Jurnal Intra Tech E-ISSN : 2549 - 0222
Vol 4, No.2, Oktober 2020

Keamanan Jaringan Menggunakan Teknik Network Intrusion Detection System (NIDS) Di Kantor Setwan Kepulauan Meranti

CL Ari Setiawan[1)], Zulfikri[2)], Adhamdi Tria Putra Abza[3)]
[123]Manajemen Informatika, AMIK Selat Panjang, Jalan Terpadu Dorak No. 100 Selat Panjang
email: clarisetiawan@gmail.com, zulfikrimkom@gmail.com, dham.abza@gmail.com

Abstrak

Gangguan keamanan dapat dibagi menjadi dua kategori, gangguan internal dan gangguan eksternal. Gangguan internal terjadi dari pihak yang sudah mengetahui kondisi jaringan, dan gangguan eksternal terjadi dari pihak yang sengaja ingin menjatuhkan dinding keamanan. Gangguan keamanan yang terjadi pada tempat yang menjadi studi kasus ini terjadi dari pihak internal yang ingin menjatuhkan sistem kerja jaringan dan ingin mencoba ketahanan dan keamanan jaringan yang ada pada tempat tersebut. Dengan menggunakan teknik NIDS (Network Base Intrusion Detection System) hal tersebut dapat diatasi dengan cara mengenali setiap pola serangan yang dilakukan oleh intruder. Untuk mendeteksi setiap gejala serangan tersebut, sistem menggunakan pola pengenalan terhadap source yang didapat dari pihak yang dianggap ancaman dalam sistem jaringan komputer. Penulis menggunakan Snort, Barnyard dan BASE yang diimplementasikan pada mesin sensor berbasis open source. Keseluruhan sistem dibangun dalam sistem LAN yang merepresentasikan sistem produksi. Hasil penelitian ini menyimpulkan bahwa setiap tindakan yang dilakukan oleh penyerang terhadap jaringan dapat diketahui oleh mesin sensor, sehingga dapat dilakukan pencegahan sebelum terjadi kerusakan data yang lebih luas.

Kata Kunci : Network Base Intrusion Detection System, Snort, BASE

1. PENDAHULUAN

Pada saat ini perkembangan teknologi Informasi semakin pesat, terutama pada sektor Jaringan Komputer. Hal ini membuat pertukaran informasi terjadi dengan cepat, dalam hitungan menit bahkan detik. Saat ini informasi merupakan sebuah aset yang sangat penting. Kemampuan komunikasi data dalam mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah instansi atau perusahaan. Disisi lain, dengan adanya kemudahan tersebut ternyata menyimpan permasalahan keamanan yang sangat krusial, yang meliputi Confidentality, Aunthenticity, Integrity, Availability.

Salah satu ancaman pada proses komunikasi data adalah Man-In-The-Middle Attack (MITM). Konsep dasar serangan ini adalah ketika penyerang berada diantara dua komputer baik secara fisik maupun tidak yang sedang melakukan proses komunikasi data, sehingga penyerang dapat memantau proses komunikasi dan dapat melihat data yang sedang ditransmisikan, atau bahkan dapat merubah data tersebut. Hal ini membuat kerahasiaan dan keaslian data tidak terjamin (Bhisma & Karan, 2017). Untuk mengurangi resiko yang ditimbulkan di instansi maupun perusahaan menerapkan sistem keamanan jaringan tingkat lanjut yang lebih baik, namun dengan syarat tanpa menghambat kinerja dari instansi atau perusahaan tersebut. Saat ini sebagian besar instansi atau perusahaan menggunakan firewall baik merupakan perangkat keras

maupun perangkat lunak sebagai sistem. Namun perlindungan yang dilakukan pada firewall belumlah mencukupi, karena firewall hanya dapat melindungi koneksi internet inbound dan outbound, selain itu firewall tidak akan bisa berbuat apa–apa jika seseorang telah memperoleh hak akses ke dalam sistem, seperti ketika seseorng telah mengakses komputer target (korban) secara fisik atau program jahat (malicious) telah terinstal di komputer (Sachin, Pradeep & Rajeshwar, 2016).

Tujuan dari penelitian ini adalah meningkatkan sistem keamanan jaringan dengan merancang dan mengimplementasikan Network Instrusion Detection System berbasis open-source dan memahami teknik-teknik cara kerja serangan Man-In-The-Middle Attack (MITM) pada jaringan lokal dan mekanisme NIDS dalam usaha pendeteksian terhadap serangan tersebut. Manfaat dari penelitian ini adalah mendeteksi setiap serangan yang dilakukan oleh intruder sehingga setiap serangan dapat diketahui oleh mesin sensor agar dapat dilakukan pencegahan sebelum terjadi kerusakan data yang lebih luas.

2. METODE PENELITIAN

Metode penelitian dilakukan dengan cara sistematik yang digunakan sebagai pedoman penelitian. Dalam penelitian ini metode yang digunakan adalah Network Development Life Cycle (NDLC) dengan mendefinisikan siklus proses analisa, desain, simulasi prototyping, implementasi, monitoring dan manajemen (Septian, Wing & Eko, 2018).

2.1. Pengumpulan Data

Terdapat beberapa tahap yang penulis lakukan dalam pengumpulan data pada metode Network Development Life Cycle (NDLC) untuk membangun sistem keamanan jaringan di Kantor Setwan Kepulauan Meranti , yaitu :

1. Analisa Jaringan
   Analisa jaringan adalah langkah untuk memahami masalah kemanan jaringan oleh suatu instansi/perusahaan. Metode yang digunakan dalam analisa kemanan jaringan yaitu denga observasi dan wawancara secara langsung di Kantor Setwan Kepulauan Meranti.

2. Desain Jaringan
   Desain jaringan merupakan proses yang dilakukan secara langkah demi langkah pada skema jaringan. Metode yang digunakan dalam desain jaringan yaitu dengan menggunakan simulasi LAN dengan Topologi Tipe Star/Bintang.

3. Simulasi Prototyping
   Pada tahapan ini penulis membangun prototype dari sistem baru yang akan dibangun dan diimplementasikan pada simulasi dengan menggunakan mesin virtual pada lingkungan virtual Simulation prototyping mendemonstrasikan fungsionalitas sistem yang akan dibangun. Penulis menggunakan VMware Fusion untuk memvirtualisasikan sistem yang akan dibangun sebagai prototype simulasi.

4. Implementasi

Tahap ini bertujuan untuk menerapkan sistem keamanan jaringan komputer di Kantor Setwan Kepulauan Meranti. Penulis menggunakan teknik *Network Instrusion Detection System* (NIDS) yang akan digunakan dalam keamanan sistem jaringan komputer.

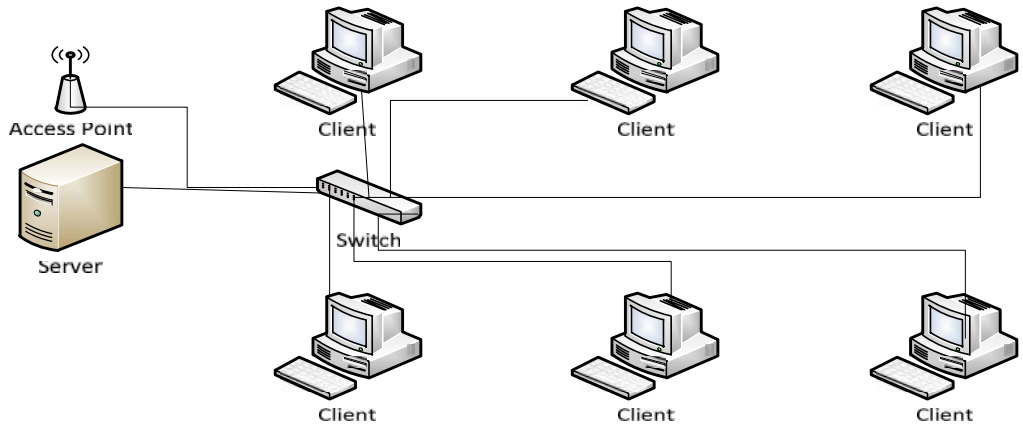
5. Monitoring
   Tahap ini bertujuan untuk mendeskripsikan proses analisis data kejadian pada sistem keamanan jaringan komputer. Penulis menggunakan fungsionalitas BASE terhadap monitoring jaringan yang aktif 24 jam.

6. Manajemen
   Pada tahapan ini penulis melakukan pengujian terhadap sistem kemanan jaringan yang telah dibangun. Penulis menggunakan pengujian DDOS, DNS Spoofing, Port Scanning, Ping Attack dan pengujian dengan serangan TCP/SYN Flooding.

2. HASIL DAN PEMBAHASAN

2.1. Analisa dan Identifikasi Jaringan

Dalam identifikasi jaringan komputer di kantor Setwan Kab. Kepulauan Meranti ditemukan beberapa permasalahan yang dihadapi diantaranya adalah sering masuknya malware ke dalam personal komputer yang terhubung ke dalam jaringan dan Penyadapan pada jalur komunikasi *(Man-in the-Mid- dle Attack)* yang dapat dilakukan lebih mudah. Karena Sistem jaringan di Kantor Setwan tidak menggunakan pengamanan enkripsapti dan otentikasi, atau menggunakan enkripsi. Sehingga memudahkan orang yang tidak berkepentingan dapat masuk ke dalam jaringan.



Gambar 1. Topologi Jaringan Kantor Setwan

Gambar 1 merupakan topologi jaringan di kantor Setwan pada saat ini dimana semua client terhubung ke dalam server. server pada system yang menyediakan *Web Service, File Transfer Protocol* (FTP), *Domain Name Server* (DNS) dan *Secure Shell* (SSH) yang sangat rentan terhadap serangan- serangan. Hardening Komputer dalam hal ini bukan berarti mengeraskan komputer dalam arti fisik. Istilah ini juga dipakai untuk melindungi perangkat komputer dari EMP (electromagnetic pulse), tetapi yang dimaksudkan disini adalah membuat komputer sukar diserang virus, trojan, worm,

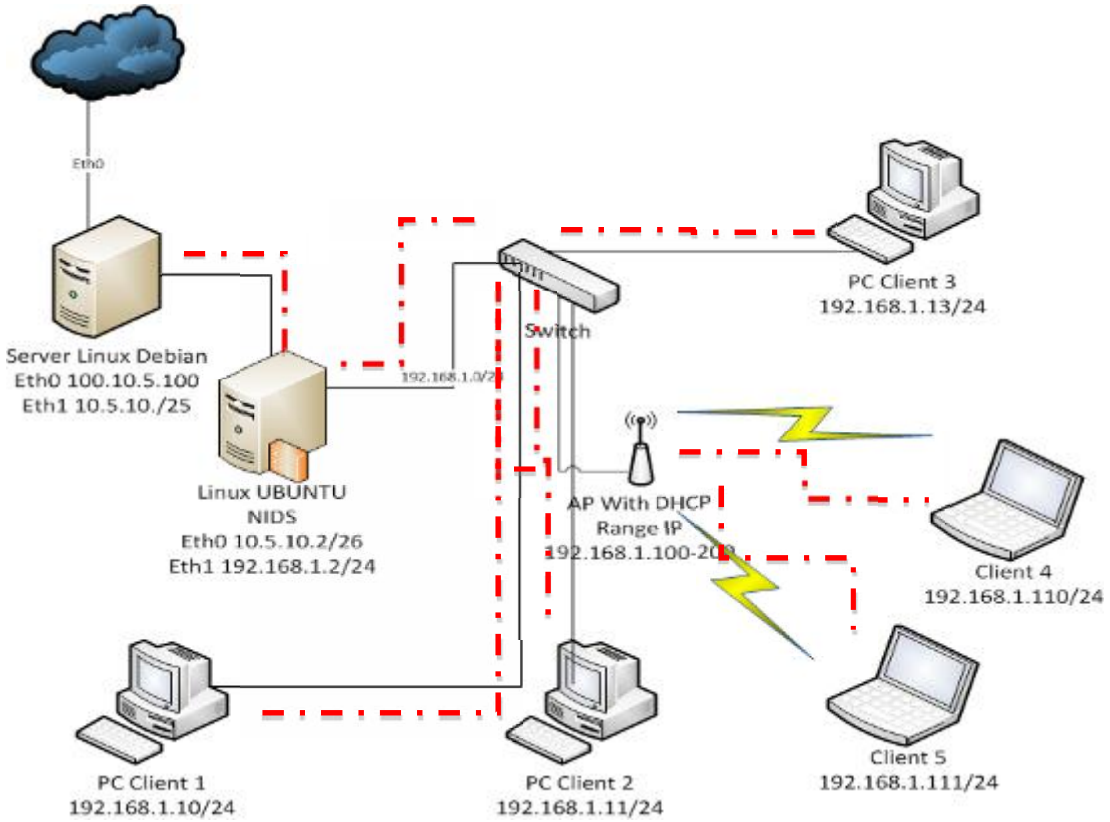
spyware, MITM dan lain-lain. Dalam hal ini penulis menggunakan Metode Network Base Intrusion Detection Sistem untuk mengamankan komputer dalam jaringan yang terdapat di Kantor Setwan Kab. Kepulauan Meranti.

Analisa kebutuhan perangkat sistem NIDS (*Network Base Intrusion Detection System*) merupakan faktor penunjang sebagai pondasi awal untuk memperoleh suatu keluaran yang diinginkan dalam penulisan ini. Penulis akan membangun dan mengimplementasikan NIDS berbasis signature/rule pen source, dengan menggunakan integrasi dari snort Barnyard dan BASE. Snort bertugas mendeteksi berbagai aktifitas intrusi dan penyerang yang terjadi pada jaringan komputer dan akan menampilkan alert bila terjadi aktifitas intrusi. Banyard bertugas mengenali file output Snort, sehingga snort dapat bekerja jauh lebih fokus mengamati trafic. BASE (*Basic Analysis Security Engine*) bertugas untuk merepresentasikan log file snort kedalam format berbasis web yang lebih bersahabat hingga dapat mempermudah proses audit dan analisis.

2.2. *Design* (Perancangan)

Tahap analisis menghasilkan rincian spesifikasi kebutuhan dari sistem yang akan dibangun. Perancangan menjadikan rincian spesifikasi kebutuhan untuk menghasilkan rancangan sistem yang akan dibangun. Dalam penelitian ini, penulis menggunakan simulasi LAN sebagai representasi sistem jaringan lingkungan produksi.

Untuk perancangan topologi Hardening Komputer pada jaringan di Kantor Setwan menggunakan NIDS hampir sama pada umumnya. Topologi yang di pakai adalah tipe *star*/bintang. Seperti terlihat pada gambar 2.



Gambar 2. Topologi Network Hardening Menggunakan NIDS

Garis merah putus-putus Merupakan Serangan Serangan Yang terdeteksi
Garis Hitam lurus Merupakan Koneksi Jaringan

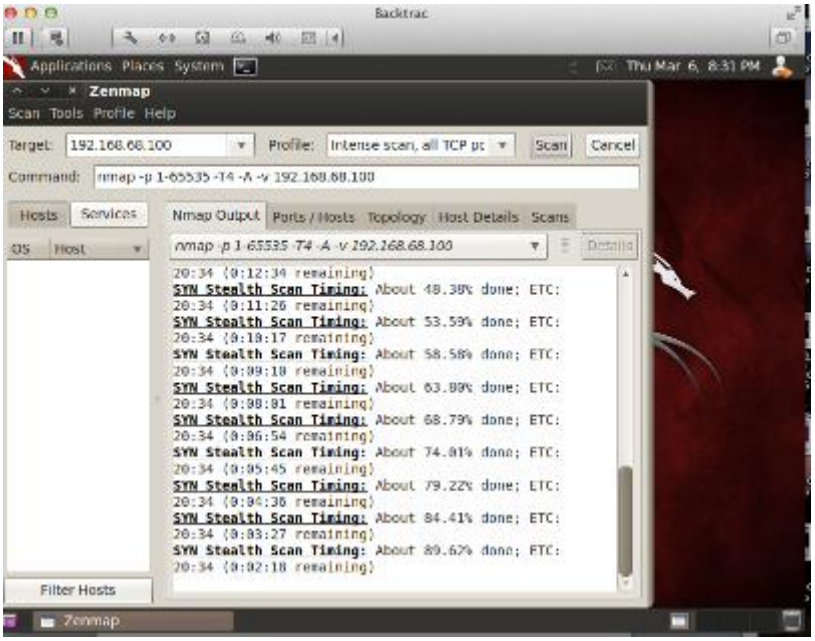
Dari perancangan topologi diatas merupakan rancangan jaringan yang akan dibangun di kantor Setwan. Server Linux menggunakan Debian 5 dalam jaringan tersebut hanya sebagai gateway internet dimana di dalam server mempunyai 2 kartu jaringan Eth0 dan Eth1. Untuk Eth0 dengan IP 100.10.5.100/24 yang terhubung ke ISP (Internet Service Provider) dan Eth1 dengan IP 10.5.10.1/26 yang terhubung ke Server Linux Ubuntu dengan 2 kartu jaringan juga. Untuk Eth0 yang terhubung ke server dengan IP 10.5.10.2/26, Eth1 yang terhubung ke jaringan local (Switch) dengan IP 192.168.1.2/24. Dalam hal ini penulis mempunyai batasan masalah yaitu hanya membahas masalah jaringan dari Server ke jaringan lokal. Disini dari jaringan yang sudah ada sebelumnya di pasangkan sebuah server dengan menggunakan OS linux Ubuntu dengan IP 192.168.1.2 untuk pemasangan NIDS agar bisa mendeteksi serangan-serangan yang terjadi di dalam jaringan. Semua lalu lintas yang mengalir di dalam jaringan nantinya akan dianalisis NIDS untuk mencari apakah ada percobaan serangan atau penyusupan ke dalam sistem jaringan. Dengan adanya Network Intrusion Detection System ini nantinya diharapkan administrator lebih mudah dalam menangani permasalahan yang terjadi di dalam jaringan.

2.3. *Simulation Prototyping*

Pada tahapan ini penulis membangun prototype dari sistem baru yang akan dibangun dan diimplementasikan pada simulasi dengan menggunakan mesin virtual pada lingkungan virtual Simulation prototyping mendemonstrasikan fungsionalitas system yang akan dibangun. Penulis menggunakan VMware fusion untuk memvirtualisasikan system yang akan dibangun sebagai prototype simulasi. Fase pembangunan prototype, dimaksudkan untuk memenuhi sejumlah tujuan :

1. Menjamin efektifitas fungsionalitas dari interkoneksi antar elemen atau komponen system.
2. Memperkecil resiko kegagalan saat proses pembangunan dan implementasi system pada lingkungan nyata.
3. Menjamin bahwa system sudah memenuhi kriteria spesifikasi perancangan sisten dan sudah menjadi solusi dari rumusan permasalahan.
4. Menjamin bahwa kesalahan yang terjadi pada saat proses perancangan pembangunan dan implementasi tidak menganggu dan tidak mempengaruhi lingkungan system nyata.

VMware fusion di gunakan untuk melakukan simulasi terinstall beberapa sistem operasi. Diantaranya adalah sistem operasi Ubuntu sebagi sensor, windows 7 sebagai target dan bactrack sebagai intruder.



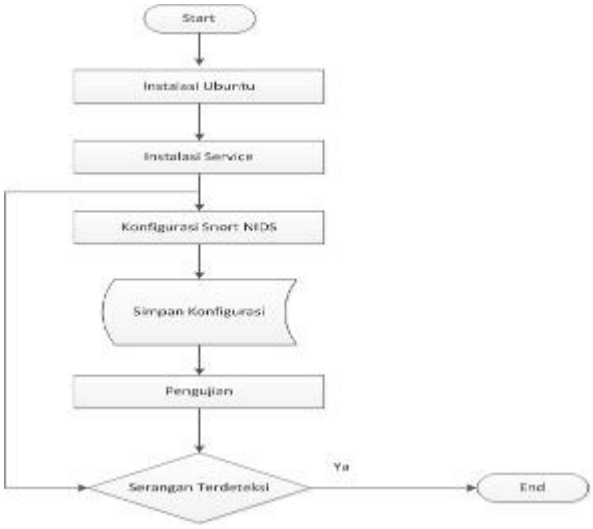
Gambar 3. Sistem Operasi Backtrack pada VMware fusion

Sistem operasi backtrack yang dimaksudkan pada gambar 3 digunakan untuk melakukan pengujian sistem. Dimana pada dasarnya backtrack biasa digunakan hacker untuk melakukan serangan-serangan dalam jaringan.

2.4. Implementasi

Untuk menerapkan teknik network hardening dibutuhkan *Network Intrusion Detection System* (NIDS), penulis menggunakan aplikasi *open-source* snort yang akan di-*install* di Ubuntu. Pada dasarnya snort merupakan sebuah *Intrusion Detection System* (IDS), sehingga hanya memerlukan Libpcap yang merupakan suatu *packet capture library* dan juga memerlukan PCRE (*Perl Compatible Regular Expression*) *library* yang merupakan fungsi dalam *regular expression pattern matching*. Namun pada Snort Inline membutuhkan *packet queing libraries*, yaitu Libnet dan Libipq *library*, yang digunakan untuk mengijinkan firewall melakukan *queue* paket dari kernel ke snort inline. Libipq digunakan oleh snort untuk dapat berhubungan dengan iptables. Penggunaan Libnet harus versi 1.0.x, karena apabila selain versi tersebut snort inline tidak dapat dijalankan.

Langkah langkah dalam melakukan konfigurasi di gambarkan penulis pada gambar 4.



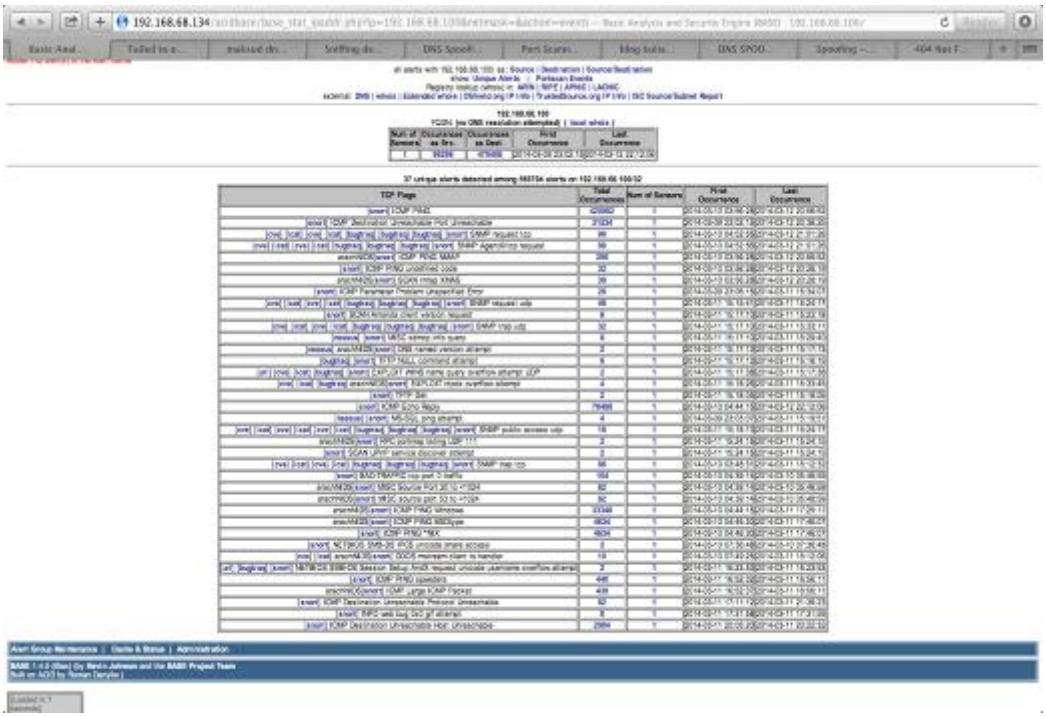
Gambar 4. Alur Konfigurasi

Dari diagram alur pada gambar 4 merupakan tahapan-tahapan untuk melakukan proses konfigurasi pada sistem.

1. Instalasi Sistem Operasi Ubuntu Pada Server
2. Pada server diinstal service yang dibutuhkan untuk menunjang kebutuhan dari sistem, service tersebut adalah : libpcap0.8 libpcap0.8-dev libmysqlclient15- dev mysql-client-5.0 mysql-server- 5.0 bison flex apache2 libapache2- mod-php5 php5-gd php5-mysql libphp-adodb php-pear libc6-dev g++ gcc pcregrep libpcre3 libpcre3-dev build-essential iptables-dev bridge-utils
3. Konfigurasi Snort, pada kegiatan ini akan dikonfigurasikan network hardening dengan menggunakan metode Network base intrusion detection sistem.
4. Simpan konfigurasi, setelah selesai konfigurasi maka hasil dari konfigursai tersebut akan disimpan.
5. Pengujian, pengujian menggunakan Zenmap, DNS Spoofing, Arp Spoofing dan MAC Flooding untuk memastikan apakah konfigurasi dari snort untuk mendeteksi serangan sudahlayak atau belum layak.
6. Serangan terdeteksi, jika pengujian terhadap ancaman sistem keamanan belum dinyatakan aman maka akan dilakukan perbaikan pada konfigurasi snort, dan jika hasil sudah membuktikan bahwa serangan serangan dapat terdeteksi maka proses konfigurasi selesai.

2.5. Monitoring

Pada bagian ini penulis akan mendeskripsikan proses analisis data kejadian melalui fungsionalitas BASE.



Gambar 5. Tampilan Daftar Alert Pada Traffic Profile By Protocol

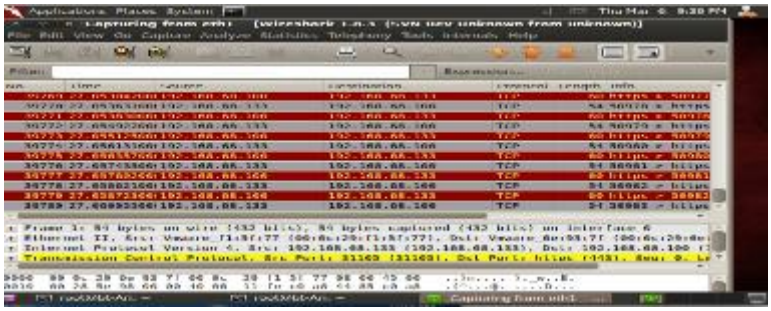
Dari informasi pada gambar 5. terlihat bahwa NIDS (*Network Base Intrusion Detection System*) secara berturut-turut mampu mendeteksi berbagai serangan yang ada pada jaringan. Setelah penulis melakukan beberapa uji coba penyerangan dan menganalisa baik terhadap komputer target maupun komputer sensor NIDS, penulis menemukan data dari komputer penyerang yang dapat digunakan untuk melakukan pencegahan terhadap penyerangan-penyerangan tersebut. Data yang berhasil diperoleh penulis adalah metode yang sering digunakan untuk melakukan penyerangan adalah alamat internet protocol, alamat MAC dan port. Suatu jaringan komputer dapat dipantau hanya dengan melalui sebuah mesin atau komputer yang bertindak sebagai sensor didalam jaringan dan terhubung kedalam sebuah jaringan, itu dapat melihat semua kejadian yang sedang terjadi didalamnya. Selain keuntungan yang didapat dalam penerapan NIDS ini, penulis juga mendapatkan hasil dari sistem NIDS dalam membantu mengamankan jaringan yaitu jika terdapat sebuah masalah pada jaringan (proses intrusi) maka dapat diketahui secara langsung oleh NIDS ini yang menggunakan Snort. Dari mana serangan itu datang, melalui port berapa, dan protokol apa yang digunakan.

2.6. Manajemen

Pada pembahasan ini penulis menggunakan beberapa aplikasi yang digunakan untuk melakukan penyerangan terhadap jaringan yang ada. Hal ini ditunjukkan untuk mengetahui jenis serangan apa saja yang sering dilakukan oleh para hacker serta serangan tersebut dilakukan melalui port mana saja yang sering digunakan. Jenis serangan yang akan penulis coba lakukan adalah TCP/SYN Flooding, PING Attack (ICMP traffic), DoS Attack, Arp Poisoning, Sniffing Attack.

1. Pengujian dengan Serangan TCP /SYN Flooding

Tahapan ini penulis melakukan penyerangan terhadap komputer client dengan metode penyerangan terhadap pembebanan jalur komunikasi TCP/IP atau biasa dikenal dengan teknik TCP flooding. Penulis melakukan uji coba dengan backtrack penyerangan SYN flood, penulis menggunakan hping3 dalam penerapannya. Serangan terhadap SYN akan menaikan trafik memory dari korban. Hasil yang didapat dari proses penyerangan ini adalah proses kerja pada computer target akan menjadi berat dan lama, terutama pada saat melakukan koneksi kedalam jaringan. Aktivitas ini akan dideteksi oleh aplikasi sniffing.

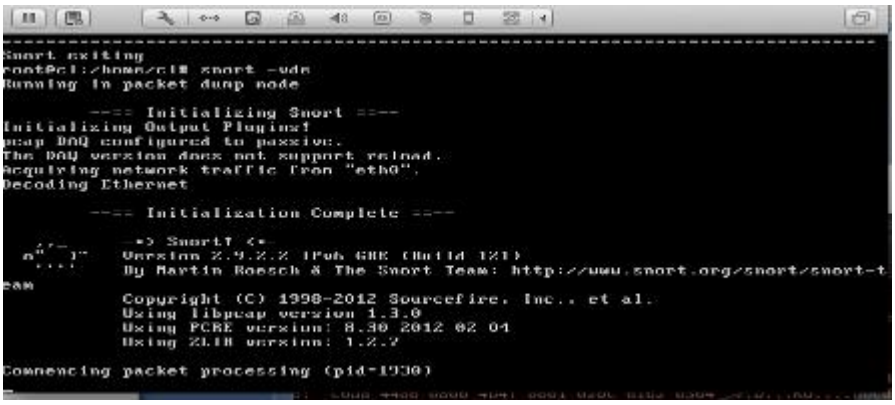


Gambar 6. Hasil Capture menggunakan wireshark

Pada gambar 6 merupakan hasil perekaman data yang ditangkap dengan menggunakan aplikasi wireshark terhadap serangan TCP flooding. Terlihat dari serangan tersebut besarnya paket dan protocol apa yang digunakan.

2. PING Attack (ICMP *Traffic*)

Pada kasus ini penulis menganalisis jenis serangan berprotokol ICMP. Pada dasarnya, traffic ICMP yang diproduksi oleh ping, dianggap sebagai satu serangan karena dapat dipergunakan penyerang atau penyusup untuk mendapatkan informasi mengenai mesin target, memastikan apakah host target dalam keadaan aktif atau tidak. Yang pertama dilakukan adalah melakukan ping dari mesin client ataupun dari mesin penyerang kedalam server NIDS yang memiliki IP address 192.168.68.134. Tahap kedua penulis menggunakan tcpdump yang terdapat pada kebanyakan instalasi default distro linux untuk menangkap dan menganalisa traffic data yang dihasilkan perintah ping penyerang atau client kedalam mesin server.



Gambar 7. Hasil Capture Snort dengan modus Sniffing

Dari data yang di dapat menggunakan tcpdump, jelas terlihat bahwa ping selalu menggunakan protocol unik ICMP dan memuat beberapa karakter unik seperti abcdefghijklmnopqrstuvwxyzabcdefghi. Tahap yang selanjutnya yaitu membuat signature dengan menggunakan parameter spesifik yang mendefinisikan traffic serangan. Dalam hal ini, penulis menggunakan protocol spesifik (ICMP), arah sumber traffic (any), dan arah tujuan traffic (192.168.68.134) sebagai parameter untuk mendefinisikan jenis serangan ini, contoh dari signature-nya adalah “alert ismp any any -> 192.168.68.134 any (msg:”ICMP ping attack”;sid:10001;)’.

Signature tersebut akan mendeteksi traffic protocol ICMP yang diisukan dari segmen jaringan manapun, melalui port berapapun ke alamat IP mesin server NIDS 192.168.68.134 pada port manapun. Penulis kembali melakukan serangan ini dengan kondisi IDS diaktifkan, proses pengujian dapat dikatakan berhasil jika *signature* dapat merespon dari serangan tersebut. Kemudian, penulis melakukan perintah ping dari mesin *client* atau dari mesin penyerang kedalam mesin sensor yang memiliki IP *address* 192.168.68.134. Hasilnya adalah sistem NIDS berhasil mendeteksi *traffic* ping yang dilancarka pada mesin penyerang dan menjelaskan bahwa terjadi “ICMP Ping Attack”

3. Pengujian dengan Serangan DOS Attack (Denial Of Services)

DoS attack adalah jenis serangan terhadap sebuah komputer atau server didalam jaringan dengan cara menghabiskan resource yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinyaengan benar, sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan komputer yang di serang tersebut. Pada tahap ini penulis menggunakan tiga buah computer yang masing-masing terdiri dari computer penyusup yang menggunakan backtrack yang berjalan pada mesin virtual, computer client yang menggunakan system operasi windows 7 yang nantinya akan menjadi korban secara tidak langsung dari proses penyerangan ini. Dimana client akan meminta IP address pada computer server yang diserang menggunakan metode DoS attack dan jenis serangan yang digunakan adalah DHCP spoofing oleh penyusup. Pada tahapan ini yang menjadi tujuan dari seorang penyusup adalah mencuri semua IP address yang disediakan oleh server dan membuat sebuah server baru agar para client yang tersambung kepada computer tersebut tidak bisa mendapatkan IP yang diberikan oleh *server* yang asli, tetapi mereka menjadi terjebak oleh IP yang disediakan oleh komputer *server* palsu yang dibuat oleh penyusup.

4. Pengujian dengan DNS Spoofing

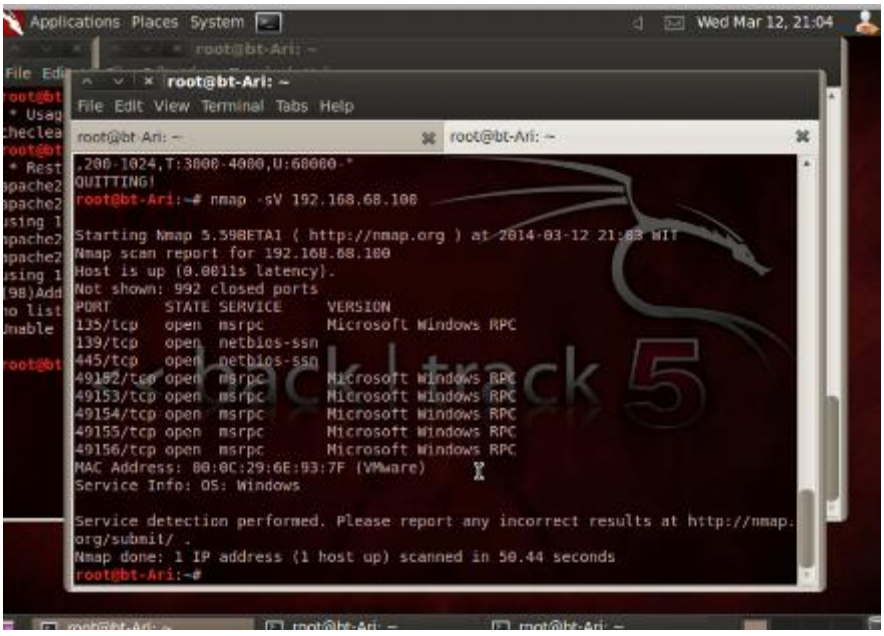
DNS Spoofing adalah salah satu metode hacking Man In The Middle Attack (MITM). Dalam pengujian ini penyerang mengintai aktifitas yang dilakukan oleh target. Pada saat target browsing melalui web browser, akan terekam kedalam mesin penyerang.

Gambar 8. Hasil Pengujian DNS Spoofing

Dari gambar 8 dijelaskan pada mesin target pada saat membuka facebook dalam web browser maka akan terekam didalam mesin penyerang.

5. Pengujian dengan menggunakan Port Scanning

Port Scanning adalah aktivitas yang dilakukan untuk memeriksa status port TCP dan UDP pada sebuah computer target. Dengan menggunakan Port scanning bisa terlihat port-port mana yang terbuka dalam komputer target, sehingga dapat mengetahui celah-celah mana yang dapat dilakukan untuk target penyerangan.



Gambar 9. Hasil Pengujian Port Scanning

4. KESIMPULAN

Kesimpulan dari penelitian ini adalah, dengan penempatan NIDS yang terpisah dengan server dan menggunakan VLAN *switch* untuk melakukan *mirroring traffic*, NIDS mampu menerima *traffic* yang menuju ke server maupun *traffic* antar *virtual*

machine di dalam server. Serangan secara langsung menggunakan 2 skenario, yaitu penyerang berada diluar system dan penyerang berada didalam system, NIDS mampu menerima *traffic*, menganalisis dan merespon serangan dengan menampilkan *alert*. NIDS yang digunakan dalam system adalah IDS *Snort* yang menggunakan *front-end BASE*. Penggunaan *front-end* pada NIDS mampu mempermudah administrator dalam memahami *alert* yang masuk.

DAFTAR PUSTAKA

Abdul Fadlil, Imam Riadi & Sukma Aji, 2017. Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan, Volume 3, Nomor 1.

Bhisma Sharma, Karan Bajaj, 2017. Packet Filtering using IP Tables in Linux. Volume 8, Nomor 4.

Fariz Alwafi, 2015. Analisis dan Implementasi Keamanan Jaringan Pada PT. Dae Myung Highness Indonesia, Volume 3, Nomor 1.

Muhammad Suyuti Ma'sum, M. Azhar Irwansyah & Heri Priyanto, 2017. Analisa Perbandingan Sistem Keamanan Jaringan Menggunakan SNORT dan Netfilter, Volume 5, Nomor 1.

Mr. Sachin Taluja, Pradeep Kumar Verma & Prof. Rajeshwar Lai Dua, 2016. Network Security Using IP Firewalls, Volume 1, Nomor 7.

Oris Krianto Sulaiman, 2016. Analisis Sistem Keamanan Jaringan dengan Menggunakan Switch Port Security, Volume 1, Nomor 1.

Pushpendra Kumar Pateriya & Srijith S. Kumar, 2017. Analysis on Man in the Middle Attack on SSL, Volume 45, Nomor 23.

Putu Riska, Putu Sugiartawan & Ichsan Wiratama, 2018. Sistem Keamanan Jaringan Komputer dengan Menggunakan Metode Port Knocking, Volume 1, Nomor 2.

Realize & Uni Hananti, 2017. Pengaruh Pengguanaan IPTABLES Firewall dan ACID Terhadap Keamanan Jaringan, Volume 3, Nomor 2.

Ridatu Ocanitra & Muhamad Ryansyah, 2019. Implementasi Sistem Keamanan Jaringan Menggunakan Firewall Security Port pada Vitaa Multi Oxygen, Volume 7, Nomor 1.

Sakshi Sharma, Gurleen Singh & Prabhdeep Singh, 2016. Security Enhancing of a LAN Network Using Hardening Technique, Volume 2, Nomor 3.

Suman Rani & Vikram Singh, 2015. SNORT: An Open Source Network Security Tool for Instrusion Detection in Campus Network Environment, Volume 2, Nomor 1.

Septian Ditama, Wing Wahyu Winarno & Eko Pranomo, 2018. Analisi Jaringan VLAN untuk Mengurangi Congestion & Broadcast Domain di Jaringa Local Area Network (Studi Kasus : SMK Negeri Takeran), Volume 3, Nomor 2.

Sugiono, 2016. Sistem Keamanan Jaringan Komputer Menggunakan Metode Watchguard Firebox Pada PT Guna Karya Indonesia, Volume 9, Nomor 1.

Zaeni Miftah, 2018. Simulasi Keamanan Jaringan dengan Metode DHCP Snooping dan VLAN, Volume 11, Nomor 2.