PERANCANGAN PENGAMANAN SERVER APACHE MENGGUNAKAN FIREWALL IPTABLES DAN FAIL2BAN

Rizky Ramadhan[1)], Jonny Latuny[2)], Samy J. Litiloly[3)]

[1)]S1 Teknik Mesin Fakultas Teknik, Universitas Pattimura
Email: ramadhan15101999@gmail.com,
[2)]Prodi Teknik Mesin, Fakultas Teknik, Universitas Pattimura
Email: jonny.latuny@staff.unpatti.ac.id,
[3)]Prodi Teknik Mesin, Fakultas Teknik, Universitas Pattimura
Email: sj.litiloly@fatek.unpatti.ac.id,

Abstrak

Penelitian ini membahas mengenai pemanfaatan firewall dan fail2ban yang dikembangkan menggunakan IpTables guna mengamankan suatu web server dari serangan atau percobaan akses dari pihak-pihak yang tidak berkepentingan. Pemanfaatan firewall dan fail2ban bertujuan agar web server serta aplikasi-aplikasi online yang digunakan aman dari akses pihak-pihak yang tidak berkepentingan serta mencegah pencurian data-data yang sensitive.

Implementasi fail2ban dilakukan dengan fokus kepada mengamankan akses koneksi SSH (secure shell) dimana fail2ban digunakan untuk memblok/memfilter IP Address yang melakukan percobaan koneksi secara beruntun (3x) dan yang masuk ke kriteria serangan.

Hasilnya adalah daftar IP Address yang diblok aksesnya setelah 3x gagal melakukan koneksi ke layanan SSH (secure shell) pada web server dari detail filtering fail2ban diambil sampel IP Address, domain, negara, dan lain-lain yang memberikan indikasi bahwa system firewall yang diterapkan dapat berfungsi dengan benar.

Kata kunci : Bruteforce, firewall IpTables, Fail2ban

1. PENDAHULUAN

Secara umum server dapat diartikan sebagai pusat data dan difungsikan sebagai pelayan yang berguna untuk pengiriman data/penerimaan data serta mengatur pengiriman dan penerimaan data di antara komputer yang tersambung, dengan kata lain server berfungsi menyediakan pelayanan terhadap klien. Server adalah komputer yang mendukung aplikasi dan telekomunikasi dalam jaringan, serta pembagian peralatan software, dan database di antara berbagai terminal kerja dalam jaringan. *(O'brien, 2011).*

Keamanan teknologi informasi (IT) merupakan sebuah hal mendasar yang penting untuk diperhatikan dalam suatu organisasi. Berbagai serangan hacker terhadap server seperti web server yang dimiliki oleh organisasi hingga pembajakan akses sering terjadi. Menurut ID-SIRTII *(Indonesia Security Incident Response Team On Internet Infrastructure)* adanya perangkat teknologi yang serba modern atau canggih akan tidak ada artinya tanpa diimbangi oleh pengamanan dan penggunaan secara tepat dan efektif serta efesien. Hal ini karena Pada era digital saat ini banyak hacker yang mencuri data-data didalam sebuah web server, untuk itu diperlukan langkah-langkah keamanan pada web server. Karena aspek keamanan menjadi faktor yang penting untuk diperhatikan pada sebuah web server dikarenakan berbagai serangan dari luar sering dilaksanakan

dengan memanfaatkan kerentanan yang ada pada server. Serangan yang timbul dapat mengakibatkan hal yang fatal terhadap suatu web server, oleh karena itu perlu dilakukan proses pengamanan web server tersebut menggunakan standard keamanan yang ada seperti firewall iptables dan file2ban karena keamanan ini berlaku unuk semua server. (Kumar , 2002).

Kejahatan siber di indonesia bisa menimbulkan kerugian mencapai US$34,2 miliar atau setara Rp 478,8 triliun (asumsi US$=Rp 14.000). Angka ini setara dengan 3,7% dari total PDB Indonesia. Ini merupakan penelitian dari Frost dan Sullivan yang diprakarsai Microsoft. Selain kerugian finansial, kejahatan siber mengurangi kemampuan berbagai organisasi di Indonesia untuk memanfaatkan peluang-peluang yang ada di era ekonomi digital saat ini, dengan tiga dari lima (61%) responden menyatakan bahwa perusahaan mereka telah menunda upaya transformasi digital karena khawatir terhadap resiko-resiko siber. Dengan batasan-batasan TI yang semakin menghilang, penjahat siber kini menemukan sasaran baru untuk diserang, Perusahaan menghadapi resiko kerugian finansial yang signifikan, dampak buruk pada sisi kepuasan pelanggan, dan penurunan reputasi di pasaran, seperti yang telah terlihat secara jelas pada kasus-kasus serangan sektor tingkat tinggi telah terjadi. (Roy Franedya, 2018).

2. METODOLOGI PENELITIAN

2.1 Metode Pengumpulan Informasi

A. Observasi

Observasi yang digunakan dalam penelitian ini adalah melakukan evaluasi dan observasi pada web server terpasang yang menggunakan firewall IP Tables dan Fail2ban.

B. Studi Literatur

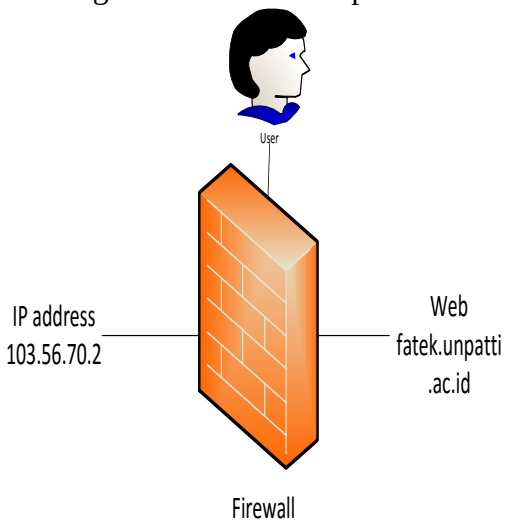
Studi literatur yang diambil dalam penelitian ini adalah pengumpulan bahan pustaka berupa jurnal, buku, white paper yang membahas tentang konfigurasi firewall untuk keamanan web server.

C. Studi Kasus

Studi kasus yang digunakan dalam penelitian ini adalah menganalisa permasalahan-permasalahan yang terjadi pada web server apache dari segi keamanan agar dapat menghasilkan perancangan perencanaan keamanan server apache agar aman dari serangan cyber atau percobaan hackking melalui pemanfaatan firewall iptables dan fail2ban.

2.2 Perancangan Sistem

Konfigurasi Perancangan Sistem Keamanan terhadap IP Address 103.56.70.2 jika ingin request untuk mengakses web fatek.unpatti.ac.id



Gambar 3.1 Pemeriksaan terhadap IP Address 103.56.70.2

Sumber : Hasil Penelitian

Berdasarkan gambar 3.1 maka dapat dijelaskan bahwa jika seorang user ingin request untuk mengakses web fatek.unpatti.ac.id maka firewall akan mengecek apakah IP Address 103.56.70.2 tidak ada didalam daftar blok/blacklist maka request diizinkan sebaliknya jika ada didalam blacklist maka request diblok.

2.3 Waktu Dan Tempat Penelitian

Waktu dan tempat penelitian dilaksanakan

dari bulan februari tahun 2021 sampai selesai pada data center universitas pattimura dan UPT-TIK (Unit Pelayanan Teknis Teknologi Informasi Dan Komunikasi) Universitas Pattimura Ambon.

2.4 Variabel Penelitian

i. Variabel Bebas
Variable bebas yang digunakan dalam penelitian skripsi ini adalah konfigurasi firewall untuk jumlah dan nomor port yang berada dalam kondisi open atau close untuk entitas pada variabel terikat.

ii. Variabel Terikat
- ✓ IP Address Versi 4 (IPV4) pada server.
- ✓ Port nomor 80, 443, 53.

3. HASIL DAN PEMBAHASAN

Pada bagian ini akan dibahas mengenai hasil dari implementasi firewall menggunakan fail2ban pada web server yang perlu diamankan. Firewall menggunakan fail2ban yang dibuat melalui konfigurasi fail2ban diperlihatkan pada bagian kode yang ditampilkan dibawah ini.

```
[DEFAULT]
ignoreip = 103.56.70.2
bantime  = 1440m
findtime  = 5m
maxretry = 3
destemail = admin@mx.unpatti.ac.id
sender = admin@unpatti.ac.id
mta = postfix
```

Bagian pertama dari konfigurasi fail2ban berisi deklarasi parameter-parameter default yang diperlukan untuk dapat menjalankan fungsi firewall pada fail2ban. Adapun parameter-paramater default yang perlu dibuat adalah kalimat [DEFAULT] yang menyatakan bahwa bagian ini adalah untuk konfigurasi default. Bagian konfigurasi default berisi parameter-parameter: ignoreip …

```
[sshd]
enabled = true
port = 22
filter = c
logpath = /var/log/auth.log
maxretry = 3
```

- ✓ Proses konfigurasi firewall iptables dan fail2ban

Proses konfigurasi fail2ban dilakukan dengan melakukan login ke server yang akan diimplementasikan firewallnya dengan koneksi SSH. Adapun langkah-langkahnya adalah sebagai berikut:

Langkah 1. Jalankan command prompt

Langkah 2. Ketik: ssh marinyo@hotumese.unpatti.ac.id (enter)

Langkah 3. Masukan password

Langkah 4. Berpindah ke folder /etc/fail2ban ketik perintah cd /etc/fail2ban (enter)

Langkah 5. Lihat isi folder dengan perintah: ls (enter)

Langkah 6. Buka file dengan nama jail.local menggunakan program teks editor nano. Gunakan perintah: nano jail.local (enter)

Langkah 7. Selanjutnya ketikan baris-baris konfigurasi seperti dibawah ini:

```
[DEFAULT]
ignoreip = 103.56.70.2
bantime  = 1440m
findtime  = 5m
maxretry = 3
destemail = admin@mx.unpatti.ac.id
sender = admin@unpatti.ac.id
mta = postfix
[sshd]
enabled = true
port = 22
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
```

Langkah 8. Simpan dan exit dari server.

Adapun penjelasan dari arti masing-masing baris konfigurasi diatas adalah sebgai berikut:

[DEFAULT] artinya parameter konfigurasi

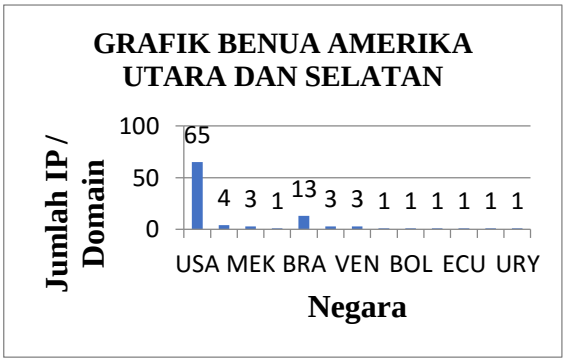
default / umum pada sistem
ignoreip = 103.56.70.2 artinya tidak memproses trafik yang datang dari IP address 103.56.70.2 (pengecualian)

```
[DEFAULT]
ignoreip = 103.56.70.2
bantime  = 1440m
findtime  = 5m
maxretry = 3
destemail = admin@mx.unpatti.ac.id
sender = admin@unpatti.ac.id
mta = postfix

[sshd]
enabled = true
port = 22
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
```

Gambar 4.1 Pengaturan parameter utama fail2ban
Sumber : upttik unpatti

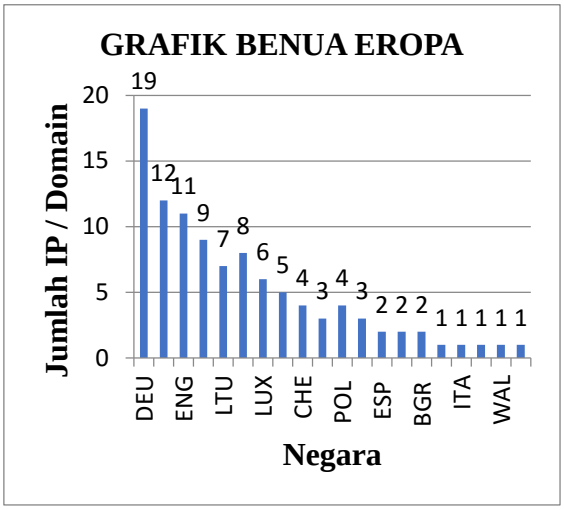
bantime = 1440m artinya waktu blok / ban selama 1440 menit atau 24 jam jika gagal login setelah batas gagal login terlampaui, *bantime* (waktu ban)- Ini adalah periode di mana alamat IP dilarang atau ditolak aksesnya untuk mencoba terhubung kembali dengan server. Secara default, ini ditentukan selama 10 menit, namun pengaturan ini dapat dilakukan sesuai dengan preferensi pengguna.
findtime (waktu cari) - Ini adalah durasi antara upaya login yang gagal sebelum larangan diterapkan. Ini diatur ke 5 menit. Artinya, jika terdapat client yang mencoba login SSH dan kegagalan login mencapai nilai maksimal dalam rentang waktu 5 menit, maka IP yang digunakan akan diblokir.
maxretry = 3 artinya batas percobaan login dan gagal hanya sampai 3 kali, setelah itu akan di blok oleh fail2ban/iptables (firewall), *maxretry* (maksimum gagal login) - Ini menunjukkan jumlah maksimum upaya koneksi yang gagal sebelum IP dilarang / ditolak. Secara default, nilai parameter ini diatur ke 5 detik yang seharusnya sesuai untuk penggunaan secara umum, tetapi dapat diubah menjadi 3 detik untuk meminimalkan serangan bombardir koneksi yang dalam jumlah banyak. Hal ini ditunjukkan pada Gambar 4.1
[sshd] artinya bagian konfigurasi untuk layanan ssh
enabled = true artinya diaktifkan
filter = sshd aktif untuk memantau layanan ssh
logpath = /var/log/auth.log artinya simpan catatan log pada file auth.log yang berada pada folder /var/log/
maxretry = 3 artinya batas percobaan login dan gagal hanya sampai 3 kali, setelah itu akan di blok oleh fail2ban/iptables (firewall)
Hasil bloking / banning oleh fail2ban dgn menggunakan iptables
Untuk melihat gunakan perintah: iptables –L (enter)
(-L artinya tampilan List atau daftar IP-IP yang kena blok).
Dari hasil proses filtering oleh fail2ban yang ditunjukan maka dapat dibuat grafik untuk beberapa kategori wilayah seperti dari benua Amerika, Eropa, Asia, Australia, Afrika dan juga berdasarkan domain.



Gambar 4.2 Grafik Hasil bloking untuk asal trafik benua amerika

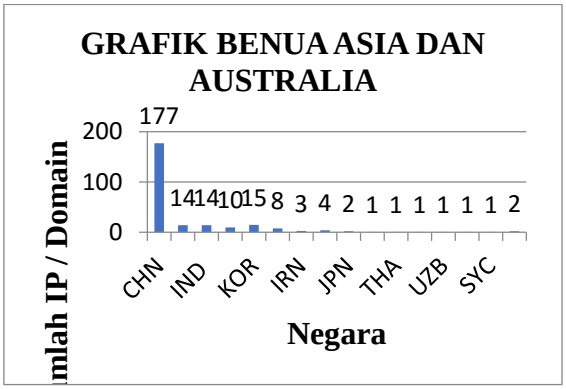
Pada grafik 4.11 ditunjukan bahwa asal trafik berdasarkan geolocation dari setiap IP diperoleh hasil untuk USA/Amerika sebesar 65 client, CAN/Canada 4 client, MEK/Meksiko 3 client, PAN/Panama 1 client, BRA/Brazil 13 client,

COL/Colombia 3 client, VEN/Venezuela 3 client, ARG/Argentina 1 client, BOL/Bolivia 1 client, CHL/Chile 1 client, ECU/Ecuador 1 client, PER/Peru 1 client dan URY/Uruguay 1 client.



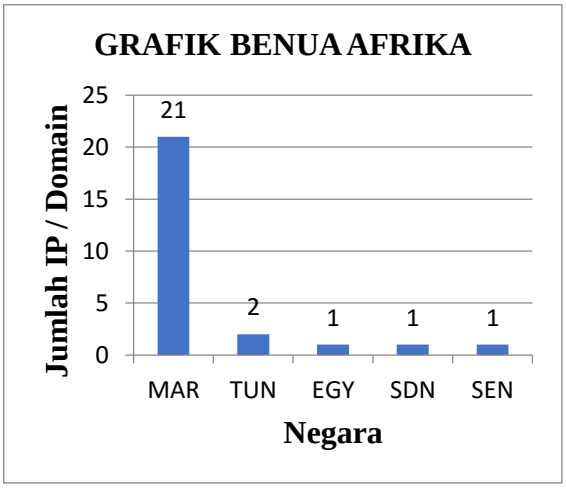
Gambar 4.3 Grafik Hasil bloking untuk asal trafik benua eropa

Pada grafik 4.12 ditunjukan bahwa asal trafik berdasarkan geolocation dari setiap IP diperoleh hasil untuk DEU/Jerman sebesar 19 client, RUS/Rusia 12 client, ENG/Inggris 11 client, NLD/Belanda 9 client, LTU Republik Lithuania 7 client, SWE/Swedia 8 client, LUX/Luksemburg 6 client, UKR/Ukraina 5 client, CHE/Swiss 4 client, CZE Republik Ceko 3 client, POL/Polandia 4 client, FRA/Prancis 3 client, ESP/Spanyol 2 client, EST/Estonia 2 client, BGR/Bulgaria 2 client, PRT/Portugal 1 client, ITA/Italia 1 client, ROU/Romania 1 client, WAL/Wales 1 client dan IRL/Irlandia 1 client.



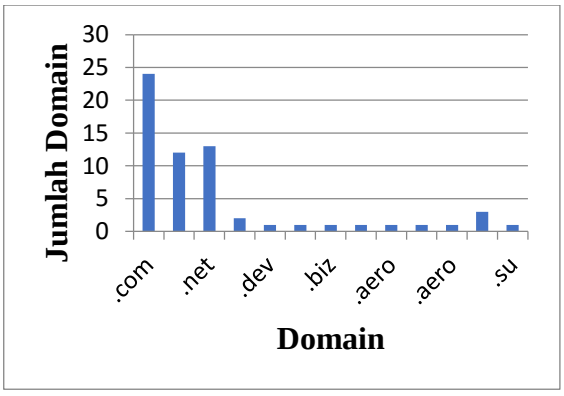
Gambar 4.4 Grafik Hasil bloking untuk asal trafik benua asia dan Australia

Pada grafik 4.13 ditunjukan bahwa asal trafik berdasarkan geolocation dari setiap IP diperoleh hasil untuk CHN/China 177 client, TUR/Turki 14 client, IND/India 14 client, SGP/Singapura 10 client, KOR/Korea Selatan 15 client, VNM/Vietnam 8 client, IRN/Iran 3 client, IDN/Indonesia 4 client, JPN/Japan 2 client, PAK/Pakistan 1 client, THA/Thailand 1 client, SAU/Saudi Arabia 1 client, UZB/Uzbekistan 1 client, NEP/Nepal 1 client, SYC/Seychelles 1 client dan AUS/Australia 2 client.



Gambar 4.5 Grafik Hasil bloking untuk asal trafik benua afrika

Pada grafik 4.14 ditunjukan bahwa asal trafik berdasarkan geolocation dari setiap IP diperoleh hasil untuk MAR/Maroko 21 client, TUN/Tunisia 2 client, EGY/Mesir 1 client, SDN/Sudan 1 client dan SEN/Sinegal 1 client.



Gambar 4.6 Grafik Hasil bloking untuk asal trafik dari domain

Pada grafik 4.15 ditunjukan bahwa jumlah trafik berdasarkan domain diperoleh hasil untuk domain .com sebesar 24 client, .org 12 client, .net 13 client, .xyz 2 client, .dev 1 client, .expert 1 client, .biz 1 client, .server 1 client, .aero 1 client, .online 1 client, .eu 3 client dan .su 1 client.

4. KESIMPULAN

Kesimpulan yang dapat diambil dari skripsi ini adalah hasil-hasil filter yang diperoleh dari data fail2ban yang berupa jumlah IP Address yang terblok beserta geolocationnya sesuai dengan data-data grafik dari benua Amerika Utara dan Selatan sebesar 97 client, Benua Eropa sebesar 102 client, Benua Asia dan Australia sebesar 255 client, dan Benua Afrika sebesar 26 client.

DAFTAR PUSTAKA

[1] Ariata C, 2021. Pengertian Apache Serta Kelebihan Dan Kekurangannya https://www.hostinger.co.id.

[2] Beon Intermedia, 2019. Penyebab Website Server Down Dan Cara Mengatasinya https://www.jagoanhosting.com/blog/penyebab-website-server-down/.

[3] Jho, 2020. Apa Itu Komputer Server, Defenisi, Fungsi, Dan Jenisnya https://www.jogjahost.co.id/blog/komputer-server/.

[4] Kumar, 2002. Sistem Pengamanan Jaringan Admin Server https://ojm.unm.ac.id/ Pendidikan Teknik Informatika Dan Komputer Universitas Negeri Makassar.

[5] Marco Van Basten, 2009. Jurnal Jaringan Komputer, Optimalisasi Firewall pada Jaringan Skala Luas https://www.scribd.com. Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

[6] Nancy I. Whitman, 2013. Impementasi Sistem Media Server Berbasis Wireles Local Area Network https://teknik.usni.ac.id/Jurnal. Jurusan Teknik Informatika Fakultas Teknik Universitas Satya Negara Indonesia.

[7] Roy Franedya, 2018. CNBC Indonesia Perkembangan Teknologi Kejahatan Siber Merebak, RI Rugi RP 478,8 Triliun https://www.cnbcindonesia.com.

[8] Novi Fuji Astuti, 2020. Fungsi Firewall Pada Jaringan Komputer Manfaat Dan Cara Kerjanya https://www.merdeka.com/jabar/

[9] Nur Hamim, 2019. Mengamankan SSH Secure Shell Connection Menggunakan File2ban https://nurhamim.net/.

[10] O'brient, 2011. komputer yang mendukung aplikasi dan telekomunikasi dalam jaringan, serta pembagian peralatan software, dan database di antara berbagai terminal kerja dalam jaringan https://eprints.akakom.ac.id.

[11] Rajil Munir, 2017. Pengertian Firewall Karakteristik Fungsi Manfaat Jenis-Jenis Dan Cara Kerja Firewall https://teropong.id/forum/2017/09/11/.

[12] Riefhid, 2010. Teknik Yang Digunakan Oleh Firewall Jaringan Komputer Dan Keamanan Jaringan https://mtsox.wordpress.com/2010/02/10/.

[13] Rizzaq Aynur Nogroho, 2019. Fungsi Server Pada Komputer Dilengkapi Jenis-Jenisnya https://hot.liputan6.com/.

[14] Syuri, 2020. Jenis-Jenis Firewall Yang Bisa Melindungi Komputer https://carisinyal.com/jenis-jenis-firewall/.
[15] Wardani, 2013. Pengertian Server HTTP Apache atau Server Web/WWW Apache https://e-journal.uajy.ac.id.
[16] Winnie Ondara, 2021. Install And Configure Fail2ban On Ubuntu 20.04 https://linoxide.com/install-and-configure-fail2ban-on-ubuntu-20-04/.