Deteksi Penyusupan Pada Server Menggunakan Metode Intrusion Detection System (IDS) Berbasis Snort

Benny Wijaya[1], Arie Pratama[2]
Program Studi Teknik Informatika [1], [2]
STMIK Atma Luhur
Pangkalpinang, Indonesia
benny.wijaya@atmaluhur.ac.id [1]

***Abstract*— The problem that is inherited cyber internet cafe is located in the Internet server security system has not been available, therefore several times Cyber internet cafe servers have problems due to attacks performed by other parties such as Ping Flood, Smurf Attack and others. There are several alternatives solution to overcome the security problems of the Cyber Internet cafe, one of which is the application of IDS (Intrusion Detection System) method. This system works by warning that there is an intrusion from outside that can read the parameters of the attacker's (Internet Protocol) IP address. With the implementation of this system, the system is able to close access to the attacks efforts on the computer network. From the test results by conducting several types of attacks such as Ping of death and some other attacks it seems that the detection system applied can work well to recognize the presence of attacks that enter the Cyber Internet Cafe network system**

Keywords*— *Intrusion Detection System (IDS), Server, Internet Protocol

***Abstrak*— Permasalahan yang ada di warnet cyber terletak pada belum terdapatnya sistem keamanan server warnet, oleh karena itu beberapa kali server warnet cyber mengalami permasalahan karena adanya penyerangan yang dilakukan oleh pihak lain seperti ping flood, smurf attack dan lain - lain. Ada beberapa alternatif solusi untuk mengatasi permasalahan keamanan warnet yang kurang maksimal salah satunya adalah penerapan metode IDS (Intrusion Detection System). Sistem ini bekerja dengan membuat peringatan bahwa adanya penyusupan dari luar yang bisa membaca parameter berupa alamat IP (*Internet Protocol)* penyerang. Dengan Implementasi sistem ini ,maka sistem mampu menutup akses terhadap usaha-usaha penyerangan terhadap jaringan komputer. Dari hasil pengujian dengan melakukan beberapa jenis serangan seperti ping of death dan beberapa serangan lain terlihat bahwa sistem pendeteksian yang diterapkan dapat bekerja dengan baik untuk mengenali adanya serangan yang masuk ke sistem jaringan warnet cyber.**

Kata Kunci*— *Intrusion Detection System (IDS), Server, Internet Protocol

I. PENDAHULUAN

Keamanan jaringan komputer sebagai bagian dari sebuah sistem informasi adalah sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Sistem harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan oleh pihak yang tidak berhak[1]. Keamanan jaringan sering dipandang sebagai hasil dari beberapa faktor. Faktor ini bervariasi tergantung pada bahan dasar, tetapi secara normal setidaknya ada beberapa hal dalam konsep keamanan jaringan diantaranya adalah kerahasiaan, integritas dan ketersediaan[2]. Sistem keamanan komputer, dalam beberapa tahun ini telah menjadi fokus utama dalam dunia jaringan komputer, hal ini disebabkan tingginya ancaman yang mencurigakan (*Suspicious Threat*) dan serangan dari Internet. Keamanan Komputer (*Security*) merupakan salah satu kunci yang dapat mempengaruhi tingkat *Realibility* (keandalan) termasuk Performance (kinerja) dan *Availability* (tersedianya) suatu Internetwork[3]. Kerusakan yang terjadi pada suatu jaringan akan mengakibatkan pertukaran data yang terjadi pada jaringan tersebut akan melambat atau bahkan akan merusak suatu sistem jaringan. Insiden keamanan jaringan adalah suatu aktivitas terhadap suatu jaringan komputer yang memberikan dampak terhadap keamanan sistem yang secara langsung atau tidak bertentangan dengan *security policy* sistem tersebut [4].

Warnet secara umum adalah tempat dimana beberapa komputer membentuk jaringan, dengan salah satu komputer bertindak sebagai komputer server yang telah di konfigurasi atau disetting dan komputer lainnya bertindak sebagai komputer client. Warnet cyber adalah warnet yang baru beroperasi dan masih dalam proses pengembangan karena warnet ini masih belum sempurna, baik dari sisi bangunan maupun dari sisi sistem yang berjalan dalam memenuhi kebutuhan trafik pengguna warnet. Permasalahan yang ada diwarnet cyber terletak pada tingkat keamanan server warnet yang belum optimal, dimana saat ini belum ada penerapan sistem keamanan pada server, sehingga beberapa kali server warnet cyber mengalami permasalahan karena adanya penyerangan yang dilakukan oleh pihak lain seperti ping flood, smurf attack dan lain – lain yang menyebabkan sistem jaringan warnet menjadi down. Ada beberapa alternatif solusi

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v9.i1.770, Copyright ©2020
Submitted : 15 Januari 2020, Revised : 4 Maret 2020, Accepted : 16 Maret 2020, Published : 24 Maret 2020

untuk mengatasi permasalahan keamanan server warnet yang kurang maksimal, salah satunya adalah penerapan metode IDS (Intrusion Detection System). IDS (Intrusion Detection System) dapat didefinisikan sebagai tool,metode,sumber daya yang memberikan bantuan untuk melakukan identifikasi, memberikan laporan terhadap aktifitas jaringan komputer [5].

Jika terindikasi adanya aktifitas yang mencurigakan terhadap aliran (traffic) paket-paket yang keluar dan masuk pada sistem, maka IDS akan merekam aktifitas tersebut. IDS merupakan software atau hardware yang melakukan otomatisasi proses monitoring kejadian yang muncul di sistem komputer atau jaringan, menganalisanya untuk menemukan permasalahan keamanan [6]Alasan mempergunakan IDS: 1) Untuk mencegah resiko timbulnya masalah; 2) Untuk mendeteksi serangan dan pelanggaran keamanan lainnya yang tidak dicegah oleh perangkat keamanan lainnya. Biasanya penyusupan berlangsung dalam tahapan yang bisa diprediksi. Tahapan pertama adalah probing, atau eksploitasi pencarian titik masuk. Pada sistem tanpa IDS , penyusup memiliki kebebasan melakukannya dengan resiko kepergok lebih kecil. IDS yang mendapati probing, bisa melakukan blok akses dan memberitahukan tenaga keamanan yang selanjutnya mengambil tindakan lebih lanjut; 3) Untuk mendeteksi usaha yang berkaitan dengan serangan misal probing dan aktivitas dorknob rattling; 4) Untuk mendokumentasikan ancaman yang ada ke dalam suatu organisasi. IDS akan mampu menggolongkan ancaman baik dari dalam maupun dari luar organisasi. Sehingga membantu pembuatan keputusan untuk alokasi sumber daya keamanan jaringan; 5) Untuk bertindak sebagai pengendali kualitas pada administrasi dan perancangan keamanan, khususnya pada organisasi yang besar dan kompleks. Saat ini IDS dijalankan dalam waktu tertentu, pola dari pemakaian sistem dan masalah yang ditemui bisa nampak. Sehingga akan membantu pengelolaan keamanan dan memperbaiki kekurangan sebelum menyebabkan insiden; 6) Untuk memberikan informasi yang berguna mengenai penyusupan yang terjadi, peningkatan diagnosa, recovery, dan perbaikan dari faktor penyebab. Meski jika IDS tidak melakukan block serangan, tetapi masih bisa mengumpulkan informasi yang relevan mengenai serangan, sehingga membantu penanganan insiden dan recovery[7][8]. Hal itu akan membantu konfigurasi atau kebijakan organisasi. Snort adalah NIDS yang bekerja dengan menggunakan signature detection, berfungsi juga sebagai sniffer dan packet logger[5]Banyak dari fitur-fitur *snort* yang mirip dengan kombinasi *TCP dump/review*, tetapi snort memiliki banyak kelebihan lainya. Sebagaimana *tools ethereal* yang terkenal, snort tersedia bebas dalam bentuk *source code* di bawah lisensi *GNU Genaral Public License*, untuk kebanyankan varian dan distro *linux/unix*, dan juga sistem-sistem *windows* [9].

Snort merupakan suatu perangkat lunak untuk mendeteksi penyusup dan mampu dapat menganalisis lalu lintas real-time, hal ini dapat mendeteksi berbagai jenis serangan. Snort bukanlah sebatas protocol analisis atau sistem pendeteksi penyusupan (*Intrusion Detection System*) IDS, melainkan sedikit gabungan diantara keduanya, dan bisa sangat berguna dalam merespons insiden-insiden peyerangan terhadap hosthost jaringan. Fitur Snort dapat menjadi penolong administrator sistem dan jaringan, dimana mampu memperingatkan kita atas penyusup yang berpeluang berbahaya [9].

II. METODOLOGI PENELITIAN

A. *Analisis Masalah*

Permasalahan pada sistem jaringan di warnet Cyber adalah belum diterapkan sistem keamanan server warnet, oleh karena itu beberapa kali server warnet cyber mengalami kelumpuhan karena ada penyerangan yang dilakukan oleh pihak lain.

B. *Alternatif solusi*

Dengan menerapkan sistem keamanan *intrusion detection system (IDS) Snort* yang bisa mendeteksi serangan yang terjadi pada sistem jaringan kemudian memberikan peringatan adanya serangan tersebut.

C. *Rancangan Aplikasi*

Perancangan sistem yang diterapkan untuk mendeteksi adanya serangan yaitu *Instrusion Detection System(IDS).* Untuk membangun sistem tersebut dibutuhkan beberapa komponen atau *tools* antara lain:

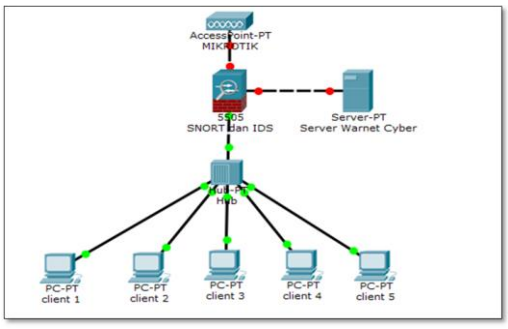
- Snort
- Namp
- Puty
- VirtualBox

1) *Manajemen Jaringan Usulan*

IDS merupakan suatu sistem yang memiliki kemampuan untuk menganalisis data secara realtime dalam mendeteksi, mencatat *(log)* dan menghentikan penyalahgunaan dan penyerangan. *IDS* merupakan *security tools* yang dapat digunakan untuk menghadapi aktivitas hacker. *IDS* ini mampu memberikan peringatan kepada administrator apabila terjadi suatu serangan atau penyalahgunaan di dalam jaringan, bahkan peringatan itu dapat pula menunjukkan alamat *IP* dari sebuah sistem penyerang[10].

2) *Topologi Jaringan Usulan*

Pada gambar 1 Topologi ini bakal diterapkan di warnet *cyber* Toboali sebagai pengamanan warnet untuk mengetahui adanya penyusupan terhadap warnet, sebab itu warnet *cyber* mengambil metode *snort* dan *IDS* sebagai alat pendeteksi serangan atau monitoring .



Gambar 1. Topologi Jaringan Usulan

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v9.i1.770, Copyright ©2020
Submitted : 15 Januari 2020, Revised : 4 Maret 2020, Accepted : 16 Maret 2020, Published : 24 Maret 2020

3) Konfigurasi Snort

Untuk mengkonfigurasi Snort yaitu dengan membuka file snort.conf yang terdapat pada folder C:\snort/etc kemudian edit dengan menggunakan text editor, akan tetapi lebih disarankan menggunakan Notepad++.

```
sudo snort --version
```

```
-*> Snort! <*-
Version 2.9.13 GRE (Build 15013)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.8.1
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.8
```

Gambar 2. Konfigurasi Snort

4) Konfigurasi Rules

Selanjutnya sebelum menjalan snort tersebut, maka membutuhkan beberapa langkah lagi yaitu dengan mengkonfigurasi rules snort agar snort dapat bekerja dengan baik.

```
sudo etc/snort/rules/local.rules
```

```
GNU nano 2.7.4                File: /etc/snort/rules/local.rules

# $Id: local.rules,v 1.11 2019/06/28 20:15:44 bmc Exp $
#------------------
# LOCAL RULES
#------------------
# This file intentionally does not come with signatures. Put your local
# additions here.
#------------------
alert icmp any any -> $HOME_NET any (msg:"ADA PING DARI LUAR SERVER WARNET CYBER";sid:10000001;rev:$
alert tcp any any -> 192.168.43.179 22 (msg:"ADA YANG SEDANG MENGAKSES SSH DI WARNET CYBER";sid:100$
alert tcp any any -> 192.168.43.179 23 (msg:"ADA YANG TELNET KE SERVER CYBER!"; sid:1000001;)
```

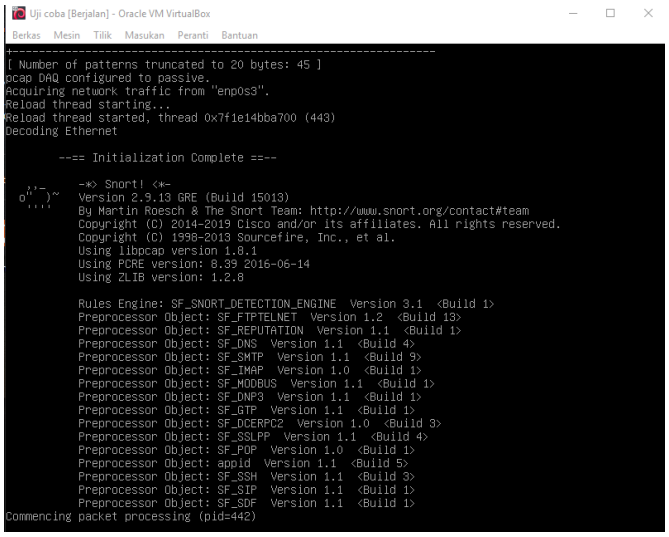
Gambar 3. Tampilan Rules

Untuk konfigurasi rules harus mencari serangan apa saja yang diperlukan contohnya ada ping dari luar beturut-turut, ada yang sedang mengakses SSH dan Tlanet ke server.

5) Menjalankan Snort

Menjalankan Snort yaitu dengan menggunakan command prompt dalam modus Administrator. Caranya adalah dengan memilih icon Command Prompt, meng-klik kanan dan memilih menu "Run As Administrator". Sebelum itu perhatikan *options* yang diberikan oleh snort

```
Snort –A console –i enp03 –c /etc/snort/snort.conf
```



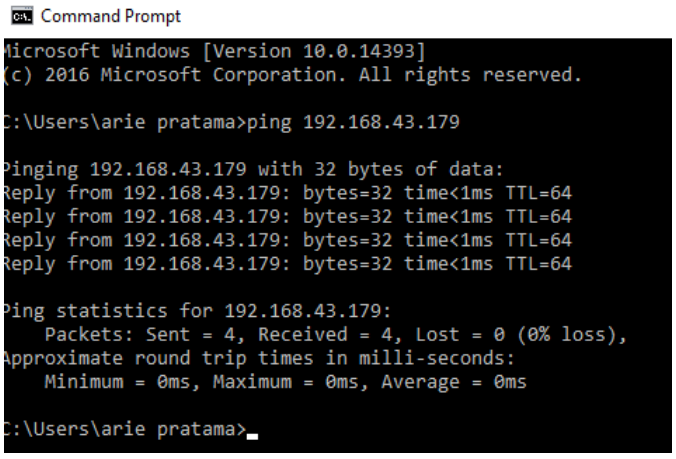
Gambar 4. Tampilan Snort Berjalan

Gambar 4 diatas menunjukkan snort sedang berjalan jadi server bisa mendeteksi adanya penyusupan terhadap server warnet cyber.

III. HASIL DAN PEMBAHASAN

A. Pengujian Jaringan Akhir

Pada pengujian akhir komputer akan terpasang sistem snort. Sistem snort akan dicoba dengan percobaan serangan dan akan menampilkan alert sesuai ancamannya.



Gambar 5. Tampilan untuk serangan ping windows

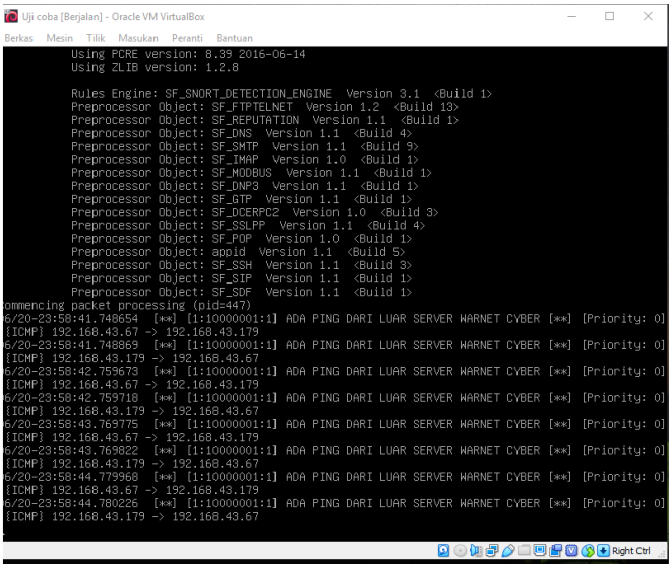
Dari gambar 5 di ketahui bahwa ip pada server adalah 192.168.43.179,setelah mendapatkan ip server nya penulis mencoba melihat ip pada windwos dengan menggunakan cmd apakah sudah tersambung atau belum.Sekarang tahap pengujian dengan melakukan serangan ping beturut-turut ke komputer target.

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v9i1.770, Copyright ©2020
Submitted : 15 Januari 2020, Revised : 4 Maret 2020, Accepted : 16 Maret 2020, Published : 24 Maret 2020

1) Tahapan Pengujian

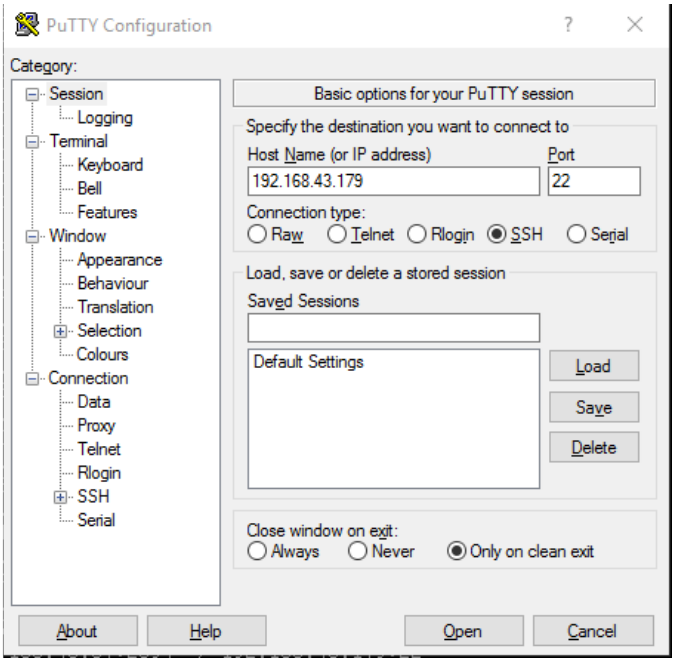
a) Ping of Death

Komputer yang terpasang Snort akan dicoba dengan metode penyerangan ping of death dari komputer penyerang. Hasil yang terjadi pada saat komputer diserang adalah seperti pada gambar 6 berikut :



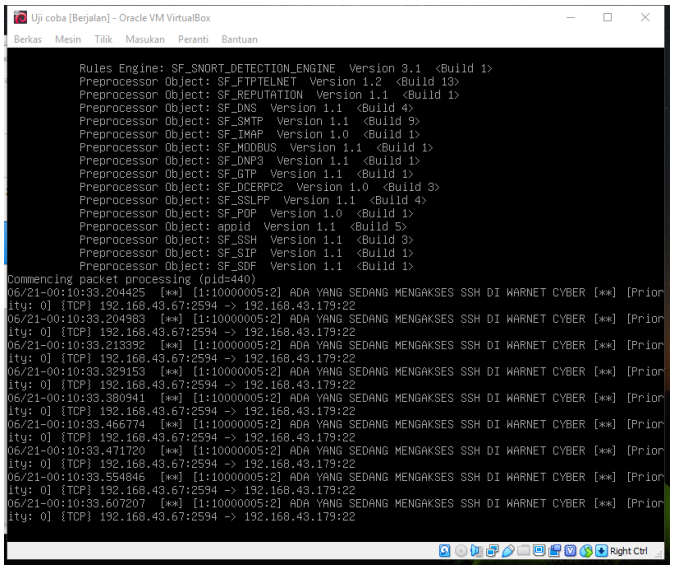
Gambar 6. Tampilan Serangan Ping

Pada gambar 6 menunjukkan IP 192.168.43.67 (komputer Penyerang) melakukan ping of death terhadap IP 192.168.43.179 (komputer yang terpasang snort) dengan peringatan “WARNING!!! ICMP Large ICMP Packet”.



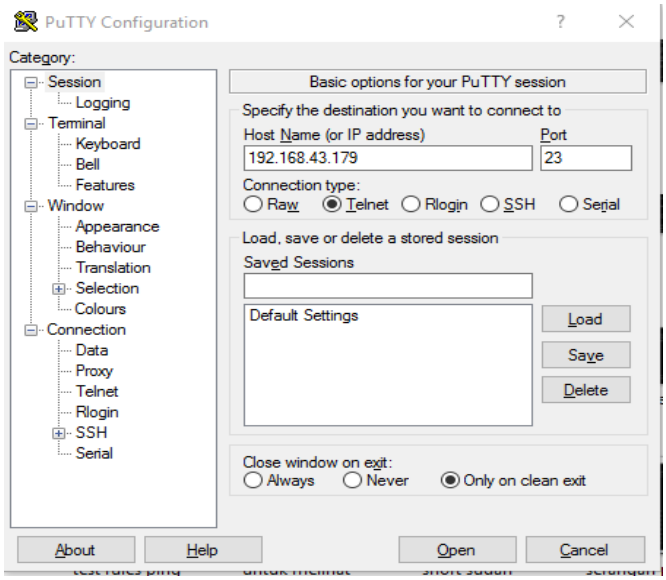
Gambar 7. Tampilan Aplikasi PUTY SSH

Dengan menggunakan aplikasi bantuan puty kita bisa memakai SSH untuk metode public-key adalah kunci yang dipublikasi ke orang lain. Sementara private key berarti kunci yang dirahasikan, jadi hanya pengguna saja yang mengetahuinnya. Lakukan serangan SSH ke komputer tujuan menggunakan Aplikasi PUTY dengan memasukkan alamat IP komputer tujuan seperti terlihat pada gambar 7.



Gambar 8. Tampilan Serangan SSH

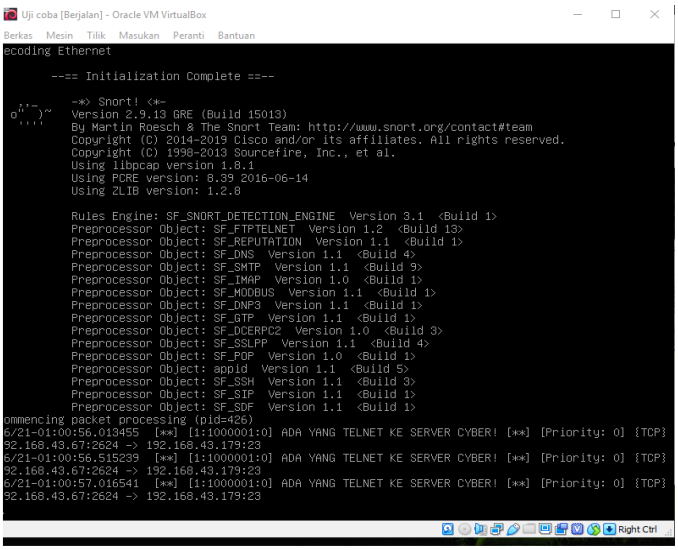
Gambar 8 menunjukkan hasil dari serangan SSH yang dilakukan terhadap komputer tujuan.



Gambar 9. Tampilan Aplikasi PUTY Telnet

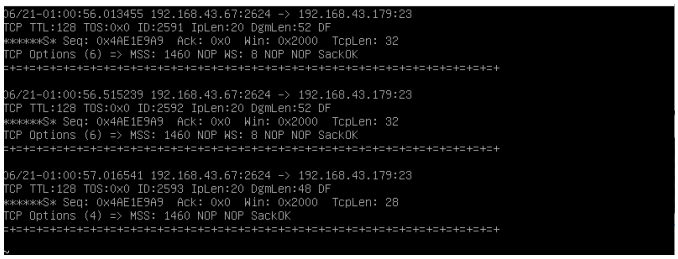
Serangan telnet yaitu untuk mengakses sebuah komputer secara jarak jauh seolah-olah sedang mengakses dari jarak dekat istilah remote access. Lakukan serangan telnet menggunakan aplikasi PUTY dengan memasukkan alamat IP komputer tujuan seperti terlihat pada gambar 9.

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v9i1.770, Copyright ©2020
Submitted : 15 Januari 2020, Revised : 4 Maret 2020, Accepted : 16 Maret 2020, Published : 24 Maret 2020



Gambar 10. Tampilan Percobaan Telnet

Gambar 10 menunjukkah hasil percobaan serangan telnet pada komputer tujuan.



Gambar 11. Tampilan log

Kita bisa mengecek ip serangan dan *ip server* menggunakan *log* itu bisa diketahui melalui tanggal serangan dan jam serangan. Tampilan Log seperti terlihat pada Gambar 11.

B. Analisis

Analisis hasil yang didapat pada pengujian snort bahwa alert yang dihasilkan oleh *snort log* dapat membaca paket-paket yang lewat sesuai kondisi yang terjadi pada jaringan. Komputer yang tidak terpasang snort tidak bisa mengetahui apa yang sedang terjadi pada komputernya seperti serangan dan penyalahgunaan jaringan seperti mengakses sosial media.

Berdasarkan percobaan serangan dengan komputer yang terpasang snort dapat mengetahui apa yang sedang terjadi seperti yang dihasilkan pada alert. Log yang dihasilkan dapat membaca suatu serangan dan penyalahgunaan jaringan sesuai dengan metode pengujiannya dengan menyeting bagian rule dari snort. Snort tidak bisa menindaklanjuti alert yang terdeteksi sebagai serangan karena sifatnya hanya mendeteksi.

IV. PENUTUP

Dengan menggunakan Metode *Intrusion Detection System* (IDS) berbasis Snort administrator jaringan bisa mengetahui aliran paket-paket yang keluar masuk sistem, IDS akan merekam semua aktifitas tersebut dan memberikan laporan paket-paket yang mencurigakan sehingga administrator jaringan dapat mengetahui jika ada serangan yang masuk kedalam jaringan.

DAFTAR PUSTAKA

[1] M. Ulfa, "Implementasi Intrusion Detection System (IDS) Di Jaringan Universitas Bina Darma," *J. Ilm. MATRIK*, vol. 15, no. 12, pp. 105–118, 2013.
[2] IBISA, *Keamanan Sistem Informasi*. Yogyakarta: Andi Offset, 2011.
[3] D. Stiawan, "Intrusion Prevention System (IPS) dan Tantangan dalam Pengembangannya," *Deris. unsri. ac. id.[Diakses 2 Novemb. 2011]*, 2009.
[4] T. Wiharjito, *Keamanan Jaringan Internet*. Jakarta: PT. Gramedia, 2006.
[5] D. Ariyus, "Intrusion detection system," *Yogyakarta Andi*, 2007.
[6] S. Axelsson, "Intrusion Detection Systems:," no. October 2002, 2015.
[7] R. and P. M. Bace, "Intrusion Detection System," 2005.
[8] J. S. Balasubramaniyan, J. O. Garcia-fernandez, D. Isacoff, E. Spafford, D. Z. Ý, and W. Lafayette, "An Architecture for Intrusion Detection using Autonomous Agents £."
[9] R. Rafiudin, *Mengganyang Hacker dengan Snort*. Yogyakarta: Andi Offset, 2010.
[10] Sutarti, P. Pancaro, Adi, and I. Saputra, Fembi, "Implementasi IDS (Intrusion Detection System) Pada Sistem Keamanan Jaringan SMAN 1 Cikeusal," *J. PROSISKO*, vol. 5, no. 1, 2018.

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v9i1.770, Copyright ©2020
Submitted : 15 Januari 2020, Revised : 4 Maret 2020, Accepted : 16 Maret 2020, Published : 24 Maret 2020