

Form Kesiadaan Membimbing Proyek Tingkat

PROYEK TINGKAT SEMESTER GANJIL|GENAP* TA 2020/2021



Tanggal : 8 December 2020

Kami yang bertanda tangan dibawah ini :

CALON PEMBIMBING 1

Kode : RMT

Nama : ROHMAT TULLOH, S.T., M.T.

CALON PEMBIMBING 2

Kode : ASM

Nama : ASEP MULYANA, S.T., M.T.

Menyatakan bersedia menjadi dosen pembimbing Proyek Tingkat bagi mahasiswa berikut,

NIM : 6705184073

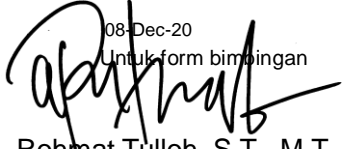
Nama : RAMA WIJAYA SHIDDIQ

Prodi / Peminatan : TT/ KEAMANAN JARINGAN_(contoh: MI / SDV)


Calon Judul PA :
IMPLEMENTASI SENSOR MALTRAIL DAN FILE2BAN UNTUK MENDETEKSI
DAN MENCEGAH SERANGAN MALWARE PADA JARINGAN SERVER
DISKOMINFO SUMEDANG DENGAN PUSH NOTIFIKASI

Dengan ini akan memenuhi segala hak dan kewajiban sebagai dosen pembimbing sesuai dengan Aturan Proyek Tingkat yang berlaku.

Calon Pembimbing 1

08-Dec-20
Untuk form bimbingan

(Rohmat Tulloh, S.T., M.T.)
NIP : 06830002

Calon Pembimbing 2


(Asep Mulyana, S.T., M.T.)
NIP. 945700113

CATATAN:

1. Aturan Proyek Akhir versi terbaru dapat diunduh dari :<http://dte.telkomuniversity.ac.id/panduan-proyek-akhir/>
2. Keputusan akhir penentuan pembimbing berada di tangan Ketua Kelompok Keahlian dengan memperhatikan aturan yang berlaku.
3. Pengajuan pembimbing boleh untuk kedua pembimbing sekaligus atau untuk salah satu pembimbing saja



Telkom University
 Jl. Telekomunikasi No.1, Terusan Buah Batu
 Bandung 40257
 Indonesia

DAFTAR NILAI HASIL STUDI MAHASISWA

NIM (Nomor Induk Mahasiswa) : 6705184073

Nama : RAMA WIJAYA SHIDDIQ

Dosen Wali : TAR / TENGKU AHMAD RIZA

Program Studi : D3 Teknologi Telekomunikasi

Mata Kuliah yang Lulus

Semester	Kode Mata Kuliah	Mata Kuliah	Nama Mata Kuliah B. Inggris	SKS	Nilai
1	DTH1E2	BENGKEL MEKANIKAL DAN ELEKTRIKAL	MECHANICAL AND ELECTRICAL WORKSHOP	2	B
1	DTH1F3	DASAR SISTEM TELEKOMUNIKASI	BASIC TELECOMMUNICATIONS SYSTEM	3	A
1	DTH1C3	DASAR TEKNIK KOMPUTER DAN PEMROGRAMAN	BASIC COMPUTER ENGINEERING AND PROGRAMMING	3	AB
1	DTH1A2	K3 DAN LINGKUNGAN HIDUP	K3 AND ENVIRONMENT	2	A
1	DUH1A2	LITERASI TIK	ICT LITERACY	2	A
1	DTH1B3	MATEMATIKA TELEKOMUNIKASI I	MATHEMATICS TELECOMMUNICATIONS I	3	AB
1	HUH1A2	PENDIDIKAN AGAMA DAN ETIKA - ISLAM	RELIGIOUS EDUCATION AND ETHICS - ISLAM	2	A
1	DTH1D3	RANGKAIAN LISTRIK	ELECTRICAL CIRCUITS	3	AB
2	DTH1H3	TEKNIK DIGITAL	DIGITAL TECHNIQUES	3	AB
2	DTH1G3	MATEMATIKA TELEKOMUNIKASI II	MATHEMATICS TELECOMMUNICATIONS II	3	C
2	DTH1I3	ELEKTRONIKA ANALOG	ANALOG ELECTRONIC	3	C
2	DTH1J2	BENGKEL ELEKTRONIKA	ELECTRONICS WORKSHOP	2	AB
2	DTH1K3	ELEKTROMAGNETIKA	ELECTROMAGNETIC	3	BC
2	HUH1G3	PANCASILA DAN KEWARGANEGARAAN	PANCASILA AND CITIZENSHIP	3	A
2	LUH1B2	BAHASA INGGRIS I	ENGLISH I	2	A
Jumlah SKS				81	3.38

Semester	Kode Mata Kuliah	Mata Kuliah	Nama Mata Kuliah B. Inggris	SKS	Nilai
2	DMH1A2	OLAH RAGA	SPORT	2	A
3	DTH2F3	TEKNIK TRANSMISI RADIO	RADIO TRANSMISSION TECHNIQUES	3	C
3	DTH2G3	SISTEM KOMUNIKASI OPTIK	OPTICAL COMMUNICATION SYSTEMS	3	AB
3	DTH2E3	SISTEM KOMUNIKASI	COMMUNICATIONS SYSTEMS	3	C
3	DTH2B3	KOMUNIKASI DATA BROADBAND	BROADBAND DATA COMMUNICATIONS	3	A
3	DTH2C2	BENGKEL INTERNET OF THINGS	INTERNET OF THINGS WORKSHOP	2	A
3	DTH2A2	BAHASA INGGRIS TEKNIK I	ENGLISH TECHNIQUE I	2	A
3	DTH2D3	APLIKASI MIKROKONTROLER DAN ANTARMUKA	MICROCONTROLLER APPLICATIONS AND INTERFACES	3	AB
4	DTH2H3	JARINGAN DATA BROADBAND	BROADBAND DATA NETWORK	3	B
4	DMH2A2	KERJA PRAKTEK	INTERSHIP	2	A
4	DMH1B2	PENGEMBANGAN PROFESIONALISME	PROFESSIONAL DEVELOPMENT	2	A
4	DTH2J2	TEKNIK TRAFIK	TRAFFIC ENGINEERING	2	AB
4	DTH2I3	DASAR KOMUNIKASI MULTIMEDIA	BASIC COMMUNICATION MULTIMEDIA	3	AB
4	DTH2M3	SISTEM KOMUNIKASI SELULER	CELLULAR COMMUNICATION SYSTEMS	3	AB
4	DTH2K3	ELEKTRONIKA TELEKOMUNIKASI	ELECTRONICS TELECOMMUNICATIONS	3	A
4	DTH2L3	TEKNIK ANTENNA DAN PROPAGASI	ANTENNA TECHNIQUES AND PROPAGATION	3	B
Jumlah SKS				81	3.38

Mata Kuliah yang Belum Lulus

Semester	Kode Mata Kuliah	Mata Kuliah	Nama Mata Kuliah B. Inggris	SKS	Nilai
4	UKI2C2	BAHASA INDONESIA	INDONESIAN LANGUAGE	2	
4	VTI2H2	BAHASA INGGRIS TEKNIK II	ENGLISH TECHNIQUES II	2	
4	VTI2K3	JARINGAN TELEKOMUNIKASI BROADBAND	BROADBAND DATA NETWORKS	3	
Jumlah SKS				15	

Semester	Kode Mata Kuliah	Mata Kuliah	Nama Mata Kuliah B. Inggris	SKS	Nilai
5	VTI3E2	CLOUD COMPUTING	CLOUD COMPUTING	2	
5	UWI3A2	KEWIRAUSAHAAN	ENTREPRENEURSHIP	2	
5	VTI3D3	KEAMANAN JARINGAN	NETWORK SECURITY	3	
5	UWI3E1	HEI	HEI	1	
Jumlah SKS				15	

Tingkat I	: 41 SKS	Belum Lulus	IPK : 3.38
Tingkat II	: 81 SKS	Belum Lulus	IPK : 3.38
Tingkat III	: 81 SKS	Belum Lulus	IPK : 3.38
Jumlah SKS	: 81 SKS		IPK : 3.38

Total SKS dan IPK dihitung dari mata kuliah lulus dan mata kuliah belum lulus. Nilai kosong dan T tidak diikutkan dalam perhitungan IPK.

Pencetakan daftar nilai pada tanggal 27 November 2020 21:56:33 oleh RAMA WIJAYA SHIDDIQ

**IMPLEMENTASI SENSOR MALTRAIL DAN FILE2BAN
UNTUK MENDETEKSI DAN MENCEGAH SERANGAN
MALWARE PADA JARINGAN SERVER DISKOMINFO
SUMEDANG DENGAN PUSH NOTIFIKASI**

PRA PROPOSAL PROYEK TINGKAT

Diajukan sebagai syarat untuk mengikuti Sidang Komite Proyek tingkat

oleh :

RAMA WIJAYA SHIDDIQ

6705184073



**D3 TEKNOLOGI TELEKOMUNIKASI
FAKULTAS ILMU TERAPAN
UNIVERSITAS TELKOM**

2020

Latar Belakang

Salah satu ancaman utama di Internet saat ini yaitu software berbahaya yang sering disebut sebagai malware. Faktanya, sebagian besar masalah keamanan Internet disebabkan oleh malware. Malware hadir dalam berbagai bentuk dan variasi, seperti virus, worm, botnet, rootkit, trojan horse, dan program denial tools lainnya. Dalam penyebarannya, malware mengeksploitasi kerentanan software di browser dan sistem operasi, atau menggunakan teknik social engineering untuk mengelabui pengguna agar dapat menjalankan program-program berbahaya. (Bayer et al. 2009).

Perusahaan anti-virus Malwarebytes (2019) merilis laporan tahunan tentang kondisi malware di seluruh dunia dalam jurnal “2019 States of Malware”. Laporan tersebut menyatakan bahwa terdapat kurang lebih 750 juta serangan malware yang terdeteksi menyerang komputer end-user (personal) sepanjang tahun 2017–2018 di seluruh dunia. Kemudian, terdapat kurang lebih 71 juta malware yang terdeteksi menyerang pengguna business-user (perusahaan/industri/lembaga) sepanjang tahun 2017–2018. Sayangnya, jumlah yang meningkat dan keragaman malware membuat teknik keamanan klasik, seperti pemindai anti-virus, tidak efektif dan, sebagai konsekuensinya, jutaan host di Internet saat ini terinfeksi dengan perangkat lunak berbahaya (Microsoft, 2009; Symantec, 2009).

Diskominfo Kabupaten Sumedang merupakan suatu perangkat daerah yang dibentuk untuk membantu dalam melaksanakan urusan pemerintahan dibidang Komunikasi, bidang Informatika, bidang Persandian dan bidang Statistik. Diskominfo Kabupaten Sumedang bertugas mengurus dan menjamin keamanan TIK, khususnya dibidang networking support, seperti menginstalasi perangkat jaringan, memperluas jaringan internet, perawatan perangkat jaringan secara berkala, dan peningkatan kualitas keamanan jaringan. Dalam usaha peningkatan kualitas keamanan jaringan, dibutuhkan sebuah sistem yang dapat mendeteksi dan memblokir malware-malware yang berusaha masuk ke dalam jaringan pemerintahan dan pelayanan publik di Kota Sumedang. Sistem Pendeteksi dan Pencegah Serangan Malware dengan Sensor Maltrail merupakan solusi dari permasalahan tersebut. Software yang digunakan untuk melakukan pendeteksian malware, yakni bernama Maltrail (Malware Trail). Cara kerja dari software ini mirip dengan mekanisme “sensor” yang memindai seluruh aktivitas traffic pada jaringan server. Kemudian, software yang digunakan untuk melakukan blocking ‘pencegahan’ dari serangan malware, yaitu Fail2Ban. Kedua sistem tersebut dikolaborasikan dan disesuaikan dengan jaringan server

Berdasarkan penelitian tersebut, diperlukan adanya sistem keamanan jaringan untuk monitoring dan pencegahan dari serangan malware yang melintasi jaringan server pada sektor OPD (Organisasi Perangkat Daerah) dan pusat-pusat pelayanan publik di wilayah Kota Sumedang. Hal ini bertujuan sebagai langkah pencegahan dari terjadinya kerugian- kerugian yang disebabkan oleh serangan malware di jaringan internet. Oleh karena itu, dibuatlah Sistem Pendeteksi dan Pencegah Serangan Malware dengan kombinasi sensor maltrail dan Fail2Ban pada Jaringan Server di Diskominfo Sumedang. Pada struktur yang akan diterapkan, software Maltrail dan Fail2Ban yang telah ada, dikonfigurasi sedemikian rupa agar dapat saling berkolaborasi pada sistem keamanan jaringan. Dari beberapa penelitian lanjutan yang telah dilakukan, sistem pendeteksi serangan malware ini dapat dikembangkan lebih jauh pada sisi otomatisasi dalam monitoring dan pencegahan malware traffic yang ada secara real-time beserta fitur notifikasi melalui aplikasi Telegram.

Beberapa penelitian yang telah dilakukan berkaitan dengan sistem Maltrail sebagai basis dari sistem malware monitoring, yaitu (Bayer et al. 2009; Suci et al. 2019; Hudzaifah et al. 2019; McGraw dan Morrisett 2000; Idika dan Mathur 2007)

Studi Literatur Penelitian Terkait

Tabel 1 Merupakan hasil studi literature terhadap penelitian yang terkait dengan judul yang diangkat.

Tabel 1 Hasil Studi Literatur

No	Judul Penelitian /Karya Ilmiah	Tahun	Keterangan
1.	Membangun Sistem Monitoring Malicious Traffic di Jaringan Dengan Maltrail [1] Devie Ryana Suchendra, Prodi D3 Teknik Komputer, Fakultas Ilmu Terapan. (Universitas Telkom)	2018	<p>Dalam proyek tingkat ini penulis merancang penelitian ini dibangun untuk memonitoring jaringan yang keluar masuk dengan menggunakan aplikasi maltrail untuk sistem deteksi lalu lintas yang berbahaya, analisis jaringan, atau pemantauan keamanan. sistem monitoring malicious traffic di jaringan dengan menggunakan maltrail.</p> <p>Perbandingan :</p> <ul style="list-style-type: none"> - Hanya bisa membangun sensor maltrail untuk memonitoring malware. Tanpa ada pencegahan untuk membloking malware. Jika dibandingkan dengan proyek tingkat yang akan dibuat terlihat perbedaan yaitu penambahan File2ban yang dikombinasikan dengan sensor maltrail untuk mendeteksi dan mencegah serangan malware dengan telegram dan email sebagai hasil notifikasi.
2.	Implementasi Teknologi Fail2Ban Untuk Perlindungan Server Mail [2] W A G I T O, S.T., M.T (Akakom Yogyakarta)	2018	<p>Dalam proyek tingkat ini penulis menerapkan Fail2Ban untuk melindungi server dan membuat suatu metode untuk mengamankan server mail dari usaha untuk menerobos password.</p> <p>Perbandingan :</p> <ul style="list-style-type: none"> - Hanya bisa menerapkan File2ban untuk mencegah dan

			melindungi server mail tanpa ada notifikasi lain.
3.	<p>Realtime Pencegahan Serangan Brute Force dan DDOS Pada Ubuntu Server [4]</p> <p>Eko Ari Irawan³, Fakultas Teknik , Program Studi Teknk Informatika (Universitas Muhammadiyah Malang)</p>	2018	<p>Dalam proyek tingkat ini penulis mengimplementasikan File2ban untuk mencegah DDOS secara realtime menggunakan pada ubuntu server.</p> <p>penggunaan fail2sql guna untuk mengirim hasil log fail2ban ke database secara realtime dan hasil log serangan yang tersimpan pada databse akan di kirim dengan menggunakan Bahasa pemograman php dan nantinya hasil log dalam database, sehingga dalam pencegahan serangan ini dapat dianalisa</p> <p>Perbandingan :</p> <ul style="list-style-type: none"> - Hanya bisa menerapkan File2ban untuk mencegah serangan, belum ada fitur tambahan untuk dimodifikasi dengan tools tools lain. Jika dibandingkan dengan proyek tingkat yang akan dibuat terlihat perbedaan bahwa tools File2ban bisa dikombinasikan dengan sensor maltrail, telegram serta email.
4.	<p>Implementasi Monitoring Jaringan Melalui Aplikasi Sosial Media Telegram Dengan Snort [3]</p> <p>Danu Kusuma¹ , Ucu Darusalam² , Deny Hidayatullah³ Fakultas Teknologi Komunikasi dan Informatika (Universitas Nasional)</p>	2020	<p>Dalam proyek tingkat ini penulis membuat sistem untuk monitoring jaringan menggunakan IDS (Intrusion Detection System) yang dimana dapat mendeteksi serangan-serangan dari pihak luar berupa alert dari Snort melalui aplikasi sosial media yaitu telegram</p> <p>Perbandingan :</p> <ul style="list-style-type: none"> - Hanya bisa terintegrasi dengan sistem monitoring, belum ada penambahan baru sebagai notifikasi seperti email/SMTP

5.	<p>Sistem Pencegahan Serangan Brute Force Pada Ubuntu Server Dengan Menggunakan FAIL2BAN [5]</p> <p>Iwan Kurniawan*) , Ferry Mulyanto, Fuad Nandiasa Program Studi Teknik Informatika</p> <p>(Universitas Pasundan)</p>	2016	<p>Dalam proyek tingkat ini penulis mengimplementasikan File2ban untuk pencegahan terhadap serangan bruteforce pada ubuntu. Oleh karena itu Administrator membutuhkan suatu sistem yang dapat membantu kerjanya. Sebuah sistem yang dapat memberikan hasil laporan apa yang terjadi pada sistem apakah itu sebuah serangan atau penyusupan</p> <p>Perbandingan :</p> <ul style="list-style-type: none"> - Hanya menggunakan file2ban untuk mencegah serangan, belum ada penambahan fitur fitur lain untuk dikombinasikan
----	--	------	---

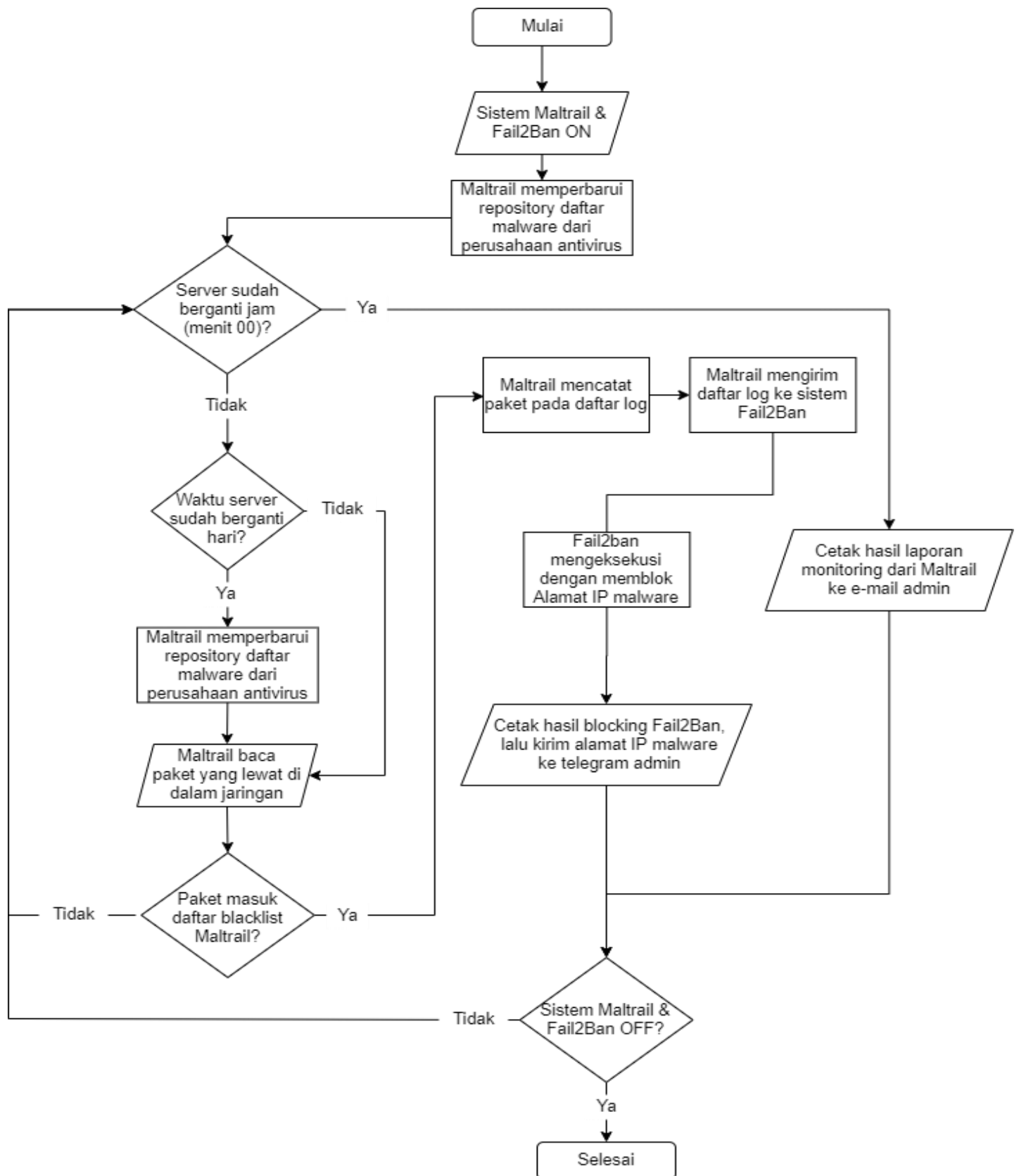
Sistem Perancangan

Pada bab ini akan dijelaskan mengenai perancangan sistem dari sensor maltrail dan file2ban untuk mendeteksi dan mencegah serangan malware. Sistem maltrail dan file2ban ini diletakkan sebagai sistem pendeteksi paket- paket data yang melewati server. Peran sistem Maltrail ini selayak dengan sensor yang mengecek apakah terdapat paket malware yang melewati traffic pada jaringan tersebut atau tidak. Sedangkan sistem Fail2Ban diletakkan berdampingan dengan Maltrail, karena Fail2Ban berperan sebagai program yang mengeksekusi, mencegah dan melarang malware yang lewat berdasarkan dari daftar log yang telah dicatat dan dideteksi oleh Maltrail dengan parameter intensitas penyerangan malware yang dilakukan. Fail2Ban ini memiliki kemampuan memblokir paket-paket ilegal sekaligus menyediakan fitur report forwarding.

Secara garis besar ketika cloud menerima packet request lalu mengirimnya ke client, paket tersebut akan melewati serangkaian tahap pemindaian paket oleh sensor Maltrail berdasarkan database yang tersedia pada datanya. Jika paket tersebut terindikasi terdapat malware, sistem Maltrail akan melakukan pencatatan berupa malware log. Selanjutnya, log tersebut akan dieksekusi oleh sistem Fail2Ban dalam bentuk alamat IP blocking atau pembatasan akses paket oleh sebuah alamat IP di dalam jaringan tersebut. Setelah alamat IP tersebut diblokir, Fail2Ban akan mengirimkan informasi pemblokirannya ke telegram dan akan muncul notifikasi bahwa ip sekian terindikasi malware. Untuk notifikasinya dipastikan realtime jadi ketika ada serangan masuk itu akan memberi tahu bahwa ip sekian terindikasi malware. Setelah itu bisa cek di server dan akan menampilkan data dari log file2ban tersebut setelah diblokir. Kemudian ip yang telah diblokir bisa di unbanned dalam interval waktu tertentu. Kemudian hasil rekapitulasi data keseluruhan dari malware tersebut itu bisa dilihat di web maltrail untuk mengidentifikasi jenis jenis malware yang masuk. Setelah itu bisa mengecek email untuk melihat laporan rekapitulasi dari sensor maltrail.



Gambar 1 Model Sistem Perancangan Sensor maltrail dan File2ban untuk mendeteksi dan mencegah Serangan Malware



Tools untuk Pengukuran

- Malware Trail

Malware Trail (Maltrail) adalah sistem pendeteksi lalu lintas *malware* berbahaya yang menggunakan daftar hitam (*blacklists*) yang *repository*-nya disediakan oleh pihak ketiga yang berisi daftar *malware* berbahaya dan mencurigakan, serta jalur statis atau lokal yang disusun dari berbagai laporan anti- virus dan daftar yang ditentukan pengguna khusus. Maltrail didasarkan pada *traffic sensor-sensor-server-client architecture*. Sensor adalah komponen mandiri yang berjalan pada *monitoring mode* atau di mesin mandiri. Ia memantau paket-paket terdaftar sebagai *blacklist packet* (berupa nama domain, URL, atau alamat IP) yang melewati jaringan tersebut. (Stampar 2014).

- Fail2Ban

Fail2Ban merupakan *software* yang dapat memindai *file log* dan melarang alamat IP yang menunjukkan tanda-tanda paket berbahaya, banyaknya kegagalan kata sandi, dan lain-lain. Umumnya, Fail2Ban digunakan untuk menambahkan *firewall rules* untuk menolak alamat IP untuk jumlah waktu tertentu, meskipun tindakan pencegahan lainnya juga dapat dikonfigurasi lebih lanjut. (Fail2ban.org 2020).

- Telegram

Telegram adalah platform IM (*instan messaging*) yang memungkinkan penggunaanya untuk bertukar pesan, menggunakan berbagai skema komunikasi (yaitu *one-to-one*, *one-to-many*, dan *many-to-many*), serta untuk melakukan panggilan suara, menggunakan berbagai teknik menjaga keamanan/privasi. Telegram mendukung pertukaran data berupa pesan teks (yang isinya teks biasa) dan pesan non-teks (dari jenis apa pun, termasuk informasi kontak, koordinat geografis, dan fail jenis apa pun). (Anglano *et al.* 2017).

- Linux

Merupakan salah satu contoh pengembangan perangkat lunak bebas dan sumber utama terbuka Utilitas sistem dan pustakanya umumnya berasal dari sistem operasi GNU, yang diumumkan tahun 1983 oleh Richard Stallman.

- Super Simple Auto Refresh

Super Simple Auto Refresh merupakan program ekstensi yang tersedia untuk *browser* Google Chrome yang dapat memperbarui halaman web secara otomatis berdasarkan interval waktu yang dapat diatur sesuai dengan kebutuhan pengguna hanya dengan menggunakan satu klik. (Super Simple Auto Refresh, 2020).

- Debian

Sistem operasi komputer yang tersusun dari paket-paket perangkat lunak yang dirilis sebagai perangkat lunak bebas dan terbuka dengan lisensi mayoritas GNU General Public License dan lisensi perangkat lunak bebas lainnya.

Referensi

- [1] Caspian. 2009. An Email Program for Sending SMTP Mail from a Command Line. [diunduh 2020 Mar 16]. Tersedia pada: <http://http://caspian.dotconf.net/menu/Software/SendEmail>.
- [2] Hudzaifah, Anang S, Devie RS. 2018. Membangun Sistem Monitoring Malicious Traffic di Jaringan dengan Maltrail. Bandung (ID): Telkom University. Vol 4 No.3: 2013—2018.
- [3] Jaquier C. 2004. Fail2Ban Intrusion and Prevention Software. GitHub. [diunduh 2020 Mar 16]. Tersedia pada: <https://github.com/fail2ban/fail2ban/wiki/How-fail2ban-works>.
- [4] Sivasubramanian B, Erum F, Richard Froom. 2010. Analyzing the Cisco Enterprise Campus Architecture. Cisco Press. [diunduh 2020 Mar 16]. Tersediapada:<https://www.ciscopress.com/articles/article.asp?p=1608131>.
- [5] Stampar M. 2016. Malicious Traffic Detection System. Github. [diunduh 2020 Mar 16]. Tersedia pada: <https://github.com/stamparm/maltrail>.
- [6] Super Simple Auto Refresh. 2020. Overview: Super Simple Auto Refresh. Chrome Web Store. [diunduh 2020 Mar 16]. Tersedia pada: <https://chrome.google.com/webstore/detail/super-simple-auto-refreshgljclgacfa-lmnebgmhknodlplmngmfpi>.
- [7] Universitas Pasundan Vol. 18 No.2: 89—96. H [ttps://doi.org/10.23969/infomatek.v18i2.496](https://doi.org/10.23969/infomatek.v18i2.496)