PENGGUNAAN SNORT PADA VIRTUALBOX UNTUK MENGANALISA AKTIVITAS SERANGAN

Medy Wisnu Prihatmono
Program Studi Sistem Informasi
STMIK Profesional Makassar
email: medy_wisnu_prihatmono@stmikprofesional.ac.id

Abstract

Ketergantungan manusia akan teknologi informasi terus meningkat seiring dengan berjalannya waktu. Memang dengan teknologi informasi segalanya menjadi lebih cepat, praktis, dan relatif sangat mudah, jarak yang begitu jauh bermil-mil akan terasa begitu dekat. Bersama dengan itu pula maka masalah baru pun akan muncul yaitu mengenai keamanan jaringan. Salah satu faktor yang menjadi ancaman dalam keamanan jaringan adalah adanya penyusup atau attacker. Attacker akan menyusup ke dalam jaringan secara tiba-tiba tanpa sepengetahuan dari admin jaringan. Bermacam-macam tujuan dari attacker mungkin hanya sekedar iseng, melihat-lihat data atau mengambilnya bahkan akan menjadi sangat berbahaya kalau sampai merusak data dan system. keamanan sistem dari waktu ke waktu, memastikan bahwa sistem dan jaringan yang dikelola terjaga dari berbagai peluang ancaman. Intrusion Detection System (IDS) membantu pengguna dalam memonitor dan menganalisa gangguan pada keamanan jaringan. Untuk mengidentifikasi adanya penyusupan atau pemindaian oleh pihak-pihak yang tidak memiliki otoritas. Selain itu adanya celah dan tidak ada sistem keamanan yang melindungi sistem menjadikan sistem rentan terhadap serangan. Tujuan Penelitian ini mengimplementasi snort pada virtualbox untuk menganalisa ping,telnet dan SSH..Penulis menggunakan software SNORT dalam penelitiannya

***Kata Kunci** : snort,virtualbox,opensource,security*

A. PENDAHULUAN

Internet sudah menjadi bagian terpenting dalam kehidupan manusia pada saat ini, dari terbitnya awal matahari hingga terbenamnya matahari. Orang-orang menggunakan Internet untuk mengakses informasi seperti berita, saham, pasar, belanja online dll. Peningkatan transaksi bisnis dan belanja secara online via internet yang sangat tinggi serta energi dan semangat pertumbuhan digital ini. Dari laporan terbaru yang dirilis oleh Internet World Statistics, jumlah pengguna internet global telah meroket selama dua dekade terakhir. Tanggal berikut menunjukkan kepada Anda betapa cepatnya perkembangan dunia internetdiperbarui pada 30 Juni 2017 [1]

Tabel 1. Negara Pengguna Internet Teratas

Top 20 Countries with Highest Number of Internet Users-June 30, 2017

#	Country or Region	Population 2017 Est.	Internet Users 30 June 2017	Internet Penetration	Growth(*) 2000-2017	Facebook 30 June 2017
1	China	1,388,232,693	738,536,782	53.2 %	3,182.4 %	1,800,000
2	India	1,342,512,706	462,124,989	34.4 %	9,142.5 %	241,000,000
3	United States	326,474,013	286,942,362	87.9 %	266.5 %	240,000,000
4	Brazil	211,243,220	139,111,185	65.9 %	2,682.2 %	139,000,000
5	Indonesia	263,510,146	132,700,000	50.4 %	6,535.8 %	129,000,000
6	Japan	126,045,211	118,453,095	94.0 %	161.8 %	26,000,000
7	Russia	143,375,006	109,552,842	76.4 %	3,434.9 %	12,000,000
8	Nigeria	191,835,936	91,568,757	47.7 %	46,089.4 %	16,000,000
9	Mexico	130,222,815	85,000,000	65.3 %	2,033.9 %	85,000,000
10	Bangladesh	164,827,718	73,347,000	44.5 %	73,247.0 %	21,000,000
11	Germany	80,636,124	72,299,285	89.6 %	261.2 %	31,000,000
12	Vietnam	95,414,640	64,000,000	67.1 %	31,900.0 %	44,000,000
13	United Kingdom	65,511,098	62,991,419	94.8 %	363.2 %	44,000,000
14	Philippines	103,796,832	57,607,240	55.5 %	2,780.4 %	69,000,000
15	Thailand	69,297,547	57,000,000	83.1 %	2,378.1 %	57,000,000
16	Iran	80,945,718	56,700,000	70.0 %	33,980.0 %	17,000,000
17	France	64,938,716	56,367,330	86.8 %	183.1 %	33,000,000
18	Turkey	80,417,526	56,000,000	69.6 %	2,700.0 %	58,000,000
19	Italy	59,797,978	51,814,790	86.7 %	282.7 %	30,000,000
20	Korea,South	50,704,971	47,013,649	92.7 %	185.3 %	17,000,000
Top 20 Countries		3,830,749,614	2,618,277,245	68.4 %	844.1 %	1,326,800,000
Rest of the World		2,480,288,356	1,067,296,374	43.0 %	1,672.2 %	653,793,930
Total World Users		7,599,828,970	3,685,967,619	51.7 %	976.4 %	1,979,793,930

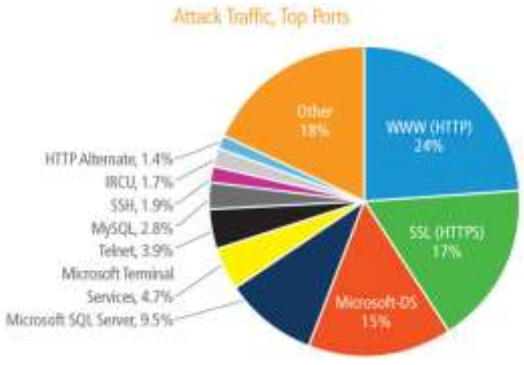
Karena begitu pesatnya kemajuan teknologi, dan dimanjakan kemudahan yang diberikan untuk para pengguna internet, tidak menutup kemungkinan mengundang juga para penjahat cyber. Akibat kejahatan cyber menyebabkan sejumlah besar kerugian, mungkin bisa secara finansial, pada perangkat keras ataupun dari perangkat lunaknya dari sistem milik dari individu atau organisasi sayangnya tidak diiringi dengan kesadaran pelaku bisnis dan masyarakat akan risiko dari serangan cyber. Bahkan sebuah laporan menunjukan masyarakat Indonesia menempati peringkat pertama sebagai negara paling berisiko mengalami serangan cyber.[2]

Gambar 1. Negara Beresiko Mengalami Serangan IT Security

Peningkatan tindakan kriminal dengan memanfaatkan teknologi internet (malware, identity theft, internet abuse, hacking, dsb) semakin sering hal ini terlihat dari berbagai kasus serangan cyber seperti pembobolan dan sinkronasi token memperlihatkan tren pergeseran pola serangan cyber, yang tadinya menargetkan bisnis dan pemerintah, kini semakin gencar menargetkan konsumen secara langsung. Peningkatan transaksi bisnis dan belanja secara online via internet yang sangat tinggi serta energi dan semangat pertumbuhan digital ini, sayangnya tidak diiringi dengan kesadaran pelaku bisnis dan masyarakat akan risiko dari serangan cyber. Bahkan

sebuah laporan menunjukan masyarakat Indonesia menempati peringkat pertama sebagai negara paling berisiko mengalami serangan cyber.

Kategori 10 besar jenis serangan yang terjadi pada akhir-akhir ini, Yang termasuk dalam serangan ini antara lain serangan terhadap port sharing microsoft-ds (port 445), telnet (port 23), WWW/HTTP (port 80), HTTPS/SSL (port 443), dan Microsoft SQL Server (port 1433). Serangan dari Indonesia paling banyak menyerang port 80 dan port 443 yang biasa digunakan oleh layanan Internet. Laporan Akamai menunjukkan bahwa ada peningkatan yang signifikan dalam volume serangan yang menargetkan Port 80 (WWW / HTTP) dan 443 (SSL / HTTPS). Untuk pertama kalinya sejak 2008 Port 445 (Microsoft-DS) bukan port yang paling ditargetkan untuk serangan, turun ke tempat ketiga.[3]



Gambar 2. Attack Traffic, Top Port

Sebagai bahan acuan dalam penelitian ini, maka diambil beberapa jurnal tentang perbedaan dengan penelitian sebelumnya, dalam proses peramalan yang terjadi dengan studi kasus penjualan rumah, untuk sebagai pembanding dan membedakan isi penelitian yang dibuat oleh penulis. Penelitian yang dilakukan oleh [4] dengan judul perancangan dan implementasi intrusion detection system di jaringan universitas diponegoro. Tujuan Penelitian yang dilakukan oleh Dyakso adalah untuk merancang IDS dengan aplikasi web yang dibuat untuk menarik informasi pada basis data sensor IDS, kemudian memproses dan merepresentasikannya dalam tabel dan grafik yang mudah dimengerti. Aplikasi web juga memiliki modul firewall IpTables untuk memblokir alamat IP penyerang. Perangkat keras yang digunakan adalah Cisco IPS 4240, dua komputer *Compaq Presario* 4010F sebagai klien dan *gateway*, dan switch Cisco Catalyst 2960. Perangkat lunak yang digunakan adalah sistem operasi Ubuntu 12.0 LTS Precise, sistem operasi BackTrack 5 R1, bahasa pemrograman PHP 5.4, *database* MySQL 5, dan alat konfigurasi sistem *web-based Webmin*.Penelitian ini menghasilkan

sistem deteksi intrusi yang lebih mudah untuk dipantau. Paket jaringan disalin oleh switch Cisco 2960 dan kemudian diteruskan ke sensor. Deteksi penyusup dilakukan oleh sensor Cisco IPS 4240. Deteksi log diolah oleh aplikasi web ke dalam tabel dan grafik. Sistem deteksi intrusi dimaksudkan untuk meningkatkan keamanan jaringan. Pada bagian yang lain penelitian yang dilakukan oleh [5] dengan judul penerapan *network intrusion detectionsystem* menggunakan snort berbasis database mysql pada hotspot kota.Tujuan Penelitian yang dilakukan Fitriyanti A.Masse adalah Untuk mendeteksi setiap gejala serangan gangguan dari dalam jaringan tersebut, Metode pengembangan sistem yang digunakan dalam penelitian ini adalah *Network Development Life Cycle*. 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 pada jaringan yang lebih luas.

Pada bagian yang lain penelitian yang dilakukan oleh [6] dengan judul Kolaborasi *Intrusion Detection System* Berbasis *Publish/Subscribe.* Tujuan penelitian yang dilakukan oleh Samsul Arifin adalah membahas tentang bagaimana membuat system keamanan jaringan dengan menggunakan kolaborasi snort IDS (Intrution Detection System)dan IPtables firewall berbasis publish/subscribe. Adapun hasil dari penelitian ini adalah Snort dan IPtables masing-masing akan saling bekerja sama untuk mendeteksi adanya penyusup dan berusaha untuk mencegahnya masuk kedalam jaringan.

Pada bagian yang lain penelitian yang dilakukan oleh [7] dengan judul implementasi ids (*intrusion detection system*) pada sistem keamananjaringan SMAN 1 Cikeusal. Tujuan penelitian yang dilakukan oleh Sutarti adalah sistem dalam menangani penyalahgunaan jaringan atau ancaman yang akan terjadi, maka diimplementasikan dengan menggunakan aplikasi Intrusion Detection System (IDS) yaitu Snort dan PfSense (Router OS) sebagai penindak lanjutnya terhadap alert snort yang dihasilkan. Adapun hasil penelitian yang dihasilkan adalah dapat mengetahui apa yang sedang terjadi yang di hasilkan pada alert seperti serangan Ping Of Death dan Port Scan. Pada PfSense menampilkan alert jika ada seseorang yang mencoba menyalahgunakan jaringan seperti mengakses sosial media facebook,

youtube, twitter dan lain-lain bisa menindak lanjuti dengan mem-block secara otomatis. Pada bagian yang lain penelitian yang dilakukan oleh [8] dengan judul deteksi penyusupan pada jaringan komputer menggunakan ids snort. Tujuan Penelitian yang dilakukan Walid Fathoni adalah menganalisa terhadap beberapa jenis serangan yang ada dan sering terjadi, sehingga dapat membantu menangkal serangan yang dilakukan hacker terhadap sistem Hasil dari penelitian ini adalah penulis berhasil mendeteksi semua serangan yang diujicobakan dan menghasilkan nilai 1 yang berarti pendeteksian berjalan dengan baik. Adapun jenis-jenis serangan diketahui yaitu :SQL Injection, Cross Site Scriping (XSS), Denial of Service (DoS), SSH Brute Force.

Berangkat dari beberapa rujukan penelitian diatas, maka penulis dalam hal ini melakukan kajian yang lebih spesifik yaitu penggunaan snort pada virtualbox untuk menganalisa aktivitas dan menampilkan jenis serangan yang terdiri dari ping, telnet, SSH .

B. METODE PENELITIAN

Fungsi Intrusion Detection System (IDS)

Beberapa alasan untuk memperoleh dan menggunakan intrusion detection system (IDS) diantaranya[9]:

1. Mencegah resiko keamanan yang terus meningkat, karena banyak ditemukan kegiatan ilegal yang diperbuat oleh orang-orang yang tidak bertanggung jawab dan hukuman yang diberikan atas kegiatan tersebut.
2. Mendeteksi serangan dan pelanggaran keamanan system jaringan yang tidak bisa dicegah oleh sistem seperti *firewall*
3. Mendeteksi serangan awal, penyerang akan menyerang suatu system yang biasanya melakukan langkah-langka awal yang mudah diketahui yaitu dengan melakukan penyelidikan atau menguji system jaringan yang akan menjadi target, untuk mendapatkan titik-titik dimana meraka akan masuk.
4. Menyediakan informasi yang akurat terhadapt gangguan secara langsung , meningkatkan diagnosis, recovery, dan mengoreksi faktor-faktor penyebab suatu serangan yang ada pada jaringan tersebut.

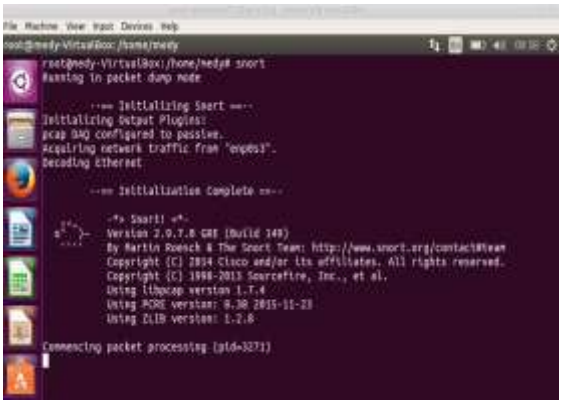
SNORT

Snort adalah *opensource network intrusion detection system (NIDS)* yang memiliki kemampuan untuk memonitoring paket-paket sekaligus menjadi *security tools* yang berguna

untuk medeteksi berbagai serangan, sebagai contoh ddos, MITM, telnet,ping dan sebagainya.[9]. Snort dapat dioperasikan dengan tiga metode [9]

1. Paket *Sniffer* : untuk melihat paket yang lewat di jaringan
2. Paket *Logger* : untuk mencatat semua paket yang lewat dijaringan untuk dianalisis di kemudian hari.
3. NIDS : pada mode ini snort akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan computer.

Pada linux pengginstalan dilakukan lewat terminal dan cara panggil aplikasinya pun bisa lewat terminal, pada bagian ini penulis mengginstall pada virtualbox snort yang ingin digunakan, Untuk lebih jelasnya bisa dilihat pada gambar 3 dibawah ini :

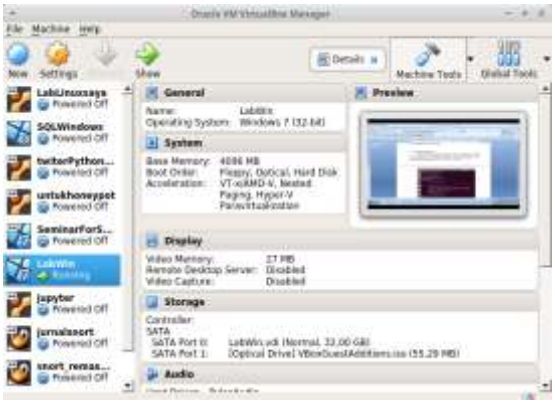


Gambar 3. Tampilan Awal Interface SNORT

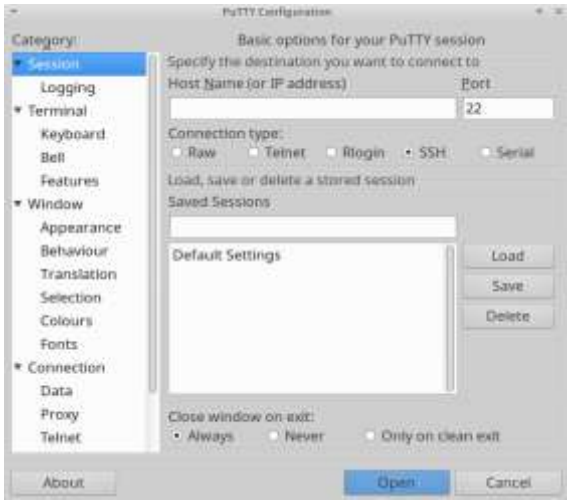
Virtualbox

Oracle VM VirtualBox adalah paket perangkat lunak virtualisasi open source x86 lintas platform, yang sekarang dikembangkan oleh Oracle Corporation sebagai bagian dari keluarga produk virtualisasi. VirtualBox adalah apa yang disebut hypervisor "host". Untuk tingkat yang sangat besar, VirtualBox secara fungsional identik pada semua platform host, dan file dan format gambar yang sama digunakan. Ini memungkinkan Anda menjalankan mesin virtual yang dibuat di satu host pada host lain dengan sistem operasi host yang berbeda; misalnya, Anda dapat membuat mesin virtual padaWindows dan kemudian menjalankannya di Linux.

VirtualBox terutama menggunakan virtualisasi perangkat lunak untuk menjalankan mesin virtual. Ini adalah perilaku default untuk mesin virtual (dengan pengecualian sistem operasi tamu 64-bit) yang dibuat dalamVirtualBox lingkungan. Namun, VirtualBox menyediakan opsi untuk mengaktifkan virtualisasi perangkat keras padavirtual basis mesinsaat berjalan pada CPU berkemampuan AMD-V dan Intel-VT. Pada lebih baru desain CPU yang, VirtualBox juga dapat menggunakan tabel paging bersarang untuk meningkatkan mesin virtual kinerja. [10] Untuk lebih jelasnya bisa dilihat pada gambar 4 dibawah ini :



Gambar 4. Tampilan Interface dari Virtualbox



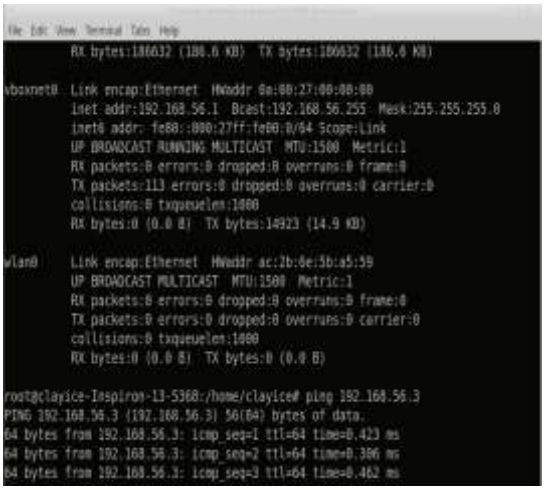
Gambar 5. Tampilan Interface dari PuTTY

PuTTY

PuTTY adalah sebuah aplikasi open-source memanfaatkan protokol jaringan seperti SSH dan Telnet. PuTTY memanfaatkan protokol tersebut untuk mengaktifkan sesi remote pada computer Tujuan utama dari PuTTY adalah menjadi aplikasi multi-platform yang mampu mengeksekusi dalam sebuah sistem operasi. Hal ini juga disebut terminal xterm. Jendela utama dari PuTTY memiliki sesi yang berjalan pada komputer remote dan dan dapat mengirim perintah langsung ke komputer remote. PuTTY memberikan beberapa keuntungan yang berbeda, terutama ketika bekerja dari jarak jauh. Hal ini dirasa lebih memudahkan untuk mengkonfigurasi.[11] . Untuk lebih jelasnya bisa dilihat pada gambar 4 dibawah ini :

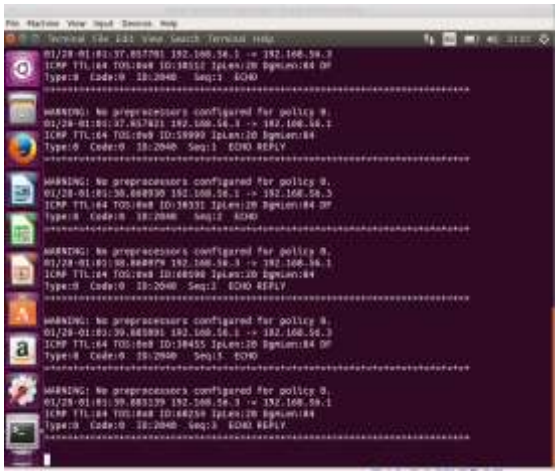
C. HASIL PENELITIAN DAN PEMBAHASAN

Pada bagian pertama, adalah bagaimana melihat hasil dari sebuah perintah ping sederhana dari sebuah komputer pihak attacker yang kemudian, akan mencoba-coba masuk kedalam server , yang dimana dari pihak attacker ingin memastikan coba-coba apakah server tersebut berfungsi sebagaimana mestinya. Untuk ipaddress dari pihak attacker misalnya 192.168.56.1 pada mesin virtualbox lalu akan mencoba ping ke ipaddress 192.168.56.3, ini merupakan ipaddress server korban. Untuk lebih jelasnya bisa dilihat pada gambar 6 dibawah ini :



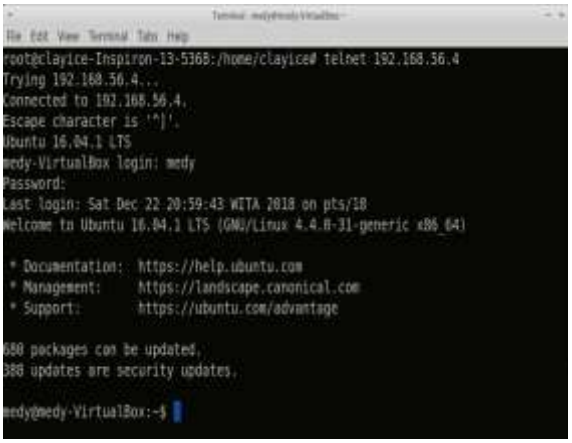
Gambar 6. Ping dari Sebuah Pihak Attacker

Kemudian hasil dari ping dari pihak attacker, akan dibaca oleh snort yang dimana langsung memberikan informasi peringatan bahwa ada sebuah aktivitas yang mencoba-coba memasuki dari server korban. Perintah peringatan yang muncul merupakan suatu aturan konfigurasi yang di buat sebelumnya pada snort tersebut. Snort menyampaikan sebuah alamat ipaddress yang mencurigakan, dengan alamat ipaddress 192.168.56.1 telah melakukan sebuah ping berulangkali, Untuk lebih jelasnya bisa dilihat pada gambar 7 dibawah ini :

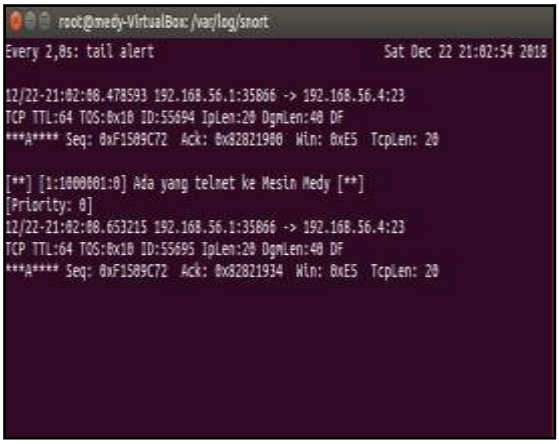


Gambar 7. Hasil ping ditampilkan di snort.

Selanjutnya untuk kasus yang lain dalam penelitian ini yaitu perintah telnet yang digunakan oleh pihak attacker. Telnet (Telecommunication network) adalah sebuah protokol jaringan yang digunakan pada Internet atau Local Area Network untuk menyediakan fasilitas komunikasi berbasis teks interaksi dua arah yang menggunakan koneksi virtual terminal. Telnet (Telecommunication network) pada posisi Port 23 dalam sebuah jaringan. Dari pihak attacker ipaddressnya yaitu 192.168.56.1 yang dimana kemudian akan melakukan Telnet pada ipaddress 192.168.65.4, khusus ip ipaddress dibuatkan pada virtualclient yang berbeda akibat cloning dari virtualbox yang dibuat sebelumnya oleh penulis, Untuk lebih jelasnya bisa dilihat pada gambar 8 dibawah ini :



Gambar 8. Aktivitas telnet dari pihak attacker

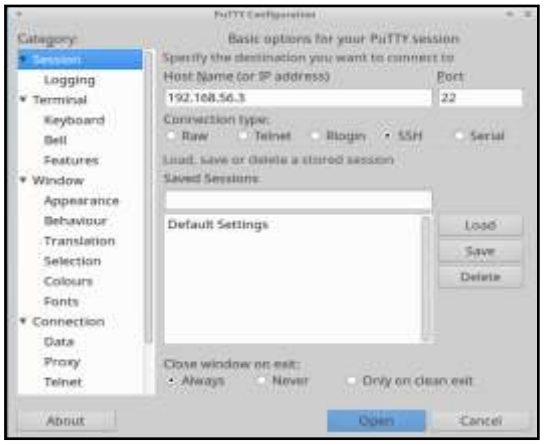


Gambar 9. Hasil aktivitas sebuah telnet

Hasil Telnet (*telecommunication network*) yang dilakukan pada pihak attacker pada port 23, kemudian snort bekerja lalu memproses sebuah Telnet (*telecommunication network*) yang dilakukan oleh pihak attacker pada suatu waktu tertentu. Snort akan menampilakan sebuah ipaddress yang telah melakukan sebuah Telnet (*telecommunication network*) yaitu 192.168.56.1 dari pihak attacker. Aturan sebuah snort sudah diatur sebelumnya, pada konfigurasi untuk mendeteksi sebuah Telnet (*telecommunication network*), dengan memunculkan pesan aktivitas serangan dalam 2 detik setiap serangan yang ada, untuk jelasnya melihat hasil sebuah telnet pada snort dapat dilihat pada gambar 9 dibawah ini:

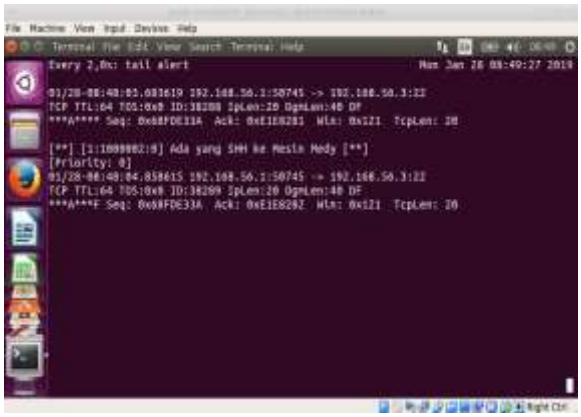
Selanjutnya untuk kasus yang lain dalam penelitian ini yaitu perintah Secure Shell (SSH). Secure Shell (SSH) adalah sebuah protokol jaringan kriptografi untuk komunikasi data yang aman, login antarmuka baris perintah, perintah eksekusi jarak jauh, dan layanan jaringan lainnya antara dua jaringan komputer, Secure Shell (SSH) menggunakan port 22 dari sebuah jaringan. Untuk melakukan sebuah Secure Shell (SSH) penulis menggunakan aplikasi PuTTY yang sudah diinstall sebelumnya pada computer pihak attacker. Dari pihak attacker menggunakan sebuah ipaddress 192.168.56.1, kemudian menjalankan PuTTY configuration dengan memasukkan ipaddress dari sebuah komputer korban yaitu 192.168.56.3 kemudian memilih pada radiobutton yaitu SSH, kemudian memasukkan port 22,

Untuk lebih jelasnya bisa dilihat pada gambar.10 dibawah ini :



Gambar 10. Sebuah Aktivitas SSH pada PuTTY

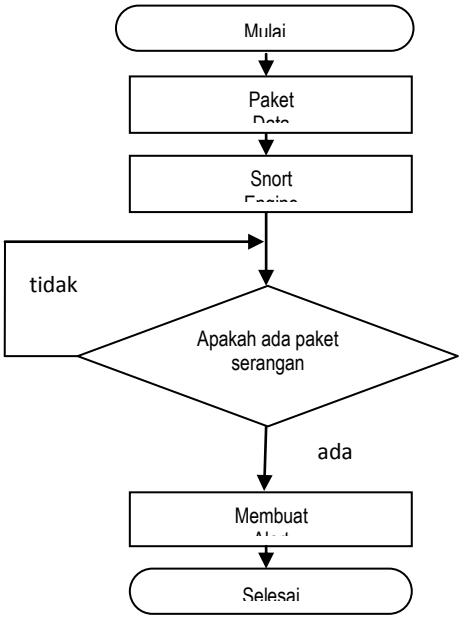
Hasil dari sebuah *Secure Shell* (SSH) yang dilakukan oleh pihak attacker dengan ipaddress asal 192.168.56.1 dan ipaddress tujuan 192.168.56.3 dengan menggunakan port 22, dengan aplikasi snort telah menganalisa sebuah kegiatan (SSH) oleh pihak attacker sebelumnya, konfigurasi snort untuk menganalisa (SHH) sudah diatur sebelumnya dengan memunculkan pesan aktivitas serangan dalam 2 detik setiap serangan yang ada, Untuk lebih jelasnya bisa dilihat hasil dari SHH bisa dilihat pada gambar.11 dibawah ini :



Gambar 11. Hasil aktivitas SSH

Pembahasan

Adapun *flowchart* untuk proses menganalisa jenis-jenis paket serangan dengan menggunakan snort ditampilkan pada gambar 12, adalah sebagai berikut :



Gambar 12. *Flowchart* Analisa Paket Serangan

Pada tahap selanjutnya akan dibahas secara detail proses pembuatan aturan – aturan dalam snort yang telah

dibuat sebelumnya, guna menjabarkan tiap fungsinya masing-masing.

Dalam sistem operasi Linux untuk menuliskan perintah-perintah didalam snort terdapat pada /etc/snort/rules , untuk proses ping analisa perintahnya sebagai berikut :

- Ada sebuah alert ke port internet control message protocol (icmp) ke dalam suatu IP address tujuan 192.168.56.3 yang ingin di buatkan pertahanan. Kemudian dibuatkan sebuah pesan ECHO PING bahwa ada yang melakukan ping dengan icode 0 dan itype 8 , kemudian dibuatkan yang sama dengan membedakan icode:0 dan itype:0 ada pesan yang berbeda pada aturannya ECHO PING yang dilanjutkan dengan pemberian nilai SID 100000.
- Ada sebuah alert ke port tcp : alert tcp any any ke 192.168.56.3 pada port 23 ini mengindentifikasikan bahwa : action diberi tanda bahaya (“alert”), semua paket ke telnet port (port 23) ke mesin 192.168.56.3, kemudian string difungsikan untuk di baca oleh admin “Ada yang telnet ke mesin medy”. Untuk sid –rule ID start mulai dari yang angka 100002, karena untuk 100000 & 100001 untuk ping
- Ada sebuah alert ke port tcp : alert tcp any any ke 192.168.56.3 pada port 22 ini mengindentifikasikan bahwa : action diberi tanda bahaya (“alert”), semua paket ke telnet port (port 22) ke mesin 192.168.56.3, kemudian string difungsikan untuk di baca oleh admin “Ada yang telnet ke mesin medy”. Untuk sid –rule ID start mulai dari yang 100003. Untuk lebih jelasnya bisa dilihat hasil dari seluruh konfigurasi bisa dilihat pada gambar.13 dibawah ini :

Gambar 13. Konfiguras pada /etc/snort/rules

Setelah melakukan konfigurasi pada snort kemudian dijalankan dengan perintah di terminal sesuai dengan gambar 14 dibawah ini, yang dimana bagian tersebut menjelaskan konfigurasi dari sebuah snort –c = configurasi yang dipakai /etc/snort/snort.conf , kemudian hasil filenya ada di simpan var/log/snort/ dalam bentuk -K ascii. Fungsinya memberitahukan file log nanti disimpan dalam format text ASCI jadi mudah dibaca dan bukan dalam bentuk binary.

Untuk lebih jelasnya bisa dilihat hasil dari seluruh konfigurasi bisa dilihat pada gambar.14 dibawah ini :

Gambar 14. Konfigurasi snort

D. KESIMPULAN DAN SARAN

Snort tidak bisa menindak lanjuti alert yang terdeteksi sebagai serangan atau penyalahgunaan jaringan karena sifatnya hanya mendeteksi. Untuk pembacaan log snort dapat dibuat lebih kompleks lagi, karena hasil log snort mempunyai banyak karakter dan Dilakukannya pengujian gangguan serangan terhadap jaringan yang berbeda, tidak hanya pada dalam satu jaringan saja

DAFTAR PUSTAKA

[1] Top 20 Countries by Number of Internet Users. https://www.coolostdesign.com/Top-20-Countries-by-Number-of-Internet-Users-a775.html (Diakses pada tanggal 27 Januari 2017)

[2] Sophos Security Threat Report 2013-the safest and riskiest countries revealed https://nakedsecurity.sophos.com/2012/12/04/sophos-security-threatreport/ (Diakses pada tanggal 27 Januari 2017)

[3] Internet attacks: top ports, countries revealed https://mybroadband.co.za/news/security/89351-internet-attacks-top-ports-countries-revealed.html (Diakses pada tanggal 27 Januari 2017)

[4] Dyakso Anindito Nugroho **Perancangan dan Implementasi Intrusion Detection System di Jaringan Universitas Diponegoro .,** Jurnal Teknologi dan Sistem Komputer, Vol.3, No.2, April 2015 (e-ISSN: 2338-0403)

[5] Fitriyanti A.Masse **Penerapan Network Intrusion Detection System Menggunakan Snort Berbasis Database Mysql pada Hotspot Kota** Jurnal Elektronik Sistem Informasi Dan Komputer, VOL 1 No.2 Juli-Desember 2015, p. ISSN: 2777-888 e. ISSN: 2502-2148

[6] Samsul Arifin ***Kolaborasi Intrusion Detection System Berbasis Publish/Subscribe*** Jurnal JITIKA, Vol. 6, No.2, Agustus 2012: 46-52

[7] Sutarti ***Implementasi IDS (intrusion detection system) Pada***

Sistem Keamanan Jaringan SMAN 1 Cikeusal Jurnal PROSISKO Vol. 5 No. 1 Maret 2018 e-ISSN: 2597-9922, p-ISSN: 2406-7733

[8] Walid Fathoni. ***Deteksi Penyusupan Pada Jaringan Komputer Menggunakan IDSSnort*** e-Proceeding of Engineering : Vol.3, No.1 April 2016 | ISSN : 2355-9365.

[9] Ariyus, Dony. 2007. Intrusion detection system, Yogyakarta:ANDI.

[10] Vasudevan.M.S ***Performance Measuring and Comparison of VirtualBox and VMware.*** 2012 International Conference on Information and Computer Networks (ICICN 2012) IPCSIT vol. 27 (2012) © (2012) IACSIT Press, Singapore

[11] ***Cara Menggunakan PuTTY***, Panduan Simpel untuk Pemula! https://gegeriyadi.com/cara-menggunakan-putty (Diakses pada tanggal 27 Januari 2017)