EVALUASI TOOLS SNORT TERHADAP PERBANDINGAN DETEKSI PENYUSUP MENGGUNAKAN SERANGAN METODE ZENMAP DAN KNOCKER PADA JARINGAN KOMPUTER

Winarti[1)]
[1]Program Studi Sistem Informasi, Universitas Gunadarma
Email: winarti.s2@gmail.com[1)]
Nomor Telp : +62 856 754 6377
Asal Negara: Indonesia

ABSTRAK

Keamanan jaringan komputer khususnya server merupakan aspek yang selalu ditingkatkan oleh System Administrator, baik dengan pengoptimalan perangkat keras maupun perangkat lunak. Perkembangan teknologi informasi memberikan celah bagi sniffer atau penyusup untuk merusak maupun mencuri data pada server. Snort adalah NIDS (Network Intrusion Detection System) yang bekerja dengan menggunakan signature detection, berfungsi juga sebagai sniffer dan packet logger yang dapat memonitor lalu lintas jaringan serta memberikan peringatan jika ada aktivitas yang mencurigakan sehingga mendeteksi adanya serangan atau percobaan penyusupan pada server. Snort dapat berjalan baik pada mesin virtual jika dilakukan tahapan instalasi yang sesuai yaitu instalasi sistem operasi Ubuntu 14.04.4, konfigurasi network adapter, instalasi dan konfigurasi Snort, instalasi dan konfigurasi Pulled Pork, terakhir tahapan instalasi dan konfigurasi Base. Metode penelitian terdiri dari tahapan analisis kebutuhan, tahapan perancangan jaringan, tahapan konfigurasi jaringan, dan tahapan pengujian. Pengujian dilakukan sebanyak dua kali, yaitu menggunakan Zenmap dan Knocker. Hasil pengujian menggunakan Zenmap didapatkan 5 kategori serangan (unclassified, Bad-unknown, Attempted-recon, Icmp-event, Policy-violation) yang ditujukan kepada server dan dari hasil pengujian kedua menggunakan knocker didapatkan snort berhasil mendeteksi 1 kategori serangan, Hasil dari deteksi tersebut terlihat bahwa Snort mampu mendeteksi serangan pada protokol ICMP, UDP dan TCP.

Kata kunci: Deteksi, penyusup, server, snort

ABSTRACT

Computer network security, especially servers, is an aspect that is always being improved by the System Administrator, both by optimizing hardware and software. The development of information technology provides loopholes for sniffers or intruders to destroy or steal data on servers. Snort is a NIDS (Network Intrusion Detection System) that works by using signature detection, also functions as a sniffer and packet logger that can monitor network traffic and provide warnings if there is suspicious activity so that it detects an attack or attempted intrusion on the server. Snort can run well on a virtual machine if the appropriate installation steps are carried out, namely Ubuntu 14.04.4 operating system installation, network adapter configuration, Snort installation and configuration, PulledPork installation and configuration, finally the Base installation and configuration stage. The research method consists of needs analysis stages, network design stages, network configuration stages, and testing stages. The test was carried out twice, namely using Zenmap and Knocker. The test results using Zenmap obtained 5 categories of attacks (unclassified, Bad-unknown, Attempted-recon, Icmp-event, Policy-violation) aimed at the server and from the results of the second test using a knocker obtained 1 category of attack (Bad-unknown) aimed at server, the results of this detection show that Snort is able to detect attacks on ICMP, UDP and TCP protocols.

Keywords: Detection, intruder, server, snort.

1. PENDAHULUAN

Jaringan Komputer adalah perangkat komputasi yang saling terhubung untuk saling berkomunikasi maupun bertukar data atau informasi dan berbagi sumber daya satu sama lain. Perangkat yang terhubung terdapat sistem komputer berupa server yang menyediakan berbagai jenis layanan tertentu dalam sebuah jaringan komputer, salah satunya adalah menyediakan layanan tempat penyimpanan data, baik data pribadi maupun data perusahaan. Server juga memberikan celah besar bagi sniffer atau penyusup untuk menyusup ke dalam sebuah server, salah satu caranya dengan sniffing ataupun port scanning dengan tujuan merusak ataupun mencuri data pada server. Dalam menghindari sniffer diperlukan penggunaan firewall untuk mengamankan sebuah server dari serangan penyusup pada sebuah jaringan komputer. Salah satu contoh firewall yang biasa digunakan yaitu Snort. Snort adalah NIDS (Network Intrusion

Detection System) yang bekerja dengan menggunakan signature detection, berfungsi juga sebagai sniffer dan packet logger yang dapat memonitor lalu lintas jaringan serta memberikan peringatan jika ada aktivitas yang mencurigakan (Yudatama; & Dkk, 2022)

Penelitian penggunaan Snort pernah dilakukan oleh Denny Wijanarko, dimana dalam penelitiannya dilakukan penggabungan Snort dengan cara SMS gate, dan dalam percobaan yang dilakukan dapat berhasil menangkap penggunaan tool scan jaringan yang berupaya mengetahui port-port yang terbuka pada server, upaya tersebut berhasil direkam oleh sensor snort dan disimpan dalam database yang kemudian diteruskan menggunakan aplikasi SMS gateway, lalu log alert akan diteruskan ke admin melalui media SMS, sehingga administrator dapat mengetahui kondisi jaringan yang dikelola (Wijanarko, 2015). Pada penelitian (Prihasmoro et al., 2016) melakukan sistem monitoring pendeteksian penyusup menggunakan Snort dengan kombinasi Iptables firewall sebagai tindak pencegahan serangan. Informasi penyusup diketahui oleh admin saat melihat alamat IP Address yang masuk yang ditampilkan oleh Snort.

Berdasar dari penelitian yang terdahulu maka akan dibuat Perancangan Sistem Deteksi Penyusup dalam Jaringan Komputer dengan menggunakan Snort pada Ubuntu untuk membantu pengguna awam atau System Administrator dalam mengetahui cara mengimplementasikan Snort pada server, sehingga dapat mendeteksi dan merekam kemungkinan-kemungkinan serangan sniffer pada server melalui sistem deteksi intrusi (intrusion detection system).

2. METODE PENELITIAN

Metode penelitian pada perancangan sistem deteksi terdiri dari tahapan analisis kebutuhan, tahapan perancangan jaringan, tahapan konfigurasi jaringan, dan tahapan pengujian. Diawali tahapan analisis kebutuhan perangkat lunak pada penelitian. Spesifikasi perangkat lunak pendukung server terintegrasi IDS terdapat dua yaitu spesifikasi perangkat lunak untuk mesin virtual yang terdiri dari sistem operasi Ubuntu, Snort, Barnyard, PulledPork, dan Base. Selanjutnya untuk spesifikasi perangkat lunak untuk mesin host menggunakan sistem operasi elementary loki, zenmap, virtualbox dan knocker. Dilanjutkan dengan tahapan perancangan jaringan dengan melakukan perancangan terhadap sistem yang dibutuhkan. Perancangan dimulai dengan membuat gambaran jaringan dan pembuatan flowchart sistem Snort. Dilanjutkan dengan tahapan konfigurasi jaringan dengan melakukan instalasi konfigurasi awal sistem operasi server. Proses instalasi pada mesin virtual harus disesuaikan dengan urutan, lalu dilanjutkan dengan melakukan konfigurasi network adapter, konfigurasi Snort, konfigurasi PulledPork, dan konfigurasi Base. Tahapan akhir pada penelitian yaitu tahapan pengujian, dimana setelah proses instalasi system operasi Ubuntu 14.04.4, instalasi snort, PulledPork, Base, konfigurasi network adapter, snort, pulledpork dan base, kemudian dilanjutkan dengan pengujian kemampuan dan kinerja dalam mendeteksi serangan-serangan pada server. Pengujian dilakukan dengan menggunakan dua tools yaitu Zenmap dan Knocker

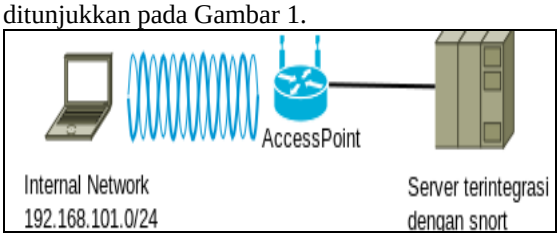
3. HASIL DAN PEMBAHASAN

3.1 Gambaran Umum Sistem Deteksi Intrusi

Sistem Deteksi Intrusi (*Intrusion Detection System*) adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan komputer (Shafitri, 2012). Sistem Deteksi Intrusi akan memonitoring lalu lintas data pada sebuah jaringan atau mengambil data dari berkas log kemudian menganalisa dengan algoritma tertentu untuk memutuskan memberi peringatan kepada administrator.

3.2 Gambaran Jaringan

Gambaran jaringan untuk pemasangan Snort ditunjukkan pada Gambar 1.

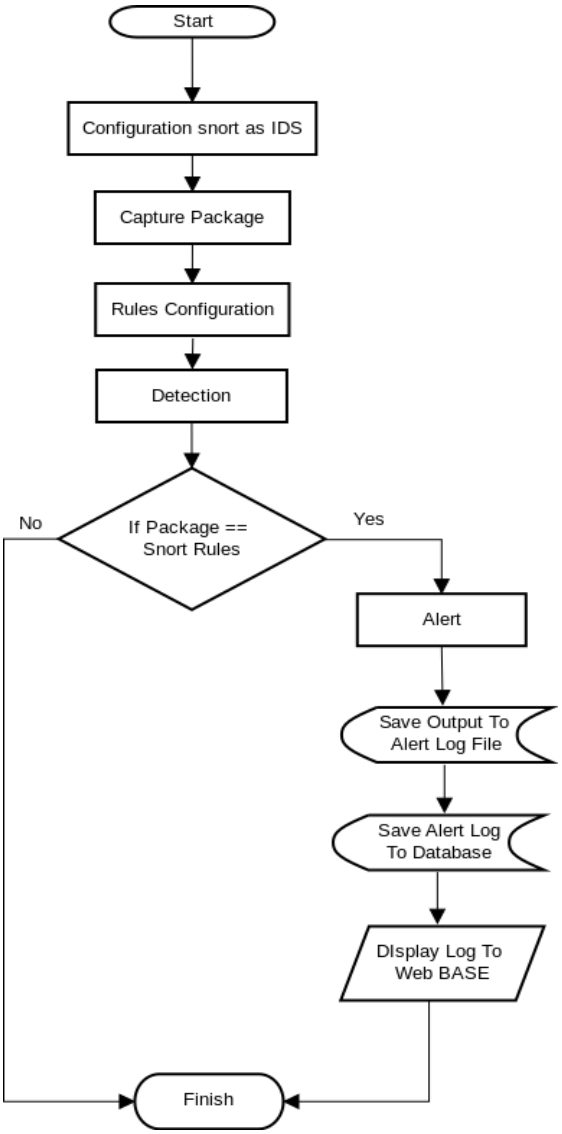


Gambar 1. Gambaran jaringan komputer

Snort IDS diimplementasikan pada Mesin virtual yang dibuat menggunakan VirtualBox, kemudian pada mesin virtual menggunakan sistem operasi ubuntu 14.04.4 64bit yang mempunyai alamat IP 192.168.101.1 yang disambungkan dengan accesspoint menggunakan mode Bridge. Pada host sistem operasi yang digunakan adalah Elementary OS Loki 64Bit kemudian pada mesin host alamat IP didapatkan secara DHCP dari accesspoint.

3.3 Flowchart Sistem Snort

Ilustrasi cara kerja Snort dengan menggunakan flowchart. Menurut (Yuniansyah, 2020) Flowchart atau diagram alur adalah kumpulan simbol-simbol yang menggambarkan urutan proses dalam menyelesaikan suatu permasalahan. Flowchart memperlihatkan urutan atau langkah-langkah dari proses pemecahan masalah. Alur flowchart Snort terlihat pada Gambar 2.



Gambar 2. Flowchart sistem snort

Alur flowchart sistem snort menjelaskan apabila ada paket atau akun yang masuk, sistem ini akan mulai bekerja yaitu dengan melakukan proses konfigurasi Snort sebagai IDS, proses konfigurasi aturan, dan melakukan deteksi apakah paket sesuai dengan aturan Snort untuk mengidentifikasi mode paket serangan. Jika tidak sesuai maka paket aman dan sistem Snort berhenti. Jika sama maka Snort akan mengeluarkan alert (peringatan), data serangan akan tersimpan ke file log alert dan database alert, lalu akan tampil log ke basis web.

3.4 Tahapan Instalasi dan Konfigurasi Jaringan

Snort dapat berjalan baik pada mesin virtual jika dilakukan tahapan instalasi secara benar dan sesuai urutan dengan ketentuan yang ada. Tahapan instalasi yang benar secara berurutan adalah instalasi sistem operasi Ubuntu 14.04.4, konfigurasi network adapter, instalasi dan konfigurasi Snort, instalasi dan konfigurasi PulledPork, tahap terakhir instalasi dan konfigurasi Base.

3.4.1 Instalasi Sistem Operasi Ubuntu 14.04.4

Instalasi sistem operasi Ubuntu merupakan proses pemasangan sebuah sistem operasi untuk membangun sebuah server yang terintegrasi dengan NIDS (*Network Intrusion Detection System*). Proses instalasi Ubuntu sama seperti instalasi sistem operasi biasa. Pada proses instalasi Ubuntu menggunakan antar muka grafis atau GUI (bukan mode terminal).

Sebelum memulai instalasi Snort, terlebih dahulu tambahkan *Repository* yang dapat diakses secara *Online* untuk distribusi ubuntu 14.04.4 yang ada di Indonesia. Beberapa *repository* di Indonesia, contohnya disediakan oleh UI, UGM, ITB dan lain sebagainya. Pada penelitian ini menggunakan *Repository* dari Universitas Gajah Mada (UGM) dengan alamat http://repo.ugm.ac.id/ubuntu/. Tambahkan alamat tersebut pada berkas /etc/apt/source.list repository berikut ini.

```
deb http://repo.ugm.ac.id/ubuntu/ trusty main restricted universe multiverse
deb http://repo.ugm.ac.id/ubuntu/ trusty-updates main restricted universe multiverse
deb http://repo.ugm.ac.id/ubuntu/ trusty-security main restricted universe multiverse
```

Setelah menambahkan *Repository* kemudian lakukan pembaharuan daftar paket pada *terminal* dengan menggunakan perintah apt-get update.

3.4.2 Konfigurasi Network Adapter

Network adapter adalah sebuah perangkat keras yang digunakan untuk menghubungkan komputer ke jaringan, yang bisa berupa kartu PCI ataupun terhubung dengan sebuah komputer secara eksternal melalui USB atau parallel port. Beberapa kartu jaringan mempunyai fitur dengan nama *Large Receive Offload (LRO)* dan *Generic Receive Offload (GRO)*. Kartu jaringan akan melakukan pengumpulan paket-paket yang telah berjalan sebelumnya, mereka diproses oleh *kernel* untuk aktif secara otomatis yang dimana LRO dan GRO dapat menyebabkan masalah pada saat pengumpulan target yang dilakukan oleh sistem Snort. Maka setelah masuk kedalam berkas tambahkan dua baris berikut ini pada bagian konfigurasi antarmuka eth0 agar kemampuan LRO dan GRO tidak aktif.

```
post-up ethtool -K eth0 gro off
post-up ethtool -K eth0 lro off
```

Restart komputer agar konfigurasi terpasang dengan baik, kemudian jalankan perintah ethtool dan jika berhasil akan muncul tampilan seperti pada Gambar 3.

Gambar 3. Uji coba konfigurasi ethtool

3.4.3 Instalasi dan Konfigurasi Snort

Terdapat empat syarat tambahan untuk memasang Snort pada Ubuntu yaitu perpustakaan

opsional yang meningkatkan kegunaannya, contohnya adalah liblzma-dev dan tiga diantaranya memberikan dekompresi bekas swf (adobe flash), openssl, dan libssl-dev yang keduanya menyediakan bekas SHA dan MD5. Setelah melakukan pemasangan paket yang dibutuhkan oleh Snort kemudian sistem membutuhkan penerjemah untuk judul perpustakaan mereka, maka dari itu dibutuhkan *compiler* nghttp2.

Setelah semua persyaratan dipasang, siap mengunduh sumber Snort, kompilasi dan kemudian memasangnya dengan perintah --enable-sourcefire memberikan *Packet Performance Monitoring (PPM)* yang memungkinkan untuk melakukan pemantauan kinerja peraturan sebelum pemrosesan dan membangun Snort dengan cara yang sama. Kemudian jika tidak terdapat kesalahan pada saat pemasangan atau konfigurasi, maka dapat disimpulkan bahwa snort sudah berhasil terpasang pada komputer, namun sampai pada proses ini snort belum bisa digunakan karena snort hanya sekedar dipasang. Untuk memeriksa apakah snort sudah berhasil dipasang dengan benar dengan perintah snort -V, seperti yang terlihat pada Gambar 4.

```
root@snort:/home/snort# snort  -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.9.0 GRE (Build 56)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.
org/contact#team
           Copyright (C) 2014-2016 Cisco and/or its affiliates.
 All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.5.3
           Using PCRE version: 8.31 2012-07-06
           Using ZLIB version: 1.2.8
```

Gambar 4. Uji coba konfigurasi snort

3.4.4 Instalasi dan Konfigurasi PulledPork

Pulledpork berfungsi sebagai pengunduh *rules* yang di *release* oleh snort.org dengan menggunakan *link code* sehingga setiap ada *update rules* dari snort.org maka *rules* yang ada di *server* juga ter-*update* secara otomatis (Wahyudi & Efendi, 2012). Hal pertama yang harus dilakukan ketika akan memasang pulledpork adalah pemasangan paket pendukungnya terlebih dahulu. Berikut ini adalah perintah dan nama paket yang dibutuhkan oleh pulledpork.

```
root@snort:~/snort# sudo apt-get install -y libcrypt-
ssleay-perl liblwp-useragent-determined-perl
```

Setelah paket pendukung pulledpork sudah terpasang, kemudian unduh dan pasang pulledpork. Caranya seperti berikut ini.

```
root@snort:~/snort# wget
https://github.com/shirkdog/pulledpork/archive/mast
er.tar.gz -O pulledpork-master.tar.gz
root@snort:~/snort# tar xzvf pulledpork-
master.tar.gz
root@snort:~/snort# cd pulledpork-master/
root@snort:~/snort/pulledpork-master/# sudo cp
pulledpork.pl /usr/local/bin
root@snort:~/snort/pulledpork-master/# sudo chmod
+x /usr/local/bin/pulledpork.pl
root@snort:~/snort/pulledpork-master/# sudo cp
etc/*.conf /etc/snort
```

Setelah mengunduh dan mengkonfigurasi berkas pulledpork, selanjutnya test apakah pulledpork sudah terpasang dengan benar, caranya seperti pada gambar 3.18.

```
root@snort:~/snort/pulledpork-master# /usr/local/bin/pulledpork
.pl -V
PulledPork v0.7.3 - Making signature updates great again!

root@snort:~/snort/pulledpork-master#
```

Gambar 5. Hasil pemasangan pulledpork

3.4.5 Instalasi dan Konfigurasi Base

Base adalah Web GUI sederhana yang digunakan oleh Snort untuk menampilkan hasil dari deteksi yang dilakukannya. Pemasangan dan konfigurasi Base ada beberapa tahapan yang harus dilakukan adalah pemasangan paket pendukung yang diperlukan oleh base yaitu php5 dan *Pear Image Graph.* Setelah pemasangan paket pendukung base, selanjutnya adalah instalasi dan konfigurasi ADODB yang berfungsi sebagai perantara antara database MySQL dengan Web Base. Setelah melakukan konfigurasi pada ADOdb selanjutnya adalah konfigurasi Base. Pada tahap ini berkas BASE perlu diunduh, selanjutnya ekstrak dan berkas hasil ekstrak tersebut dipindahkan ke dalam direktori /var/www/html/base, lalu membuat konfigurasi Base. Pertama gandakan terlebih dahulu berkas base_conf.php.dist dengan nama base_conf.php, kemudian lakukan perubahan pada berkas base_conf.php tersebut. Langkah proses seperti berikut ini.

```
root@snort:~/snort# cd /var/www/html/base
root@snort:~/var/www/html/base# sudo cp
base_conf.php.dist base_conf.php
root@snort:~/var/www/html/base# sudo nano
/var/www/html/base/base_conf.php
```

Setelah selesai mengkonfigurasi berkas base_conf.php selanjutnya berikan hak akses pada direktori Base. Setelah semua selesai kemudian restart apache dan akan lebih baik jika merestart seluruh sistem (merestart komputer) agar konfigurasi dapat berjalan dengan baik pada sistem komputer. Setelah pemasangan dan konfigurasi BASE selesai, kemudian lakukan pengujian melalui mesin pencarian, masukkan alamat IP yang digunakan untuk sistem Snort sebelumnya, yaitu 192.168.101.1 kemudian masukkan alamatnya yaitu berada pada direktori /base/index.php. Secara lengkapnya bisa diakses pada alamat http://192.168.101.1/base/index.php. Sampai pada tahap ini proses pemasangan dan konfigurasi Snort sudah selesai, selanjutnya adalah pengujian dari sistem snort.

3.5 Pengujian Snort

Setelah pemasangan Snort dan Base selesai dilakukan, selanjutnya adalah melakukan pengujian terhadap kemampuan dan kinerja Snort dalam mendeteksi serangan-serangan yang ditujukan kepada server, proses ini dilakukan untuk mengetahui apakah Snort berjalan dengan benar dan dapat melakukan pendeteksian terhadap serangan

yang ditujukan kepada server. Pada pengujian ini penulis menggunakan dua *tools* untuk menguji kemungkinan serangan tersebut yang diantaranya adalah Zenmap dan Knocker.

Pada pengujian terhadap kinerja snort menggunakan Zenmap dan Knocker diperlukan alamat IP yang akan dilakukan pengujian, dalam penulisan ini alamat IP yang digunakan adalah 192.168.101.1. Pengujian ini dilakukan pada sistem operasi Elementary OS Loki.

Dari dua kali pengujian yang telah dilakukan sebelumnya yaitu menggunakan Zenmap Dan Knocker. Snort berhasil mendeteksi serangan-serangan yang ditujukan kepada server. Pada pengujian pertama didapatkan 5 kategori serangan yang ditujukan kepada server yang dijelaskan pada Tabel 1.

Tabel 1. Hasil pengujian menggunakan zenmap

Klasifikasi	Jumlah	Presentasi
unclassified	2821	72%
Bad-unknown	4	0%
Attempted-recon	2	0%
Icmp-event	1077	28%
Policy-violation	1	0%

Terlihat tipe kerentanan yang paling banyak terdeteksi adalah pada *unclassified dan Icmp-event.* Unclassiffied atau tidak terklasifikasi yang artinya penyerang dapat mendapatkan informasi mengenai server, informasi ini dapat dimanfaatkan oleh penyerang untuk melakukan peretasan terhadap server. Kemudian *Icmp-event* adalah sebuah keterhubungan satu komputer dengan komputer lain, contohnya paling sederhananya adalah melakukan sebuah *ping.* Kemudian pada pengujian yang kedua dilakukan menggunakan knocker yang dijabarkan pada Tabel 2.

Tabel 2. Hasil pengujian menggunakan knocker

Klasifikasi	Jumlah	Presentase
Bad-unknown	2	100%

Hasil pengujian menggunakan Knocker terlihat hanya terdapat satu kerentanan yang terdeteksi pada Snort, yaitu Bad-unknown yang artinya adalah sebuah permintaan yang dilakukan oleh klient. Permintaan tersebut dapat berupa informasi mengenai data-data yang dimiliki oleh server, sebagai contohnya adalah informasi mengenai port yang terbuka pada server. Informasi ini bisa dimanfaatkan oleh peretas untuk masuk ke dalam sebuah server kemudian mengambil atau memanipulasi data yang ada.

4. KESIMPULAN

Sumber daya perangkat keras yang diperlukan untuk memasang Snort pada penulisan ini adalah 1GB memori RAM dan 20GB memori penyimpan, kemudian menggunakan sistem operasi Ubuntu 14.04.4. Snort dapat berjalan baik pada mesin virtual jika dilakukan tahapan instalasi secara benar dan sesuai urutan dengan ketentuan yang ada. Tahapan instalasi yang benar secara berurutan adalah instalasi sistem operasi Ubuntu 14.04.4, konfigurasi network adapter, instalasi dan konfigurasi Snort, instalasi dan konfigurasi PulledPork, tahap terakhir instalasi dan konfigurasi Base. Pengujian dilakukan sebanyak menggunakan Zenmap dan Knocker. Hasil pengujian menggunakan Zenmap didapatkan 5 kategori serangan yang ditujukan kepada server dan dari hasil pengujian kedua menggunakan knocker, snort berhasil mendeteksi 1 kategori serangan. Dari hasil pengujian yang dilakukan, Sistem Deteksi Intrusi (*Intrusion Detection System*) berguna untuk mendeteksi adanya serangan atau percobaan penyusupan pada server yang bertujuan untuk mengambil alih suatu data atau informasi. Hasil dari deteksi tersebut terlihat bahwa Snort mampu mendeteksi serangan pada protokol ICMP, UDP dan TCP.

DAFTAR PUSTAKA

Prihasmoro, S. A., Rachmawati, R. Y., & Fatkhiyah, E. (2016). Simulasi Sistem Deteksi Penyusup Dalam Jaringan Komputer Berbasis Web Interface Serta Pencegahan Untuk Meningkatkan Keamanan. *Jurnal Jarkom*, *4*(1), 50–59.

Shafitri. (2012). Analisis Dan Implementasi Instrusion Detection System (Ids) Untuk Pemberitahuan Serangan Pada Keamanan Sistem Jaringan Komputer Melalui Email. *It Telkom Journal On Ict*, *1*(2).

Wahyudi, T., & Efendi, R. (2012). Perancangan Keamanan Jaringan Komputer Menggunakan Snort Dengan Notifikasi Sms. *J. Teknol. Inf. Dan Komun*, 1–8.

Wijanarko, D. (2015). Sistem Keamanan Jaringan Komputer Menggunakan Snort. *Jurnal Teknologi Informasi Dan Terapan*, *2*(1), 171–175.

Yudatama;, U., & Dkk. (2022). Audit Sistem Informasi Teori, Framework Dan Studi Kasus Menggunakan Framework. *Indie Press.*

Yuniansyah. (2020). Algoritma Dan Pemrograman Menggunakan Bahasa Pemrograman Jawa (Teori Dan Aplikasinya). *Jurnal Teknologi Informasi Dan Komunikasi*, *6*(1).