PENERAPAN SISTEM KEAMANAN INTRUSION DETECTION SYSTEM SNORT PADA JARINGAN DISKOMINFO KABUPATEN OKI

[1]M. Zidan Pratama, [2*]Ade Putra
[1]Teknik Komputer, Fakultas Vokasi, Universitas Bina Darma
[2]Komputerisasi Akuntansi, Fakultas Vokasi, Universitas Bina Darma
[*]ade.putra@binadarma.ac.id

Abstract - *The Office of Communication and Informatics Kab.OKI is a place where an agency in charge of managing data and providing information, facilitates communication between communities. The problem that often occurs in the Communication and Information Office of OKI Regency lies in server security. Therefore, the implementation of the Intrusion Detection System using Snort is carried out on the security of the Communication and Information Office of OKI Regency. The purpose of the Intrusion Detection system is to use Snort to detect attacks according to the attack category in the Snort Rules. The methods used include system requirements analysis, system block diagram designer, installation and configuration and system testing. The research implementation is a combination of hardware and software. By implementing an Intrusion Detection system using Snort, it can detect the type of attack, the attacker's IP address and the time of the attack.*

Keywords: Intrusion Detection System, Snort, Network Security, Linux, Ping.

Abstrak - Dinas Komunikasi dan Informatika Kab. OKI adalah tempat dimana suatu dinas yang bertugas mengolah data dan memberikan informasi, memperlancar komunikasi antar masyarakat. permasalahan yang sering terjadi di Dinas Komunikasi dan Informatika Kab.OKI terletak pada keamanan server . Maka dari itu dilakukan penerapan Intrusion Detection System menggunakan Snort terhadap keamanan Dinas Komunikasi dan Informatika Kab. OKI. Tujuan dilakukannya Intrusion Detection system menggunakan Snort untuk mendeteksi serangan sesuai dengan kategori serangan pada Rules Snort. Metode yang digunakan meliputi analisis kebutuhan sistem, perancang diagram blok sistem, instalasi dan konfiguasi dan pengujian sistem. Pelaksanaan penelitian merupakan kombinasi dari perangkat keras dan perangkat lunak. Dengan menerapkan Intrusion Detection system menggunakan Snort dapat mendeteksi jenis serangan, alamat IP penyerang dan waktu penyerangan.

Kata kunci: Intrusion Detection System, Snort, Keamanan Jaringan, Linux, Ping.

1. Pendahuluan

Ketika PC terhubung dengan sekelompok PC lainnya baik secara local atau melalui web PC dapat di hubungkan . Betapa pentingnya data tidak mengherankan jika banyaknya penyerangan dilakukan oleh sekelompok yang tidak bertanggung jawab . Sekelompok ini dapat menyerang sepenuhnya tujuan untuk mengambil, mengubah, dan memusnahkan data-data di PC.Interupsi adalah upaya yang dilakukan untuk berpikir dua kali atas keamanan asset PC. Sistem pendeteksi penyusupan *Intrusion Detection System (IDS)* adalah sistem yang mampu mendeteksi serangan dan ancaman yang terjadi pada suatu jaringan komputer baik yang berkaitan dengan jaringan local ataupun internet. *Intrusion Detection System (IDS)* yang bersifat open source ialah *Snort* . *Snort* ialah *Network Intrusion Detection System (NIDS)* yang bekerja dengan menganalisa paet yang melintas *Traffic* jaringan. *Intrusion Detection System (IDS)* cocok untuk berjalan di semua

tahapan kerangka kerja dan siap untuk menggantikan tugas firewall sehingga penangkalan harus dimungkinkan saat pemrogram menyerang [1]. Penggunaan teknik keamanan organisasi dengan mengkoordinasikan antara *Intrusion Detection System*, *Sistem Firewall*, Sistem Basis Data dan Sistem Pemantauan yang terkait dengan tinjauan agen seluler [2].

Didalam *Snort* terdapat database yang memuat *rules* yang dikategorikan sebagai penyusupan. *Snort* memasukan rel analisa *Signatures* dan *Anomaly Detection* . Metode *Signatures* ialah jika *rules* selaras *traffic* yang sedang dideteksi tambah *Traffic* yang menyimbolkan terjadi penyerangan. Sedangkan *Rel Anomaly* ialah rules yang mengandung *traffic* sama *traffic* yang sedang di deteksi . *Snort* adalah produk untuk mengidentifikasi penyusup dan dapat menyelidiki lalu lintas yang konstan, dapat mengenali berbagai jenis serangan. *Snort* bukan hanya konvensi atau kerangka investigasi *Intrusion detection System* (IDS), namun agak dari campuran antara keduanya, dan dapat sangat berharga dalam bereaksi terhadap serangan episode terhadap jaringan telah. Sorotan *Snort* dapat menjadi bantuan untuk kerangka kerja dan ketua organisasi, yang dapat mengingatkan kita tentang penghancur gerbang yang mungkin berbahaya.

Suatu serangan dapat dideteksi atau tidak oleh *Snort* di konfigurasikan pada pegaturan jaringan dan *Snort* yang ada. Pengujian *Snort Intrusion Detection System* dilengkapi dari beberapa contoh serangan untuk menguji kehandalan *Snort* dalam membedakan serangan pada kerangka keamanan. Mengingat efek samping dari pengujian kerangka kerja *Snort IDS* dengan *ping of Deatch, SSH, Telnet. Snort* dapat memberikan peringatan tentang serangan keamanan pada kerangka kerja jaringan. Konsekuensi dari peringatan ini dapat digunakan sebagai sumber perspektif untuk memutuskan strategi keamanan jaringan. Pada Penelitian ini di rumuskan dari cara melakukan *Intrusion Detection System* pada Dinas Komunikasi dan Informatika Kabupaten OKI, penerapan *Intrusion Detection System* menggunakan aplikasi *Snort* dan cara mendapatkan hasil dari pengujian penelitian ini.

Dinas Komunikasi dan Informatika Kabupaten OKI adalah tempat dimana suatu dinas yang bertugas mengelola data dan memberikan informasi, memperlancar komunikasi antar masyarakat. Dinas Komunikasi dan Informatika Kabupaten OKI juga bertugas untuk membentuk jaringan komputer, mengontrol suatu jaringan. Dinas Komunikasi dan Informatika Kabupaten OKI terbilang baru di kalangan Perangkat daerah Kabupaten OKI. Dinas Komunikasi dan informatika terbilang cepat dalam pengembangan jaringan komputer terutama dalam akses internet. Tetapi dalam segi keamanan masih terbilang belum sempurna walau sudah diterapkan beberapa jenis keamanan. Permasalahan yang sering terjadi Dinas Komunikasi dan Informatika terletak pada tingkat keamanan server. Beberapa penyerangan dilengkapi dengan pertemuan-pertemuan sembrono, misalnya banjir penyerangan smurf dan lain-lain. Ada beberapa pilihan untuk mengatasi masalah keamanan pekerja yang belum digenjot, salah satunya adalah penggunaan strategi *Intrusion Detection system* (IDS). IDS (*Intrusion Detection System*) dapat dicirikan sebagai instrumen, strategi, atau aset yang memberikan bantuan untuk mengenali, menulis tentang pergerakan jaringan PC. Tujuan dari penelitian ini adalah mendeteksi penyusupan pada jaringan Dinas Komunikasi dan Informatika Kabupaten OKI, Menerapkan *Intrusion Detection System* dan juga membangun sistem keamanan IDS menggunakan aplikasi *Snort.*

2. Tinjauan Pustaka

2.1 Jaringan Komputer

Jaringan PC adalah Kumpulan PC mandiri yang terhubung satu sama lain, menggunakan konvensi korespondensi sehingga semua PC yang saling terhubung dapat berbagi data, proyek, asset dan juga dapat menggunakan perangkat lain secara bersamaan, khususnya printer, hard drive, dan lain-lain [3]. Adapun jenis Jaringan Komputer terdiri dari :

1) LAN (*Local Area Network*)
   Local area network merupakan jaringan lokal yang pada untuk dalam area terbatas. Misalkan pada sebuah gedung atau sebuah ruangan. Seringkali jaringan lokal pada sebut jaringan private. LAN mampu pada pakai dalam sekala mini yang memakai resources secara bersama, misalkan penggunaan printer bersama, penggunaan media penyimpanan secara bersama,dan sebagainya [4].

2) MAN (*Metropolitan Area Network*)
   Metropolitan area network menggunakan metode misalnya LAN namun cangkupannya lebih luas. Cangkupan MAN sanggup satu kampung, beberapa gedung yg berada pada satu komplek yang sama, beberapa desa dan beberapa kota. Dapat dikatakan MAN pengembangan dari LAN.
3) WAN (*Wide Area Network*)
   Wide area network (WAN) jangkauannya lebih luas berdasarkan dalam MAN. Cangkupan MAN hanya satu kawasan, satu Negara, satu pulau dan satu dunia, metode yang digunakan Wide Area Network sama seperti yang pada gunakan LAN & MAN. Umumnya WAN terhubung melalui jaringan telepon digital. Namun media transmisi lainpun dapat digunakan.

2.2 Keamanan Jaringan

Keamanan jaringan adalah proses mencegah dan mengidentifikasi penggunaan jaringan komputer yang tidak sah. Keamanan jaringan komputer itu sendiri bertujuan untuk memprediksi secara langsung atau tidak langsung risiko pada jaringan komputer berupa ancaman fisik dan logis atau tidak langsung. Dalam jaringan komputer konsep keamanan jaringan secara umum memiliki tiga aspek yaitu risiko atu tingkat bahaya, ancaman, dan kerentanan sistem.

2.3 IDS (Intrusion Detection System)

Sistem deteksi perintah dapat didefinisikan untuk menyediakan alat, metode dan sumber daya untuk membantu mengidentifikasi dan memberikan laporan aktivitas jaringan komputer. Sistem deteksi perintah (IDS) sebenarnya tidak cocok untuk pemahaman ini, karena IDS tidak mendeteksi intruksi dan hanya mendeteksi aktivitas lalu lintas jaringan yang tidak layak. IDS (*Intrusion Detection System*) secara khusus melindungi sistem dimana IDS telah diinstal, IDS tidak melindungi suatu sistem saja [5]. IDS (*Intrusion Detection System*) memiliki dua jenis sistem deteksi perintah, yaitu NIDS (sistem deteksi perintah jaringan) dan HIDS (sistem deteksi perintah host).

2.4 Snort

Snort adalah aplikasi atau alat keamanan yang digunakan untuk mendeteksi intruksi jaringan (Intruksi, serangan pemindaian dan berbagai bentu ancaman lainnya) dan menghientikannya. *Snort* berjalan dalam 4 mode yaitu *mode snifer, Mode packet logger, intrusion detection system dan inline mode* [6]. *Snort* adalah perangkat lunak yang mendeteksi penyusup, dapat menganalisa paket data yang melintas jaringan secara real time dan masuk ke database, serat dapat mengindentifikasi berbagai serangan [5]

3. Metodologi Penelitian

3.1 Analisis Masalah

Masalah yang sering di hadapi di sistem jaringan Dinas Komunikasi dan Informatika (Diskominfo) Kabupaten OKI ialah belum maksimalnya keamanan *server*. Karena itu Dinas Komunikasi dan Informatika Kabupaten OKI seringkali kehilangan data dan adanya penyerangan yang dilakukan oleh pihak ketiga yang tidak bertanggung jawab.

3.2 Alternatif Solusi

Menerapkan sistem keamanan *Intrusion Detection System* (IDS). *Snort* dapat mendeteksi serangan yang terjadi pada sistem jaringan dan kemudian memberikan peringatan terhadap seragan tersebut.

3.3 Rancangan Aplikasi

Rancangan sistem yang digunakan untuk mendeteksi serangan adalah *Intrusion Detection System* (IDS). Untuk membangun sistem, diperlukan beberapa komponen atau alat, antara lain :

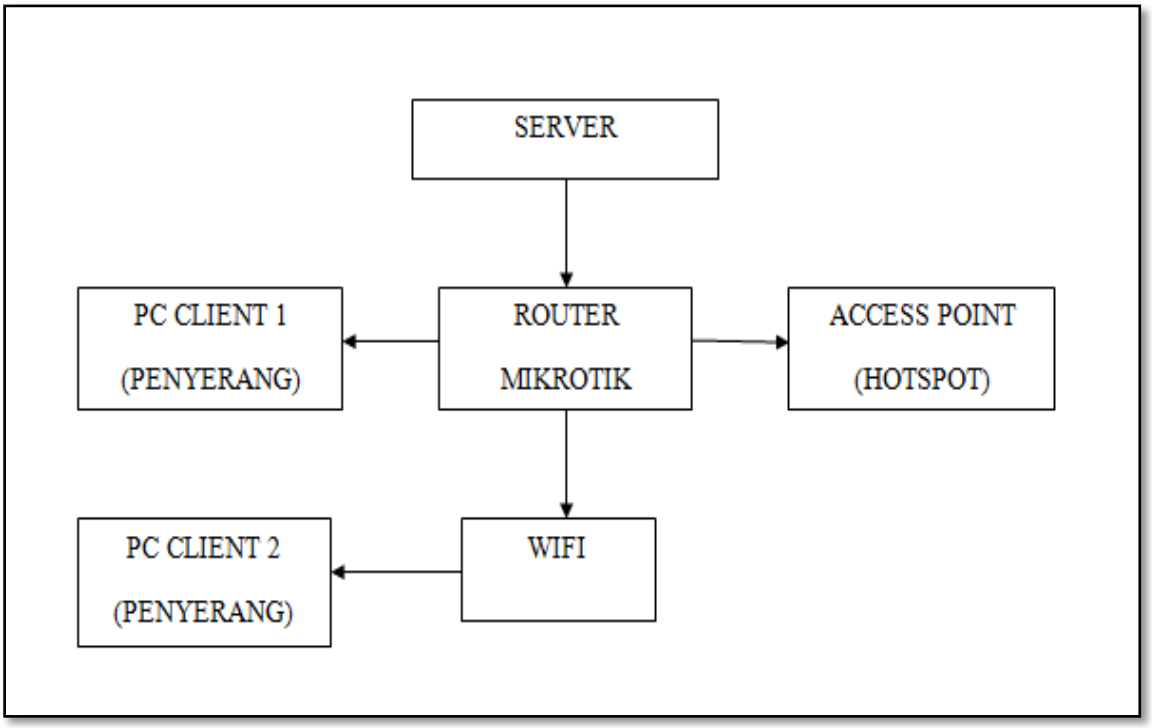
1) *Snort Ubuntu Dekstop 18.04 LTS Linux*
2) *CMD (Command Prompt)*

3) *Puty*
4) *Virtual Box*
5) *Ubuntu Dekstop 18.04 LTS*

3.4 Topologi Usulan

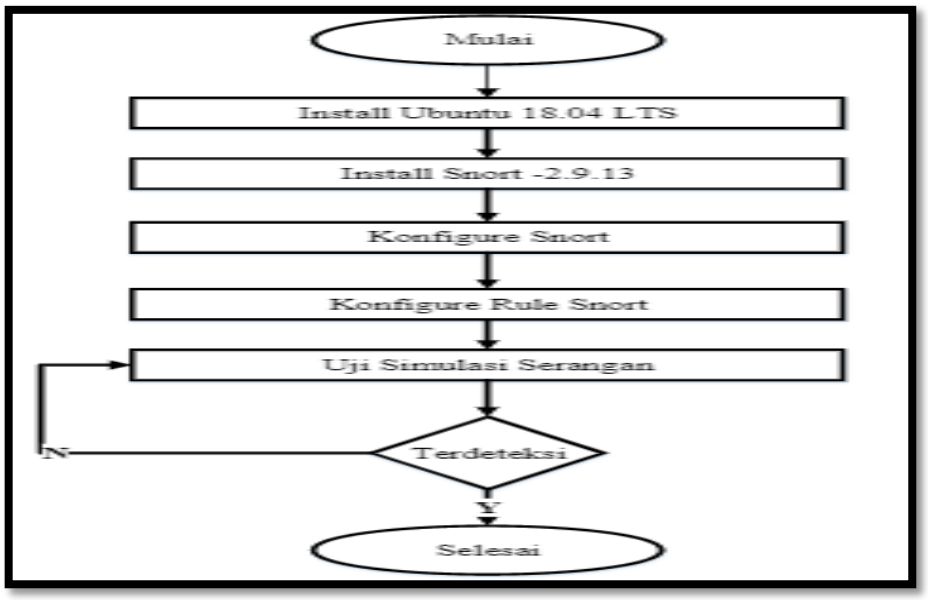
Pada gambar Topologi ini akan digunakan pada Dinas Komunikasi dan Informatika OKI sebagai pengamanan untuk mengetahui adanya penyusupan terhadap Dinas Komunikasi dan Informatika Kab OKI, sebab itu Dinas Komunikasi dan Informatika Kab OKI menerapkan metode *snort* dan *IDS* sebagai tools pendeteksi serangan. Adapun peran dari topologi jaringan usulan ini sebagai berikut :

1) Server
   Server adalah suatu sistem yang di sebut peladen atau sistem komputer yang memiliki layanan khusus berupa penyimpanan data. Server di dalam penelitian ini dijadikan objek untuk mengakses seluruh data yang akan diuji.
2) Router mikrotik
   Router mikrotik adalah suatu penghubung atau pemecah jaringan pusat ke client yang mengakses jaringan tersebut. Pada penelitian ini Router Mikrotik berperan sebagai penghubug antara laptop administrator
3) Acces Point
   Access point adalah titik dimana router mikrotik memecah jaringan ketempat yang telah ditentukan agar dapat digunakan.
4) PC client
   a. PC client 1 (penyerang)
      Pada *pc client* 1 (penyerang) ini tugas nya menyerang *router* yang ada pada Dinas Komunikasi dan Informatika Kabupaten OKI.
   b. PC client 2
      Pada PC *client* 2 ini bertugas menyerang Wifi yang ada pada Dinas Komunikasi dan Informatika Kab OKI.



Gambar 1. Topologi Usulan

3.5 Tahap Penelitian



Gambar 2. Diagram aliran perancangan dan pengujian

4. Hasil dan Pembahasan

4.1 Hasil

Dalam pengujian terakhir yang mana telah dipasangkan Snort pada jaringan yang akan di serang . Alat pengujian snort ini dilakukan melalui Ubuntu Dekstop 18.04 LTS. Pengujian ini bertujuan untuk melihat traffic jaringan atas seranganataupun penyalahgunaan dengan metode penyerangan yang telah disesuaikan pada rules Snort itu sendiri. Pengujian penyerangan ini dilakukan terhadap dua jaringan yang ada di Dinas Komunikasi dan Informatika Kabupaten OKI yaitu jaringan yang terhubung melalui WIFI dan jaringan yang terhubung melalui Router.

Tabel 1. Rekap hasil penelitian pengujian jaringan WIFI

No	Pengujian Terhadap Jaringan	Jenis Serangan	Metode	Hasil Pengujian
1	Pengujian Terhadap jaringan WIFI Dinas Komunikasi dan Informatika Kab OKI	Serangan Ping Of Deatch	Serangan Ping Of Deatch ini dilakukan melalui bantuan aplikasi CMD (*command Prompt)* dengan perintah *Ping 192.168.1.241 –l 6000*, menyerang dengan cara melebihi kapasitas *byte* normal	*Snort* mendeteksi traffic jaringan yang masuk dari serangan *Ping Of Deatch* dengan peringatan *"Ada Ping Dari Luar "[**] ICMP LARGE ICMP PACKET* dengan *ip* Penyerangan *192.168.1.242* . akibatnya jaringan menjadi lemot atau lambat
		Serangan SSH menggunakan *Puty*	Serangan SSH ini menggunakan bantuan dari aplikasi *Puty.* Cara nya memasukan *ip 192.168.1.241* tujuan dan memasukan *port* 22 dan memilih jenis	Hasil yang diperoleh ialah *Snort* mendeteksi traffic jaringan yang masuk yaitu dengan peringatan " *Ada Yang Mengakses SSH "* tercantum juga waktu penyerangan dan terdeteksi *ip* penyerang *192.168.1.242*

			penyerangan yaitu SSH	
		Serangan *Telnet* menggunakan *Puty*	Serangan SSH ini menggunakan bantuan dari aplikasi *Puty*. Cara nya memasukan *ip 192.168.1.241* tujuan dan memasukan *port* 23 dan memilih jenis penyerangan yaitu *Telnet*	*Snort* mendeteksi adanya traffic jaringan yang masuk dengan peringatan " *Ada Yang Telnet Ke Server "* dengan waktu penyerangan yang terdeteksi dan *ip* penyerangan 192.168.1.242

Tabel 2. Hasil rekap penelitian pengujian jaringan Router

No	Pengujian Terhadap Jaringan	Jenis Serangan	Metode	Hasil Pengujian
1	Pengujian Terhadap jaringan Router Dinas Komunikasi dan Informatika Kab OKI	Serangan *Ping Of Deatch*	Serangan Ping Of Deatch ini dilakukan melalui bantuan aplikasi CMD (*command Prompt)* dengan perintah *Ping 10.10.0.54 –t*	*Snort* mendeteksi adanya traffic *ping* yang terus menerus tanpa henti dengan peringatan *"Ada Ping Dari Luar "[**] ICMP LARGE ICMP PACKET* dengan *ip* Penyerangan *10.10.0.53* akibatnya jaringan menjadi lemot atau lambat
		Serangan SSH menggunkan bantuan aplikasi *Snort*	Serangan SSH ini dilakukan melalui bantuan aplikasi *Puty*. Dengan memasukan *ip 10.10.0.54* dengan *port* 23 dan memilih penyerangan SSH	*Snort* mendeteksi adanya traffic masuk dengan peringatan " *Ada Yang Mengakses SSH "* tercantum juga waktu penyerangan dan terdeteksi *ip* penyerang *10.10.0.53* dengan waktu penyerangan yang terdeteksi
		Serangan TELNET menggunakan bantuan aplikasi *Puty*	Serangan Telnet ini dilakukan melalui bantuan aplikasi *Puty* sama hal nya dengan serangan SSH . caranya dengan memasukan *ip* penyerang *10.10.0.54* dengan port 22 dan pemilihan penyerangan Telnet	Hasil yang didapat ialah *Snort* mendeteksi adanya traffic jaringan yang masuk dengan peringatan " *Ada Yang Telnet Ke server "* dengan ip penyerang 10.10.0.53 dan waktu penyeranganyang juga terdeteksi

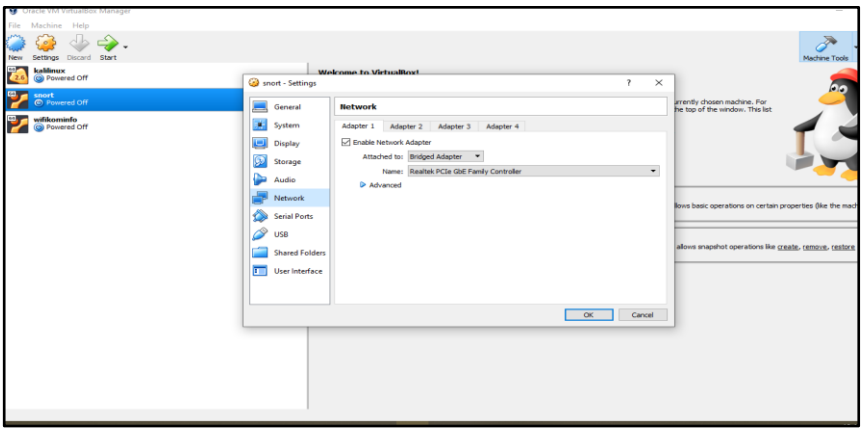
4.2 Pembahasan

4.2.1 Pengujian jaringan awal

Pengujian jaringan awal ini tentang rancangan *Intrusion Detection System* (IDS) menggunakan *Snort* pada Dinas Komunikasi dan Informatika Kab OKI . Pengujian jaringan awal dapat dilihat sebagai berikut :

1) Ketika ada upaya untuk menyerang atau menyalahgunakan jaringan terhadap komputer yang tidak terpasang *snort*, komputer ini tidak dapat mengetahui jika ada ada *traffic* yang sedang menyerang komputer.

2) Snort tidak bisa terbaca di komputer tanpa menginstall snort, karena untuk melihat traffic jaringan komputer harus menginstall snort terlebih dahulu.
3) *Snort* di install pada *Ubuntu Dekstop 18.04 LTS* , yang dimana untuk menggunakan ubuntu itu sendiri perlu bantuan dari aplikasi *Virtual Box* dengan cara penginstall di *virtual box* tersebut .
4) *Ubuntu Dekstop 18.04 LTS* digunakan untuk mengecek *ip* jaringan yang terhubung pada *Wifi* dan juga yang terhubung pada *Router* melalui kabel LAN di Dinas Komunikasi dan Informatika Kab OKI.
5) Sebelum pengecekan pada jaringan yang terhubung, dilakukan penganturan *network* (jaringan) pada setting *Virtual Box.* Agar *Ubuntu* dapat mendeteksi jaringan yang terhubung dilakukan pengaturan pada bagian setting yang terdapat pada tampilan awal *Virtual Box* setelah itu pilih *network,* selanjutnya melakukan setting pada *Adapter* 1 dengan cara memilih *Bridged adapter* Dapat dilihat pada gambar 3.

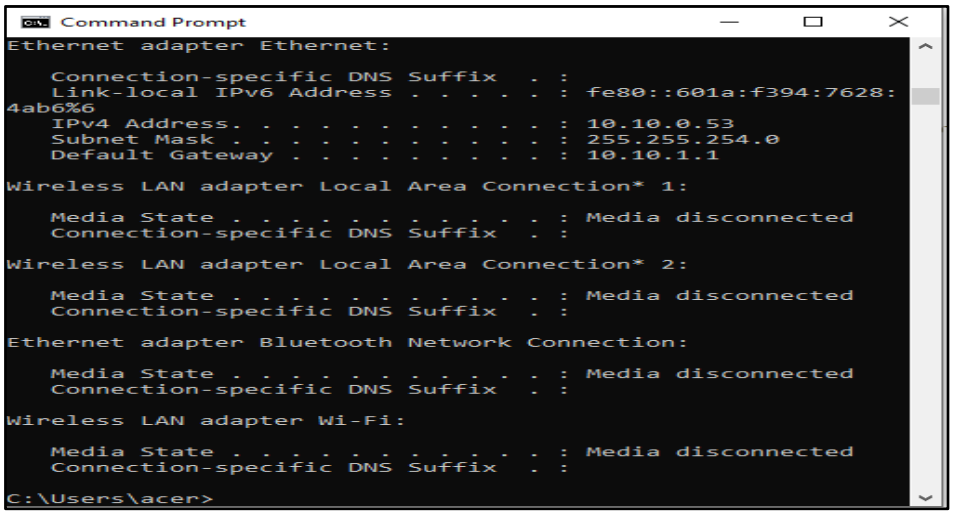


Gambar 3. Tampilan utama setting network *Virtual Box*

4.2.2 Pengecekan IP pada PC *Client*

1) Pengecekan IP jaringan PC client 1 untuk penyerangan pada Router

Pada tahapan yang pertama ini, PC *client* yang pertama berperan sebagai penyerang jaringan yang terhubung pada *router* Dinas Komunikasi dan informatika Kab OKI. Pengecekan jaringan ini dibantu dengan bantuan dari *tools* CMD (*Command prompt*). Untuk menampilkan CMD dilakukan dengan cara mengklik *windows explore* yang terletak pada pojok kiri bawah layar PC kemudian mengetikan CMD. Untuk tampilan dan perintahnya dapat dilihat pada gambar 4.



Gambar 4. Tampilan IP jaringan PC *client* 1 Router

Pada gambar 4 dapat kita lihat tampilan pada *CMD.* Pada tampilan menu *CMD* untuk menampilkan IP yang sedang terhubung pada PC *client* yaitu dengan menuliskan perintah *ipconfig* lalu *Enter*, maka IP jaringan yang sedang terhubung pada PC *Client* akan tampil beserta *subnet mask dan Default gateway* nya .

2) Pengecekan IP jaringan PC *client* 2 untuk penyerangan WIFI

Pengecekan ini dilakukan dengan cara mengklik symbol WIFI yang terdapat di pojok kanan bawah pada PC *Client.* Setelah itu klik tulisan *properties* pada jaringan yang terhubung, maka akan tampil IP jaringan yang di gunakan pada PC *client* untuk menyerang WIFI Dinas Komunikasi dan Informatika Kab OKI. Tampilan IP jaringan dapat dilihat pada gambar 5.

Gambar 5. Tampilan IP jaringan PC client 2 WIFI

5. Kesimpulan

Intrusion Detectin System (IDS) menggunakan *Snort* berguna untuk sistem pendeteksi serangan yang dilakukan untuk melumpuhkan sebuah komputer server suatu jaringan. Kesimpulan yang di dapat dari hasil penelitian ini adalah sebagai berikut :

1) *Intrusion Detection System* (Sistem Deteksi Intrusi) adalah sistem yang dapat mendeteksi serangan dan ancaman yang terjadi pada jaringan komputer, termasuk jaringan lokal dan jaringan internet
2) Menurut hasil pengujian yang dilakukan, Snort dapat diimplementasikan sebagai *intrusion detection system (IDS)* pada sistem operasi *Ubuntu desktop 18.04, LTSm Linux* untuk mendeteksi serangan berupa *ping of deatch , Ssh , Telnet*. Serangan itu sendiri dilakukan pada *Command prompt* dan *tools puty.*
3) Snort dapat memperingatkan serangan keamanan, jadi anda bisa meningkatkan keamanan jaringan. Dapat atau tidaknya sebuah serangan terdeteksi oleh *Snort intrusion Detection System (IDS)* tergantung pada *rules* dengan jenis signature pada sebuah pola serangan.
4) Metode yang digunakan *Snort* merupakan metode analisa *signature* dan *anomaly detection*. Metode *signatures* bekerja dengan membandingkan antara *rules* sebuah traffic yang sedang dideteksi dengan traffic yang mengidentifikasi terjadinya penyerangan.
5) Dari hasil penelitian ini bahwasanya *snort* hanya digunakan sebagai pendeteksi adanya penyerangan terhadap system.

Referensi

[1] Santoso dkk, *Manajemen Keamanan Jaringan informasi menggunakan IDS/IPS*, Strata guard Studi Kasus STIMK Amikom Yogyakarta, 2011.
[2] B. Sugiantoro dan J. E. Istianto, “Analisa Sistem Keamanan Intrusion Detection System (IDS), Firewall System, Database System Dan Monitoring System Menggunakan Agent Bergerak”, *semnasIF*, pp. 21–29, 2010.

[3] A. Kristanto, *Jaringan Komputer*, Brata Ilmu: Yogyakarta, 2003.
[4] I. Sofiana, *Membagun Jaringan Komputer*, Bandung: Informatika, 2015.
[5] D. Ariyus, *Intrusion Detection System*, *Sistem Deteksi Penyusupan Pada Jaringan Komputer*, Andi: Yogyakarta, 2007.
[6] R. Rafiudin, *Mengganyang Hacker dengan Snort*, Yogyakarta: Penerbit Andi, 2010.