P-ISSN : 2337 - 8344
E-ISSN : 2623 - 1247

Jurnal InformaSI dan Komputer

Diterbitkan Oleh :
STMIK DIAN CIPTA CENDIKIA KOTABUMI

Volume.8 **Nomor.2** **Tahun**

P-ISSN : 2337 - 8344
E-ISSN : 2623 - 1247

Penerbit:
STMIK DIAN CIPTA CENDIKIA KOTABUMI
Bekerjasama dengan LPPM STMIK DCC Kotabumi

PENGANTAR REDAKSI

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

Harapan, dengan diterbitkannya Jurnal Informatika dan Komputer (InfoKom) ini sebagai salah satu bentuk sumbangan pemikiran dalam pengembangan ilmu informatika dan komputer yang berkaitan dengan kajian-kajian di bidang tekhnologi Informatik, Komunikasi Data dan Jaringan Komputer, perancangan dan Rekayasa Perangkat Lunak, serta ilmu-ilmu yang terkait dengan bidang Informatika 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 Informatika dan Komputer (JIK) menerima naskah ringkasan untuk dimuat pada jurnal Informatika dan Komputer (InfoKom) 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 kamu sangat mengharapkan peran aktif dari peneliti untuk bersama-sama menjaga dan memelihara keberlangsungan dari jurnal Informatika 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 Informatika 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 Informatika dan Komputer (InfoKom) STMIK Dian Cipta Cendikia Kotabumi. Semoga apa yang telah diperbuat untuk kebaikan akan menjadi amal ibadah, amin.

Kotabumi, 25 Oktober 2020

Dewan Redaksi

JURNAL INFORMASI DAN KOMPUTER

Volume 8 Nomor 2 Oktober 2020

Jurnal Informasi dan Komputer merupakan Sarana informasi ilmu pengetahuan, Tekhnologi dan Komunikasi yang berupa hasil penelitian, tulisan ilmiah, Ataupun 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.

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 Telpon/Fax 0724 23003
Email : lppm-stmik@dcc.ac.id

P-ISSN: 2337-8344
E-ISSN: 2623-1247

JURNAL INFORMASI DAN KOMPUTER
VOL. 8 NO. 1 THN. 2020

DAFTAR ISI

Halaman

Sistem Pakar Identifikasi Penyakit Kelapa Sawit Dengan Metode Fuzzy Mamdani Dan Certainty Factor Studi Kasus : "Kelompok Tani Desa Banjar Kertarahayu"
Asep Afandi, Rustam,
(Universitas Gunadarma, IIB Darma Jaya) 01-11

Rancang Bangun Sistem Informasi Pemetaan Toko Oleh-Oleh Dan Souvenir Khas Lampung Dikota Bandar Lampung Berbasis Android
Yuli Syafitri, Muhammad Rizal
(IIB Darma Jaya Bandar Lampung, AMIK DCC Bandar Lampung).....12-23

Implementasi Data Mining Menggunakan Multi Regresi Untuk Memprediksi Rerata Kedatangan Masyarakat,
Dwi marisa Efendi, Riski Oskar Pratama,
(IIB Darma Jaya, STMIK Dian Cipta Cendikia Kotabumi) 24-28

Audit Sistem Informasi Pembayaran Spp Menggunakan It-Il Version 3
Ferly Ardhy, Ardiana Safitri
(IIB Darma Jaya,STMIK Dian Cipta Cendikia Kotabumi) 29-37

Penerapan Metode Extreme Programming Smartschool Pada SMK Nusantara 1 Kotabumi
Merri Parida, Ahmad Basori Ali
(AMIKOM Yogyakarta, STMIK Dian Cipta Cendikia Kotabumi)..... 38-47

Penerapan Metode Extreme Programming Pada Sistem Informasi Layanan Perpustakaan SMP Negeri 3 Negara Batin Berbasis Web Mobile
Nurmayanti[1], Yoga Iman Wijaya[2] Sistem Informasi, Sistem Informasi
STMIK Dian Cipta Cendikia Kotabumi 48-54

Analisis Celah Keamanan Jaringan Dan Server Menggunakan Snort Intrusion Detection System
Aliy Hafiz,Triandi Kurniawan, Nuari Anisa Sivi, Fathurrahman Kurniawan Ikhsan,
Panji Andhika Pratomo
(AMIK Dian Cipta Cendikia, UNU Lampung, UMITRA Indonesia, STMIK Pringsewu).....55-65

Sistem Informasi Data Penjualan Dan Stok Barang Di Toko Rudi Etalase Berbasis Web
Ngajiyanto, Rima Mawarni, Sigit Mintoro, Fachri Pawiga
(AMIKOM Yogyakarta, STMIK Eresha, IIB Darma Jaya, STMIK Dian Cipta Cendikia Kotabumi)..... 66-72

Penerapan Data Mining Untuk Prediksi Penjualan Produk Triplek Pada Pt Puncak Menara Hijau Mas
Rustam, Sidik Rahmatullah, Supriyato, Sri Wahyuni
(IIB Darma Jaya, AMIKOM Yogyakarta, IIB Darma Jaya, STMIK DCC Kotabumi)..... 73-84

Sistem Informasi Penjualan Helm Secara Online Pada Toko Dewi Di Kotaagung Kabupaten

Tanggamus (Studi Kasus Toko Dewi Kotaagung)
Rima Mawarni, Dewi Triyanti, Dewi Zaurati, S.Kom
(STMIK Eresha , IIB Darma Jaya, AMIK Dian Cipta Cendikia Pringsewu) 85-90

ANALISIS CELAH KEAMANAN JARINGAN DAN SERVER MENGGUNAKAN SNORT INTRUSION DETECTION SYSTEM

Aliy Hafiz[1],Triandi Kurniawan[2],Nuari Anisa Sivi[3],Fathurrahman Kurniawan Ikhsan[4],Panji Andhika Pratomo[5]
[1,2]AMIK Dian Cipta Cendikia, [3]UNU Lampung, [4]UMITRA Indonesia, [5]STMIK Pringsewu
Jl. Cut Nyak Dien No. 65 Durian Payung (Palapa) Bandar Lampung
E-mail : hafizdahsyat@gmail.com[1],triandi5556@gmail.com[2],nuaruasivi@gmail.com[3],
fathuriks@gmail.com[4],panjiandhikap@gmail.com[5].

ABSTRAK

Backdoor atau disebut juga pintu belakang adalah akses khusus yang dibuat oleh penyerang untuk dapat masuk kembali kedalam sistem yang telah dibobol. Kebanyakan dari pemilik website mengabaikan security system website tersebut karena kurangnya pengetahuan mengenai security atau kurangnya tenaga pengelola dalam manajemen, sehingga menguntungkan bagi seorang attacker untuk mudah masuk kedalam sistem. Perlu adanya sistem keamanan yang mampu mendeteksi backdoor karena akibatnya yang sangat buruk bagi sistem. Sistem ini disebut dengan intrusion detection system, adapun yang banyak digunakan adalah Snort IDS. Sistem keamanan ini berbasis website yang mampu mendeteksi celah keaamanan salah satunya keberadaan backdoor.

Kata Kunci *: Snort, IDS, Keamanan, Website*

ABSTRACTS

Backdoor or also known as back door is a special access made by the attacker to be able to re-enter the system that has been compromised. Most of the website owners ignore the security system of the website because of a lack of knowledge about security or lack of management personnel, making it profitable for an attacker to easily enter the system. There is a need for a security system that is able to detect backdoors because the consequences are very bad for the system. This system is called an intrusion detection system, while the one that is widely used is the Snort IDS. This security system is based on a website that is able to detect security holes, one of which is the existence of a backdoor.

Keywords: *Snort, IDS, Security, Website*

1. PENDAHULUAN

Perkembangan internet yang sedemikian pesat menjadikan keamanan suatu data atau informasi pada server yang terhubung dengan publik menjadi sangatlah penting untuk diperhatikan. Menurut Yusep, kerentanan terhadap serangan kejahatan lewat dunia maya di Indonesia masih terjadi. Pada 2012, jaringan internet negara mengalami lebih dari satu juta serangan. Serangan itu berupa pencurian data, pemalsuan data, pengubahan data (misalnya halaman muka situs web), phising, pembocoran data, spionase industri, penyalahgunaan data oleh orang dalam, dan kejahatan lainnya[1].

Keamanan server komputer sebagai bagian dari sebuah sistem sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya[2]. Keamanan sebuah jaringan komputer dapat dikelompokkan menjadi dua bagian yaitu keamanan yang bersifat fisik dan bersifat non fisik.

Website menjembatani para penggunanya untuk mendapatkan berbagai macam informasi dari mana saja. Akibatnya kebutuhan akan informasi semakin meningkat, sehingga membuat para developer website berlomba-lomba menyajikan berbagai inovasi baik dalam interface, fitur maupun integrasi plugin terhadap CMS (*Content Management System*) yang mereka gunakan agar pengguna mudah, nyaman dan sering berkunjung untuk mendapatkan informasi baik layanan maupun dukungan. Hal itu memicu timbulnya suatu kebutuhan security untuk sistem komputer.

Kejahatan online atau Cyber Crime yaitu kejahatan dengan jenis serangan seperti Virus, Worm, Trojan, DoS, Web Deface, Pembajakan Software sampai dengan masalah pencurian kartu kredit. Oleh karena keamanan sistem komputer sangat rentan, suatu usaha pencegahan dan pendeteksian diperlukan. Berbagai macam teknik yang digunakan[3].

Seorang attacker untuk bisa masuk ke dalam sebuah sistem server menggunakan berbagai macam teknik eksplotasi atau disebut eksploit kemudian untuk dapat masuk kembali kedalam sistem dengan mudah maka attacker akan memasang backdoor. Backdoor bisa berupa shell yang memanfaatkan bug di sebuah sistem server atau website. Shell tersebut akan di simpan kedalam direktori website yang kiranya sulit untuk di jangkau atau di deteksi oleh pemilik website, dilain itu juga attacker akan membuat sanitasi berupa nama yang sama terhadap file yang familiar dengan sistem, sehingga ketika pemilik website melihat disangkanya merupakan sebuah sistem.

Backdoor (Pintu belakang) merupakan akses khusus yang dibuat oleh penyerang untuk dapat masuk kedalam sistem tanpa diketahui oleh operator sistem. Kebanyakan dari pemilik website mengabaikan security system website tersebut karena kurangnya pengetahuan mengenai security atau kurangnya tenaga pengelola dalam manajemen, sehingga menguntungkan bagi seorang attacker untuk mudah masuk kedalam web server. Perlu adanya sistem yang mampu mendeteksi backdoor secara rinci, diantaranya mampu mengetahui celah website, dan exploits yang digunakan attacker [4].

Penelitian serupa tentang IDS Snort yaitu seperti yang dilakukan oleh AY Ananta menghasilkan bahwa IDS Snort sangat baik untuk mendeteksi adanya serangan ke dalam jaringan [5]. Kemudian penelitian yang dilakukan oleh Wijaya, bahwasanya IDS Snort mampu mendeteksi penyusupadan ke dalam server[6]. Hadirnya firewall telah banyak membantu dalam pengamanan, akan tetapi seiring berkembangnya teknologi sekarang ini hanya dengan firewall keamanan tersebut belu bisa dijamin sepenuhnya. Karena itu telah berkembang sistem IDS sebagai pembantu pengamanan data pada suatu jaringan komputer. Dengan adanya IDS (Intrusion Detection System). Maka serangan-serangan tersebut lebih dapat dicegah ataupun dihilangkan. Intrusion Detection System berguna untuk mendeteksi adanya serangan dari penyusup.

2. METODE PENELITIAN

2.1 Metode IDS Snort

Berikut adalah metode yang ada pada IDS Snort dalam melakukan pendeteksian pada backdoor[7]:

1. Paket decoder

Paket Decoder berfungsi untuk mengambil paket dari berbagai jenis network interface dan mempersiapkan paket yang akan di preprocessed atau dikirim ke Detection Engine.

2. Preprocessors

Preprocessor adalah komponen atau plug-in yang dapat digunakan dengan Snort untuk mengatur atau memodifikasi paket data sebelum detection engine melakukan beberapa operasi untuk mengetahui apakah paket yang digunakan oleh penyusup. Beberapa preprocessor juga melakukan deteksi dengan mencari anomaly dalam header paket dan menghasilkan alert. Preprocessor sangat penting untuk setiap IDS untuk mempersiapkan paket data

yang akan dianalisa terhadapat aturan dalam detection engine.

3. Detection Engine

Detection Engine adalah bagian paling penting dari Snort. Detection Engine bertanggung jawab untuk mendeteksi jika ada aktivitas intrusi dalam sebuah paket. Detection Engine menggunakan rule Snort. Untuk tujuan ini, rule dibaca dengan struktur data internal atau dimana mereka cocok dengan semua paket. Jika sebuah paket cocok dengan rule apapun, maka tindakan yang tepat akan dilakukan atau diambil tetapi jika tidak paket akan dibuang.

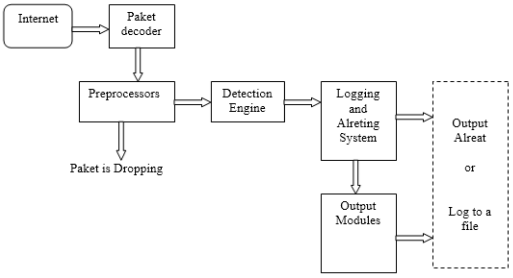
Detection Engine adalah time-critical bagian dari Snort. Tergantung pada seberapa kuat mesin adan berapa banyak aturan telah ditetapkan, mungkin diperlukan jumlah waktu yang berbeda untuk merespon paket yang berbeda, jika lalu lintas (traffic) di jaringan terlalu tinggi, maka ketika Snort NIDS bekerja dalam model ini, mungkin ada beberapa paket yang di drop dan mungkin tidak mendapatkan real-time respone yang benar.

Beberapa faktor beban pada detection engine :
1. Jumlah rule
2. Kekuatan mesin dalam menjalankan Snort
3. Kecepatan internet yang digunakan dalam mesin Snort.
4. Load pada jaringan.
5. Database yang banyak file
6. Logging and Alreting System

Tergantung pada apa yang detection engine temukan dalam sebuah paket, paket digunakan untuk mencatat aktivitas atau menghasilkan peringatan. Nantinya log akan disimpan dalam bentuk file teks sederhana.

4. Output Modules

Output module atau plug-in dapat melakukan operasi yang berbeda tergantung pada administrator dalam menyimpan output yang dihasilkan oleh logging dan system alert dari Snort. Pada dasarnya modile ini mengontrol jenis output yang dihasilkan oleh logging dan memperingatkan system.



Gambar 1. Komponen Snort

2.2 Analisis Kebutuhan

Backdoor adalah cara yang digunakan untuk masuk kedalam sistem tanpa sepengetahuan administrator. Backdoor bertujuan untuk mempermudah memasuki sistem itu kembali jika jalan yang sudah dibuat dengan exploit telah ditutup oleh administrator. Maka dibuatlah simulasi yang saling berhubungan yang bertujuan untuk melakukan analisis terhadap Backdoor yang menggunakan IDS snort. Berdasarkan Hasil kebutuhan perangkat lunak software dan OS yang dibutuhkan adalah
1. Linux Ubuntu
2. Windows 10
3. Virtual Box
4. IDS Snort
5. Browser Google Chrome
6. Jaringan LAN/WiFi

1. Analisa kebutuhan hardware spesifikasi hardware komputer yang dibutuhkan untuk implementasi IDS serta perangkat pengujian adalah sebagai berikut :

Perangkat/ OS	Spesifikasi	Ket
Linux Ubuntu Server 14.04 LTS	Core i3, Ram 2 GB, HDD 500 GB	1 unit
Windows	Core i3, Ram 2 GB, HDD 500 GB	2 unit
Switch	TP-LINK 8-Port Gigabit Desktop Switch - TL-SG108	1 unit

2. Analisa kebutuhan perangkat lunak kebutuhan software komputer yang dibutuhkan untuk

implementasi IDS serta perangkat pengujian adalah sebagai berikut :

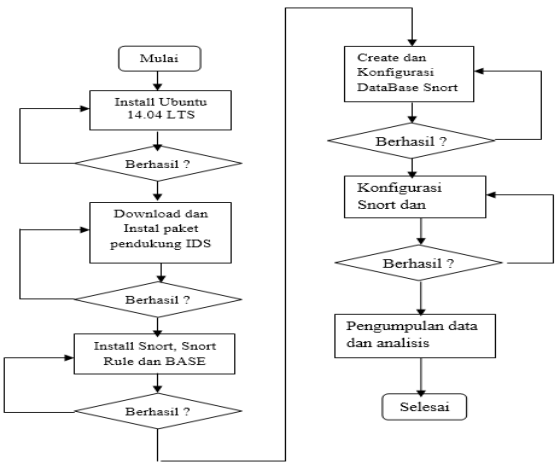
Sistem	Tools/Framework	Ket
IDS	Snort	Versi 2.9.6.0
Database	Mysql	Versi 14.14
Web server	Apache	Versi 2.4.7
Backend Web server	PHP	Versi 5
Browser	Mozilla Firefox	Versi 61.0

2.3 Perancangan

Tahap analisis menghasilkan rincian spesifikasi kebutuhan dari sistem yang akan dibangun. Perancangan menjadikan rincian spesifikasi kebutuhan untuk menghasilkan spesfikasi rancangan sistem yang akan dibangun.

2.3.1 Perancangan Sistem

Agar sistem Intrusion Detection System (IDS) dapat berjalan dengan baik, diperlukan beberapa proses instalasi, seperti instalasi system operasi yang akan digunakan dan instalasi paket-paket pendukung yang dibutuhkan, seperti : Snort. Proses-proses tersebut dapat diliat pada diagram alir dibawah ini.



Gambar 2. Diagram Alir Untuk Mendeteksi Backdoor

Berdasarkan pada gambar diatas dapat dijelaskan sebagai berikut :

1. Pada peroses pertama yaitu diawali dengan instalsi sistem operasi pada PC. Sistem operasi yang digunakan pada PC adalah Linux Ubuntu Server 14.04 LTS. Setelah selesai dan berhasil mengistal selanjutnya akan menginstal paket-paket pendukung untuk sistem.
2. Selanjutnya download dan install paket paket pendukung dari IDS tersebut, seperti: Apache, PHP dan Mysql. Jika berhasil lanjut ketahap berikutnya.
3. Tahap berikutnya adalah installasi Snort. Sebagai inti dari sistem yang akan kita bangun. Setelah berhasil melakukan installasi tersebut dilanjutkan ketahap berikut.
4. Membuat database dari snort, agar nantinya semua log dan sistem yang kita bangun bisa menyimpan semua kejadian kedalam database, setelah berhasil mebuat database lanjut ke proses berikutnya yaitu mengkonfigurasi database.
5. Setelah selesai membuat dan mengkonfigurasi database dilanjutkan ke konfigurasi Snort
6. Setelah semua proses selesai, tahap terakir adalah melakukan pengujian pada sistem dan pengumpulan data serta menganalisis.

2.4 Proses pengaktifan Snort

Pada proses pengaktifan snort perlu di perhatikan rules yang akan digunakan serta seluruh perangkat berkerja dengan baik, sehingga pengujian dapat berjalan bernga lancar, pada tahap pertama pengaktifan snort IDS dengan menggunakan perintah berikut:

Table1. Sintaks IDS Snort

No	Sintak	Keterangan
1	Sudo	Sintak ini digunakan untuk menjalankan program dibawah user dengan hak akses penuh (root/administrator)
2	Snort	Merupakan sintak nama

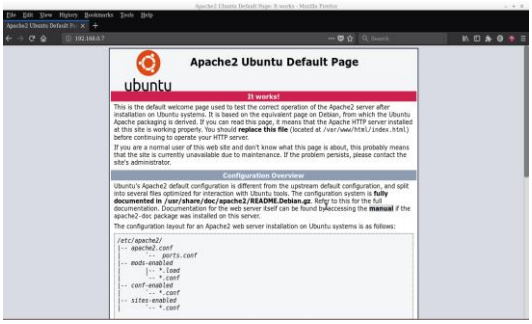
		program snort
3	-A console	Sintak ini merupakan opsi yang ada pada snort yang mana selurh alert akna di kirimkan ke layar monitor (screen)
5	-i eth0	Sintak ini digunakan untuk mendefinisikan port ethernet mana yang akan di monitoring oleh snort, dalam percobaan ini port dengan nama eth0 digunakan dalam pengawasan snort.
7	-c /etc/snort/snort .conf	Sintak ini digunakan untuk memberi tahu dimana tempat file configurasi yang akan digunakan oleh snort
9	-l /var/log/snort	Sintak ini digunakan untuk memberitahu dimana tempat menyimpan log alert yang dihasilkaa.

3. HASIL DAN PEMBAHASAN

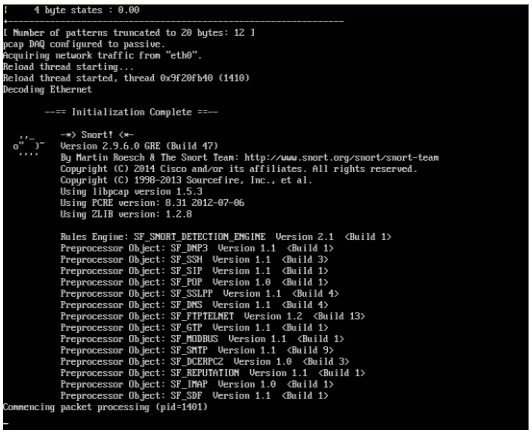
Pada tahap ini sistem diuji pada keadaan normal, sehingga akan diketahui jika terjadi kesalahan deteksi oleh snort, pengujian dilakukan dengan melakukan koneksi normal dengan menggunakan web browser serta sistem snort yang telah diaktifkan. Pada pengujian yang dilakukan dengan cara membuka alamat web default apache yang terdapat pada web server. Dari kegiatan yang dilakukan dapat dilihat pada gambar 4.1 yang mana web menampilkan konten dari index.html yang tersimpan pada web server.

3.1 Proses Pengujian dengan Serangan

Pada saat permintaan halaman yang dilakukan oleh pengguna sistem snort melakukan deteksi pada aliran data yang masuk pada web server, dimana pada percobaan yang dilakukan pada aliran data normal ini menghasilkan sistem snort tidak mendeteksi adanya serangan yang terjadi pada webserver yang dapat dilihat paga gambar 3.



Gambar 3. Tampilan Browser Normal



Gambar 4. Tampilan snort pada saat tidak ada serangan

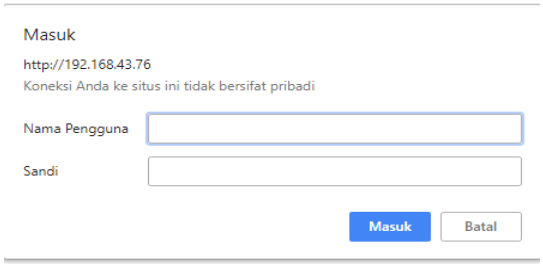
Pada percobaan dengan hasil gambar 3 menunjukkan dengan permintaan normal pada web server, sistem snort tidak mendeteksi serangan yang terjadi sehingga dapat diambil kesimpulan bahwa sistem bekerja dengan baik.

3.2 Proses Pengujian dengan Serangan

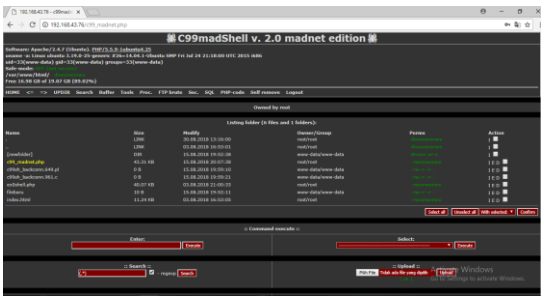
Pada tahap ini sistem di lakukan percobaan dengan menjalanakn php backdoor pada web browser. Dengan terlebih dahulu mengaktifkan sistem snort yang telah terpasang. Dalam pengujian ini dipergunakan backdoor php dengan nama "c99_madnet" yang mana memiliki perintah yang lengkap dan memiliki halaman login pada gambar 4 untuk masuk kedalam sistem backdoor yang sudah di simpan pada sistem webserver. Pada saat penyerang mengaktifkan backdoor yang ada dengan mengetikkan nama pada url web browser maka seketika halaman login backdoor aktif yang mana meminta usernam dan password, serta sistem

IDS Snort yang langsung menumukan adanya serangan yang terjadi pada webserver dengan memnuculkan pesan peringatan pada layar monitor , seperti yang terlihat pada gambar 5.

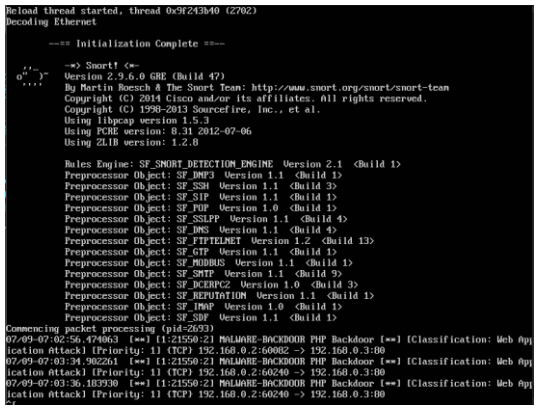
Setelah penyerang berhasil masuk pada backdoor yang ditanamnya maka akan muncul tampilan seprti pada gambar 4. Dimana gambar 4.4 merupakan halaman utama backdoor c99_madnet. Dalam backdoor ini penyerang dapat melakukan banyak hal, mulai dari mengunggah file, menghapus file, mencari file, membuat file, membuat folder dan lain sebagainya.



Gambar 5. Halaman Login Backdoor



Gambar 6. Tampilan saat php backdoor dijalankan



Gambar 7. Tampilan saat terjadi serangan

Pada percobaan penyerangan yang dilakukan didapatkan sistem snort dapat mendeteksi serangan yang yang dilakukan pada saat penyerang mengaktifkan web shell backdoor pada browser untuk mengambil alih situs yang ada.

Sistem *backdoor* yang digunakan dalam serangan yang dilakukan merupakan jenis *backdoor webshell* yang mana backdoor ditanamam pada sistem web server yang mana menjalankan aplikasi berbasih PHP. *Backdoor* ini menggunakan bahasa pemrograman PHP yang berjalan pada web server. Program *backdoor* yang ditanam pada *webserver* memiliki nama c99madshell dimana *backdoor* ini memiliki kemampuan untuk mencari, membuat, menghapus, mengubah berkas yang ada pada *webserver*, *backdoor* ini juga mampu mencuri kata kunci masuk yang telah di enkripsi berbentuk hash.

Dalam pengujian yang dilakukan digunakan sistem *snort* yang merupakan sistem IDS yang telah banyak digunakan dalam mendeteksi serangan yang terjadi pada jaringain internet. Dalam penggunaan sistem *snort* ini dibutuhkan *rules* yang dapat diunduh secara gratis di halaman *website snort.* Dikarenakan *rules* yang harus ada pada sistem *snort,* maka jika tidak terdapat *rules* yang digunakan untuk mendeteksi serangan yang dimaksud, pada tahap selanjutnya harus dibuatkan *rules* yang dapat mendeteki serangan yang diamati dan *rules* yang dibuat ini harus dapat membedakana antara koneksi normal yang dilakukan oleh pengguna atau koneksi yang dilakukan oleh penyerangan yang akan memasuki sistem.

3.3 Perbandingan dengan IDS lain

Pada percobaan dengan menambahkan *rules* baru pada sistem deteksi, sistem snort dapat membedakan antara koneksi serangan dan koneksi normal yang terjadi pada server. Sistem IDS *snort* hanya mampu mendeteksi serangan jika terdapat *rules* yang ditambahkan pada sistem IDS *snort.*

Tabel 2. Perbandingan snort dan IDS lain

NO	Snort	IDS Lain
1	Menggunakan lebih sedikit sumber daya server.	Menggunakan banyak sumber daya server.

2	Memberikan log paket serangan yang lengkap dimana log ini dapat digunakan untuk mengoptimalkan *rules* yang ada.	Log deteksi kurang lengkap, sehingga sulit untuk mengoptimalkan *rules* yang ada.

4. KESIMPULAN

Menggunakan IDS dapat mengurangi dampak buruk dari penyerangan yang dilakukan. Backdoor merupakan jalan pintas bagi penyerang untuk masuk ke dalam sistem. Bagaimanapun penelitian ini masih jauh dari sempurnya, maka untuk penelitian selanjutnya diharapkan meneliti tentang bagaimana menutup celah dari keamanan.

DAFTAR PUSTAKA

[1] Yudha, F., & Panji, A. M. (2018). Perancangan Aplikasi Pengujian Celah Keamanan Pada Aplikasi Berbasis Web. *Cyber Security Dan Forensik Digital*, *1*(1), 1-6.

[2] Munawar, Z., & Putri, N. I. (2020). Keamanan Jaringan Komputer Pada Era Big Data. *J-Sika| Jurnal Sistem Informasi Karya Anak Bangsa*, *2*(01), 14-20.

[3] Prathivi, R., & Vydia, V. (2017). Analisa Pendeteksian Worm Dan Trojan Pada Jaringan Internet Universitas Semarang Menggunakan Metode Kalsifikasi Pada Data Mining C45 Dan Bayesian Network. *Jurnal Transformatika*, *14*(2), 77-81.

[4] Hutabarat, A. P. (2019). *Analisa Dan Perancangan Keamanan Jaringan End User Dari Serangan Exploit Menggunakan Metode Penetration Testing* (Doctoral Dissertation, Universitas Internasional Batam).

[5] Ananta, A. Y. (2017). Seleksi Notifikasi Serangan Berbasis Ids Snort Menggunakan Metode K-Means. *Jurnal Smartics Vol*, *3*(2).

[6] Wijaya, B., & Pratama, A. (2020). Deteksi Penyusupan Pada Server Menggunakan Metode Intrusion Detection System (Ids) Berbasis Snort. *Jurnal Sisfokom (Sistem Informasi Dan Komputer)*, *9*(1), 97-101.

[7] Risyad, E., Data, M., & Pramukantoro, E. S. (2018). Perbandingan Performa Intrusion Detection System (Ids) Snort Dan Suricata Dalam Mendeteksi Serangan Tcp Syn Flood. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer E-Issn*, *2548*, 964x.

[8] Rahmatullah, Sidik. "Perancangan Jaringan Local Area Network (Lan) Dan Dns Server Menggunakan Routing Protokol Open Shortest Path First (Ospf) Pada Bumiputera Bandar Jaya." *Jurnal Informasi Dan Komputer* 4.2 (2017): 37-54.

[9] Ardy, Ferly. "Istem Informasi Pengisian Nilai Berbasis Java Web Menggunakan Local Server Pada Smk 2 Mei Bandar Lampung." *Jurnal Cendikia* 14.1 April (2016): 54-60.

[10] Efendi, Dwi Marisa, And Ferly Ardhy. "Prediction Of Coffee Prices With Backpropagation Neural Networks." *Prosiding International Conference On Information Technology And Business (Icitb)*. 2019.