

P-ISSN : 2337 - 8344

E-ISSN : 2623 - 1247

Jurnal InformaSI dan Komputer



**Diterbitkan Oleh :
STMIK DIAN CIPTA CENDIKIA KOTABUMI**

Volume 10 Nomor 2 Tahun 2022

Penerbit

Lembaga Penelitian STMIK Dian Cipta Cendikia Kotabumi

**Hak atas naskah/tulisan tetap berada pada penulis, isi diluar tanggung jawab
penerbit dan Dewan Penyunting**



PENGANTAR REDAKSI

Puji syukur dipanjatkan kehadiran Tuhan Yang Maha Esa, atas karunia dan limpahan rahmatNYA jualah Jurnal Informasi dan komputer (JIK) STMIK Dian Cipta Cendikia Kotabumi ini dapat terwujud. Jurnal Informasi dan Komputer (JIK) yang terbit dua (2) kali dalam setahun ini merupakan suatu wadah untuk penyebar luasan hasil-hasil penelitian, studi pustaka, karya ilmiah yang berkaitan dengan Informasi dan Komputer khususnya bagi dosen-dosen STMIK Dian Cipta Cendikia Kotabumi serta umumnya para cendekiawan, praktisi, peneliti ilmu Informatika dan Komputer.

Harapan, dengan diterbitkannya Jurnal Informasi dan Komputer (JIK) ini sebagai salah satu bentuk sumbangan pemikiran dalam pengembangan ilmu informatika dan komputer yang berkaitan dengan kajian-kajian di bidang teknologi Informatik, Komunikasi Data dan Jaringan Komputer, perancangan dan Rekayasa Perangkat Lunak, serta ilmu-ilmu yang terkait dengan bidang Informasi dan Komputer lainnya.

Berkenaan dengan harapan tersebut, kepada para peneliti, dosen dan praktisi yang memiliki hasil-hasil penelitian, kajian pustaka, karya ilmiah dalam bidang tersebut diatas, dengan bangga redaksi Jurnal Informasi dan Komputer (JIK) menerima naskah ringkasan untuk dimuat pada jurnal Informasi dan Komputer (JIK) STMIK Dian Cipta Cendikia Kotabumi dengan berpedoman pada penulisan naskah jurnal sebagaimana dilampirkan pada halaman belakang (Bagian kulit dalam) buku jurnal ini.

Mutu dari suatu jurnal ilmiah tidak hanya ditentukan oleh para pengelolanya saja, tetapi para penulis dan pembaca jualah yang mempunyai peranan besar dalam meningkatkan mutu jurnal Informatika dan Komputer ini. Merujuk pada realita ini kami sangat mengharapkan peran aktif dari peneliti untuk bersama-sama menjaga dan memelihara keberlangsungan dari jurnal Informasi dan Komputer STMIK Dian Cipta Cendikia Kotabumi ini. Yang juga tidak kalah pentingnya dari partisipasi tersebut diatas, adalah saran dan kritik yang membangun dari pembaca yang budiman agar kiranya dapat disampaikan langsung kepada redaksi JIK. Saran dan kritik yang membangun akan dijadikan masukan dan pertimbangan yang sangat berarti guna peningkatan mutu dan kualitas Jurnal Informasi dan Komputer STMIK Dian Cipta Cendikia Kotabumi.

Tak lupa diucapkan terima kasih yang tak terhingga atas perhatian dan kerjasama dari semua pihak yang tak dapat disebutkan satu persatu hingga dapat diterbitkan nya Jurnal Informasi dan Komputer (JIK) STMIK Dian Cipta Cendikia Kotabumi. Semoga apa yang telah diperbuat untuk kebaikan akan menjadi amal ibadah, amin.

Kotabumi, 25 Oktober 2022



Dewan Redaksi

JURNAL INFORMASI DAN KOMPUTER

Volume 10 Nomor 2 Oktober 2022

Jurnal Informasi dan Komputer merupakan Sarana informasi ilmu pengetahuan, Teknologi dan Komunikasi yang berupa hasil penelitian, tulisan ilmiah, Atau pun studi pustaka. Jurnal ini terbit dua kali setahun pada bulan April dan Oktober. Berisi hasil penelitian ilmiah di bidang informatika yang bertujuan untuk menghubungkan adanya kesenjangan antar kemajuan teknologi dan hasil penelitian. Jurnal ini di terbitkan pertama kali pada tahun

2013.

Penanggung Jawab:

Ketua STMIK Dian Cipta Cendikia Kotabumi

Pembina:

Ketua STMIK Dian Cipta Cendikia Kotabumi
Ketua Lembaga Penelitian STMIK Dian Cipta Cendikia Kotabumi

Pimpinan Redaksi

Dwi Marisa Efendi, S.Kom., M.T.I

Redaksi pelaksana

Rustam, S.Kom., M.T.I (Institut Teknologi Bisnis Dan Bahasa Dian Cipta Cendikia) Nurmayanti M.Kom (Institut Teknologi Bisnis Dan Bahasa Dian Cipta Cendikia) Sukatmi, S.Kom., M.Kom (Institut Teknologi Bisnis Dan Bahasa Dian Cipta Cendikia) Sampurna Dadi Riskiono, M.Kom (Universitas Teknokrat Indonesia)
Ifo Wahyu Pratama, S.Kom., M.T.I (Institut Teknologi Bisnis Dan Bahasa Dian Cipta Cendikia)
Sri Wahyuni, M.Kom, (Universitas Panca Sakti Bekasi)
Rima Mawarni, M.Kom, (STMIK Dian Cipta Cendikia Kotabumi)

Mitra Bestari

Dr. RZ. ABDUL AZIZ, ST., MT (Institut Informatika dan Bisnis Darmajaya)
Dr. Dadang Sudrajat, S.Si, M.Kom (STMIK IKMI Cirebon)
Dr. Septafiansyah Dwi Putra, S.T., M.T (Politeknik Negeri Lampung)
Darma Pala Riau)

Dr. Evi Grativiani, S.E., M.S.I (Universitas Sebelas Maret)

Dr. Mohammad Iqbal, S.Kom, MMSI (Universitas Gunadarma)

Rohmat Indra Borman (Universitas Teknokrat Indonesia)

Ferry Wongso, S.Kom., M.Kom (STMIK

Ferly Ardhy, S.Kom., M.T.I (Universitas Aisyah Pringsewu)

Firmansyah, S.E., M.Si (STMIK Darma Pala Riau)

Amarudin (Universitas Teknokrat Indonesia)
Alhibarsyah, St., M.Kom (STMIK Tunas Bangsa Bandar Lampung)

Kemal Farouq Mauladi, S.Kom .M.Kom (Universitas Islam Lamongan)

Wira Jaya Hartono, S.Pd., M.Pd (STMIK Darma Pala Riau)

Dwi Marisa Efendi, S.Kom, M.T.I (Institut Teknologi Bisnis Dan Bahasa Dian Cipta Cendikia)

Ni Luh Ratniasih, S.Kom., M.T (Institut Teknologi dan Bisnis STIKOM Bali)

Ni Komang Sri Julyantari, S.Kom., M.T (Institut Teknologi dan Bisnis STIKOM Bali)

Penerbit : STMIK Dian Cipta Cendikia Kotabumi
Bekerja Sama Dengan LPPM STMIK Dian Cipta Cendikia Kotabumi.

Alamat Redaksi/Penerbit:

Jl. Negara No. 3 Candimas Kotabumi Lampung Utara

No Telp/Fax 0724 23003

Email : lppm-stmik@dcc.ac.id



JURNAL INFORMASI DAN KOMPUTER VOL. 10 NO. 2 THN. 2022

DAFTAR ISI

Halaman

Pengembangan Aplikasi Pelelangan Menggunakan Framework Codeigniter Berbasis Web Yuli Syafitri ¹ , Reni Astika ² , Lusia Septia Eka Esti Rahayu ³ (AMIK Dian Cipta Cendikia).....	01-07
Pengelompokan Status Gizi Balita Dengan Data Langsung Dan Data Tidak Langsung Ni Komang Sri Julyantari ¹ , Ni Made Dewi Kansa Putri ² (ITB STIKOM Bali).....	09-17
Penerapan Data Mining Menggunakan Algoritma Apriori Dalam Memprediksi Penjualan Produk Ferly Ardhy ¹ , Ockhy Jey Fhiter Wassalam ² , Tahta Herdian Andika ³ , Salman Alfarisi Salimu ⁴ (Universitas Aisyah Pringewu).....	18-23
Analisis Celah Keamanan Jaringan Menggunakan Pengujian Intrusion Detection System Dan Microsoft Network Monitor Aliy Hafiz ¹ , Sukatmi ² (AMIK Dian Cipta Cendikia).....	24-28
Rekayasa Perangkat Lunak Inventory Barang Dengan Metode Fast Pada Petshop Salsa Di Bandarlampung Pitrawati ¹ , Verawati ² , Riska Bilgisa Putri ³ (AMIK Dian Cipta Cendikia).....	29-38
Komparasi Algoritma Winnowing Dan Algoritma Manber Dalam Mendeteksi Kemiripan Tugas Mahasiswa Ida Bagus Ketut Surya Arnawa (ITB STIKOM Bali).....	39-46
Klasifikasi Quality Of Service Layanan Internet Menggunakan Algoritma Naive Bayes Cindyk Irawanto ¹ , Odi Nurdian ² , Gifthera Dwilestari ³ (STMIK IKMI Cirebon).....	47-54
Implementasi Metode Rc6 Untuk Keamanan Pesan Berbasis Android Suci Ananda Sari ¹ , Wiwien Hadikurniawati ² (Universitas Stikubank Semarang).....	55-61
Sistem Deteksi Manusia Dengan Metode Aggregate Channel Features (Acf) Umi Kholifah ¹ , Veronica Lusiana ² (Universitas Stikubank Semarang).....	62-69
Pengukuran Kualitas Website Kota Administrasi Jakarta Utara Terhadap Kepuasan Pengguna Menggunakan Metode Webqual4.0 Rachma Dien ¹ , Iwan ²	

(Universitas Nusa Mandiri).....	70-81
Penerapan Model V Dalam Pengembangan Sistem Penjualan Online Pada Toko Lapak Teknik Tools Suhermanto ¹ , Septi Kristin Anantasia ² (Universitas Panca Sakti Bekasi).....	82-89
Analisis Sentimen Program Migrasi Tvdigital Menggunakan Algoritmanaive Bayesdengan Chi Square Virgaria Zuliana ¹ , Garno ² , Iqbal Maulana ³ (Universitas Singaperbangsa Karawang).....	90-95
Perbandinganmetodesimple Queuedan Queue Treedalam Optimalisa Simanajemen Bandwidth Nafis NaufalAnwari ¹ , Puwantoro ² , TesaNurPadilah ³ (Universitas SingaperbangsaKarawang).....	96-100
Tingkat Keefektifan Pengembangan Sistem Informasi Dalam Era Revolusi Industri 4.0 Rizky Rahmat Illahi ¹ , Nafis Naufal Anwari ² , Aji Primajaya ³ (Universitas Singaperbangsa Karawang).....	101-105
Sistem Pendukung Keputusan Pemilihan Mobil Menggunakan Metode Copras Abdul Patahudin ¹ , Felix Andreas Sutanto ² (UnisbankSemarang).....	106-111
Analisis Dan Perancangan Sistem Informasipenjualan Jasa Pencucian Sepatu Dan Tas Pada Sojishoesandbagcareberbasismobile DandiRamasenjaya ¹ , KundangKarsonoJuman ² (Universitas Esa Unggul).....	112-121
Sistem Pendukung Keputusan Pemilihan Komputer Berdasarkan Komponen Menggunakan Metode Hybrid Ahp Dan Mooraberbasis Web Febian Ageng Resta (Universitas Stikubank Semarang).....	222-228
Perancangan Sistem Perpustakaan Onlinedi Ma Al Hasan Dengan Metode Spiralberbasis Web Suhermant ¹ , Riza Apriansyah ² (Universitas Panca Sakti Bekasi).....	129-135
Evaluasi Sistem Informasi Electronic Daily Perform Report (E-Dpr Denganmenggunakanframeworkcobit 5 Afif Khoirul Abdi ¹ , Endro Kuswoyo ² , Indah Purnamasari ³ (UniversitasNusaMandiri).....	136-142
Sistem Pengambilan Keputusan Perceraian Dipengadilan Negeri Kotabumi Dengan Metode Saw Nurmayanti ¹ , MerriParida ² , DesiMalina ³ (STMIK Dian Cipta Cendikia Kotabumi).....	143-154
Penerapan Metode Algoritma Apriori Dalam Memprediksi Penjualan Sparepart Motor (Pt. Lautan Teduh Interniaga Dealer Yamaha Kotabumi) Sidik Rahmatullah ¹ , Sigit Mintoro ² , Karmila Permatasari ³ (STMIK Dian Cipta Cendikia Kotabumi).....	155-163
Sistem Pakar Diagnosa Penyakit Ibu Hamil Menggunakan Metode Certainty Factor (Cf) Untuk Menurunkan Risiko Kematian Ibu Hamil Berbasis Android	

Aliy Hafiz ¹ , Ferry Susanto ² , Donny Muda Priyangan ³ , Chandra Kirana ⁴ (AMIK Dian Cipta Cendikia).....	164-169
Sistem Pendukung Keputusan Pemilihan Perguruan Tinggi Swasta Sehat Dengan Metode Analytical Hierarchy Process (Ahp) (Study Kasus : Provinsi Lampung) Sulasminarti (AMIK Dian Cipta Cendikia Pringsewu).....	170-181
Penerapan Metode V-Model Dalam Perancangan Sistem Penjualan Online Produk Furniture Menggunakan Php Mysql Di Pd Dua Putri Yuyun Yuningsih (UniversitasPancaSaktiBekasi).....	182-188
Penerapan Metode K-Nearest Neighbour Untuk Sistem Penentuan Peminjaman Modal Nasabah Bank Syariah Indonesia Cabang Cikarang Berbasis Website Melina Rahmadiyah ¹ , Parman Suparman ² (Universitas Panca Sakti Bekasi).....	189-197
Penerapan Internet Of Things Pada Stop Kontak Lampu Berbasis Arduino M. Abu Jihad Plaza R ¹ , Yulina ² , Sigit Gunanto ³ (Universitas Muhammadiyah Kotabumi).....	198-204
Penerapan Metode Profile Matching Dalam Penentuan Peserta Pelatihan Terbaik (Studi Kasus: Lpk Prima Buana Indonesia Cabang Purwakarta) SriWahyunin ¹ , FarizRizalMubarok ² (Universitas PancaSaktiBekas).....	205-217
Sistem Penunjang Keputusan Dengan Metode Ahp Menentukan Peringkat Siswa Berdasarkan Hard Skill Dan Soft Skill Haris Munandar ¹ , Tumini ² (Universitas PancaSaktiBekas).....	218-224
Sistem Informasi Penjualan Kuliner Pada Kedai Linda Berbasis Web Di Kotaagung Kabupaten Tanggamus” (Studi Kasus Kedai Linda Kotaagung) Rima Mawarni ¹ , Supriyanto ² , Dodi Afriansyah ³ , Linda Riyanti ⁴ (STMIK Dian Cipta Cendikia Kotabumi).....	225-230
Penerapan Sistem Informasi Penampungan Aspirasi Masyarakat Berbasis Website Halim Saputro ¹ , Agustami ² , Wahid Susanto ³ , Iwan ⁴ (Universitas Nusa Mandiri).....	231-235
Pengembangan Skema Paten Pada Sistem Informasi Hak Kekayaan Intelektual Lppm Universitas Dhyana Pura I Made Dwi Ardiada ¹ , Putu Wida Gunawan ² , Gerson Feoh ³ (Universitas Dhyana Pura).....	236-245
Pengembangan Game Edukasi Untuk Meningkatkan Pemahaman Materi Anatomi Tubuh Bagi Siswa Sd Menggunakan Metode Research And Development Moch Feri Izulhaq ¹ , Ade Irma Purnamasari ² , Arif Rinaldi Dikananda ³ (STMIK IKMI Cirebon).....	246-251
Pengembangan Game Edukasi Tebak Surah Pendek Untuk Mengasah Daya Pikir Siswa Menggunakan Metode Research And Development Musofi ¹ , Nana Suarna ² , Arif Rinaldi Dikananda ³ (STMIK IKMI Cirebon).....	252-256
Klasifikasi Jenis Kucing Menggunakan Algoritma Principal Component Analysis Dan K-Nearest	

Neighbor Aisyah Nur Ramadhayani ¹ , Veronica Lusiana, ² (Universitas Stikubank Semarang).....	257-263
Audit Pelayanan Kir Pada Dinas Perhubungan Lampung Utara Menggunakan Metode It-Val Merri Parida ¹ , Nurmayanti ² , Nova Alda Yanti ³ (STMIK Dian Cipta CendikiaKotabumi).....	264-273

ANALISIS CELAH KEAMANAN JARINGAN MENGGUNAKAN PENGUJIAN INTRUSION DETECTION SYSTEM DAN MICROSOFT NETWORK MONITOR

Aliy Hafiz¹, Sukatmi²

AMIK Dian Cipta Cendikia¹²

Jl. Cut Nyak Dien No. 65 Palapa Durian Payung Bandar Lampung

E-mail : hafiz@dcc.ac.id¹, Sukatmi@dcc.ac.id²

ABSTRAK

Kejahatan dunia maya dewasa ini sepatutnya mendapat perhatian semua pihak secara seksama. Dengan menggunakan aplikasi IDS dan Network Monitoring seperti Microsoft Network Monitor bisa mendeteksi serangan yang menargetkan server. Pencegahan serangan dengan pendeteksian anomali yaitu dengan membandingkan lalu lintas jaringan yang sedang diawasi dengan lalu lintas jaringan yang biasanya terjadi. Dengan kemampuan ini Snort dapat mempermudah penanganan keamanan jaringan komputer.

Kata kunci : IDS, SNORT, Network, Anomali

ABSTRACTS

Cybercrime today deserves the attention of all parties carefully. Using IDS and Network Monitoring applications such as Microsoft Network Monitor can detect attacks targeting servers. Attack prevention with anomaly detection is by comparing the network traffic being monitored with network traffic that usually occurs. With this capability Snort can simplify the handling of computer network security.

Keywords: contains a maximum of 5 important words in the study.

1. PENDAHULUAN

Isu keamanan jaringan berkembang seiring meningkatnya arus lalu lintas penggunaan jaringan dan internet. Diperlukan perangkat keamanan seperti firewall yang dapat menghentikan paket data yang tidak diizinkan, kriptografi dengan cara mengenkripsi data yang dikirimkan sehingga orang yang tidak berkepentingan tidak dapat mengambil informasi dari paket tersebut dan Snort sebuah aplikasi berbasis IDS.

Snort adalah sebuah software open source yang memiliki banyak fungsing yang sangat membantu administrator dalam menangani ancaman yang telah terjadi. Snort memiliki banyak fungsi yang diantaranya adalah mode IDS yang dapat

memberikan sebuah peringatan kepada administrator apabila sedang terjadi sebuah ancaman pada jaringan komputer [1].

Perancangan Snort yang baik harus meperhatikan apakah rule yang dibuat berhasil dalam mendeteksi sebuah penyusupan yang terjadi. Disisi lain kita tidak boleh melupakan kemampuan dari mesin yang digunakan dalam pengimplementasian Snort. Melihat permasalahan tersebut dalam penelitian ini mencoba untuk membuat sebuah rule dan melakukan percobaan pengaplikasian rule tersebut kemudian dari hasil percobaan ini kita dapat melihat efektifitas rule yang telah dibuat apakah dapat menangkap tindakan penyusupan dengan tepat[2].

2. METODE PENELITIAN

1. Deskripsi Sistem

Sistem ini dirancang untuk melakukan pendeteksian terhadap sejumlah aktivitas mencurigakan yang sedang terjadi pada jaringan komputer. Awalnya sistem akan menangkap paket data yang pada jaringan komputer. Kemudian paket data tersebut akan dianalisis berdasarkan rules yang telah diimplementasikan. Dari analisis tersebut dapat diambil keputusan apakah sedang terjadi sebuah ancaman atau tidak. Apabila terjadi sebuah ancaman maka sistem akan mengeluarkan peringatan kepada administrator dan juga melakukan pencatatan terhadap paket data tersebut untuk dapat diteliti lebih jelas oleh administrator.

2. Tinjauan Pustaka

1. SNORT

Snort adalah sebuah software keamanan yang sangat berguna untuk mengamati aktivitas dalam suatu jaringan komputer. Snort bersifat open source GNU (General Public License), sehingga boleh digunakan dengan bebas dan gratis, kode sumber (source code) untuk Snort juga bisa didapatkan dan dimodifikasi sendiri. Dalam penggunaannya Snort masih berbasis command line sehingga cukup merepotkan bagi user yang terbiasa dengan pemakaian Graphical User Interface (GUI). Snort dapat menjadi sebuah packet sniffer yang memungkinkan Snort untuk membaca lalu lintas jaringan komputer yang ada[3].

2. Rule IDS

Rule berupa *script* yang dapat mengenali adanya tindakan penyusupan yang sedang terjadi pada jaringan komputer kita berdasarkan *signature*. fungsi dari rule inilah yang membuat Snort sangat baik dalam pendeteksian penyusupan. Setiap rule memiliki dua logical bagian, rule header dan rule option. Rule header mengandung informasi tentang aksi yang akan diambil. Rule header juga mengandung kriteria untuk pencocokan sebuah rule terhadap paket data. Sedangkan *rule option*

biasanya mengandung peringatan dan informasi tentang bagian mana dari paket yang harus digunakan untuk menghasilkan pesan[4].

3. Microsoft Network Monitor

Microsoft Network Monitor merupakan software yang dapat digunakan untuk mengetahui lalu lintas data yang sedang dikirim dan diterima melalui jaringan komputer saat itu maupun dari file data yang diambil sebelumnya sehingga dapat dilakukan analisa. Software ini menyediakan pilihan penyaringan untuk analisis kompleks mengenai jaringan data[5].

Fitur Microsoft Network Monitor diantaranya :
Parser Configuration Management: Parser sekarang telah terinstal dengan profil yang memudahkan anda untuk beralih antara parser configuration dengan Parser Profiles toolbar button. Konfigurasi ini juga menyembunyikan, menghilangkan kebutuhan untuk mengkompilasi ulang ketika Anda beralih di antara keduanya.

Color Rules: Network Monitor sekarang dapat menyimpan set aturan warna ke file untuk mempermudah sharing. Anda juga dapat mengklik kanan di Frame Summary dan Frame Detail Windows untuk menambahkan Peraturan Warna baru.

4. NAT (Network Address Translation)

NAT adalah cara untuk menyembunyikan beberapa komputer yang menggunakan IP *private* di belakang IP publik. Dengan menggunakan NAT, komputer internal di jaringan tetap bisa menggunakan internet meskipun menggunakan IP *private*. Tetapi sebaliknya, pengguna internet tidak bisa mengenali workstation yang ada di dalam NAT[6].

3. Metode Pengujian

Pengujian dilakukan terhadap beberapa jenis serangan yang terjadi pada jaringan komputer. Melakukan intrusi terhadap suatu sistem dapat berupa port scanning, ping of death, dan brute force.

3. HASIL DAN PEMBAHASAN

Berikut ini adalah hasil dari pengujian yang telah dilakukan baik dari aplikasi IDS dan Microsoft Network Monitor yang memonitor paket pada jaringan.

1. Mulai SNORT

Yaitu menggunakan command :

```
snort -T -c /etc/snort/snort.conf
```

hasil :

```
Running in packet dump mode

--- Initializing Snort ---
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{3F433250-3DF9-4F95-8AA3-949EFD210A8A}".
Decoding Ethernet

--- Initialization Complete ---

-> Snort! <-
o" )~ Version 2.9.11.1-NIN32 GRE (Build 268)
.... By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2017 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.38 2015-11-23
Using ZLIB version: 1.2.3

Commencing packet processing (pid=9516)
```

Gambar 1. Memulai Snort

2. Menentukan Rule

1. Rule Ping

Rule digunakan oleh snort untuk acuan dalam melakukan pendeteksian. Dengan kata lain, rule ini adalah kumpulan aturan pendeteksian terhadap beberapa kemungkinan serangan pada suatu jaringan komputer. Dalam kasus ini saya akan memberikan contoh rule terhadap serangan ping.

Letak file yang digunakan untuk menyimpan rule dibawah ini berada di /etc /snort /rules /local.

Commad:

```
alert icmp any any -> any any (msg:"Ada Serangan Ping";sid:10000001;rev:0;)
simpan.
```

2. IDS Mode

Command:

```
snort -v
snort -vd
snort -vde
```

```
snort -v -d -e
```

Keterangan:

-v, untuk melihat header TCP/IP serta paket yang lewat pada jaringan.

-d, untuk melihat isi paket.

-e, untuk melihat header link layer paket seperti ethernet header.

3. Packet Logger Mode

Digunakan untuk mencatat semua paket yang lewat di jaringan di analisa dikemudian hari.

Command:

```
snort -dev -l /var/log/snort
snort -dev -l /var/log/snort -h 172.20.10.0/24
snort -dev -l /var/log/snort -b
```

Untuk membaca log yang dihasilkan oleh mode packet logger

Command:

```
snort -dv -r /var/log/snort/paket.log
snort -dvr /var/log/snort/paket.log icmp
snort -r /var/log/snort/snort.log
```

Dengan IDS Mode, berarti snort akan difungsikan untuk mendeteksi serangan yang dilakukan melalui jaringan komputer. Dalam penggunaan mode IDS ini di perlukan setup dari berbagai rules / aturan yang akan membedakan sebuah paket normal dengan paket yang membawa serangan. Karena saya sudah menunjukkan setup rule diatas, mari jalankan Snort IDS Mode! Jangan lupa ya, harus menggunakan hak akses root (#).

4. IDS Full Mode

Command:

```
snort -A full -c /etc/snort/snort.conf
```

```

C:\Windows\system32\cmd.exe - snort -v
Total sessions: 0
-----
Reputation Preprocessor Statistics
Total Memory Allocated: 0
-----
Snort exiting
C:\Snort\bin\snort -v
Running in packet dump mode

---- Initializing Snort ----
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "Device\NPF_{3F433250-3DF9-4F95-8AA3-949EFD210ABA}".
Decoding Ethernet

==== Initialization Complete ====

--> Snort! <--
Version 2.9.11.1-WIN32 GRE (Build 268)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2017 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.38 2015-11-23
Using ZLIB version: 1.2.3

Commencing packet processing (pid=5740)

```

Gambar 2. Memulai Snort

5. Hasil Log File

Hasil Deteksi Melalui Log File

Command:

tail -f /var/log/snort/alert

```

[**] [1:10000001:0] Ada Serangan Ping [**]
[Priority: 0]
06/05-07:57:30.366395 192.168.43.12 -> 192.168.43.212
ICMP TTL:64 TOS:0x0 ID:30132 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:27320 Seq:2 ECHO

[**] [1:10000001:0] Ada Serangan Ping [**]
[Priority: 0]
06/05-07:57:30.366448 192.168.43.212 -> 192.168.43.12
ICMP TTL:64 TOS:0x0 ID:57476 IpLen:20 DgmLen:84
Type:0 Code:0 ID:27320 Seq:2 ECHO REPLY

[**] [1:10000001:0] Ada Serangan Ping [**]
[Priority: 0]
06/05-07:57:31.365425 192.168.43.12 -> 192.168.43.212
ICMP TTL:64 TOS:0x0 ID:30351 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:27320 Seq:3 ECHO

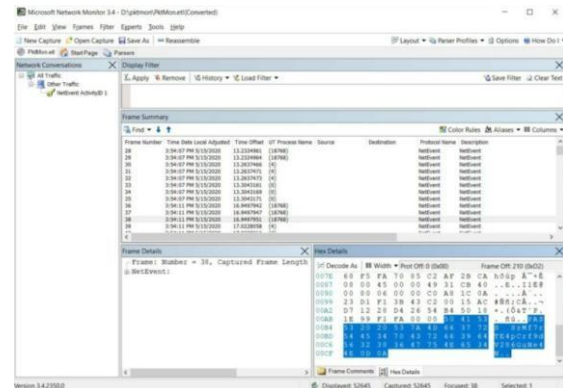
[**] [1:10000001:0] Ada Serangan Ping [**]
[Priority: 0]
06/05-07:57:31.365487 192.168.43.212 -> 192.168.43.12
ICMP TTL:64 TOS:0x0 ID:57655 IpLen:20 DgmLen:84
Type:0 Code:0 ID:27320 Seq:3 ECHO REPLY

```

Gambar 3. Log File

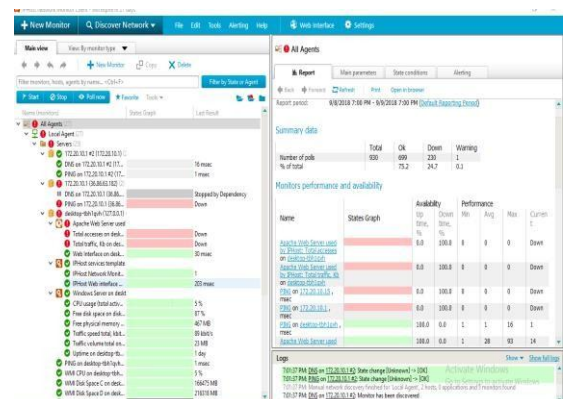
3. Pembahasan

Setelah berhasil konfigurasi SNORT langkah selanjutnya adalah analisa menggunakan Microsoft Network Monitor. Adapun langkahnya adalah sebagai berikut:



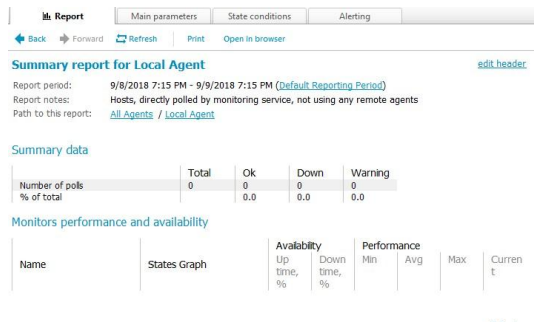
Gambar 4. Microsoft Network Monitor

Pada Microsoft Network Monitor menunjukkan adanya anomali pada jaringan yang ditandai paket paket yang tidak seharusnya ada ketika jaringan dalam kondisi normal. Dengan adanya paket tertentu akan menandai adanya serangan yang terjadi seperti berupa port scanning, ping of death, dan brute force.



Gambar 5. Microsoft Network Monitor

Pada gambar di atas memperlihatkan kondisi jaringan yang dalam keamanan diserang. Dimana paket paket yang ada terdapat paket data berupa port scanning, ping of death, dan brute force.



Gambar 6. Hasil Setelah Dipasang IDS

Paket data yang semula muncul sebelum dipasang IDS kemudian di deteksi dan dilarang untuk masuk maka kondisi lalu lintas jaringan bisa normal kembali.

4. KESIMPULAN

Kejahatan dunia maya dewasa ini sepatutnya mendapat perhatian semua pihak secara seksama. Dengan menggunakan aplikasi IDS dan Network Monitoring seperti Microsoft Network Monitor bisa mendeteksi serangan yang menargetkan server. Pencegahan serangan dengan pendeteksian anomali yaitu dengan membandingkan lalu lintas jaringan yang sedang diawasi dengan lalu lintas jaringan yang biasanya terjadi. Dengan kemampuan ini Snort dapat mempermudah penanganan keamanan jaringan komputer.

DAFTAR PUSTAKA

- [1] Hafiz, A., Kurniawan, T., Sivi, N. A., Ikhsan, F. K., & Andhika, P. (2020). Analisis Celah Keamanan Jaringan Dan Server Menggunakan Snort Intrusion Detection System. *Jurnal Informasi Dan Komputer*, 8(2), 55-65
- [2] Mutaqin, A. F. (2016). Rancang Bangun Sistem Monitoring Keamanan Jaringan Prodi Teknik Informatika Melalui Sms Alert Dengan Snort. *Jurnal Sistem Dan Teknologi Informasi (Justin)* Vol, 1(1), 1.
- [3] Ferihadi, F., & Ilman Zuhri, Y. (2020). *Perbandingan Jaringan Vpn Menggunakan Pptp (Point To Point Tunnel Protocoll) Dan L2tp (Studi Kasus: Kantor Pemerintah Walikota Palembang)* (Doctoral Dissertation, Universitas Bina Darma).
- [4] Anggoro, B. S., & Sulistyio, W. (2019, November). Implementasi Intrusion Prevention System Suricata Dengan Anomaly-Based Untuk Keamanan Jaringan Pt. Grahamedia Informasi. In *Seminar Nasional Aptikom (Semnastik) 2019* (Pp. 280-288).
- [5] Adidrajat, F. T., & Mulyani, A. (2019). Load Balancing Web Server Berbasis Cloud Dengan Menggunakan Algoritma Round-Robin Pada Sampoerna University. *Journal Of Information System, Applied, Management, Accounting And Research*, 3(4), 37-44.
- [6] Purwaningtyas, R., Prasertijo, A. B., & Sofwan, A. (2011). *Perancangan Program Bantu Pembelajaran Topologi Jaringan Lokal Secara Visual Menggunakan Borland Delphi 6.0* (Doctoral Dissertation, Jurusan Teknik Elektro Fakultas Teknik Undip)