ISSN 2338-1523
E-ISSN 2541-576X

Volume 6 No. 1
Mei 2018

ANALISIS *NETWORK SECURITY SNORT* MENGGUNAKAN METODE *INTRUSION DETECTION SYSTEM (IDS)* UNTUK OPTIMASI KEAMANAN JARINGAN KOMPUTER

Parningotan Panggabean, S.Kom., M.Kom[1)]
[1]email: ingot.id@gmail.com
Program Studi Sistem Informasi, STMIK GICI

ABSTRAK

Perkembangan teknologi informasi, khususnya jaringan komputer memungkinkan terjadinya pertukaran informasi yang mudah, cepat dan semakin kompleks. Keamanan jaringan komputer harus diperhatikan guna menjaga validitas dan integritas data serta informasi yang berada dalam jaringan tersebut. Masalah yang dihadapi adalah adanya Log Bug yang didapatkan pada komputer server Dinas Lingkungan Hidup Kota Batam yang diindikasikan adanya serangan Denial of Service (DoS) pada komputer tersebut. Berdasarkan masalah diatas maka penulis mencoba membuat sebuah penelitian yang berjudul "Analisis Network Security Snort menggunakan metode Intrusion Detection System (IDS) untuk Optimasi Keamanan Jaringan Komputer" dan diharapkan dapat mendeteksi serangan Denial of Service (DoS). Intrusion Detection System (IDS) adalah sebuah tool, metode, sumber daya yang memberikan bantuan untuk melakukan identifikasi, memberikan laporan terhadap aktivitas jaringan komputer. Aplikasi yang digunakan untuk mendeteksi serangan menggunakan Snort. Snort dapat mendeteksi serangan DoS. Serangan DoS dilakukan dengan menggunakan aplikasi Loic.

Kata kunci : *Network Security, Intrusion Detection System (IDS), Snort.*

ISSN 2338-1523
E-ISSN 2541-576X

Volume 6 No. 1
Mei 2018

ABSTRACT

The development of information technology, especially computer network allows the exchange of information easier, faster and more complex. Network security must be considered in order to maintain the validity and integrity of the data and information that are within the network. The problem faced is the Log Bug obtained on computer servers Dinas Lingkungan Hidup Kota Batam which indicated the existence of Denial of Service (DoS) on that computer. Based on the above problems, the writer tries to make a study entitled "Analysis of Network Security using Snort Intrusion Detection System (IDS) for Computer Network Security Optimization" and is expected to detect Denial of Service (DoS). Intrusion Detection System (IDS) is a tool, method, resources that provide assistance to identify, report on the activities of the computer network. Applications used to detect attacks using Snort. Snort can detect DoS attacks. DoS attacks carried out by using LOIC application.

Keyword *: Network Security, Intrusion Detection System (IDS), Snort.*

ISSN 2338-1523
E-ISSN 2541-576X

Volume 6 No. 1
Mei 2018

PENDAHULUAN

Perkembangan teknologi informasi, khususnya jaringan komputer memungkinkan terjadinya pertukaran informasi yang cepat dan semakin kompleks. Pengaturan jaringan komputer yang baik tentu akan memaksimalkan pemanfaatan informasi tersebut. Oleh karena itu jaringan komputer harus diatur dan diawasi sehingga kelancaran pengiriman informasi dapat berjalan dengan baik. Semakin besar dan luas sistem jaringan komputer, semakin sulit untuk mengatur dan mengawasinya.

Jaringan komputer dapat melemah atau kurang optimal ketika jaringan komputer tersebut di serang oleh penyusup atau hacker dan *cracker* untuk kepentingan atau keuntungan pihak lain. Penyusup adalah *hacker* atau *cracker* yang selalu mencoba untuk mendapatkan akses dari sebuah sistem keamanan, *instrusi* sistem yang terjadi ketika orang yang tidak berhak mencoba untuk mendapatkan akses atau mengganggu operasi normal dari sistem informasi, (Dr. Khamitkar, 2012).

Penelitian ini dilakukan pada Dinas Lingkungan Hidup Pemerintah Kota Batam. Untuk mendukung kinerja Dinas Lingkungan Hidup kota Batam, saat ini instansi tersebut miliki jaringan komputer yang terkoneksi dengan jaringan publik atau disebut dengan *Internet* yang memiliki kecepatan akses data yang tinggi dari salah satu penyedia jasa internet di indonesia. Dengan terkoneksinya setiap komputer tersebut tentu telah banyak mempermudah pekerjaan yang bersifat komputerisasi pada Dinas Lingkungan Hidup kota Batam dan telah membawa dampak positif yang menangani persampahan di wilayah kota Batam. Seperti halnya pengiriman *email*, akses data *client-server*, penyimpanan data di server, memantau pergerakan setiap armada pengangkut sampah melalui *Global Positioning System (GPS) Tracking* dan manfaat lainnya yang dapat dirasakan oleh Pemerintah Kota Batam. Selain memberikan dampak yang positif, dampak negatif timbul terlihat dari ancaman permasalahan keamanan jaringan juga menjadi suatu permasahan yang sangat kompleks.

Ancaman-acaman keamanan jaringan seperti *attacker*, *intruder*, dan *cracker* semakin hari semakin meluas. Setiap informasi yang ada pada sistem jaringan komputer Dinas Lingkungan Hidup Kota Batam tentu harus dijaga kerahasiaan atau privacy data agar tidak digunakan oleh pihak yang tidak mempunyai hak untuk menggunakan informasi yang ada pada komputer *server* tersebut.

Permasalahan yang dihadapi penulis sehingga membuat penelitian ini adalah adanya *Log Bug* yang didapatkan pada komputer server yang diindikasikan adanya serangan *Denial of Service (DoS)* pada jaringan komputer Dinas Lingkungan Hidup kota Batam. Tujuan dari penelitian ini adalah penerapan sistem keamanan jaringan komputer menggunakan Snort untuk mendeteksi serangan *Denial of Service (Dos)* pada jaringan internal maupun external Dinas Lingkungan Hidup Pemerintah Kota Batam.

Agar masalah yang akan dibahas tidak meluas, dan tujuan dari penelitian ini tidak menyimpang dari pemahaman serta pembahasan yang terlalu luas, maka penulis membuat batasan masalah pada Serangan *Denial of Service (DoS)* yang akan dideteksi dengan mengunakan *Snort Intrusion Detection System (IDS).*

METODE PENELITIAN

Dalam penulisan skripsi ini, penulis melakukan beberapa tahapan dalam menyelesaikan penelitian. Adapun tahapan penelitian yang dilakukan adalah:

ISSN 2338-1523
E-ISSN 2541-576X

Volume 6 No. 1
Mei 2018

a. Peneliti memulai penelitian ini dengan mencari suatu permasalahan atau fenomena yang dianggap perlu untuk diteliti pada objek penelitian ini, yaitu di Dinas Lingkungan Hidup Kota Batam.
b. Setelah permasalahan tersebut didapatkan, maka peneliti membuat batasan masalah.
c. Teknik pengumpulan data yang digunakan dalam penelitian ini adalah observasi (*action research*) dengan instrumen yang digunakan adalah peneliti yang melakukan pengamatan pada objek penelitian.
d. Setelah data-data tersebut didapatkan, maka penulis merancang sistem keamanan yang baru.
e. Pengujian terhadap sistem keamanan yang baru dilakukan dengan dengan harapan dapat menjadi solusi dari permasalahan di atas.
f. Hasil penelitian didapatkan dari hasil pengujian sistem keamanan yang baru.
g. Dari hasil pengujian ditarik kesimpulan atas penelitian yang dilakukan dan saran terhadap sistem keamanan yang diteliti.

Menurut (Badrul, 2015) Dalam memudahkan pembuatan dan pengumpulan data yang diperlukan dalam sebuah penelitian maka perlu dirumuskan metode pengumpulan data, metode pengumpulan data pada penelitian ini adalah sebagai berikut:

1. Metode Studi Pustaka
   Melakukan pendalaman terhadap teori-teori yang berkaitan dengan studi kasus. Selain itu juga menggunakan beberapa jurnal yang digunakan sebagai acuan dalam melakukan penelitian ini.
2. Wawancara
   Penulis melakukan proses wawancara dalam membangun seragan jaringan komputer ke server dan tanya jawab terhadap pokok-pokok persoalan tentang server yang ada saat ini.
3. Metode Penelitian Tindakan/ Action Research
   Dalam rangka penyelesaikan penelitian ini maka digunakan metode penelitian tindakan dalam analisa, perancangan sistem, instalasi perangkat dan pengujian sistem.

Penelitian ini menggunakan metode *Intrusion Detection System (IDS)* dalam mendeteksi serangan jaringan komputer. (Najoan, 2015) *Intrusion Detection System* (*IDS*) dapat didefinisikan sebagai *tool*, metode, sumber daya yang memberikan bantuan untuk melakukan identifikasi, memberikan laporan terhadap aktivitas jaringan komputer.

Aplikasi yang digunakan untuk melakukan penyerangan ke komputer server dalam penelitian ini adalah aplikasi *Loic (Low Orbit Ion cannon). Loic (Low Orbit Ion)* merupakan sebuah tool atau aplikasi yang berfungsi untuk melumpuhkan server sebuah situs website dengan mengirimkan packet sebanyak mungkin sesuai dengan kemauan si penyerang ke komputer server yang dituju melalui domain atau ip server komputer target.

HASIL DAN PEMBAHASAN

Sistem yang akan diuji adalah sistem yang sudah dibangun pada komputer server yaitu sistem keamanan Snort. Pada penelitian ini yang akan uji adalah keamanan Snort. Terdapat tiga Skenario pengujian sistem keamanan Snort, yaitu sebagai berikut:

1. Menguji Keamanan Sistem *Snort* terhadap Serangan DoS metode *TCP Flooding.*
2. Menguji Keamanan Sistem Snort terhadap Serangan DoS metode *UDP Flooding.*

ISSN 2338-1523
E-ISSN 2541-576X

Volume 6 No. 1
Mei 2018

3. Menguji Keamanan Sistem Snort terhadap Serangan DoS metode *HTTP Flooding*.

Indikator keberhasilan dari pengujian tiga metode di atas adalah keberhasilan mendeteksi serangan *Denial of Service (DoS)* dari masing-masing metode.

Implementasi skenario pertama, kedua dan ketiga akan dilakukan dengan melakukan serangan ke komputer target menggunakan ip address penyerang, ip address target, metode DoS dan port yang akan diserang seperti pada tabel 5.1 di bawah ini.

Tabel 5.1 Skenario Penyerangan pada I

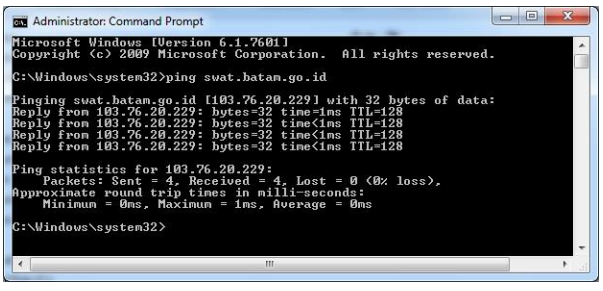
No	IP Address Penyerang	IP Address Target	Metode Serangan	Port
I	103.76.20.2	103.76.20.229	TCP Ping Flooding	80
I	103.76.20.2	103.76.20.229	UDP Ping Flooding	80
I	103.76.20.2	103.76.20.229	HTTP Ping Flooding	80

Tahap Implementasi Skenario Pengujian

1. Serangan DoS dengan metode *TCP Flooding*

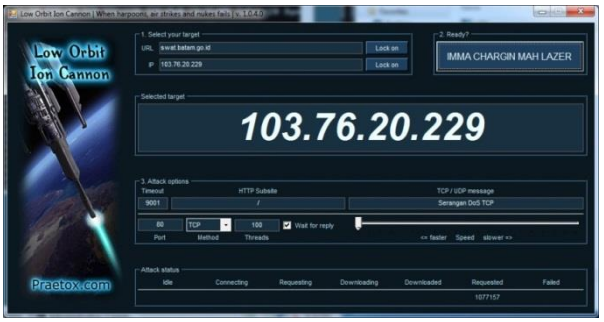
Tahap-tahap dari serangan-serangan DoS metode *TCP Flooding* adalah sebagai berikut:

a. Lakukan perintah ping melalui CMD pada domain "swat.batam.go.id untuk mengecek komunikasi data komputer penyerang ke komputer server seperti pada gambar 5.1 di bawah ini.



Gambar 5.1 Ping ke komputer target untuk serangan TCP

b. Penyerangan dari komputer penyerang dengan menggunakan aplikasi *LOIC* dengan metode *Transmission Control Protocol (TCP) Flooding* seperti pada gambar 5.2 di bawah ini.

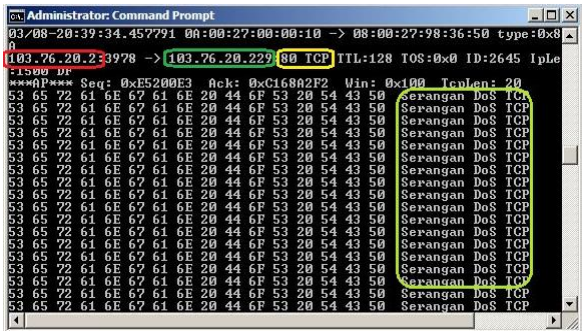


Gambar 5.2 Serangan metode TCP pada LOIC

Domain target/url : swat.batam.go.id
Ip address : 103.76.20.229
Timeout : 9001

TCP/UDP Message : Serangan DoS TCP
Port : 80
Method : TCP
Treads : 100

c. Hasil monitoring *snort* pada komputer server pada saat penyerangan dilakukan seperti pada gambar 5.3 di bawah ini.



Gambar 5.3 Deteksi serangan DoS TCP pada Snort

Pada gambar 5.3 di atas terlihat ip address komputer penyerang yaitu 103.76.20.2 dan ip address komputer yang

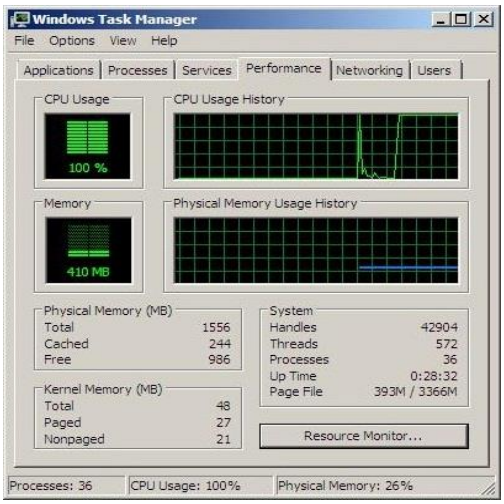
ISSN 2338-1523
E-ISSN 2541-576X

Volume 6 No. 1
Mei 2018

diserang yaitu 103.76.20.229 dengan serangan DoS menggunakan metode TCP melalui port 80.

d. Monitoring penggunaan CPU pada komputer server

Salah satu dampak daripada serangan DoS adalah membuat komputer menjadi over load. Teori ini dapat dibuktikan pada gambar 5.4 di bawah ini. Terlihat pada penggunaan CPU pada saat serangan dilakukan hingga 100 %.

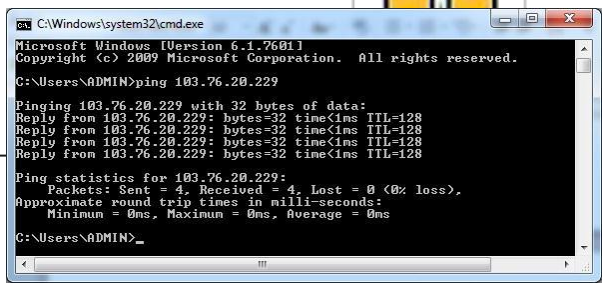


Gambar 5.4 Monitoring CPU serangan DoS TCP

2. Serangan DoS dengan metode *UDP Flooding*

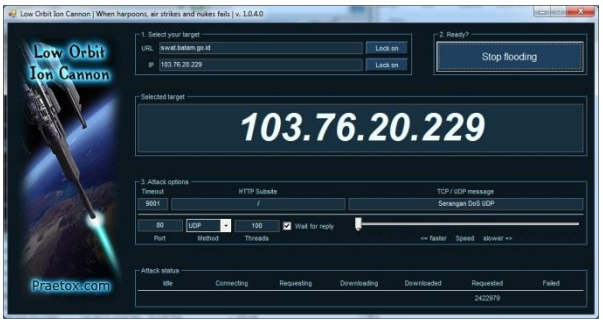
Tahap-tahap dari serangan-serangan DoS metode *UDP Flooding* adalah sebagai berikut:

a. Lakukan kembali perintah ping ke komputer target untuk mengecek komunikasi data antara komputer penyerang dengan komputer target seperti pada gambar di 5.5 di bawah ini.



Gambar 5.5 Ping ke komputer target untuk serangan UDP

b. Lakukan penyerangan dari komputer penyerang menggunakan aplikasi *LOIC* dengan metode *User Datagram Protocol (UDP) Flooding* seperti pada gambar 5.6 di bawah ini.



Gambar 5.6 Serangan dengan metode UDP pada LOIC

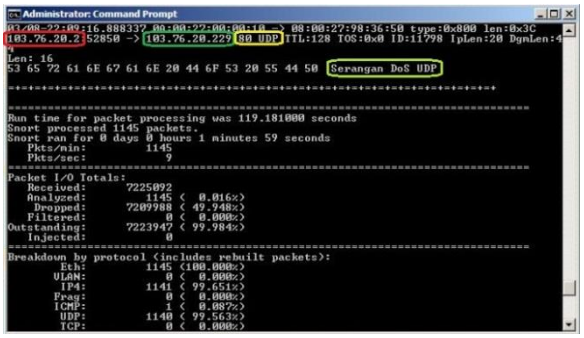
Domain target/url : swat.batam.go.id
Ip address : 103.76.20.229
Timeout : 9001
TCP/UDP Message : Serangan DoS UDP
Port : 80
Method : UDP
Treads : 100

c.

d. Hasil monitoring pada komputer server pada saat penyerangan dilakukan dapat dilihat pada gambar 5.7 di bawah ini.

ISSN 2338-1523
E-ISSN 2541-576X

Volume 6 No. 1
Mei 2018

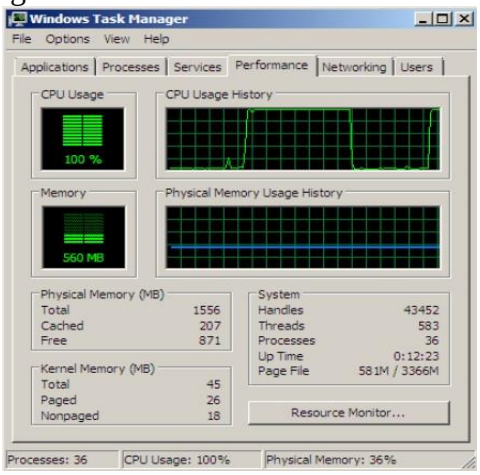


Gambar 5.7 Deteksi serangan DoS UDP pada Snort

Pada gambar 5.7 di atas terlihat ip address komputer penyerang yaitu 103.76.20.2 dan ip address komputer yang diserang yaitu 103.76.20.229 dengan serangan DoS menggunakan metode UDP melalui port 80.

e. Monitoring penggunaan CPU pada komputer server

Dampak dari serangan DoS metode UDP meningkatnya penggunaan resource sumber daya komputer server seperti CPU hingga 100% atau over load yang ditunjukkan pada gambar 5.8 di bawah ini.



Gambar 5.8 Monitoring CPU serangan DoS UDP

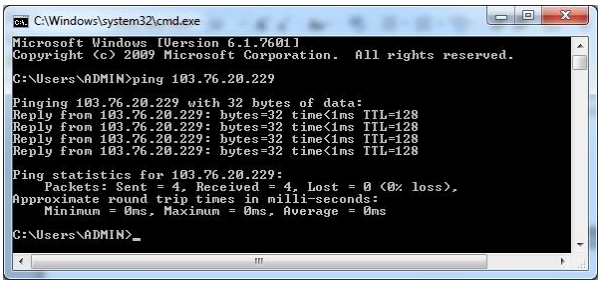
3. Serangan DoS dengan metode *HTTP Flooding*

Tahap-tahap dari serangan-serangan DoS metode *HTTP Flooding* adalah sebagai berikut:

ISSN 2338-1523
E-ISSN 2541-576X

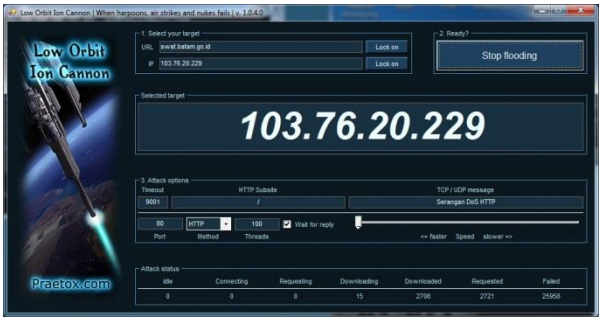
Volume 6 No. 1
Mei 2018

a. Lakukan kembali perintah ping untuk domain target seperti pada gambar di 5.9 di bawah ini.



Gambar 5.9 Ping ke komputer target untuk serangan HTTP

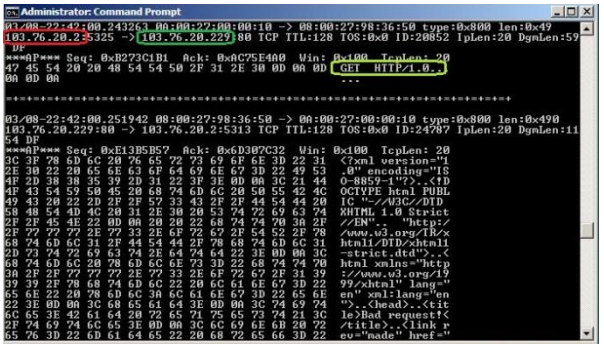
b. Lakukan penyerangan menggunakan aplikasi LOIC dengan metode *HTTP Flooding* seperti pada gambar 5.10 di bawah ini.



Gambar 5.10 Serangan metode HTTP menggunakan LOIC

Domain target/url : swat.batam.go.id
Ip address : 103.76.20.229
Timeout : 9001
TCP/UDP Message : Serangan DoS HTTP
Port : 80
Method : HTTP
Treads : 100

c. Hasil monitoring serangan seperti pada gambar 5.11 di bawah ini.

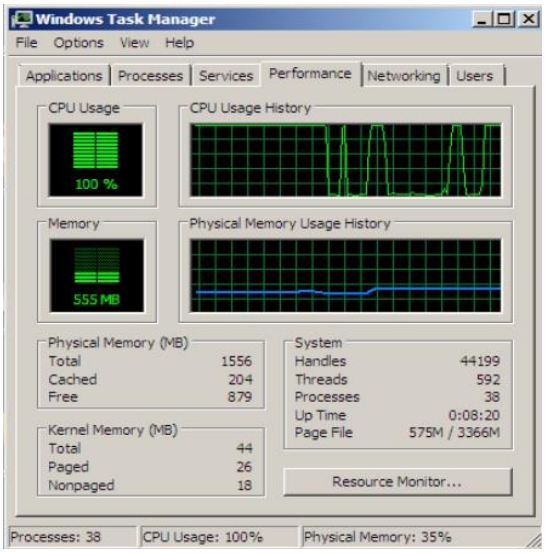


Gambar 5.11 Deteksi serangan DoS metode HTTP pada Snort

Pada gambar 5.11 di atas terlihat ip address komputer penyerang yaitu 103.76.20.2 dan ip address komputer yang diserang yaitu 103.76.20.229 dengan serangan DoS menggunakan metode HTTP melalui port 80

d. Monitoring penggunaan CPU pada komputer server

Dampak dari serangan DoS metode HTTP meningkatnya penggunaan resource sumber daya komputer server seperti CPU hingga 100% bahkan over load yang ditunjukkan pada gambar 5.12 di bawah ini.



ISSN 2338-1523
E-ISSN 2541-576X

Volume 6 No. 1
Mei 2018

Gambar 5.12 Monitoring CPU serangan DoS HTTP

Hasil Implementasi Skenario Sistem

Hasil pengujian ketiga skenario di atas dirangkum pada tabel di bawah ini.

Tabel 5.4 Hasil Implementasi Skenario pada Sistem I

No	IP Address Penyerang	IP Address Target	Metode Serangan	Port	Hasil
I	103.76.20.2	103.76.20.229	TCP Flooding	80	Terdeteksi
I	103.76.20.2	103.76.20.229	UDP Flooding	80	Terdeteksi
I	103.76.20.2	103.76.20.229	HTTP Flooding	80	Terdeteksi

T

aTabel 5.4 di atas menunjukkan implementasi skenario penyerangan terhadap ip address target menggunakan salah satu metode serangan melalui salah satu port lalu lintas jaringan dan terdeteksi

dengan adanya flooding paket data dari ip address penyerang seperti salah satu contoh pada gambar 5.3 di atas serta dampak penggunaan CPU komputer target yang berlebihan atau mencapai 100% seperti pada gambar 5.4 di atas.

KESIMPULAN

Berdasarkan hasil pengujian pada bab v dalam penelitian ini dapat ditarik kesimpulan sebagai berikut:

a. Snort dapat mendeteksi serangan Denial of Service (DoS) menggunakan metode *TCP Ping Flooding* dengan menangkap ip address penyerang yang menghasilkan respon dan dampak pada CPU komputer yang berlebihan.
b. Snort dapat mendeteksi serangan *Denial of Service (DoS)* menggunakan metode *UDP Ping Flooding* dengan menangkap ip address penyerang yang menghasilkan respon dan dampak pada CPU komputer yang berlebihan.
c. Snort dapat mendeteksi serangan *Denial of Service (DoS)* menggunakan metode *HTTP Ping Flooding* dengan menangkap ip address penyerang yang menghasilkan respon dan dampak pada CPU komputer yang berlebihan.
d. Metode *Intrusion Detection System* dapat mengoptimalkan tingkat keamanan jaringan komputer melalui pendeteksian serangan sehingga administrator jaringan dapat melakukan tindakan pencegahan.

UCAPAN TERIMAKASIH

Terimakasih yang tulus dan ikhlas juga kepada semua pihak yang telah banyak membantu dalam menyelesaikan tesis ini, antara lain :

1. Bapak H. Herman Nawas selaku Ketua Yayasan Perguruan Tinggi Komputer (YPTK) Padang yang telah memberikan dukungan kepada penulis dalam menyelesaikan pendidikan ini.
2. Bapak Prof. Dr. H. Sarjon Defit, S.Kom., M.Sc. selaku Rektor Universitas Putra Indonesia YPTK Padang yang telah mendidik dan banyak membantu penulis di dalam penyelesaian tesis ini.
3. Bapak Dr. Julius Santony, S.Kom.,M.Kom. selaku Dekan Fakultas Ilmu Komputer Universitas Putra Indonesia “YPTK” Padang.
4. Bapak Dr. Ir. Rusdianto Roestam, M.Sc sebagai Pembimbing I yang telah mendidik dan banyak membantu penulis di dalam penyelesaian tesis ini.
5. Bapak Dr. Ir. Sumijan, M.Sc selaku pembimbing II yang telah mendidik dan banyak membantu penulis di dalam penyelesaian tesis ini.
6. Bapak Dr. Ir. Gunadi Widi Nurcahyo,M.Sc. selaku Ketua Program Studi Pasca Sarjana Magister Ilmu Komputer Universitas Putra Indonesia “YPTK” Padang.
7. Seluruh Dosen Program Pascasarjana Universitas Putra Indonesia ”YPTK” Padang yang mendistribusikan pengetahuannya kepada penulis selama mengikuti perkuliahan.

8. Bapak dan Ibu Staf Administrasi Program Pascasarjana Universitas Putra Indonesia "YPTK" Padang yang telah banyak membantu penulis dalam penanganan administrasi akademis selama penulis aktif sebagai mahasiswa.
9. Bapak Ir. A Dendi Noviardi Purnomo. Selaku Kepala Dinas Lingkungan Hidup Pemerintah Kota Batam.
10. Bapak M. Fairus Ramadhan Batubara, SSTP, M.Si. Selaku Kepala Bidang Dinas Persampahan/Kebersihan Pemerintah Kota Batam.

DAFTAR PUSTAKA

1. Agnesie Pratiwi Masero, Joko Triyono, Dina Andayati (2013). "Perancangan Pengelolaan Jaringan It Pada Institut Sains & Teknologi Akprind Menggunakan Teknologi Vpn (Virtual Private Network)" *Jurnal JARKOM*. 1. 20-30, ISSN:2338-6312.
2. Andi Nurul Hidayat (2016). "Analisis Keamanan Berselancar Internet Pada Website Menggunakan Internet Security Firewall". *Jurnal Elektronik Sistem Informasi Dan Komputer*. 2. 1-4, e. ISSN: 2502-2148.
3. Dista Amalia Arifah (2011). "Kasus Cybercrime Di Indonesia". *Jurnal Bisnis dan Ekonomi (JBE)*. 18. 185-195, ISSN: 1412-3126.
4. Doddy Ferdiansyah (2013). "Pemanfaatan Teknologi Honeypot Dalam Meningkatkan Availability Pada Sistem Jaringan". *Jurnal INFOMATEK - Informatika, Manajemen dan Teknologi*. 15. 11-18, ISSN:1411-0865.
5. Dyakso Anindito Nugroho, Adian Fatchur Rochim, Eko Didik Widianto (2015). "Perancangan Dan Implementasi Intrusion Detection System Di Jaringan Universitas Diponegoro". *Jurnal Teknologi dan Sistem Komputer* . 3. 171-178, e-ISSN: 2338-0403.
6. Eka Varianto, Mohammad Badrul (2015). "Implementasi Virtual Private Network Dan Proxy Server Menggunakan Clear Os Pada Pt.Valdo International". *Jurnal Teknik Komputer Amik BSI*. 1. ISSN. 2442-2436.
7. Fitriyanti A.Masse, Andi Nurul Hidayat, Badrianto (2015). "Penerapan Network Intrusion Detection System Menggunakan Snort Berbasis Database Mysql Pada Hotspot Kota". *Jurnal Elektronik Sistem Informasi Dan Komputer*. 1. 1-16, e. ISSN: 2502-2148.
8. Harjono, Agung Purwo Wicaksono (2014). "Sistem Deteksi Intrusi dengan Snort (Intrusion Detection System with Snort)". 3. 31-34, ISSN: 2086-9398.
9. Hasibuan, Z.A. (2007). Metodologi Penelitian Pada Bidang Ilmu Komputer dan Teknologi Informasi. *Fasilkom Universitas Indonesia*. Depok
10. Ida Bagus Verry Hendrawan Manuaba, Risanuri Hidayat, Sri Suning Kusumawardani (2012). "Evaluasi Keamanan Akses Jaringan Komputer Nirkabel (Kasus: Kantor Pusat Fakultas Teknik Universitas Gadjah Mada)". *Jurnal Teknik Elektro dan Teknologi Informasi Fakultas Teknik Universitas Gadjah Mada*. 1. 13-17, ISSN 2301-415613.
11. Maria Ulfa, Megawaty (2015). "Perancangan dan Implementasi Sistem

ISSN 2338-1523
E-ISSN 2541-576X

Volume 6 No. 1
Mei 2018

Keamanan Berbasis IDS di Jaringan Internet Universitas Bina Darma". *Jurnal Nasional Pendidikan Teknik Informatika (JANAPATI)*.4.45-49, ISSN 2087-2658.

13. Mr. Nishidh D. Patel, Prof. Vrushank Shah, Prof. Kruti j. Pancholi (2013). "An analysis of Network Intrusion Detection System using SNORT". *IJSRD - International Journal for Scientific Research & Development*. 1. 410-412, ISSN (online): 2321-0613.
14. Muhammad Zunaidi, Beni Andika, Saniman (2014). "Membentuk Jaringan Peer To Peer Menggunakan Kabel Firewire Ieee-1394 Dengan Metode Bridge". *Jurnal Ilmiah Sain dan Komputer (SAINTIKOM)*. 13. 107-120, ISSN : 1978-6603.
15. Nagoor Meerasaheb Lanke, CH. Raja Jacob (2014). "Detection of DDOS Attacks Using Snort Detection". *International Journal of Emerging Engineering Research and Technology*. 2. 13-17, ISSN 2349-4409.
16. Novriyanto, ST., MSc, Haris Simare Mare, ST., MT, Wenni Syahfiri (2011)."Sistem Pendeteksian Penyusupan Jaringan Komputer dengan Active Response Menggunakan Metode Hybrid Intrusion Detection, Signatures dan Anomaly Detection". *Seminar Nasional Aplikasi Teknologu Informasi (SNATI)*. 140-145, ISSN: 1907-5022.
17. Pritika Mehra (2012). "A brief study and comparison of Snort and Bro Open Source Network Intrusion Detection Systems". *International Journal of Advanced Research in Computer and Communication Engineering*. 1.383-386, ISSN : 2278-1021.
18. Rana M Pir (2015). "Intrusion Detection Systems with Snort". *International Journal of Engineering Development and Research*. 3. 479-488, ISSN: 2321-9939.
19. Randy Mentang, Alicia A. E. Sinsuw, Xaverius B. N. Najoan (2015). "Perancangan Dan Analisis Keamanan Jaringan Nirkabel
20. Menggunakan Wireless Intrusion Detection System". *E-journal Teknik Elektro dan Komputer*. 7.35-44, ISSN: 2301-8402.
21. Sahid Aris Budiman, Catur Iswahyudi, Muhammad Sholeh (2014). "Implementasi Intrusion Detection System (Ids) Pada Server Debian Menggunakan Jejaring Sosial Sebagai Media Notifikasi". *Jurnal Jarkom*. 2. 36-45, ISSN:2338-6313.
22. Suman Rani, Vikram Singh 92015). "SNORT: Am Open Source Network Security Tool for Intrusion Detection in Campus Network Environment". *International Journal of Computer Technology and Electronics Engineering (IJCTEE)*. 2, ISSN 2249-6343.
23. Teguh Wahyudi, Rissal Efendi (2015). "Perancangan Keamanan Jaringan Komputer Menggunakan Snort Dengan Notifikasi Sms". *Jurnal Teknologi*

Informasi dan Komunikasi. 6. 1-8, ISSN:2087-0868.

24. Undang-Undang Republik Indonesia (2008). "Tentang Informasi dan Transaksi Elektronik". No. 11.