yang akan di rotasi dan di hapus, maka penulis menyimpul kan yayasan assyifa al khoeriyah membutuhkan sebuah sistem inforamsi yang dapat membantu mengelola data serangan tersebut.

Keywords: *brute force, sistem informasi, serangan keamanan*.

Pendahuluan

Perkembangan teknologi dan ilmu pengetahuan pada masa globalisasi ini dirasakan telah semakin pesat, perkembangan teknologi ini dikarenakan hasil dari pemikiran manusia yang semakin maju. Hal tersebut dapat di lihat dari perkebangan ilmu komputer yang semain hari semakin berkembangan dengan pesat. Perkembangan teknologi semakin mendukung bagi penyebaran informasi yag bermanfaat kepada masyarakat luas dan dapat menjangkau segala lapisan. Salahsatu media penyebaran informasi yang dapat menjangkau segala lapisan dan tidak terbatas pada batas-batas geografis adalah internet Namun di sisi lain internet bisa menjadi sebuah alat yang berbahaya baik dengan mudah tersebarnya konten negatif seperti konten pornografi dan sebagain nya, ataupun mudah nya aktifitas-aktiftas kriminal yang berbasis *cyber*, dengan semakain terbuka nya akses informasi melalui internet seseorang dapat dengan mudah mengakases sebuah konten tentang tatacara melakukan hacking atau kejahatan cyber lain nya, seseorang dapat dengan mudah saling berkomunikasi dan berkoordinasi dengan orang lain nya di belahan bumi yang berbeda untuk merancanakan serta merancang sebuah aksi criminal yang be basis cyber.

Salah satu jenis serangan *hacking* atau gangguan pada server di ineternet adalah *brute force*, Salahsatu teknik penanganan serangan *brute force* adalah dengan menggunakan aplikasi

p-ISSN 2086-7395
http://ejournal.unsub.ac.id/index.php/Fasilkom

intrusion prevention system yang dinamakan fail2ban, 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 (Kurniawan, Mulyanto, & Nandiasa, 2016), namun fail2ban adalah sebuah tool yang berbasis cli (*command line interface*) dan informasi *blocking* hanya tertulis di sebuah log file sehingga cukup menyulitkan untuk proses manajemen dan pengolahan informasi serangan nya, serta penanganan untuk jangka panjang terhadap sebuah ip yang telah melakukan serangan secara berkali kali. Yayasan assyifa al khoeriyyah dalam penanganan nya terhadap serangan *brute force* menggunakan fail2ban, namun fail2ban yang saat ini berjalan masih menggunakan aplikasi fail2ban yang default standar konfigurasi untuk penangan serangan *brute force* dan serangan lain nya . Secara default fail2ban dalam menulis informasi serangan yang terjadi pada server kedalam sebuah log file kedalam /var/ log/fail2ban.log. Fail2ban di yayasan assyifa al khoeriyyah terpasang di mail server yang kondisi nya di pasang langsung berada di publik interface tanpa ada lagi firewall yang berda di depan nya
sehingga fail2ban menjadi salah satu firewall utama untuk server terebut. Namun fail2ban yang di konfigurasi hanya secara standar menjadikan informasi serangan hanya bersifat sementara yang hanya di tulis kedalam sebuah log file yang kemudian log file tersebut akan di rotasi dan kemudian di hapus.

Maka berdsarkan uraian di atas diperlukan sebuah sebuah sistem inforamsi yang berbasis GUI *graphical user interface*) yang dapat memudahkan pengelolaan data serangan *Brute force* yang di hasilkan dari fail2ban untuk dapat membantu seorang administrtor jaringan dalam melakukan tindakan penangan terhadap serangan dan pengambilan keputusan untuk penanganan jangka panjang. Informas serangan *brute force* dari fail2ban jika di simpan kedalam database akan bermanfaat untuk menampilkan informasi informasi penting yang akan bermanfaat untuk penangan serangan di masa yang akan datang.

Kajian Teori

Keamanan Sistem

Keamanan informasi didefinisikan secara singkat dan sederhana sebagai proses menjaga kerahasiaan, integritas dan ketersediaan informasi, tiga hal fundamental yang biasa dikenal sebagai C-I-A triad atau triad keamanan informasi (Lenawati, Winarno, & Amborowati, 2017). Keamanan sistem merupakan proses menjaga sebuah sistem komputer dari akses yang tidak berhak dan proses menjaga kerahsiaan, integritas dan ketersediaan sumberdaya komputer tersebut yang di guakan untuk melayani apliaksi yang berjalan di atas nya.

Serangan *Brute force*

A Brute Force attack is a method or an algorithm to determine a password or user name using an automatic process. Sebuh serangan brute force adalah metode atau sebuah algoritma yang di gunakan untuk menentukan sebuah *password* atau *user name* menggunakan sebuah proses otomatis (Karawash, 2016).

Gambaran singkat tehnik serangan bruteforce

p-ISSN 2086-7395
http://ejournal.unsub.ac.id/index.php/Fasilkom

Teknik serangan *brute force* bukanlah teknik hacking yang serumit yang berkembang saat ini, seorang penyerang hanya perlu mencoba semua kombinasi user dan passowrd yang cocok yang di gunakan untuk melakukakan akses ke dalam sebuah sistem komputer, inti teknik *Brute force* adalah dengan mencoba seluruh kemungkinan password yang dapat di gambarkan dengan formula sebagai berikut :

Tabel 1 Formula algoritma serangan bruteforce

KS = $L^{(m)} + L^{(m+1)} + L^{(m+2)} + \ldots\ldots\ldots\ldots\ldots + L^{(m)}$
L = Jumlah karakter yang kita ingin definisakan m= Panjang minimum dari kunci M=Panjang maksimal dari kunci

pada penerapan nya, ketika seorang penyerang ingin memecah kan sebuah password dengan karakter set "ABCDEFGHIJKLMNOPQRSTUVWXYZ" dengan Panjang password 7 karakter misal "rahasia" maka jumlah percobaan password yang butuhkan untuk memecahkan password tersebut adalah:

Tabel 2 Perhitungan banyak kombinasi percobaan yang di butuhkan

KS = $26^{(1)} + 26^{(1+1)} + 26^{(1+2)} + 26^{(1+3)} + \ldots\ldots\ldots\ldots\ldots 26^{(1+7)}$
$= 26 + 676 + 17576 + 456976 + 11881376 + 308915776 + 8031810176 + 208827064576$
$= 217180147158$

Dari perhitunga diatas didapatkan untuk dapat meretas password "rahasia" di butuhkan 217180147158 kali password yang harus di coba.

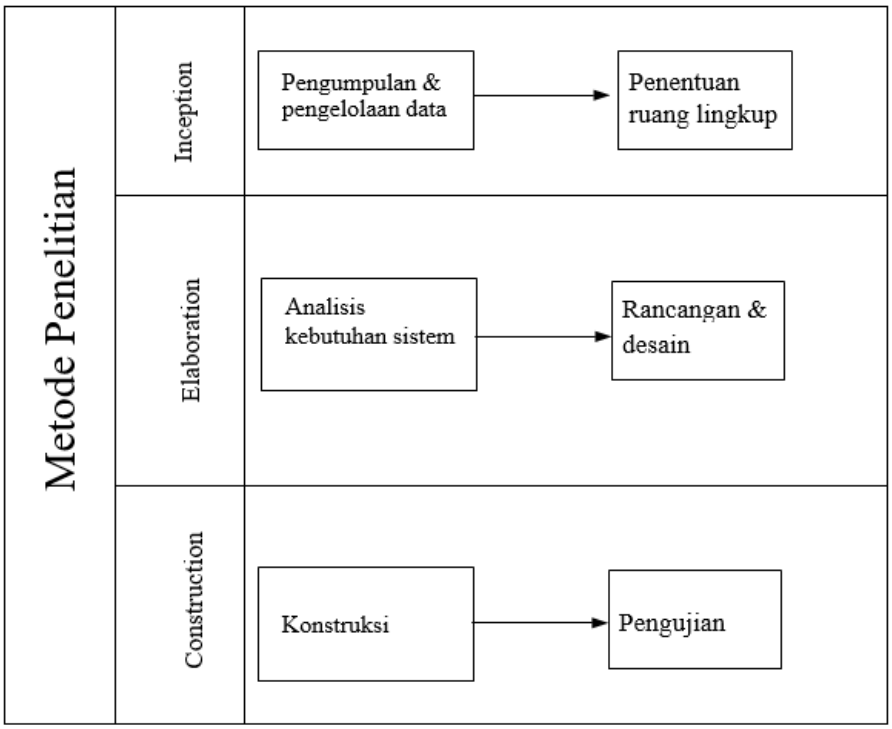
Dampak serangan bruteforce terhadap sebuah sistem komputer

Serangan brute force jika menyerang sebuah host di dalam jaringan akan membuat koneksi secara terus menerus kepada komputer target guna melakukan percobaan login secara brutal, dalam kasus serangan dengan beberapa host zombie sekaligus melakukan brute force ke sebuah target yang sama akan menyebabkan banjir nya koneksi menuju target sehingga jika target adalah sebuah server, server tersebut akan menjadi seolah olah down. Dampak lain yang sangat dirasakan juga adalah habis nya resource sebuah komputer hanya untuk menangani proses percobaan login dari penyerang brute force tersebut baik berupa resource RAM, Bandwidth jaringan maupun CPU.

p-ISSN 2086-7395
http://ejournal.unsub.ac.id/index.php/Fasilkom

Metodologi

Adapun metodologi yang di gunakan pada penelitian ini adalah menggunakan metode penelitian pengembangan sistem dengan RUP (Relational Unified Process) yang penulis hanya akan mengacu pada tiga tahap dalam pengembangan sistem dengan RUP yaitu tahap inception, elaboration, dan construction.



Gambar 1 Metode Penelitian

1. Inception

1. Tahap pengumpulan data
   Pada tahap ini penulis melakukan studi literatur dan melakukan observasi langsung lapangan, untuk melihat kondisi object penelitian dan interkasi interkasi yang terjadi dari object yang akan penulis teliti, kemudian data dan informasi yang di dapat akan di gunakan untuk pengembangan di tahap selanjutnya. Penulis juga akan melakukan studi literatur melalui buku, jurnal ilmiah dan sumber lain guna mendukung penelitian.
2. Tahap pengolaan data
   Pada tahap ini akan dilakukan analisis dan identifikasi terhadap permasalahan yang ada dari proses bisnis yang saati ini sedang berjalan dengan menggunakan data data dan informasi yang telah di kumpulkan sebelum nya.
3. Tahap penentuan ruang lingkup
   Pada tahap ini akan di tentukan seberapa besar ruang lingkup pengembangan sistem dalam penelitian, hal ini digunakan untuk membatasi pengerjaan analisis dan pembuatan desain agar tidak melebar dan lebih fokus. Penetuan ruang lingkup didapat dari proses pengumpulan data dan observasi lapangan.

p-ISSN 2086-7395
http://ejournal.unsub.ac.id/index.php/Fasilkom

2. Elaborasi

Pada tahap ini penulis akan melakukan perancangan sistem dari analisis kebutuhan proses bisnis yang saat ini berjalan kemudian hasil analisis akan diterpakan pada rancangan sistem yang akan di bangaun kemudian menentukan kebutuhan fungsional dan non fungsional sistem. Rancangan akan di visualisasikan dengan pemodelan UML (Unified Modeling Language) dan untuk memberikan gambaran sistem akan menggunakan use case diagram, class diagram dan sequence diagram.

3. Konstruksi

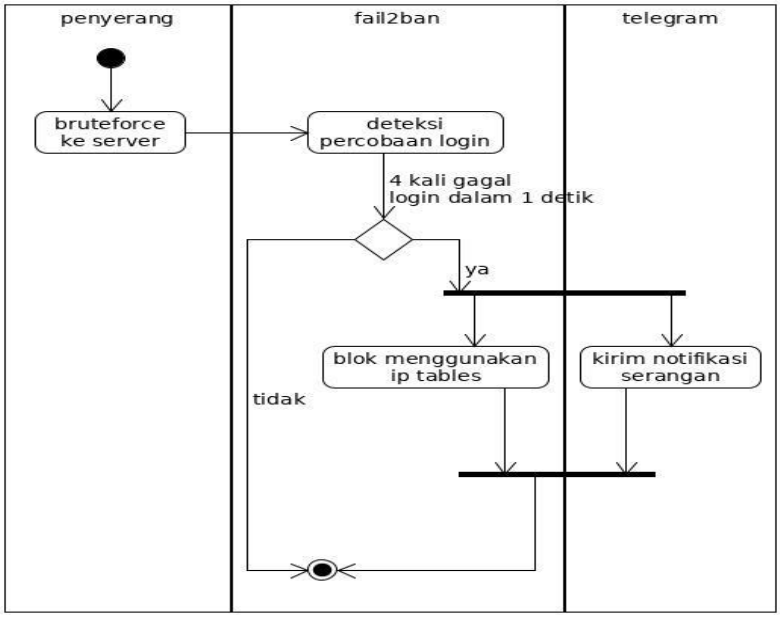
Pada tahap ini akan berfokus pada pengembangan apliaksi dari sisi penerpan rancangan menjadi coding yang kemudian dilakukan pengujian dari kebutuhan fungsional yang telah di tetapkan.

Hasil dan Pembahasan

Gambaran sistem yang berjalan di Assyifa

Dalam perkembangan yayasan assyifa al-khoeriyyah, yayasan menciptakan unit unit yang men support kegiatan utama yayasan yaitu dalam bidang pendidikan, dakwah dan sosial. Yayasan juga mengembangkan sistem informasi management untuk mendukung kegiatan kegiatan tersebut melalui unit IT yang ada, dalam bagian ini akan di terangkan sistem informasi yang saat ini berjalan di yayasan assyifa al-khoeriyyah.

1. Gambaran proses bisnis penangan serangan bruteforce yang berjalan saat ini



Gambar 2 Proses Bisnis Serangan Bruteforce

2. Kebutuhan fungsional sistem

p-ISSN 2086-7395
http://ejournal.unsub.ac.id/index.php/Fasilkom

Tabel 3 Kebutuhan Fungsional Sistem

Nomor SRS	Deskripsi	Aktor
SRS-F-1	Sistem mampu menangani login pengguna	administrator
SRS-F-2	Sistem mampu melakukan kelola data user	
SRS-F-2.1	Sistem mampu melakukan proses rubah password user	
SRS-F-2.2	Sistem mampu melakukan proses tambah pengguna	
SRS-F-2.3	Sisitem mam melakukan proses hapus penggunan	
SRS-F-3	Sistem mampu menampilkan statistik serangan bruteforce	
SRS-F-3.1	Sistem mampu menampilakan jumlah serangan hari ini	
SRS-F-3.2	Sistem mampu menampilkan hari saat serangan bruteforce terbanyak terjadi.	
SRS-F-3.3	Sistem mampu menampilkan total jumlah serangan	
SRS-F-3.4	Sistemmampumenampilkan jumlah ip yang telah di lakukan blacklist permanen (statis)	
SRS-F-4	Sistem mampu melakukan kelola data ip penyerang	
SRS-F-4.1	Sistem mampu menampilkan daftar ip penyerang	

3. Kebutuhan non fungsional sistem

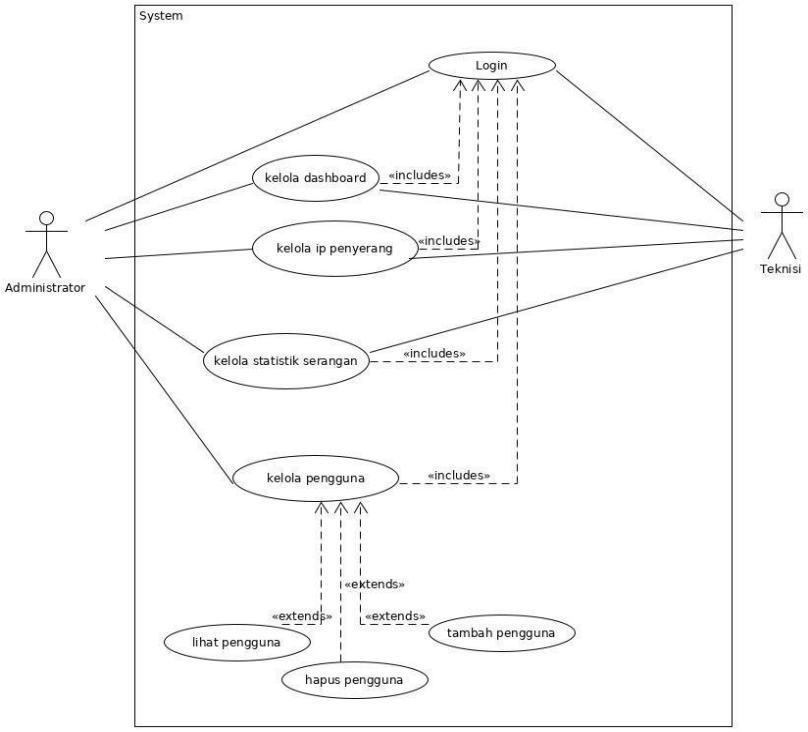
Tabel 4 Kebutuhan Non Fungsional

Nomro SRS	Deskripsi
SRS-NF-1	Sistem memiliki antar muka yang user friendly
SRS-NF-2	Sistem dapat dijalankan dengan berbagai web browser
SRS-NF-3	Sistem dapat melakukan query ke api ip geolocation
SRS-NF-4	Sistem menggunakan enskripsi password

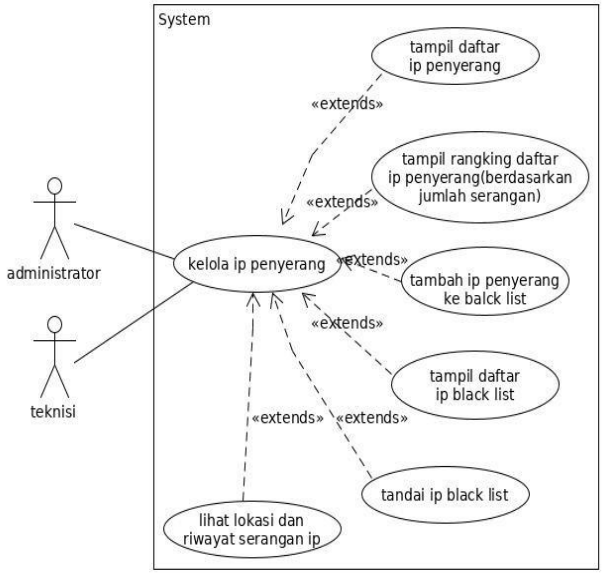
p-ISSN 2086-7395
http://ejournal.unsub.ac.id/index.php/Fasilkom

4. Use Case Diagram (keseluruhan)

Diagram usecase mendefinisikan perilaku dari sistem, Termasuk dari perilaku sistem adalah interaksi antara sistem dengan aktor – aktor penggunanya. Setiap usecase menggambarkan fungsionalitas yang disediakan oleh sistem untuk penggunanya. Gambar 3.3 memperlihatkan diagram usecase dari sistem yang akan dibangun.



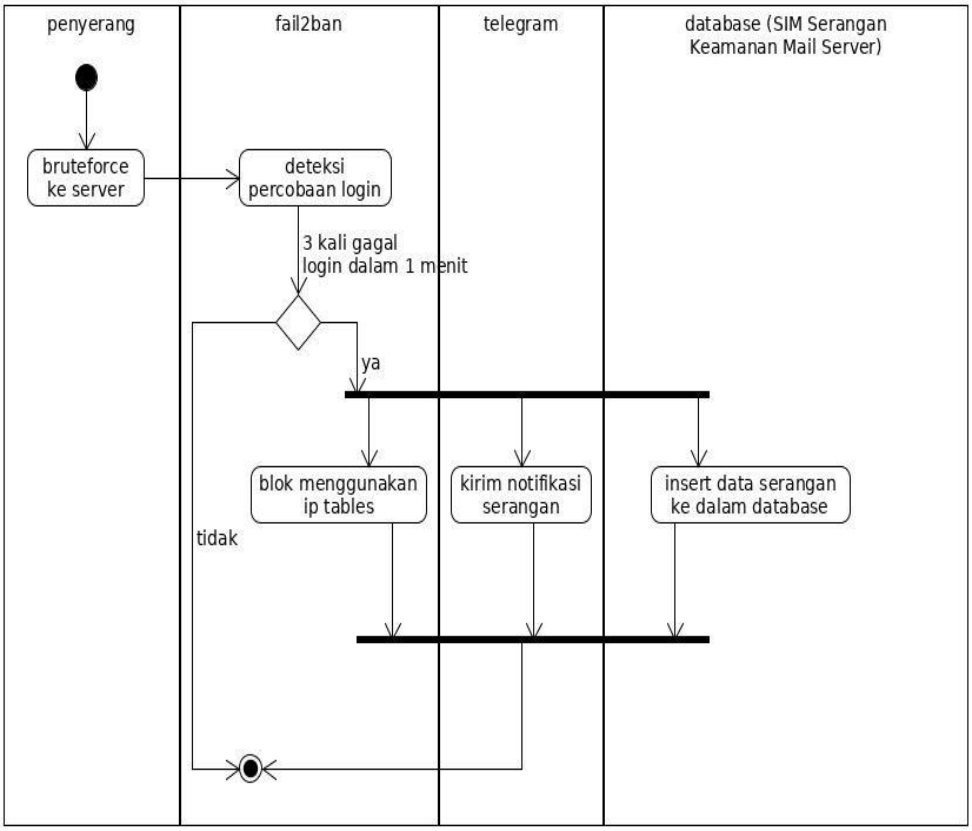
Gambar 3 Usecase Keseluruhan



Gambar 4 Usecase Kelola ip penyerang

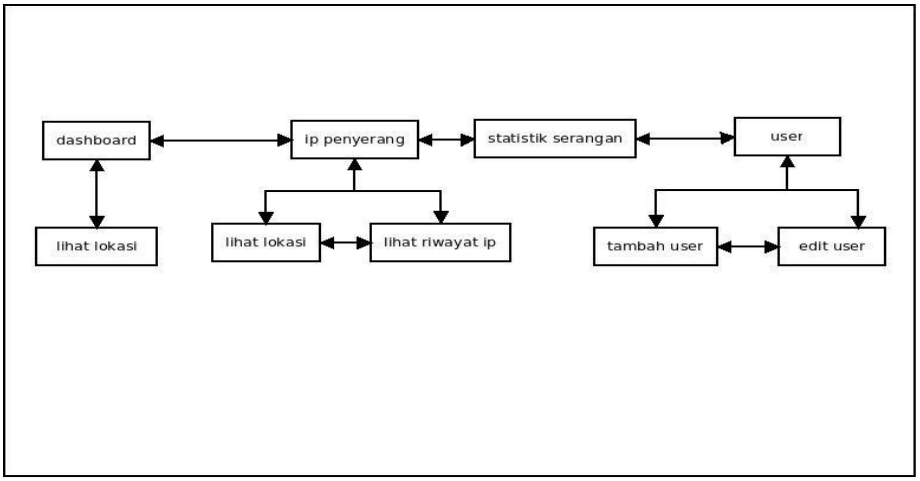
p-ISSN 2086-7395
http://ejournal.unsub.ac.id/index.php/Fasilkom

5. Proses bisnis penanganan bruteforce



Gambar 5 Proses Bisnis Penanganan Bruteforce

6. Rancangan diagram Navigasi Sistem

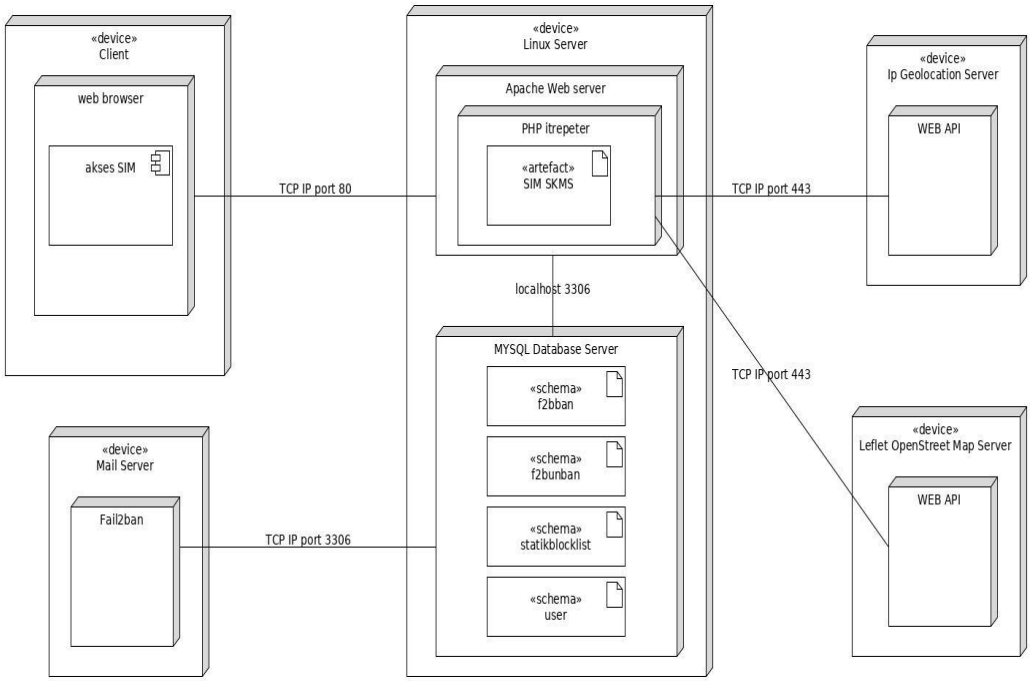


Gambar 6 Rancangan Diagram Navigasi Sistem

p-ISSN 2086-7395
http://ejournal.unsub.ac.id/index.php/Fasilkom

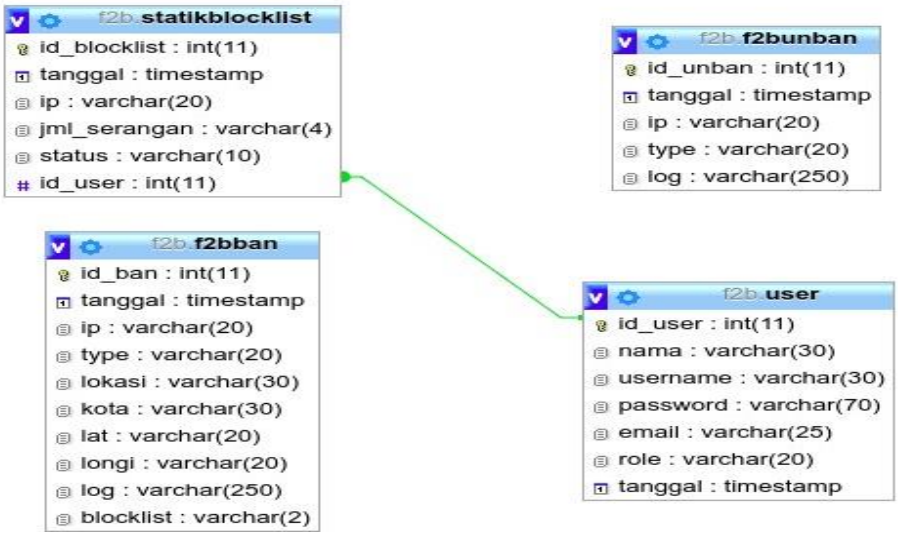
7. Deployment diagram

Deployment diagram di gunakan penulis untuk menggambarkan deployment view implementasi sistem informasi monitoring serangan keamanan mail server. Deployment diagram adalah sebuah tipe UML diagram yang menggambarkan implementasi arsitektur sistem yang mencakup hardware, software dan koneksi nya.



Gambar 7 Deployment Diagram

8. Relasi Tabel

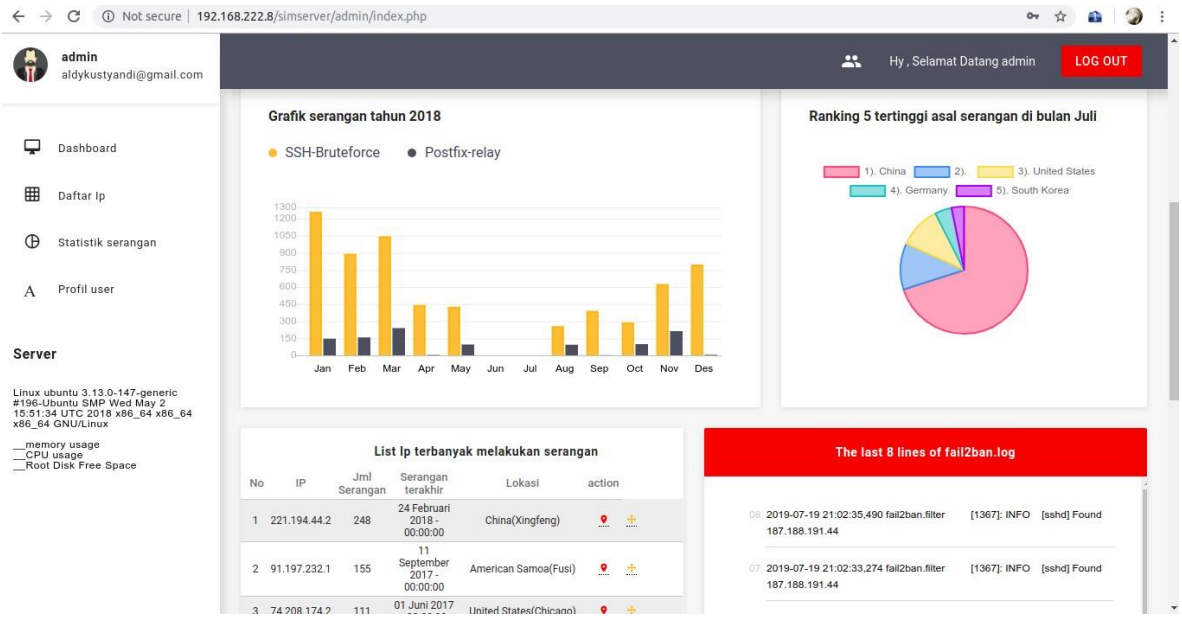


Gambar 8 Relasi Tabel Database

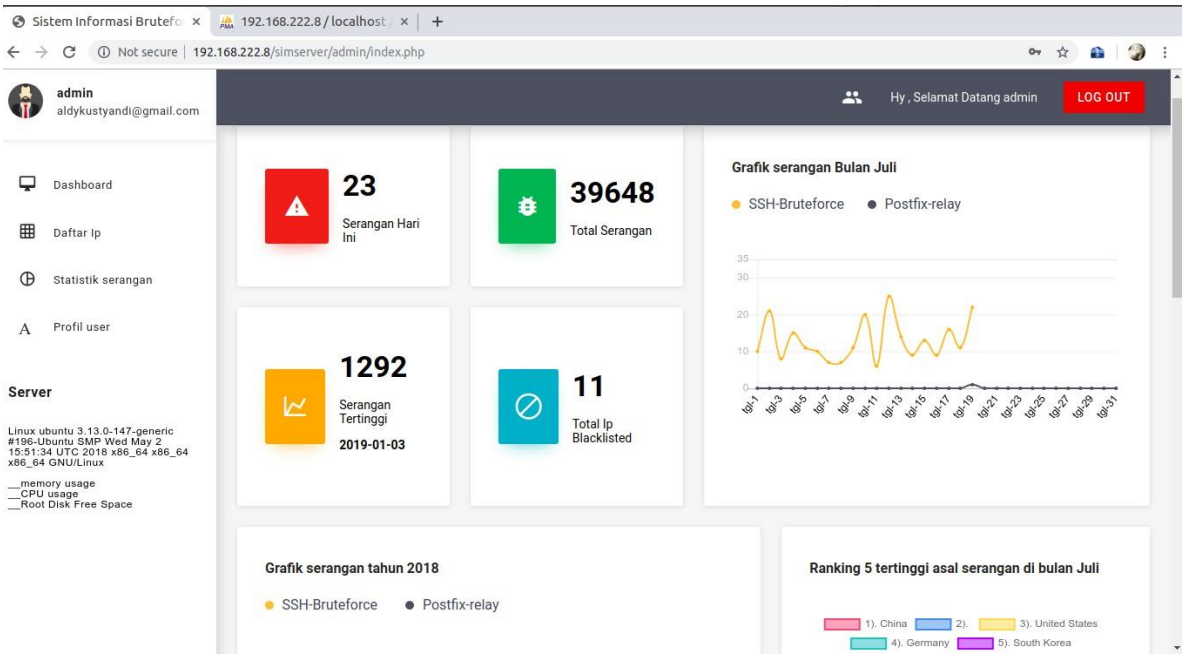
p-ISSN 2086-7395
http://ejournal.unsub.ac.id/index.php/Fasilkom

9. Tampilan Interface

a. Antarmuka dashboard



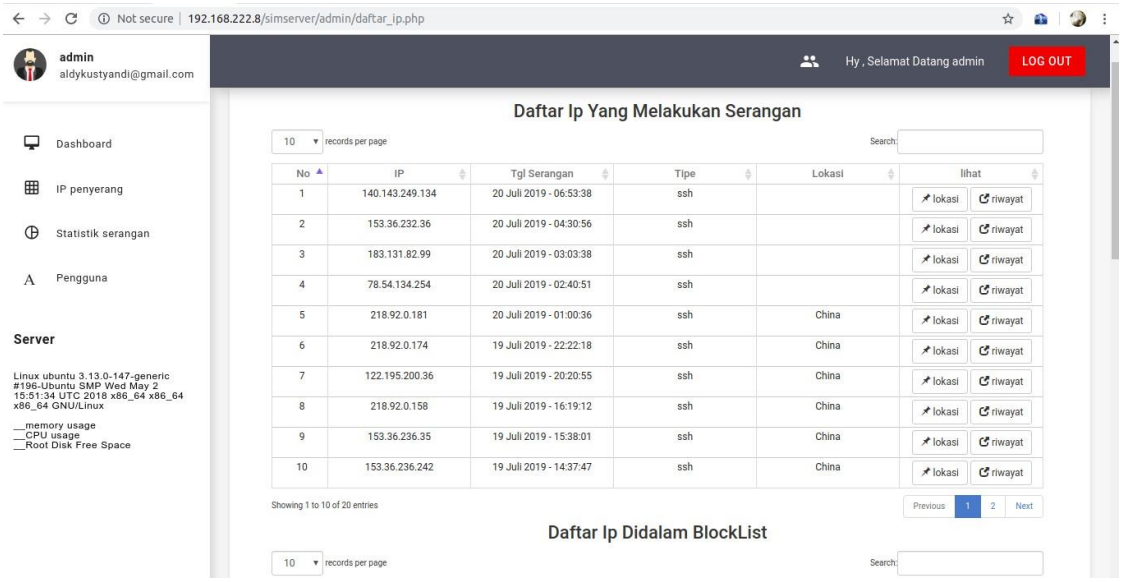
b.



Gambar 9 Antarmuka Dashboard

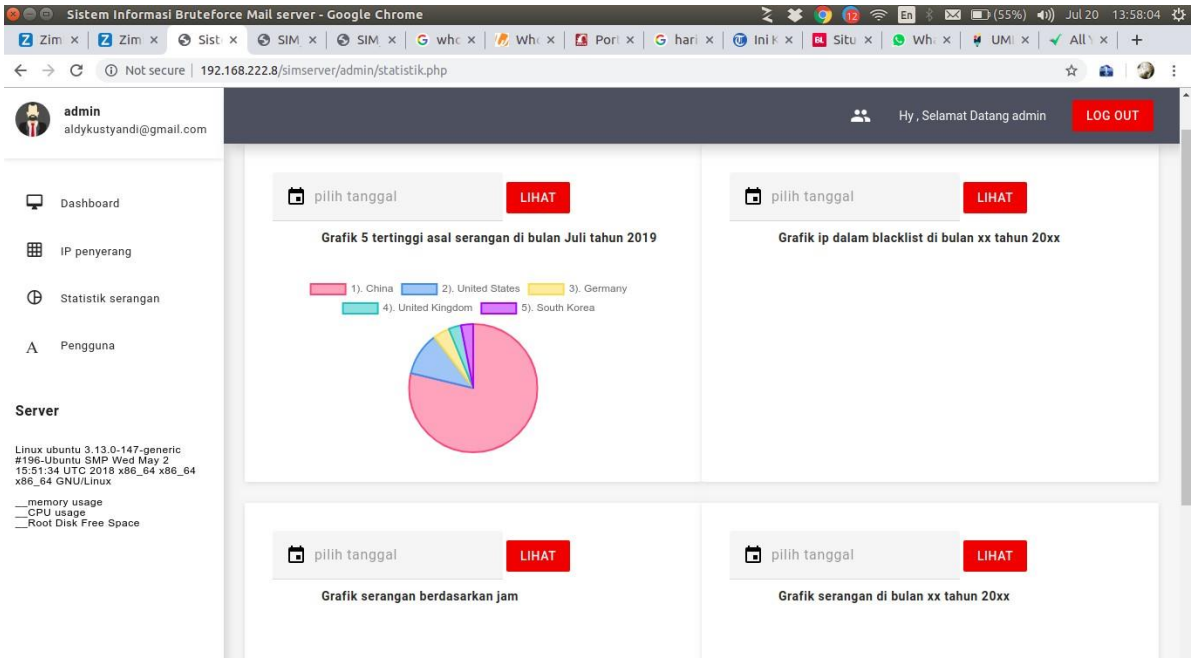
p-ISSN 2086-7395
http://ejournal.unsub.ac.id/index.php/Fasilkom

b. Antarmuka IP Penyerang



Gambar 10 Antarmuka IP Penyerang

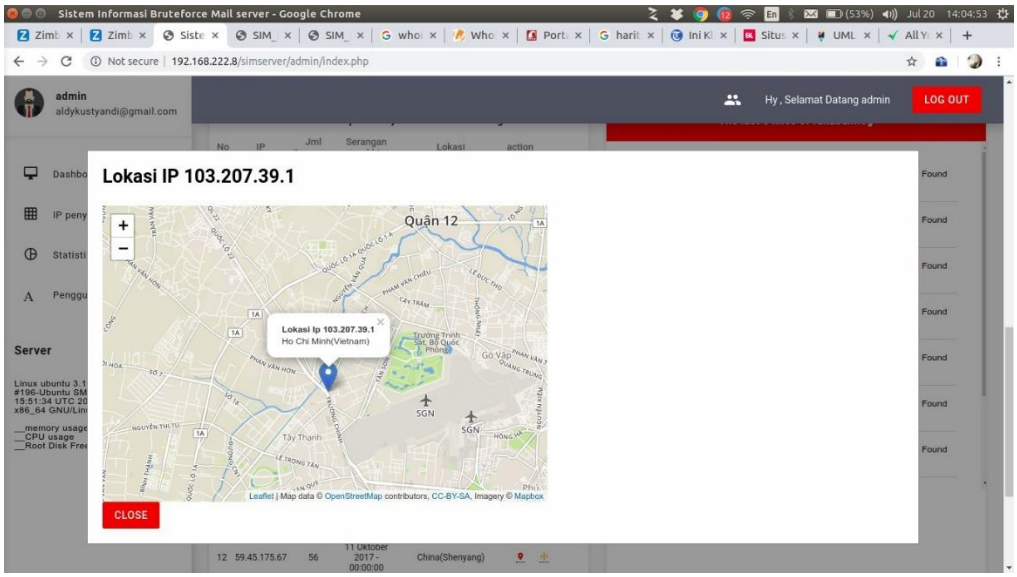
c. Antarmuka Statistik Serangan



Gambar 11 Antarmuka Statistik Serangan

p-ISSN 2086-7395
http://ejournal.unsub.ac.id/index.php/Fasilkom

d. Antarmuka Pop Up Lokasi IP Penyerang Halaman Dashboard



Gambar 12 Antarmuka Lokasi IP Penyerang

Penutup

Kesimpulan dari pembahasan pembangunan sistem informasi monitoring serangan keamanan mail server di yaysan assyifa al khoeriyyah dari mulai analisis, perancangan hingga implementasi adalah :

1. Sistem informasi yang di bangun dapat membantu mail server administrator dan teknisi jaringan di yayasan assyifa al khoeriyyah untuk mengetahui tren serangan dari waktu ke waktu.
2. Dengan adanya sistem ini data serangan tidaklah hilang sehingga dapat membantu dalam penentuan penangan serangan di masa depan.
3. Dengan adanya sistem ini riwayat serangan sebuah ip penyerang dengan data profil ip penyerang tersebut dapat tersimpan dengan baik dan mudah dicari sehinga mempercepat proses penangan serangan.

Daftar Pustaka

Karawash, A. (2016). Brute force attack - OWASP. *Owasp*, (April). Retrieved from https:// www.owasp.org/index.php/Brute_force_attack

Kurniawan, I., Mulyanto, F., & Nandiasa, F. (2016). Sistem Pencegahan Serangan Bruteforce Pada Ubuntu Server Dengan Menggunakan Fail2Ban. *Infomatek*, *18*(2), 96.

Lenawati, M., Winarno, W. W., & Amborowati, A. (2017). Tata Kelola Keamanan Informasi pada PDAM Menggunakan ISO/IEC 27001:2013 Dan COBIT 5. *Sentra Penelitian Engineering Dan Edukasi*, *9*(1), 44–49. https://doi.org/10.1007/978-981-10-2618- 8_18

Pramudita, K. E. (2011). Brute Force Attack dan Penerapannya pada Password Cracking, (2011), 6.

p-ISSN 2086-7395
http://ejournal.unsub.ac.id/index.php/Fasilkom

Sandra, S., Stiawan, D., & Heryanto, A. (2016). Visualisasi Serangan Brute Force Menggunakan Metode K-Means dan Naïve Bayes, *2*(1), 315–320.

Somya Ramos, Suprihadi, landhung budi prasetyo. (2012). M edication E vent M onitoring S ystem, *3*(5), 99–110.