IMPLEMENTASI SISTEM DETEKSI PENYUSUP JARINGAN MENGGUNAKAN SNORT DENGAN MENGIRIM PESAN MELALUI APLIKASI TELEGRAM

TUGAS AKHIR

ANDRE SYARIF FIRJATULLAH
41518010009

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2022

http://digilib.mercubuana.ac.id/

IMPLEMENTASI SISTEM DETEKSI PENYUSUP JARINGAN MENGGUNAKAN SNORT DENGAN MENGIRIM PESAN MELALUI APLIKASI TELEGRAM

Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:
ANDRE SYARIF FIRJATULLAH
41518010009

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2022

http://digilib.mercubuana.ac.id/

LEMBAR PERNYATAAN ORISINALITAS

Yang bertanda tangan dibawah ini:

NIM	:	41518010009
Nama	:	Andre Syarif Firjatullah
Judul Tugas Akhir	:	Implementasi Sistem Deteksi Penyusup Jaringan Menggunakan Snort Dengan Mengirim Pesan Melalui Aplikasi Telegram

Menyatakan bahwa Laporan Tugas Akhir saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 01 Juli 2022

Andre Syarif Firjatullah

UNIVERSITAS
MERCU BUANA

http://digilib.mercubuana.ac.id/

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa	:	Andre Syarif Firjatullah
NIM	:	41518010009
Judul Tugas Akhir	:	Implementasi Sistem Deteksi Penyusup Jaringan Menggunakan Snort Dengan Mengirim Pesan Melalui Aplikasi Telegram

Dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Noneksklusif** (*None-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul diatas beserta perangkat yang ada (jika diperlukan).

Dengan Hak Bebas Royalti/Noneksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan mempublikasikan tugas akhir saya.

Selain itu, demi pengembangan ilmu pengetahuan di lingkungan Universitas Mercu Buana, saya memberikan izin kepada Peneliti di Lab Riset Fakultas Ilmu Komputer, Universitas Mercu Buana untuk menggunakan dan mengembangkan hasil riset yang ada dalam tugas akhir untuk kepentingan riset dan publikasi selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 01 Juli 2022

UNIVERSITAS
MERCU BUANA

METERAI TEMPEL
10000
A0255AAJX833780434

Andre Syarif Firjatullah

Universitas Mercu Buana

http://digilib.mercubuana.ac.id/

SURAT PERNYATAAN LUARAN TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa	:	Andre Syarif Firjatullah
NIM	:	41518010009
Judul Tugas Akhir	:	Implementasi Sistem Deteksi Penyusup Jaringan Menggunakan Snort Dengan Mengirim Pesan Melalui Aplikasi Telegram

Menyatakan bahwa :

1. Luaran Tugas Akhir saya adalah sebagai berikut :

No	Luaran	Jenis		Status	
1	Publikasi Ilmiah	Jurnal Nasional Tidak Terakreditasi		Diajukan	✓
		Jurnal Nasional Terakreditasi	✓		
		Jurnal International Tidak Bereputasi		Diterima	
		Jurnal International Bereputasi			
	Disubmit/dipublikasikan di :	Nama Jurnal	: Faktor Exacta		
		ISSN	: 1979-276x		
		Link Jurnal	: https://journal.lppmunindra.ac.id/		
		Link File Jurnal Jika Sudah di Publish	:		

2. Bersedia untuk menyelesaikan seluruh proses publikasi artikel mulai dari submit, revisi artikel sampai dengan dinyatakan dapat diterbitkan pada jurnal yang dituju.
3. Diminta untuk melampirkan scan KTP dan Surat Pernyataan (Lihat Lampiran Dokumen HKI), untuk kepentingan pendaftaran HKI apabila diperlukan

MERCU BUANA

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 01 Juli 2022

METERAI TEMPEL
10000
0011EAJX833780428

Andre Syarif Firjatullah

http://digilib.mercubuana.ac.id/

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41518010009
Nama	:	Andre Syarif Firjatullah
Judul Tugas Akhir	:	Implementasi Sistem Deteksi Penyusup Jaringan Menggunakan Snort Dengan Mengirim Pesan Melalui Aplikasi Telegram

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 10 Agustus 2022

Penguji

Umniy Salamah, ST., MMSI

UNIVERSITAS
MERCU BUANA

http://digilib.mercubuana.ac.id/

LEMBAR PERSETUJUAN PENGUJI

NIM	:	4151810009
Nama	:	Andre Syarif Firjatullah
Judul Tugas Akhir	:	Implementasi Sistem Deteksi Penyusup Jaringan Menggunakan Snort Dengan Mengirim Pesan Melalui Aplikasi Telegram

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 28 Juli 2022

TANDA TANGAN DIGITAL DOSEN PENGUJI

(Rahmat Rian Hidayat, ST, MMSI)

UNIVERSITAS
MERCU BUANA

http://digilib.mercubuana.ac.id/

LEMBAR PERSETUJUAN PENGUJI

NIM	:	4151810009
Nama	:	Andre Syarif Firjatullah
Judul Tugas Akhir	:	Implementasi Sistem Deteksi Penyusup Jaringan Menggunakan Snort Dengan Mengirim Pesan Melalui Aplikasi Telegram

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 28 Juli 2022

TANDA TANGAN DIGITAL DOSEN PENGUJI

(Muhammad Rifqi, S.Kom, M.Kom)

http://digilib.mercubuana.ac.id/

LEMBAR PENGESAHAN

NIM	:	4151810009
Nama	:	Andre Syarif Firjatullah
Judul Tugas Akhir	:	Implementasi Sistem Deteksi Penyusup Jaringan Menggunakan Snort Dengan Mengirim Pesan Melalui Aplikasi Telegram

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 28 Juli 2022

Menyetujui,

(Wawan Gunawan, S.Kom, MT)
Dosen Pembimbing

Mengetahui,

(Wawan Gunawan, S.Kom, MT)	(Ir. Emil R. Kaburuan, Ph.D., IPM.)
Koord. Tugas Akhir Teknik Informatika	Ka. Prodi Teknik Informatika

UNIVERSITAS
MERCU BUANA

http://digilib.mercubuana.ac.id/

KATA PENGANTAR

Puji syukur kita panjatkan kehadirat Allah SWT, yang telah melimpahkan rahmat dan karunia-Nya, sehinggan pada akhirnya penulis dapat menyelesaikan tugas akhir ini dengan baik. Adapun judul tugas akhir yang penulis buat adalah "**Implementasi Sistem Deteksi Penyusup Jaringan Menggunakan Snort Dengan Mengirim Pesan Melalui Aplikasi Telegram**".

Penulisan laporan tugas akhir ini diajukan untuk memenuhi salah satu syarat kelulusan dalam memperoleh gelar Strata 1 (satu) pada Universitas Mercu Buana. Dalam penulisan tugas akhir ini tidak lepas dari hambatan dan kesulitam, namun berkat bimbingan, bantuan, nasihat dan saran serta kerjasama dari berbagai pihak, khususnya pembimbing, segala hambatan tersebut dapat diatasi dengan baik.

Dalam penulisan ini tentunya tidak lepas dari kekurangan, baik aspek kualitas maupun aspek kuantitas dari materi penelitian yang disajikan. Semua ini didasarkan dari keterbatasan yang dimiliki penulis. Selanjutnya dalam penulisan tugas akhir ini penulis banyak diberi bantuan oleh berbagai pihak.

Dengan tidak mengurangi apresiasi kepada semua pihak yang telah membantu penulis secara khusus, baik langsung maupun tidak langsung penulis menyampaikan rasa hormat dan ucapan terima kasih kepada :

1. Kedua Orang Tua yang telah banyak memberikan dukungan baik secara moril maupun materi dan masukan dalam pembuatan tugas akhir ini.
2. Emil R. Kaburuan, Ph.D. selaku kepala program studi Teknik Informatika Universitas Mercu Buana.
3. Wawan Gunawan S.Kom., M.T. selaku Koordinator Tugas Akhir program studi Teknik Informatika Universitas Mercu Buana,
4. Wawan Gunawan S.Kom., M.T. selaku Dosen Pembimbing Tugas Akhir yang selalu memberikan saran, bimbingan, dan arahannya dalam penyusunan Tugas Akhir ini,
5. Sahabat – sahabat saya yang telah memberi dukungan dan nasihat selama pengerjaan proyek akhir ini,

http://digilib.mercubuana.ac.id/

6. Rekan kerja IT Operation di P.T. Bank Tabungan Negara yang telah memberi saran dan membantu penulis dalam perancangan serta konfigurasi jaringan,
7. Nabila Putri Salia S.Ak. yang selalu memberikan semangat bagi penulis untuk menyelesaikan penyusunan skripsi ini.
8. Semua pihak yang membantu dalam menyelesaikan Tugas Akhir ini yang tidak bisa saya sebut satu persatu.

Tiada kata lain yang dapat penulis ungkapkan untuk mengucapkan terima kasih terhadap semua pihak yang telah banyak membantu dalam menyelesaikan laporan ini dan semoga Allah selalu melimpahkan rahmat dan hidayah-Nya kepada kita semua, Amin. Harapan Penulis yaitu semoga Tugas Akhir ini dapat bermanfaat dengan baik dan berguna bagi orang lain.

Jakarta, 1 Juli 2022
Penulis,

(Andre Syarif Firjatullah)

UNIVERSITAS
MERCU BUANA

http://digilib.mercubuana.ac.id/

DAFTAR ISI

HALAMAN SAMPUL i
HALAMAN JUDUL i
LEMBAR PERNYATAAN ORISINALITAS ii
SURAT PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR ... iii
SURAT PERNYATAAN LUARAN TUGAS AKHIR iv
LEMBAR PERSETUJUAN PENGUJI v
LEMBAR PENGESAHAN viii
ABSTRAK ix
ABSTRACT x
KATA PENGANTAR xi
DAFTAR ISI xiii
NASKAH JURNAL 1
KERTAS KERJA 15
BAB 1. LITERATUR REVIEW 16
BAB 2. ANALISIS DAN PERANCANGAN 28
BAB 3. SOURCE CODE 35
BAB 4. DATASET 37
BAB 5. TAHAPAN EKSPERIMEN 40
BAB 6. HASIL SEMUA EKSPERIMEN 43
DAFTAR PUSTAKA 48
LAMPIRAN DOKUMEN HAKI 50
LAMPIRAN KORESPONDENSI 52

UNIVERSITAS MERCU BUANA

http://digilib.mercubuana.ac.id/

NASKAH JURNAL

Faktor Exacta

Vol. 13, No. 1, March 2020, pp. xx~xx
eISSN: 2502-339X, pISSN: 1979-276X, DOI: 10.30998/faktorexacta.vx3ix.xxxx ❒ 1

IMPLEMENTASI SISTEM DETEKSI PENYUSUP JARINGAN MENGGUNAKAN SNORT DENGAN MENGIRIM PESAN MELALUI APLIKASI TELEGRAM

Andre Syarif Firjatullah[1], Wawan Gunawan[2]
[1,2] Teknik Informatika, Universitas Mercu Buana

Article history:

Received Sep 9, 2019
Revised May 20, 2020
Accepted Jun 11, 2020

Server merupakan suatu hal yang perlu mendapatkan perhatian lebih mengenai tingkat keamanannya, Server yang memiliki celah keamanan dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Administrator harus memastikan bahwa sistem benar-benar aman, dan salah satu cara untuk menjaga keamanan server adalah dengan menggunakan intrusion detection system (IDS) snort untuk mendeteksi penyusupan yang dianggap berbahaya.

Article Info

Keywords:

Intrusion Detection System (IDS)
Snort
Bot Telegram

ABSTRACT

Penelitian ini mengimplementasikan sebuah sistem deteksi penyusup jaringan
menggunakan snort dengan mengirim pesan melalui aplikasi telegram. Sistem keamanan jaringan dalam penelitian ini di bangun dengan menggunakan Intrusion Detection System (IDS) snort dan Bot telegram. Snort merupakan suatu sistem yang berfungsi untuk mengetahui jika adanya intrusi ketika ada yang melakukan ddos attack dan port scanning maka snort akan mendeteksi adanya serangan tersebut dan akan mengirim pesan alert ke dalam sebuah grup chat administrator. Hasil dari penelitian ini snort mampu mendeteksi adanya serangan intrusi dan bot telegram mampu memberikan pesan alert ke dalam grup administrator secara real-time

Copyright © 2020 Universitas Indraprasta PGRI. All rights reserved.

Corresponding Author:

Andre Syarif Firjatullah,

http://digilib.mercubuana.ac.id/

Teknik Informatika,
Universitas Mercu Buana,
Jl. Raya, RT.4/RW.1, Meruya Sel., Kec. Kembangan, Jakarta, Daerah Khusus Ibukota Jakarta 11650. Email: 41518010009@student.mercubuana.ac.id

1. PENDAHULUAN

Di era globalisasi, perkembangan telekomunikasi khususnya perkembangan jaringan komputer menjadi salah satu hal yang paling mendasar dalam kehidupan sekarang ini. Mengingat PT Bank XYZ merupakan perusahaan perbankan yang memiliki cabang di seluruh Indonesia, keamanan jaringan merupakan aspek sangat penting terutama untuk perusahaan yg bergerak di bidang perbankan. keamanan komputer adalah cabang teknologi yang disebut keamanan informasi yang diterapkan pada komputer. Tujuan keamanan komputer termasuk melindungi informasi dari pencurian atau kerusakan, atau menjaga ketersediaan, seperti yang didefinisikan dalam kebijakan keamanan [1]. Menurut pakar keamanan komputer Garfinkel dan Spafford, komputer dapat dikatakan aman jika bisa diandalkan dan suatu perangkat lunak bekerja sesuai dengan yang diharapkan. Hal ini membuat semua komputer yang terhubung ke jaringan komputer sangat rentan Serangan atau aktivitas berbahaya yang dilakukan oleh orang lain untuk mengambil data, manipulasi data, bahkan merusak data berharga untuk tujuan tertentu [2]

Diperlukan suatu sistem yang dapat menanggulangi dengan sebaik-baiknya terhadap kemungkinan ancaman dalam waktu singkat, hal ini akan mempercepat proses penanggulangan gangguan dan pemulihan sistem atau layanan. Salah satu metode yang dapat digunakan untuk mengatasi masalah tersebut adalah dengan menggunakan sistem deteksi intrusi (IDS). Adapun aplikasi yang mendukung sistem deteksi intrusi (IDS)

***Journal homepage**: http://journal.lppmunindra.ac.id/index.php/Faktor_Exacta*

adalah Snort [1]. Pengujian Snort IDS ini menggunakan metode serangan yang digunakan untuk menguji kehandalan Snort dalam mendeteksi serangan yang terjadi pada sistem keamanan [3]

Pada penelitian ini masalah yang diangkat adalah bagaimana cara agar serangan intrusi dapat terdeteksi dan administrator dapat mengetahui jika ada serangan intrusi hanya dari handphone secara real-time melalui aplikasi telegram sebagai notifikasi alert yang bertujuan untuk menjaga keamanan server dari serangan intrusi.

Dari hasil penelitian terdapat beberapa penelitian terdahulu yang hampir serupa dengan penelitian yang dilakukan penulis, beberapa di antaranya : Berdasarkan hasil penelitian sebelumnya snort berhasil mendeteksi sebanyak 966 serangan melalui protokol TCP, UDP sebanyak 179.049 paket, dan ICMP sebanyak 283 paket. Dampak serangan DoS menggunakan software LOIC dan

http://digilib.mercubuana.ac.id/

metode serangan ping flood menggunakan command line membuat menurunkan kinerja komputer target. Hal ini dibuktikan dengan penggunaan CPU yang meningkat dari 24% menjadi 90% sampai 100%, serta penggunaan memori yang meningkat dari 703 MB menjadi 1,17 GB. Hal ini membuktikan bahwa serangan DoS memakan jalur paket dengan meminta sejumlah besar paket dari target, dan jika serangan pada target memakan waktu lama, tidak hanya akan menurunkan kinerja komputer tetapi bahkan menyebabkan komputer target untuk down [4] Penelitian selanjutnya mengimplementasikan sistem keamanan jaringan dengan menggunakan aplikasi Snort IDS (Intrusion Detection System), Dengan mengecek keamanan jaringan dengan aplikasi IDS Snort, dengan dua penempatan Snort di VI Lab IST AKPRIND LAN Base Network 3 Yogyakarta, hasil yang didapat saat pengujian Port Scanning, serangan SSH dan DoS, penempatan Snort dalam lebih baik dari penempatan snort luar [5].

Perbedaan dalam penelitian sebelumnya dengan penelitian ini yaitu menggunakan Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) sebagai sistem untuk mendeteksi dan memblokir penyusup di server jaringan komputer, dan Snort sebagai peringatan berbasis aturan untuk melindungi jaringan komputer. Intrusion Detection System (IDS) akan diimplementasikan pada sistem operasi berbasis Linux sedangkan Intrusion Prevention System (IPS) akan diimplementasikan melalui firewall atau iptables. Menurut penelitian ini, pengujian dan analisis waktu respon sistem deteksi intrusi (IDS) dilakukan dengan menggunakan 3 model serangan: TCP Flood, UDP Flood, dan ICMP Flood. Pengujian pada sistem IDS yang diserang oleh 1 klien dan 2 klien secara bersamaan menghasilkan nilai akurasi peringatan yang sama, dengan rata-rata 99,98%. Rata-rata waktu respon adalah 0,53 detik saat diuji dengan 1 klien dan 0,32 detik dengan 2 klien [6]

Penelitian menggunakan metode Intrusion Detection System (IDS) menginstal snort di PC Server dapat memantau dan melindungi keamanan jaringan di jaringan yang sama dengan PC Server sebagai pusatnya. Tidak perlu lagi menginstal snort di komputer lain. IDS snort dapat mendeteksi serangan DDOS, Nmap dan lainnya Menggunakan snort dapat membantu Administrator memantau jaringan secara real-time karena snort dapat memberikan peringatan segera jika serangan terdeteksi, sehingga administrator dapat segera menindaklanjuti peringatan tersebut [7] Di Sini informasi akan disimpan dalam database mysql menggunakan kami telah membuat antarmuka pengguna untuk menampilkan semua sistemi informasi tentang peringatan yang dihasilkan. Informasi termasuk IP sumber, IP tujuan, peringatan yang dihasilkan, tanggal dan waktu paket sudah diterima. Dalam hal ini, kami menggunakan sistem untuk tujuan pengujian jadi sumber dan tujuan IP adalah loop saya alamat, tetapi ketika dijalankan di server itu memberi Sumber dan tujuan IP dari sistem yang dihasilkan dan menerima paket [8]

Dari latar belakang tersebut penulis membuat impelementasi sistem pendeteksi penyusup jaringan menggunakan SNORT dengan variable bash shell dengan mengirim pesan menggunakan aplikasi telegram. Harapannya dengan menerapkan SNORT dapat menjaga keamanan jaringan sehingga dengan menerapkan SNORT jaringan bisa di monitoring dan dapat melacak adanya penyusup yang menggunakan jaringan tersebut.

http://digilib.mercubuana.ac.id/

Intrusion Detection System

Intrusion Detection System adalah sistem pencegahan penyusup dengan menggunakan suatu perangkat lunak (software) atau perangkat keras (hardware) yang bekerja secara otomatis untuk memonitor keadaan. pada jaringan komputer dan dapat menganalisis masalah keamanan jaringan [9]. Intrusion Detection system (IDS) dapat didefinisikan sebagai tools, metode, sumber daya yang memberikan bantuan untuk melakukan identifikasi, memberikan laporan terhadap aktivitas jaringan komputer. Kemampuan dari IDS adalah memberikan peringatan kepada administrator server saat terjadinya sebuah aktivitas tertentu yang tidak diinginkan administrator sebagai penanggung jawab sebuah sistem, selain meberikan peringatan, IDS juga mampu melacak aktivitas yang merugikan sebuah system [10]. Suatu IDS dapat melakukan pengamatan (monitoring) terhadap paket – paket yang melawati jaringan dan berusaha menemukan apakah terdapat paket – paket yang berisi aktivitas – aktivitas mencuruigakan. Intrusion Detection system (IDS) berfungsi melakukan pengamatan (monitoring) kegiatan – kegiatan yang tidak lazim pada jaringan sehingga awal dari langkah para penyerang bisa diketahui. Dengan demikian administrator bisa melakukan tindakan pencegahan dan bersiap atas kemungkinan yang akan terjadi [11].

Snort

Snort adalah Intrusion Detection System jaringan open source yang mampu menjalankan analisis realtime dan paket logging pada IP network. Snort dapat menjalankan analisis protokol, content searching atau maching, dan dapat digunakan untuk mendeteksi berbagai serangan dan penyusupan [12] . Snort merupakan suatu perangkat lunak untuk mendeteksi penyusup maupun menganalisa paket yang melintasi jaringan computer secar realtime traffic dan logging ke dalam database serta mampu mendeteksi berbagai serangan yang berasal dari luar jaringan [13]. Snort dapat digunakan pada platform sistem operasi Linux, BSD, Solaris, Windows dan sistem operasi lainnya. Snort merupakan suatu intrusion detectiom system yang dipakai oleh banyak orang. www.snort.org menyediakan layanan untuk update rule dan signature, mailing list, forum diskusi, komunitas project dan layanan lain yang memudahkan user untuk mendapatkan informasi.

Snort dapat dioperasikan dengan tiga mode:

1. Packet Sniffer, untuk melihat paket yang lewat di jaringan.
2. Packet Logger, untuk mencatat semua paket yang lewat dijaringan untuk dianalisis dikemudian hari.
3. NIDS deteksi penyusup pada jaringan, pada mode ini snort akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer [11].

Instant Messaging Telegram

Instant Messaging Telegram adalah sebuah perangkat lunak atau aplikasi saat ini yang sangat populer di kalangan masyarakat. Tujuan utama aplikasi tersebut yaitu menyajikan fitur obrolan yang berjalan secara real time sehingga pesan langsung dapat terkirim dan diterima. Aplikasi instant messaging berjalan secara online atau dengan kata lain membutuhkan koneksi Internet. Saat ini terdapat banyak aplikasi instant messaging yang digunakan oleh masyarakat untuk mengobrol dengan individu maupun komunitas [14].

http://digilib.mercubuana.ac.id/

Fitur yang disajikan aplikasi tersebut tidak hanya melalui text based saja, tetapi bisa juga untuk melakukan obrolan melalui suara, bertukar foto, audio, video hingga dokumen digital. Salah satu aplikasi yang memiliki fitur tersebut yaitu Telegram. Telegram secara definisi merupakan alternatif layanan aplikasi perpesanan untuk ponsel (mobile) maupun desktop yang berbasis cloud dengan keamanan tingkat tinggi serta kecepatan aksesnya

Aplikasi instant messaging tersebut tersedia untuk berbagai device seperti ponsel yang berjalan pada system operasi Android, iOS, Windows Phone. Tidak hanya berjalan pada perangakt mobile, tetapi juga dapat berjalan system desktop seperti Windows dan Linux. Meskipun terlihat sederhana aplikasi instant messaging Telegram memiliki fitur yang lebih unggul dibandingkan aplikasi instant messaging lainnya. Telegram diklaim sebagai aplikasi yang aman dimana menyediakan pilihan pesan end-to-end yang akan di enskripsi [15]

Telegram Bot API

Telegram Bot API (Application Progamming Interface) adalah sebuah perangkat lunak atau aplikasi yang digunakan untuk berinteraksi antara Bot dengan penggunannya maka dari itu dibutuhkanlah sebuah API. (Mutaqin, 2016). Bot tersebut dapat melakukan beberapa pekerjaan yaitu:

1. Mengintegrasikan dengan layanan lainnya, Bot dapat mengirimkan komentar jarak jauh atau mengendalikan smart home. Selain itu, bot juga mampu mengirimkan pemberitahuan melalui Telegram ketika terjadi sesuatu di suatu tempat
2. Menciptakan alat khusus, Bot mampu memberikan pemberitahuan maupun memberikan sebuah peringatan, ramalan cuaca, terjemahan, atau layanan lain.
3. Membangun single player ataupun multiplayer game, Keunggulan lainnya yaitu bot mampu memainkan permainan seperti catur.
4. Membangun layanan social, Sebuah bot dapat menghubungkan orang-orang untuk mencari mitra percakapan berdasarkan kepentingan Bersama [15]

2. METODE

Jenis Penelitian

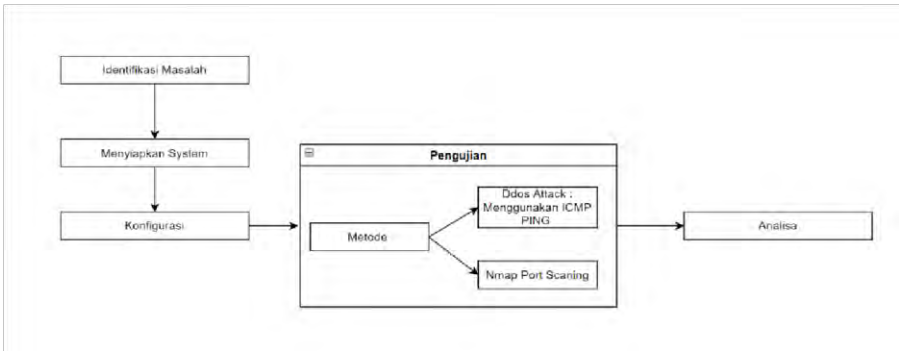
Metode yang digunakan dalam penelitian ini adalah penelitian Action Research, yang menggunakan studi kasus observasi sistematis, pengumpulan data, analisis informasi, dan metode pelaporan hasil.

Metode Pengumpulan Data

Metode pengumpulan data yang digunakan pada penelitian ini adalah observasi yaitu melakukan implementasi sistem deteksi penyusup jaringan menggunakan snort menggunakan linux ubuntu dengan melakukan pengujian terhadap sistem tersebut apakah sistem berjalan dengan baik dan mampu mendeteksi adanya penyusup di suatu jaringan yang menggunakan jaringan tersebut.

UNIVERSITAS MERCU BUANA

TAHAPAN PENELITIAN



Gambar 1 Tahapan Penelitian

Penjelasan terkait tahapan penelitian seperti pada gambar 1 dapat dijelaskan sebagai berikut:

1. Identifikasi Masalah bagaimana cara agar serangan intrusi dapat terdeteksi dan administrator dapat mengetahui jika ada serangan intrusi hanya dari handphone secara real-time melalui aplikasi telegram sebagai notifikasi alert yang bertujuan untuk menjaga keamanan server dari serangan intrusi.
2. Menyiapkan System
   Pada penelitian ini system yang di gunakan untuk mendeteksi serangan adalah snort yang bertujuan untuk meningkatkan keamanan pada server dari serangan intrusi.
3. Konfigurasi
   Melakukan konfigurasi pada local.rules dan nmap rules sedangkan untuk menyambungkan snort dengan bot telegram dilakukan konfigurasi menggunakan script bash shell agar bot telegram dapat mengirim pesan ke administrator setiap ada serangan intrusi.
4. Pengujian
   Pengujian dilakukan dengan 2 metode, yaitu :
   - Ddos Attack
     Jenis ddos attack yang di gunakan yaitu dengan menggunakan ICMP PING.
   - Nmap Port Scaning
     Nmap port scanning yang menggunakan aplikasi Nmap untuk melakukan port scanning.
5. Analisa
   Analisa bertujuan agar dapat mengetahui apakah system berjalan dengan baik atau tidak, dilakukannya analisa mulai dari penyerangan, pendeteksian, dan terkirimnya pesan alert ke pada administrator. Pesan alert yang di kirimkan oleh bot telegram kepada administrator terdapat keterangan hari, tanggal, waktu, dan jenis serangan intrusi yang dilakukan.

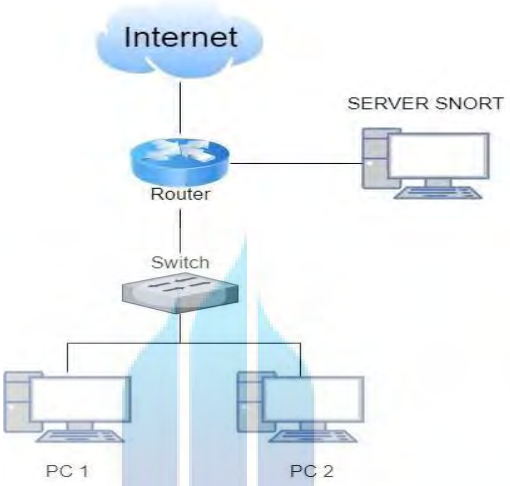
UNIVERSITAS MERCU BUANA

TAHAPAN EKSPERIMEN

Berdasarkan Gambar 1 Tahapan Penelitian dapat diuraikan langkah – langkah yang dilakukan selama perancangan, konfigurasi dan pengujian dapat dijelaskan. Penjelasan langkah – langkah tersebut adalah :

A. Topology Jaringan Rancangan Awal

Sistem Operasi yang digunakan untuk pengujian ini menggunakan sistem operasi Linux Ubuntu dan windows, percobaan serangan ini menggunaka beberapa laptop yang dijadikan sebagai attacker dengan tools yang digunakan tools Nmap dan ddos attack. Setelah dilakukan attacker menggunakan Nmap dan ddos attack, snort akan mendeteksi adanya serangan dapat dilihat pada gambar 2.

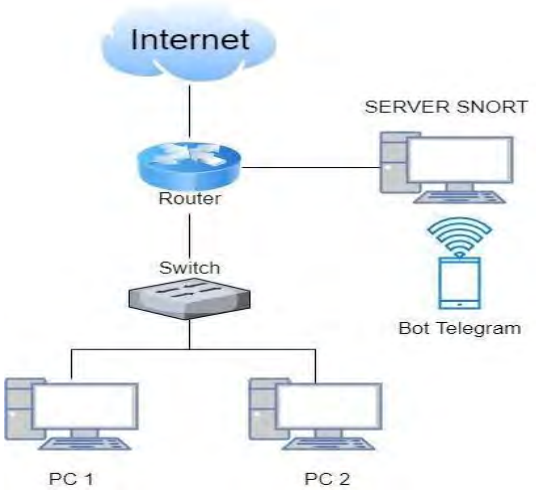


Gambar 2 Topology Jaringan Rancangan Awal

B. Topology Jaringan Rancangan Akhir

Pada rancangan akhir ini dilakukan pengembangan terhadap system snort, yaitu dengan melakukan penambahan aplikasi telegram yang berfungsi sebagai pesan alert. Sistem Operasi yang digunakan untuk pengujian ini menggunakan sistem operasi Linux Ubuntu dan windows, percobaan serangan ini menggunaka beberapa laptop yang dijadikan sebagai attacker dengan tools yang digunakan tools Nmap dan ddos attack. Setelah dilakukan attacker menggunakan Nmap dan ddos attack, snort akan mendeteksi adanya serangan tersebut dan bot telegram secara otomatis akan mengirim pesan ke administrator melalui aplikasi telegram dapat dilihat pada gambar 3.

UNIVERSITAS MERCU BUANA



Gambar 3 Topology Jaringan Rancangan Akhir

Setelah installasi selesai dilakukan lalu masuk ke file konfigurasi snort yang terdapat pada file snort.conf yang terletak pada direktori **/etc/snort/snort.conf**.

C. Konfigurasi snort.conf

Pengaturan yang utama yang di perlukan adalah konfigurasi jaringan ip address server lalu menambahkan rules nmap.rules di dalam snort.conf agar nmap port scan dapat terdeteksi merujuk pada gambar 4 dan gambar 5.

```
  GNU nano 4.8
# Step #1: Set the network variables.  For more information, see README.variables
#################################################

# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overriden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 192.168.10.115

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET
```

Gambar 4 Setting ip address

```
# site specific rules
include $RULE_PATH/local.rules
include $RULE_PATH/nmap.rules
```

Gambar 5 Penambahan Rules

D. Konfigurasi Rules

Konfigurasi rules ini bertujuan agar snort dapat mengirimkan text alert apabila adanya serangan pada jaringan dengan mengedit ***nano /etc/snort/rules/local.rules dan nano /etc/snort/rules/nmap.rules*** merujuk pada gambar 6 dan gambar 7.

```
root@andre-VirtualBox: /home/andre
GNU nano 4.8                                                    /etc/snort/rules/local.rules
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ---------------
# LOCAL RULES
# ---------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
alert icmp any any -> $HOME_NET any (msg:"ADA PENYUSUP JARINGAN"; sid:10000001; rev:001;)
lert tcp any any -> $HOME_NET 21 (msg:"FTP connection attempt";sid:10000011; rev:1;)
alert tcp any any <> $HOME_NET 21 (msg:"FTP failed login"; content:"Login incorrect";sid:10000012; rev:1;)
alert icmp any any -> $HOME_NET any (msg:"ICMP test"; sid:10000013; rev:1; classtype:icmp-event;)
alert tcp any any -> $HOME_NET any (msg:"TCP Port Scanning"; detection_filter:track by_src, count 30, seconds 60; sid:1000006; rev:2;)
```

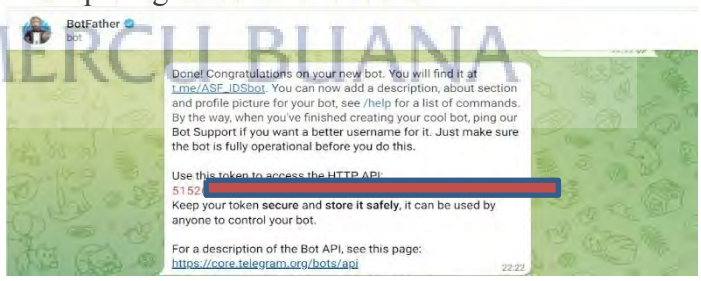
Gambar 6 Konfigurasi local.rules

```
root@andre-VirtualBox: /home/andre
GNU nano 4.8                                                    /etc/snort/rules/nmap.rules
alert icmp any any -> $HOME_NET any (msg: "NMAP ping sweep Scan"; dsize:0;sid:10000004; rev:1;)
alert tcp any any -> $HOME_NET 22 (msg: "NMAP TCP Scan";sid:10000005; rev:2; )
alert tcp any any -> $HOME_NET 22 (msg:"Nmap XMAS Tree Scan";flags:FPU;sid:1000006; rev:3;)
alert tcp any any -> $HOME_NET 22 (msg:"Nmap FIN Scan";flags:F;sid:1000008; rev:4;)
alert tcp any any -> $HOME_NET 22 (msg:"Nmap NULL Scan";flags:0;sid:1000009; rev:5;)
alert udp any any -> $HOME_NET any (msg:"Nmap UDP Scan";sid:1000010; rev:6;)
```

Gambar 7 Konfigurasi Nmap.rules

E. Membuat Bot Telegram dan Konfigurasi Bot Telegram

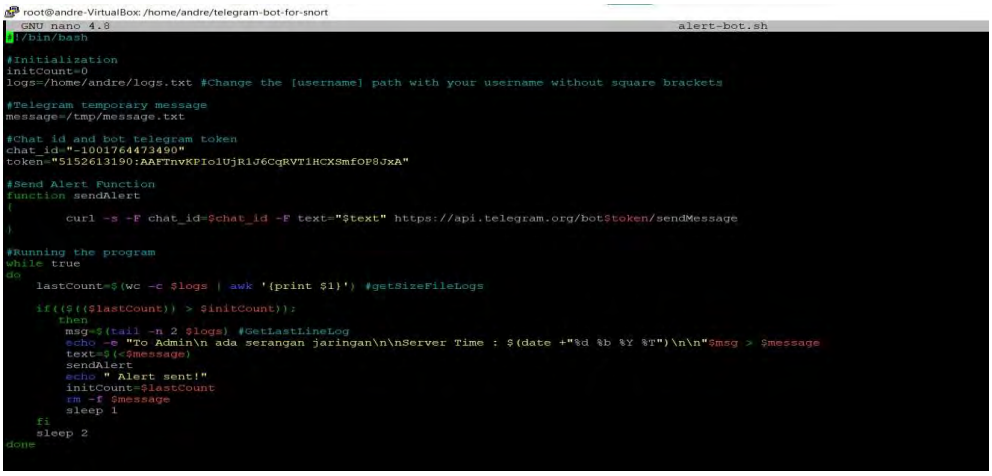
Bot telegram ini berguna untuk mengirimkan pesan berupa alert ke dalam sebuah group telegram yang mana group tersebut berisi team keamanan jaringan. Apabila adanya serangan terhadap jaringan baik berupa ping maupun dengan nmap port scanning. Bot telegram dapat dibuat menggunakan bot father dapat dilihat pada gambar 8.



Gambar 8 Membuat Bot Telegram

Setelah bot telegram telah dibuat maka selanjutkan melakukan konfigurasi pada bot telegram di snort dengan mencantumkan chat_id dan token bot telegram yang telah di dapatkan dari bot father agar pesan alert dapat terkirim secara otomatis ke dalam group team keamanan jaringan apabila terjadi serangan dengan menggunakan perintah ***nano bot-alert.sh*** dapat dilihat pada gambar 9.

UNIVERSITAS MERCU BUANA



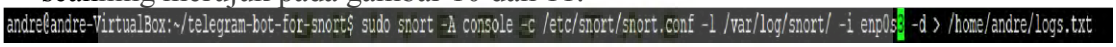
Gambar 9 Membuat Bot Telegram dan Konfigurasi Bot Telegram

3. HASIL DAN PEMBAHASAN

Pada bagian ini akan menampilkan keseluruhan hasil eksperimen yang telah di lakukan. Tahap ini menguji setiap skenario untuk melihat apakah simulasi jaringan yang dirancang pada tahap sebelumnya telah berjalan sesuai dengan rancangan.

A. Menjalankan Snort

Untuk menjalankan snort dapat dilakukan dengan menggunakan perintah ***sudo snort -A console -c /etc/snort/snort.conf -l /var/log/snort/ -i enp0s3 -d > /home/[username]/logs.txt*** yang mana nantinya snort akan otomatis mendeteksi adanya serangan baik berupa PING maupun berupa Nmap port scanning merujuk pada gambar 10 dan 11.



MERCU BUANA

Gambar 10 Script Menjalankan Snort

Gambar 11 Tampilan Snort Berjalan

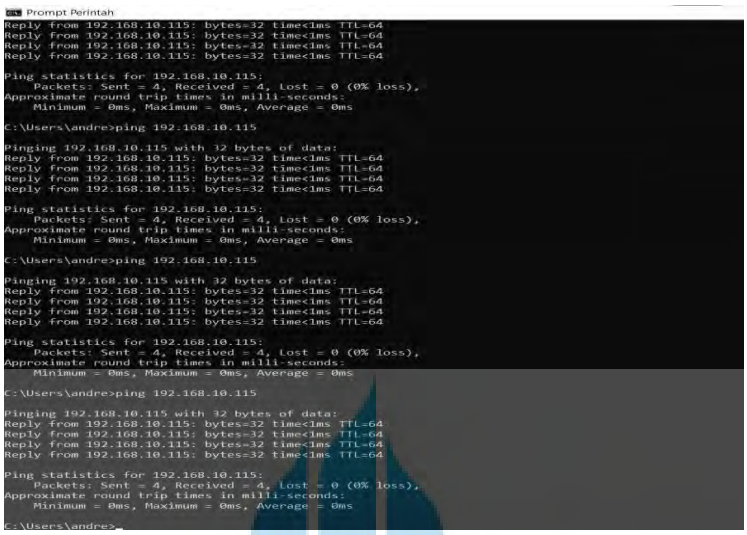
B. Menghubungkan Telegram

Untuk menghuhubungkan telegram dengan snort dapat dilakukan dengan menggunakan perintah ***./alert-bot.sh*** nantinya bot telegram otomatis akan memberikan notifikasi dengan mengirim pesan alert ke dalam grup chat dapat dilihat pada gambar 12.

Gambar 12 Menghubungkan Telegram

C. Pengujian Dengan Ddos Attack

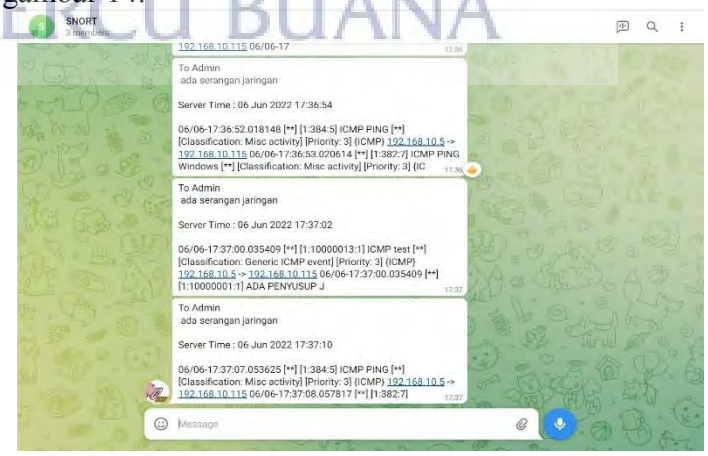
Setelah Snort dan Telegram di aktifkan maka kita melakukan Pengujian pertama dengan melakukan ddos attack dengan metode menggunakan ICMP PING di cmd dengan target ip address **192.168.10.115** dapat dilihat pada gambar 13.



Gambar 13 Pengujian Ddos Attack Menggunakan Metode Ping

D. Notifikasi Telegram Ddos attack

Ketika adanya aktivitas ddos dengan metode PING maka snort akan mendeteksi serta mengirimkan pesan alert ke dalam grup dengan keterangan ICMP PING WINDOWS dan ip address yang melakukan kegiatan tersebut dapat dilihat pada gambar 14.

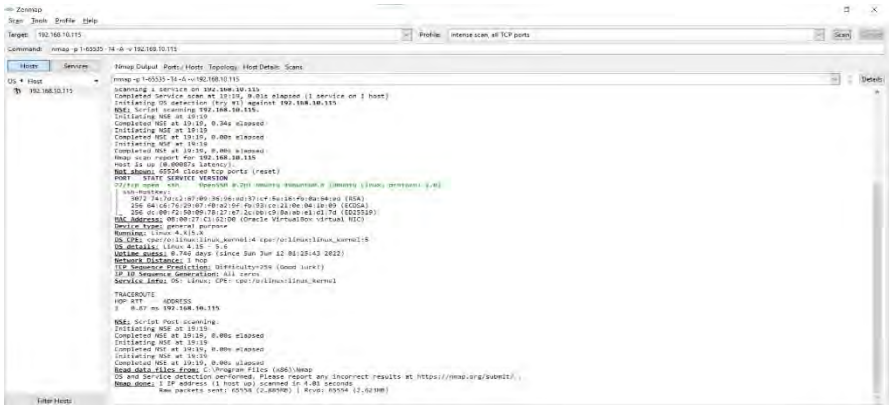


Gambar 14 Notifikasi Telegram Ping

E. Pengujian Nmap Port Scanning

Melakukan Pengujian ke dua dengan menggunakan Nmap Port scanning dengan target ip address **192.168.10.115** dapat dilihat pada gambar 15.

UNIVERSITAS MERCU BUANA



Gambar 15 Melakukan Nmap Port Scanning

F. Notifikasi Telegram Nmap Port Scanning

Saat ada aktivitas Nmap port scanning snort akan mendeteksi serta mengirimkan notifikasi pesan alert dengan keterangan NMAP TCP SCAN dan ip address yang melakukan kegiatan tersebut ke dalam grup telegram dapat dilihat pada gambar 16 .

Gambar 16 Notifikasi Telegram Nmap Port Scanning

UNIVERSITAS MERCU BUANA

G. Tampilan Snort mengirim pesan ke telegram

Ketika melakukan pengujian menggunakan PING maupun menggunakan NMAP port scanning snort akan mengirim pesan alert ke telegram dapat dilihat pada gambar 17.

Gambar 17 Tampilan Snort mengirim pesan ke telegram

H. Hasil Akurasi Deteksi Pengujian

hasil dari aktivitas pengujian terhadap server bertujuan untuk mengetahui seberapa tingkat akurasi dari tiap tiap aktivitas. Mulai dari penyerangan, pendeteksi hingga terkirimnya notifikasi alert ke aplikasi telegram. Hasil catatan tersebut diukur melihat tingkat akurasi snort.

No.	Jenis Serangan	Tingkat Akurasi Deteksi (WIB)		
		Awal Serangan	Terdeteksi	Terkirim Notifikasi
1.	Ddos Attack	18:28:13	18:28:15	18:28:16
2.	Port Scanning	19:21:03	19:21:05	19:21:06
3.	Ddos Attack	19:26:07	19:26:09	19:27:00
4.	Port Scanning	19:34:05	19:34:07	19:34:09
5.	Ddos Attack	19:40:10	19:40:12	19:40:13
.....	.....	.....	.....	.....
400.	Port Scanning	22:31:15	22:31:17	22:31:18

Tabel 1 Hasil Akurasi Pengujian

No.	Jenis Serangan	Selisih Waktu Deteksi Serangan (Detik)		
		Jumlah Serangan	Terdeteksi	Terkirim Notifikasi
1	Ddos Attack	200	2 Detik	1 Detik
2	Port Scanning	200	2 Detik	1 Detik

Tabel 2 Selisih Waktu Deteksi

Dari hasil tabel di atas kita dapat melihat tingkat akurasi dari sistem deteksi snort saat dilakukannya pengujian dengan menggunakan ddos attack menggunakan metode ICMP PING sebanyak 200 pengujian dan port scanning sebanyak 200 pengujian. Hasilnya Snort dapat mendeteksi serangan 1-2 detik, sedangkan dari waktu terdeteksi sampai dengan snort mengirim pesan alert ke telegram terdapat delay hanya sekitar 1 detik.

4. PENUTUP

Hasil dari penelitian ini dapat disimpulkan, Dengan menerapkan IDS (Intrusion Detection System) SNORT pada suatu jaringan komputer, seseorang yang menjadi administrator jaringan dapat mengetahui jika terjadi serangan atau upaya penyusupan terhadap salah satu server yang dimiliki. IDS (Intrusion Detection System) yang dibangun dapat memberikan notifikasi real-time kepada administrator jaringan melalui aplikasi Telegram, Snort dapat mendeteksi serangan 1-2 detik, sedangkan waktu dari terdeteksi sampai dengan snort

UNIVERSITAS MERCU BUANA

mengirim pesan alert ke telegram kedalam grup chat administrator terdapat delay hanya sekitar 1 detik.

DAFTAR PUSTAKA

[1] A. Erlansari, F. F. Coastera, and A. Husamudin, "Early Intrusion Detection System (IDS) using Snort and Telegram approach," *Sisforma*, vol. 7, no. 1, pp. 21–27, 2020, doi: 10.24167/sisforma.v7i1.2629.

[2] B. Fachri and F. H. Harahap, "Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer," *J. Media Inform. Budidarma*, vol. 4, no. 2, p. 413, 2020, doi: 10.30865/mib.v4i2.2037.

[3] I. P. A. E. Pratama and N. K. M. Handayani, "Implementasi IDS Menggunakan Snort Pada Sistem Operasi Ubuntu," *J. Mantik Penusa*, vol. 3, no. 1, pp. 176–181, 2019.

[4] R. Widodo and I. Riadi, "Intruder Detection Systems on Computer Networks Using Host Based Intrusion Detection System Techniques," *Bul. Ilm. Sarj. Tek. Elektro*, vol. 3, no. 1, p. 21, 2021, doi: 10.12928/biste.v3i1.1752.

[5] S. Kasus, L. Vi, J. Kampus, and I. S. T. Akprind, "Jurnal JARKOM Vol . 8 No . 1 Juni 2020 Jurnal JARKOM Vol . 8 No . 1 Juni 2020," *J. JARKOM*, vol. 8, no. 1, pp. 10–19, 2020.

[6] J. Informatika, "Implementasi Metode Intrusion Detection Systems (IDS) dan Intrusion Prevention Systems (IPS) Berbasis Snort Server Untuk Keamanan Jaringan LAN," *J. Inform.*, vol. 18, no. 1, pp. 71–84, 2018, doi: 10.30873/ji.v20i2.

[7] V. Prisscilya, T. Santoso, and J. T. Informatika, "Implementasi Keamanan Jaringan Menggunakan Intrusion," *J. Inf. Technol.*, pp. 1–8, 2021. [8] I. Journal, "SNORT".

[9] G. Tambunan and M. IGN, "Implementasi Keamanan Ids / Ips Dengan Snort Dan," *Semin. Nas. Mhs. Ilmu Komput. dan Apl. Jakarta-Indonesia, 28 Januari 2020 IMPLEMENTASI*, pp. 10–16, 2020.

[10] Y. Abdulloh, J. Triyono, and U. Lestari, "Pengaruh Penempatan Snort Terhadap Keamanan Jaringan (Studi Kasus Laboratorium Vi Jaringan Kampus 3 Ist Akprind Yogyakarta)," *J. JARKOM*, vol. 8, no. 1, pp. 10–19, 2020.

[11] B. Sudradjat, "Sistem Pendeteksian dan Pencegahan Penyusup Pada Jaringan Komputer Dengan Menggunakan Snort dan Firewall," *JISAMAR (Journal Inf. Syst. Applied, Manag. Account. Res.*, vol. 1, no. 1, pp. 10–24, 2017.

[12] M. Akbar, "PERANCANGAN SOFTWARE IDS SNORT UNTUK PENDETEKSIAN SERANGAN INTERRUPTION (Netcut) PADA JARINGAN WIRELESS," *J. INSTEK (Informatika Sains dan Teknol.*, vol. 3, no. 1, pp. 121–129, 2018, doi: 10.24252/instek.v3i1.5007.

[13] S. Z. H. 201. Muhammad Halmi Dar, "Syaiful Zuhri Harahap 1) , Muhammad Halmi Dar 2)," vol. 6, no. 3, pp. 24–27, 2018.

[14] J. Fahana, R. Umar, and F. Ridho, "QUERY : Jurnal Sistem Informasi Volume : 01 , Number : 02 , October 2017 ISSN 2579-5341 (online) Pemanfaatan Telegram Sebagai Notifikasi Serangan untuk Keperluan Forensik Jaringan QUERY : Jurnal Sistem Informasi Volume : 01 , Number : 02 , October 2017," *QUERY J. Sist. Inf.*, vol. 5341, no. October, pp. 6–14, 2017.

[15] D. Tri Atmaja, E. Budhy Prasetya, and P. Edi Kresnha, "Notifikasi Adanya Serangan Pada Jaringan Komputer Dengan Mengirim Pesan Melalui Aplikasi Telegram Dan Kontrol Server," *J. Univ. Muhammadiyah Jakarta*, pp. 1–8, 2018, [Online]. Available: https://jurnal.umj.ac.id/index.php/semnastek/article/view/3449

UNIVERSITAS MERCU BUANA

KERTAS KERJA

Ringkasan

Kertas kerja ini berisi tentang kelengkapan material dari artikel jurnal dengan judul "Implementasi Sistem Deteksi Penyusup Jaringan Menggunakan Snort Dengan Mengirim Pesan Melalui Aplikasi Telegram ". Seluruh hasil penelitian Tugas Akhir yang tidak dimasukkan kedalam artikel jurnal. Pada kertas kerja ini disajikan terdiri dari literatur review, analisis perancangan, source code, dataset yang digunakan, tahapan eksperimen dan seluruh hasil eksperimen.

- Bagian 1 : Literature Review menjabarkan mengenai beberapa jurnal yang terkait dengan penelitian.
- Bagian 2 : Analisis dan Perancangan menjabarkan jenis penelitian dan metode pengumpulan data
- Bagian 3 : Source Code menjabarkan kumpulan kode disetiap proses yang dilakukan peneliti
- Bagian 4 : Pengambilan dataset yang akan dilakukan.
- Bagian 5 : Tahapan Eksperimen berisi langkah langkah yang dilakukan selama perancangan, konfigurasi, dan pengujian
- Bagian 6 : Hasil semua eksperimen secara keseluruhan yang mencakup skenario pengujian yang dilakukan oleh peneliti.

UNIVERSITAS MERCU BUANA