PENERAPAN SURICATA SNORBY BARNYARD2 SEBAGAI PENGAMAN DARI SERANGAN DISTRIBUTED DENIAL OF SERVICE (DDoS)

PRA PROPOSAL PROYEK TINGKAT

Diajukan sebagai syarat untuk mengikuti Sidang Komite Proyek tingkat

oleh :

HASNATUL HUSNI

6705184106

D3 TEKNOLOGI TELEKOMUNIKASI

FAKULTAS ILMU TERAPAN

UNIVERSITAS TELKOM

2020

Latar Belakang

Seiring berkembangnya teknologi, khususnya keamanan jaringan yang semakin berkembang menuntut agar sistem keamanan untuk berkembang. Suricata merupakan suatu sistem pencegah serangan yang membutuhkan firewall. Pada penelitian ini, penggunaan suricata untuk sistem IPS (Intrusion Prevention System) untuk identifikasi ancaman yang sering terjadi DDoS (Distributed Denial of Service) dimana serangan ini memanfaatkan sejumlah besar komputer untuk menjalankan serangan DoS kepada server, web services, atau sumber daya jaringan lainnya. Teknologi ini dapat mencegah serangan yang akan masuk ke jaringan local dengan memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor saat serangan teridentifikasi.

Dengan adanya permasalahan tersebut, maka dilaksanakan penelitian dengan judul "PENERAPAN SURICATA SNORBY BARNYARD2 SEBAGAI PENGAMAN DARI SERANGAN DISTRIBUTED DENIAL OF SERVICE (DDoS)". Sehingga dapat memberikan keamanan jaringan dan mendeteksi dari serangan DDoS menggunakan sistem tersebut.

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.	Penerapan Intrusion Prevention System (IPS) Suricata Sebagai Pengamanan Dari Serangan Distributed Denial of Service (DDoS) **[1]**	2020	Pada penelitian ini menggunakan suricata, ELK Stack, HPING3, Loic, Wireshark. Untuk hasil serangan di rekam pada ELK Stack ke dalam IPS suricata yang dibuat.
2.	Implementasi Intrusion Prevention System Suricata dengan Anomaly-Based untuk Keamanan Jaringan PT. Grahamedia Informasi Bagas Suryo Anggoro1 , Wiwin Sulistyo2 **[2]**	2019	Penelitian ini bertujuan mengimplementasikan Intrusion Prevention System (IPS) . Metode yang digunakan : SDLC (Security Development Life Cycle) dengan model waterfall menurut bassil. Penelitian ini menggunakan kombinasi honeypot untuk melihat ancaman yang tidak terbaca pada firewall. Untuk pengujian IPS menggunakan SQL injection.
3.	IMPLEMENTASI SURICATA UNTUK MENINGKATKAN KEAMANAN PADA CLOUD COMPUTING **[3]**	2019	Pada penelitian ini IDS Suricata berfungsi untuk pendeteksian serangan Port scanning, Brute force, Denial Of Service, Backdoor dan mengukur efektifitas penerapan rules-rules serangan tersebut pada Cloud Computing.

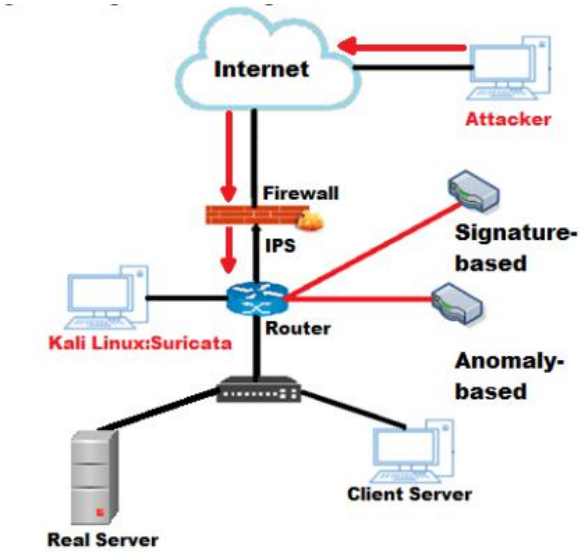
4.	Implementasi Network Intrusion Detection System pada Sistem Smart Identification **[4]**	2016	Pada penelitian ini menggunakan gammu, suricata, snorby, barnyard. Gammu disini berguna untuk membuat sms gate away ketika terjadi serangan. Teknologi yg digunakan adalah NIDS dengan smart identification melalui sms gate away. Serangan berupa port scanning, Dos, Metaspoit.
5.	ANALISIS DAN IMPLEMENTASI SURICATA, SNORBY, DAN BARNYARD2 PADA VPS UBUNTU **[5]**	2015	Dalam penelitian ini penulis menggunakan suricata untuk detection, snorby dan barnyard untuk remote server nya. Penulis menggunakan NIDS (Network Detection System) sebagai deteksi pada suricata dengan rules yang telah dibuat. Pengujian NIDS : 1. Pengujian Request Packet Data 2. Pengujian Menggunakan Nmap 3. Pengujian Menggunakan Tool Hydra 4. Pengujian Menggunakn Sqlmap Pengujian Menggunakan Metasploit Konsol

Rancangan Sistem

Pada bab ini akan dijelaskan mengenai implementasi suricata, snorby barnyard2 terhadap serangan DDoS (*Distributed Denial of Service*). untuk implementasi tersebut dilakukan dengan menggunakan teknologi IPS (*Intrusion Prevention System*) dimana dapat mendeteksi serangan DDoS serta dapat memblock serangan tersebut. Berbeda halnya IDS (*Intruction Detection System*) yang hanya dapat mendeteksi serangan tanpa memblok serangan yang terdeteksi.

Sistem IPS menggunakan suricata snorby barnyard2 ini diuji menggunakan serangan DDoS dengan bantuan tools HPING3 dan LOIC. IPS (*Intrusion Prevention System*) tersebut akan mendeteksi serangan kedalam sebuah log. Serta memblock serangan ketika rules serangan diaktifkan.

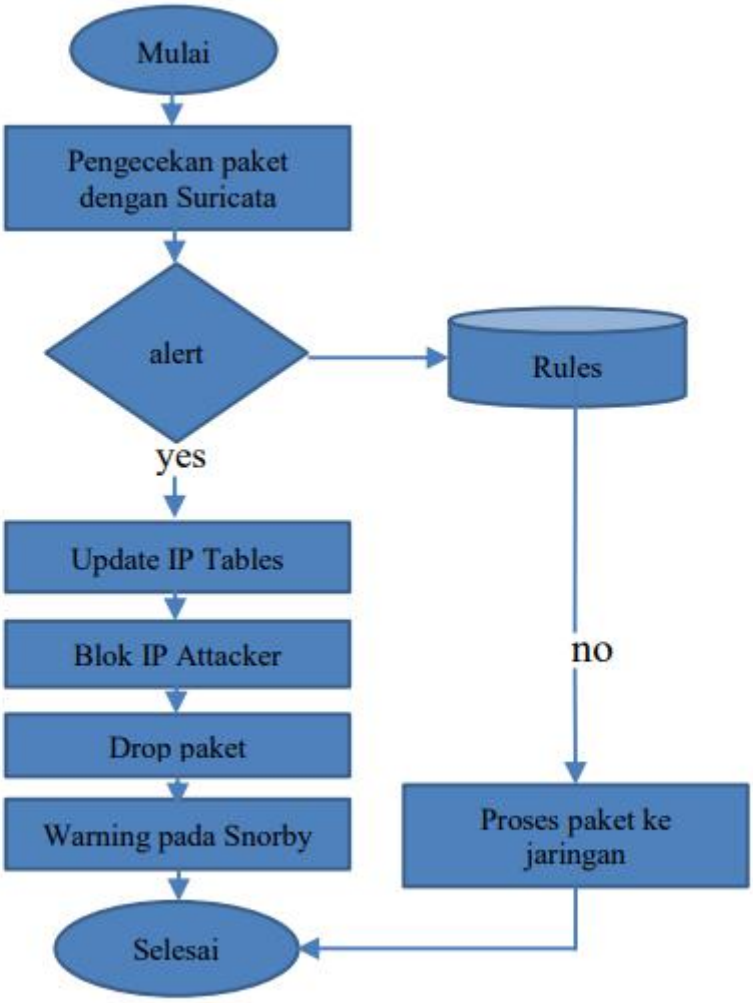
Berikut perancangan skema :



Gambar Perancangan IPS

Secara garis besar attacker akan melakukan penyerangan terhadap server yang dimana sudah terinstall suricata snorby barnyard yang sudah di setting sedemikian rupa sehingga dapat mendeteksi serangan. Suricata akan merekam semua kegiatan attacker sedangkan snorby akan memonitoring sistem yang telah dibuat oleh suricata itu sendiri. Log serangan disimpan pada fast.log pada suricata. Untuk barnyard berfungsi sebagai penerjemah alert dan log sistem itu sendiri. Serangan DDoS akan disajikan pada Snorby dalam bentuk grafik.

Berikut flowchart IPS



Alur IPS dengan suricata, snorby, barnyard2 :

1. Melakukan instalasi suricata, snorby, barnyard2.
2. Mengaktifkan suricata, snorby, barnyard2.
3. Mengkonfigurasi rules suricata sebagai IPS (*Intrusion Prevention System).*
4. Jika terdapat lalu lintas jaringan maka akan disesuaikan dengan *rules* pada suricata . *Rules* tersebut akan mendeteksi apakah lalu lintas tersebut acaman atau tidaknya,
5. Jika terdeteksi sebagai ancaman maka lalu lintas jaringan tersebut akan terupdate pada iptables sebagai serangan.

6. Setelah itu dilakukan blok terhadap lalu lintas tersebut (blok IP attacker).

7. Semua aktifitas akan terekam pada interface snorby.

8. Pemetaan hasil pada snorby berupa grafik.

Alur serangan :

1. Serangan dilakukan pada kali linux menggunakan HPING3 terhadap komputer target.

2. Serangan dilakukan menggunakan LOIC terhadap komputer target

3. Serangan dilakukan pada kali linux menggunakan Brute force.

4. Melakukan *scanning port* terhadap komputer target.

Tools yang digunakan :

Perangkat Lunak	Keterangan
Ubuntu 18.04	Sistem Operasi yang digunakan untuk Server IPS.
Kali linux	Sistem Operasi yang digunakan untuk sebagai penyerang.
Suricata	Perangkat lunak yang digunakan untuk mendeteksi serangan
Snorby	Perangkat lunak yang digunakan untuk menampilkan notifikasi melalui web interface
Barnyard	Perangkat lunak yang digunakan untuk membuat alert menjadi database dan

	dimasukan kedalam database Snorby
HPING3	Sebagai jenis serangan yang digunakan.
Loic	Sebagai jenis serangan yang digunakan.
Nmap	Perangkat lunak yang digunakan untuk melakukan port scanning pada server target.
Brute force	Sebagai jenis serangan yang digunakan

Referensi

[1] Istiana Adesty, "Penerapan Intrusion Prevention System (IPS) Suricata Sebagai Pengamanan Dari Serangan Distributed Denial of Service (DDoS)," 2020.

[2] Bagas Suryo Anggoro, "Implementasi Intrusion Prevention System Suricata dengan Anomaly-Based untuk Keamanan Jaringan PT. Grahamedia Informasi," 2019.

[3] Satri Bagus Pribadi, "IMPLEMENTASI SURICATA UNTUK MENINGKATKAN KEAMANAN PADA CLOUD COMPUTING," 2019.

[4] Sofyan Hadi, Periyadi, S.T., M.T., "Implementasi Network Intrusion Detection System pada Sistem Smart Identification," 2016.

[5] M. K. S. M. Alim Nuryanto, "ANALISIS DAN IMPLEMENTASI SURICATA, SNORBY, DAN BARNYARD2," 2015.

Form Kesediaan Membimbing Proyek Tingkat

PROYEK TINGKAT SEMESTER GANJIL|GENAP* TA 2020/2021

Telkom University

Tanggal : 10 Desember 2020

Kami yang bertanda tangan dibawah in i:

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	6705184106
Nama	: Hasnatul Husni
Prodi / Peminatan	: TT/ Keamanan Jaringan(contoh: MI / SDV)
Calon Judul PA	: PENERAPAN SURICATA SNORBY BARNYARD2 SEBAGAI PENGAMAN DARI SERANGAN DISTRIBUTED DENIAL OF SERVICE (DDoS)

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

Calon Pembimbing 1	Calon Pembimbing 2
10-Dec-20 untuk persetujuan form pbb a/n hasnatul husni	
(Rohmat Tulloh, S.T,M.T.)	(Asep Mulyana, S.T,M.T)
NIP.06830002	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) : 6705184106
Nama : HASNATUL HUSNI
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	DTH1D3	RANGKAIAN LISTRIK	ELECTRICAL CIRCUITS	3	A
1	HUH1A2	PENDIDIKAN AGAMA DAN ETIKA - ISLAM	RELIGIOUS EDUCATION AND ETHICS - ISLAM	2	A
1	DTH1B3	MATEMATIKA TELEKOMUNIKASI I	MATHEMATICS TELECOMMUNICATIONS I	3	A
1	DUH1A2	LITERASI TIK	ICT LITERACY	2	A
1	DTH1A2	K3 DAN LINGKUNGAN HIDUP	K3 AND ENVIRONMENT	2	A
1	DTH1C3	DASAR TEKNIK KOMPUTER DAN PEMROGRAMAN	BASIC COMPUTER ENGINEERING AND PROGRAMMING	3	AB
1	DTH1F3	DASAR SISTEM TELEKOMUNIKASI	BASIC TELECOMMUNICATIONS SYSTEM	3	AB
1	DTH1E2	BENGKEL MEKANIKAL DAN ELEKTRIKAL	MECHANICAL AND ELECTRICAL WORKSHOP	2	AB
2	DTH1G3	MATEMATIKA TELEKOMUNIKASI II	MATHEMATICS TELECOMMUNICATIONS II	3	AB
2	DTH1H3	TEKNIK DIGITAL	DIGITAL TECHNIQUES	3	AB
2	DTH1I3	ELEKTRONIKA ANALOG	ANALOG ELECTRONIC	3	A
2	DTH1J2	BENGKEL ELEKTRONIKA	ELECTRONICS WORKSHOP	2	B
2	DTH1K3	ELEKTROMAGNETIKA	ELECTROMAGNETIC	3	A
2	HUH1G3	PANCASILA DAN KEWARGANEGARAAN	PANCASILA AND CITIZENSHIP	3	A
2	LUH1B2	BAHASA INGGRIS I	ENGLISH I	2	A
2	DMH1A2	OLAH RAGA	SPORT	2	A
Jumlah SKS				83	3.76

Semester	Kode Mata Kuliah	Mata Kuliah	Nama Mata Kuliah B. Inggris	SKS	Nilai
3	DTH2A2	BAHASA INGGRIS TEKNIK I	ENGLISH TECHNIQUE I	2	A
3	DTH2D3	APLIKASI MIKROKONTROLER DAN ANTARMUKA	MICROCONTROLLER APPLICATIONS AND INTERFACES	3	AB
3	DTH2C2	BENGKEL INTERNET OF THINGS	INTERNET OF THINGS WORKSHOP	2	A
3	DTH2F3	TEKNIK TRANSMISI RADIO	RADIO TRANSMISSION TECHNIQUES	3	B
3	DTH2G3	SISTEM KOMUNIKASI OPTIK	OPTICAL COMMUNICATION SYSTEMS	3	A
3	DTH2E3	SISTEM KOMUNIKASI	COMMUNICATIONS SYSTEMS	3	A
3	DTH2B3	KOMUNIKASI DATA BROADBAND	BROADBAND DATA COMMUNICATIONS	3	A
4	DMH2A2	KERJA PRAKTEK	INTERSHIP	2	A
4	DTH2H3	JARINGAN DATA BROADBAND	BROADBAND DATA NETWORK	3	AB
4	DTH2I3	DASAR KOMUNIKASI MULTIMEDIA	BASIC COMMUNICATION MULTIMEDIA	3	A
4	DTH2J2	TEKNIK TRAFIK	TRAFFIC ENGINEERING	2	AB
4	DTH2K3	ELEKTRONIKA TELEKOMUNIKASI	ELECTRONICS TELECOMMUNICATIONS	3	A
4	DTH2L3	TEKNIK ANTENNA DAN PROPAGASI	ANTENNA TECHNIQUES AND PROPAGATION	3	AB
4	DMH1B2	PENGEMBANGAN PROFESIONALISME	PROFESSIONAL DEVELOPMENT	2	A
4	DTH2M3	SISTEM KOMUNIKASI SELULER	CELLULAR COMMUNICATION SYSTEMS	3	AB
5	DUH2A2	KEWIRAUSAHAAN	ENTREPRENEURSHIP	2	AB
Jumlah SKS				83	3.76

Mata Kuliah yang Belum Lulus

Semester	Kode Mata Kuliah	Mata Kuliah	Nama Mata Kuliah B. Inggris	SKS	Nilai
4	VTI2K3	JARINGAN TELEKOMUNIKASI BROADBAND	BROADBAND DATA NETWORKS	3	
4	UKI2C2	BAHASA INDONESIA	INDONESIAN LANGUAGE	2	
4	VTI2H2	BAHASA INGGRIS TEKNIK II	ENGLISH TECHNIQUES II	2	
Jumlah SKS				13	

Semester	Kode Mata Kuliah	Mata Kuliah	Nama Mata Kuliah B. Inggris	SKS	Nilai
5	VTI3E2	CLOUD COMPUTING	CLOUD COMPUTING	2	
5	UWI3E1	HEI	HEI	1	
5	VTI3D3	KEAMANAN JARINGAN	NETWORK SECURITY	3	
Jumlah SKS				13	

Tingkat I	: 41 SKS	Belum Lulus	IPK : 3.78
Tingkat II	: 81 SKS	Belum Lulus	IPK : 3.77
Tingkat III	: 83 SKS	Belum Lulus	IPK : 3.76
Jumlah SKS	: **83 SKS**		**IPK : 3.76**

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 **11 Desember 2020 14:51:26** oleh **HASNATUL HUSNI***