e-ISSN. 2685-4066
Jurnal BITE
Vol.1 No.1 (Juni) 2019, Hal 78-88

IMPLEMENTASI IPS BERBASIS PORTSENTRY DAN VULNERABILITY ASSESMENT BERBASIS OPENVAS UNTUK PENGAMANAN WEB SERVER

[1]Edy Satriawan, [2]Raisul Azhar, [3]I Putu Hariyadi
[1]Mahasiswa, [2,3]Dosen, Program Studi Teknik Informatika
STMIK Bumigora Mataram,Jl.Ismail Marzuki, Mataram
[1]edysatriawan91@gmail.com, [2]raisulazhar@stmikbumigora.ac.id,
[3]putu.hariyadi@stmikbumigora.ac.id

ABSTRAK

Jaringan komputer merupakan jaringan telekomunikasi yang menghubungkan satu komputer atau lebih agar dapat saling bertukar data dan informasi. Manfaat yang sedemikian besar tersebut tentunya akan berkurang dengan adanya gangguan yang muncul terhadap jaringan. Adapun salah satu masalah yang dapat menganggu keamanan sistem adalah masuknya user atau hacker yang bermaksud merusak sistem jaringan. Dalam penerapan pengamanan web server berbasis Intrusion Prevention System (IPS), penulis menggunakan aplikasi Portsentry dan IPTables. Portsentry dan IPTables berfungsi sebagai firewall terhadap serangan seperti DDoS, Ping Attack, dan Portscanning, serta penggunaan OpenVAS dalam penerepanan metode Vulnerability Assesment dalam melakukan scannin terhadap sistem, untuk dapat mengetahui kekelemahan-kelemahan terhadap sistem yang dibangun, sehingga dapat dilakukan upaya perbaikan terhadap sistem agar menjadi lebih baik. Metodologi Penelitian yang penulis adopsi yaitu Network Development Life Cycle (NDLC), NDLC merupakan pendekatan proses dalam komunikasi data yang menggambarkan siklus yang tiada awal dan tiada akhir dalam membangun sebuah jaringan komputer mencakup sejumlah tahapan yaitu Analysis, Design, Simulation Prototype, Implementation, Monitoring dan Management.
Kata Kunci : *IPS, Vulnerability Assesment, Portsentry, OpenVAS, Portscanning, Ping Attack, DDoS, Firewall*

ABSTRACT

Computer network is a telecommunications network that connects one or more computers in order to exchange data and information. Such a large benefit will certainly decrease with the presence of interference that arises on the network. One of the problems that can disrupt system security is the entry of users or hackers who intend to damage the network system. In applying the security of a web server based on Intrusion Prevention System (IPS), the author uses the Portsentry application and IPTables. Portsentry and IPTables function as a firewall against attacks such as DDoS, Ping Attack, and Portscanning, as well as the use of OpenVAS in the adoption of Vulnerability Assessment methods in scannin the system, to be able to find weaknesses in the system being built, so that improvements can be made to the system to be better. The Research Methodology that the author adopts is Network Development Life Cycle (NDLC), NDLC is a process approach in data communication that describes an endless and endless cycle in building a computer network covering a number of stages namely Analysis, Design, Simulation Prototype, Implementation, Monitoring and Management.
Keyword : *IPS, Vulnerability Assesment, Portsentry, OpenVAS, Portscanning, Ping Attack, DDoS, Firewall*

I. PENDAHULUAN

Jaringan komputer merupakan jaringan telekomunikasi yang menghubungkan satu komputer atau lebih agar dapat saling bertukar data dan informasi. Manfaat jaringan komputer antara lain adalah memungkinkan pemakaian sumber daya yang ada secara bersama-sama seperti perangkat keras, perangkat lunak dan sistem operasi, selain itu dapat juga digunakan sebagai media untuk melakukan komunikasi. Manfaat yang sedemikian besar tersebut tentunya akan berkurang dengan adanya gangguan yang muncul terhadap jaringan, ketika jaringan hanya melibatkan perangkat lokal saja atau dengan kata lain tidak terhubung dengan jaringan internet maka gangguan mungkin menjadi sesuatu yang kurang untuk diperhitungkan. Namun ketika jaringan lokal sudah terhubung dengan jaringan internet maka keamanan akan menjadi suatu yang harus dipertimbangkan. Adapun salah satu masalah yang dapat menganggu keamanan sistem adalah masuknya *user* atau *hacker* yang bermaksud merusak sistem jaringan.

Hadirnya *firewall* dapat memberikan solusi dalam pengamanan sistem jaringan

komputer seperti munculnya banyak metode dan *software* atau aplikasi untuk mendukung sistem keamanan *firewall*. Salah satu metode dari *firewall* adalah *Intrusion Prevention System (IPS)* dan *Vulnerability Assessment* (VA). *Intrusion Prevention System* (*IPS*) merupakan pendekatan yang sering digunakan untuk membangun system keamanan komputer, *IPS* mengkombinasikan teknik *firewall* dan metode *Intrusion Detection System* (*IDS*) dengan sangat baik. Teknologi ini dapat digunakan untuk mencegah serangan yang akan masuk ke jaringan lokal dengan memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor, disaat attack telah teridentifikasi, *IPS* akan menolak akses (*block*) dan mencatat (*log*) semua paket data yang teridentifikasi tersebut, [1]. Sedangkan *Vulnerability Assesment (VA)* adalah analisa keamanan yang menyeluruh serta mendalam terhadap berbagai dokumen terkait keamanan informasi, hasil *scanning* jaringan, konfigurasi pada sistem, cara pengelolaan, kesadaran keamanan orang – orang yang terlibat dan keamanan fisik, untuk mengetahui seluruh potensi kelemahan kritis yang ada, [2].

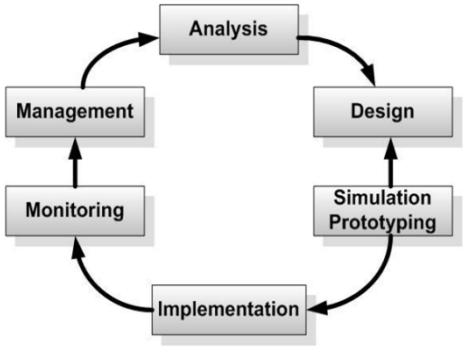
Dalam penerapan pengamanan *web server* berbasis *Intrusion Prevention System (IPS),* penulis menggunakan aplikasi *Portsentry*. *Portsentry* merupakan sebuah perangkat lunak yang di rancang untuk mendeteksi adanya serangan *Portscanning* dan melakukan respon secara aktif jika terjadinya serangan melalui *port*. Metode *Vulnerability Assessment* (VA) berbasis *OpenVAS* penulis gunakan sebagai metode untuk mendeteksi, mengidentifikasi, dan mempelajari kelemahan-kelemahan yang mungkin terdapat pada sistem keamanan *Intrusion Prevention System* (*IPS*) berbasiskan *Portsentry*.

Berdasarkan pada latar belakang yang telah dikemukan diatas dapat dirumusan masalah yaitu bagaimana menganalisa sistem keamanan *IPS (Intrusion Prevention System)* berbasiskan *Portsentry* untuk mendeteksi dan pencegahan serangan *Portscanning, Destribtion a Denial of Services (DdoS)* dan *Ping Attack* dengan menggunakan metode *Vulnerability Assesment?*.

II. METODOLOGI

1. Metode Penelitian

Metodologi Penelitian yang penulis adopsi pada penelitian ini yaitu *Network Development Life Cycle* (*NDLC*). *NDLC* merupakan model yang mendefinisikan siklus proses perancangaan atau pengembangan suatu sistem jaringan komputer. *NDLC* terdiri dari 6 tahapan yaitu *analisys, design, simulation prototype, implementation, monitoring* dan *management.*



Gambar 2.1 Tahapan *NDLC*

Dari 6 tahapan penulis hanya menggunakan 3 dari 6 tahapan tersebut. Hal ini dikarenakan hasil yang ingin dicapai hanya sampai tahap percobaan/penelitian dengan menggunakan *simulasi prototyping* sebelum diimplementasikan ke sebuah sistem yang sebenarnya.

A. Analysis

Tahap ini merupakan Tahap awal untuk melakukan analisa kebutuhan, analisa permasalahan yang muncul,analisa keinginan user, dan analisa topologi / jaringan yang sudah ada saat ini, [3].

B. Design

Pada tahap ini penulis melakukan perancangan topologi yang akan diterapkan untuk mensimulasikan penerapan metode *IPS* dan *vulnerability asessment* guna dalam pengamanan *web server*.

C. Simulation Prototyping

Setelah penulis menganalisis dan mendesain jaringan yang akan dibangun selanjutnya penulis membuat simulasi dan konfigurasi dengan media virtualisasi dengan memanfaatkan beberapa *tools* simulator. Pada tahapan ini, jika telah mengetahui hasil dari simulasi yang diterapkan ternyata didalam proses simulasi ada penambahan *tools* maupun *hardware,* maka secara otomatis berdasarkan gambar diatas proses tahapan ini akan kembali ke

tahap *Design*, dikarenakan pada tahap *Design* ini akan terjadi perubahan topologi jaringan maupun penambahan pengelamatan *IP*.

2. Tahap Pengumpulan dan Analisa Data

A. Pengumpulan Data

Pada tahap pengumpulan data dilakukan pengumpulan data tentang *IPS (Intrusion Prevention System)* dan *Vulnerability Assesment (VA)* dari berbagai sumber antara lain buku, internet, paper, *ebook*, dan jurnal ilmiah.

B. Analisa Data

Dari studi literature dan jurnal, buku, hasil penelitian tentang *IPS (Intrusion Prevension System)* dan *Vulnerabilty Assesment (VA)* dapat disimpulkan bahwa kedua metode ini mempunyai fungsi yang sama yaitu untuk mengamankan sistem jaringan dengan cara yang berbeda. Cara kerja dari metode *IPS* adalah menghalangi suatu serangan sebelum terjadi eksekusi dalam memori, serta membandingkan file *checksum* yang tidak semestinya mendapatkan izin untuk dieksekusi, sedangkan cara kerja dari metode *Vulnerability Assesment* adalah menganalisa keamanan yang menyeluruh terhadap berbagai dokumen terkait kemanan informasi, hasil *scanning* jaringan, konfigurasi pada sistem, untuk mengetahui seluruh potensi kelemahan sistem jaringan yang ada.

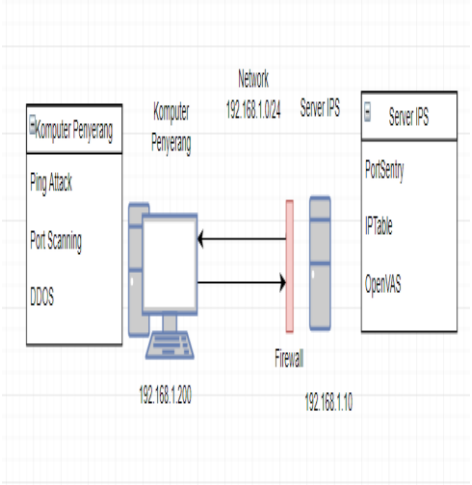
C. Identifikasi Kebutuhan Perangkat Keras Dan Lunak

Pada tahapan ini akan dilakukan analisa kebutuhan seperti kebutuhan *hardware* dan kebutuhan *software* yang akan digunakan dalam simulasi ujicoba yang akan dilakukan nantinya. Berikut kebutuhan *hardware* dan *software* yang akan digunakan pada simulasi ujicoba:

- **Analisa Kebutuhan *Hardware***
  1. Laptop ACER Aspire E1-431
  2. Memory 5 GB
  3. Prosesor Intel Pentium CPU B960
- **Analisa Kebutuhan *Software***
  1. Virtualisasi *VMWARE*
  2. Sistem operasi *UBUNTU* 14.04 LTS
  3. Software *OPENVAS*
  4. Menggunakan *Software PORTSENTRY*
  5. Tool *ZenMAP*, *PING*, dan
  6. Menggunakan *IPTABLES*.

3. Desain

A. Desain Topology Jaringan



Gambar 2.2 Topologi Jaringan Ujicoba

Pada gambar topologi jaringan diatas dapat diterangkan bahwa komputer penyerang memiliki beberapa metode untuk melakukan penyerangan melewati *firewall* yang ada di sisi *server IPS* diantaranya ping attack, port *scanning* dan *ddos*. Pada sisi *server IPS* memiliki *firewall* yang terdiri dari *iptables* dan *portsentry* yang bertugas untuk melakukan pengamanan serta berperan aktif dalam menangani serangan, dan *OpenVAS* untuk melakukan monitoring apabila ada terjadi serangan sehingga administrator jaringan dapat dengan mudah menemukan celah keamanan yang di serang dan melakukan penanggulangan secepat mungkin.

B. Desain Pengalamatan

Berikut adalah tabel pengalamatan yang dibuat berdasarkan dari topology yang akan digunakan pada saat melakukan Ujicoba.

Tabel 2.1 Pengalamatan *IP*

IP Address	Network	Device
192.168.1.10	192.168.1.0/24	*Server IPS*
192.168.1.200	192.168.1.0/24	Komputer Penyerang

4. **Simulation Prototyping**

Pada tahapan ini akan dilakukan simulasi berdasarkan topology yang telah di buat , yang kemudian dilakukan konfigurasi dan ujicoba. Berikut adalah langkah konfigurasi dan ujicoba pada *server IPS*;

A. Tahap Konfigurasi

Berikut adalah tahapan konfigurasi yang dilakukan pada server *IPS* dan Komputer penyerang;

1. Konfigurasi Pada *Server IPS*
   - Melakukan konfigurasi pada *server Ubuntu* sebagai *server IPS* dan selanjutnya Melakukan Update Packet Aplikasi pada Repository server Ubuntu sebelum melakukan instalasi.
   - Instalasi aplikasi *Port Sentry* sebagai alat untuk manahan serangan *portscanning*.
   - Melakukan konfigurasi aplikasi *Portsentry* terhadap kebutuhan untuk mengaktifkan fitur *Blocking* yang ada di aplikasi *portsentry*.
   - Penambahan *repository OpenVAS* pada *Server Ubuntu* yang berfungsi sebagai pendukung untuk melakukan instalasi.
   - Melakukan *update packet* aplikasi pada *repository server ubuntu* sebelum melakukan instalasi. *Update* ini diperlukan agar saat ingin melakukan instalasi aplikasi tidak terjadi *error* yang disebabkan packet yang belum terupdate karena masih dalam versi yang lama.
   - Instalasi aplikasi *OpenVAS* yang digunakan untuk melakukan *Vulnerabilty* pada sistem.
   - Melakukan konfigurasi aplikasi *OpenVAS* agar bisa digunakan untuk melakukan scanning pada sistem *server IPS*.
2. Konfigurasi Pada Komputer Penyerang.
   - Melakukan instalasi *software* untuk penyerangan terhadap *server IPS*.
   - Melakukan instalasi *software Nmap* sebagai alat Penyerangan *Portscanning*.
   - Instalasi *software XOIC* yang digunakan untuk melakukan teknik penyerangan *Distributed Denial of Service (DdoS)*.

B. Scenario Pengujian

Pada tahapan ini berisi langkah – langkah untuk melakukan ujicoba pada topologi yang telah di rancang. Berikut langkah – langkah ujicoba yang akan dilakukan ;

1. Pengujian dilakukan secara protype dengan mensimulasikan antara komputer yang bertindak sebagai server dan komputer yang bertindak sebagai penyerang.
2. Sebagai komputer yang berfungsi sebagai penyerang, akan melakukan *scanning* terhadap *port*, melakukan Utilitas *Ping*, dan melakukan penyerangan *DDoS*.
3. Sebagai komputer *server* akan melakukan *blocking* terhadap serangan yang dilakukan penyerang.
4. Proses penyerangan dari komputer *client* dan komputer *server* dilakukan pengamatan.

   Setelah tahapan-tahapan scenario pengujian diatas dilakukan, selanjutnya akan melakukan:
5. Verifikasi pada *server IPS* untuk aplikasi *Portsentry*.
6. Melakukan verifikasi pada *server IPS* untuk aplikasi *OpenVAS*.
7. Melakukan verifikasi koneksi antara komputer penyerang dengan *server IPS*.
8. Verifikasi aplikasi untuk melakukan penyerangan pada komputer penyerang.
9. Melakukan pengujian serangan dengan melakukan *port scanning*, *Ping Attack*, dan *DDoS* pada server *IPS* sebelum *Script PortSentry* dijalankan.
10. Melakukan monitoring dengan menggunakan *OpenVAS*.
11. Pengujian serangan dengan melakukan *Portscanning*, *Ping Attack*, dan *DDoS* pada *server IPS* setelah *Script PortSentry* dijalankan.

12. Melakukan monitoring dengan menggunakan *OpenVAS.*
13. Melakukan analisa hasil dari masing – masing pengujian.

III. HASIL DAN PEMBAHASAN

Pada bab hasil dan pembahasan ini berisi langkah pengujian system keamanan *IPS* dengan menggunakan *portsentry* dan hasil analisa dari konfigurasi yang dirancang pada server *IPS* tersebut setelah terjadinya penyerangan. Adapun hasil dan pembahasan yang dilakukan adalah sebagai berikut:

1. Hasil Konfigurasi

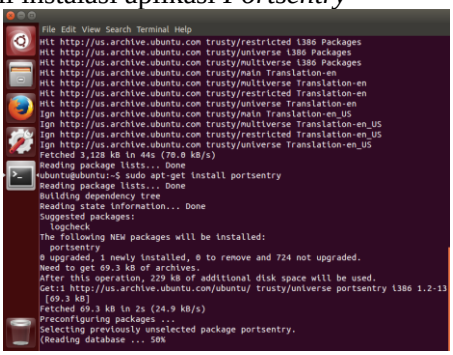
Pada tahapan ini akan dijelaskan konfigurasi yang dilakukan pada *server IPS* dan Komputer yang bertindak sebagai penyerang. Berikut adalah langkah – langkah konfigurasi yang penulis lakukan pada masing – masing perangkat:

A. Hasil Konfigurasi *server Ubuntu* sebagai *server IPS.*

Berikut adalah konfigurasi yang diterapkan pada *server IPS*:

Hasil Konfigurasi *Server IPS*

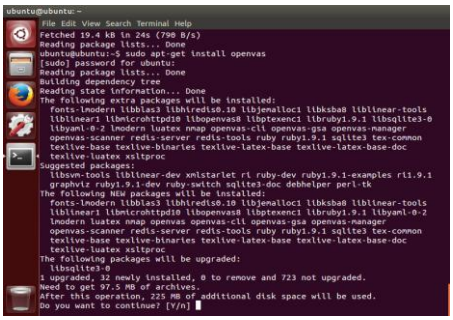
A. Hasil instalasi aplikasi *Portsentry*



Gambar 3.1 Instalasi aplikasi *portsentry*

Pada tahapan ini penulis melakukan instalasi *packet* aplikasi *portsentry* pada system *Ubuntu linux* dengan menggunakan perintah *#Sudo apt-get install portsentry* .

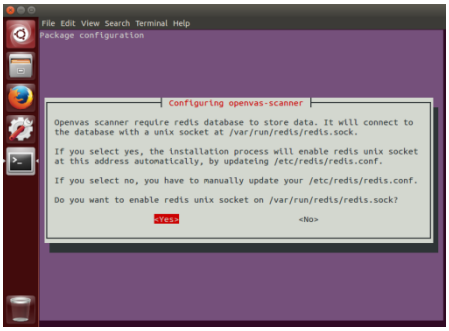
C. Pada langkah berikut ini penulis akan melakukan Instalasi Aplikasi *OpenVAS* pada *server IPS* yang dapat dilihat pada gambar 3.2 berikut;



Gambar 3.2 *Update packet* aplikasi pada *repository*

Gambar 3.2 menerangkan cara instalasi *packet* aplikasi openvas yang dilakukan dengan menggunakan perintah *#sudo apt-get install openvas.*

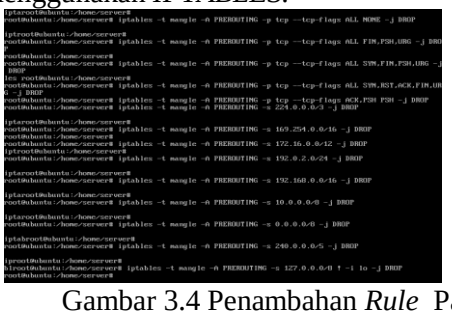
D. Hasil konfigurasi awal aplikasi *openvas* setelah dilakukan instalasi.



Gambar 3.3 Konfigurasi aplikasi *openvas*

Pada gambar 3.3 ditunjukan gambar konfigurasi openvas scanner

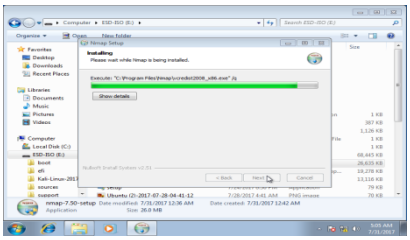
E. Menambahkan *rule* untuk mencegah serangan *DDoS* pada *server IPS* dengan menggunakan *IPTABLES.*



Gambar 3.4 Penambahan *Rule* Pada *IPtables*

B. Hasil Konfigurasi Pada Komputer Penyerang

a. Instalasi *software Nmap* Untuk Melakukan Penyerangan



Gambar 3.5 Instalasi *Sofware NMAP*

Pada gambar 3.5 menerangkan instalasi palikasi untuk melakukan penyerangan dengan menggunakan *nmap*.

b. Hasil instalasi dan konfigurasi aplikasi *XOIC* pada komputer penyerang.

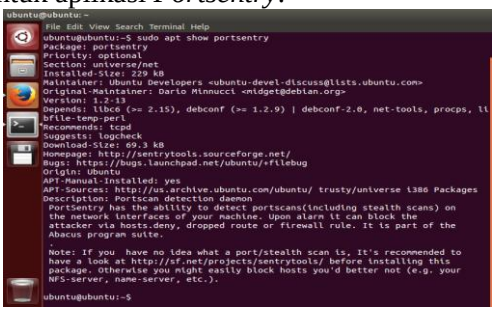
Gambar 3.6 Instalasi *Sofware XOIC*

Pada gambar 3.6 menerangkan instalasi aplikasi *software xoic* untuk melakukan penyerangan *DDoS* pada *server IPS.*

2. Pengujian

Pada tahapan ini penulis akan melakukan pengujian pada *server IPS* yang akan dilakukan dengan beberapa tahapan dari melakukan verifikasi pengujian dan melakukan pengujian, berikut tahapan yang akan dilakukan;

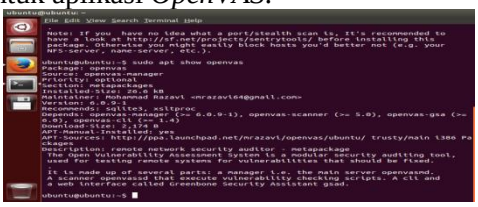
A. Melakukan verifikasi pada *server IPS* untuk aplikasi *Portsentry*.



Gambar 3.7 Melakukan verifikasi aplikasi *Portsentry*

Pada gambar 3.7 menunjukkan verifikasi aplikasi *portsentry* pada *server IPS.*

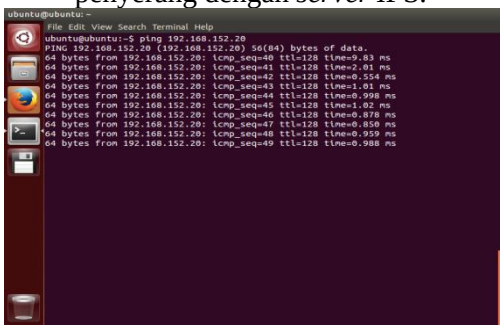
B. Melakukan verifikasi pada *server IPS* untuk aplikasi *OpenVAS*.



Gambar 3.8 Melakukan verifikasi aplikasi *OPenVAS*

Pada gambar 3.8 menunjukkan langkah verifikasi aplikasi *OPENVAS* pada *server IPS.*

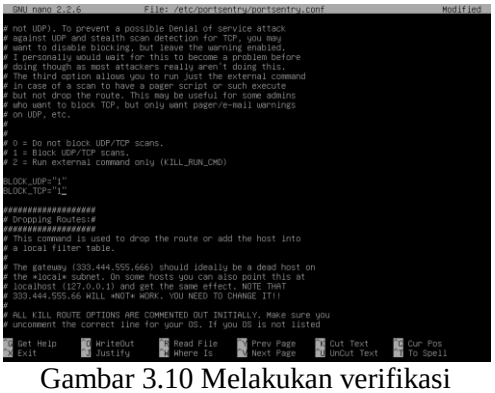
C. Memverifikasi koneksi antara Komputer penyerang dengan *server IPS.*



Gambar 3.9 Melakukan verifikasi Koneksi Antara Komputer Penyerang dengan *Server IPS.*

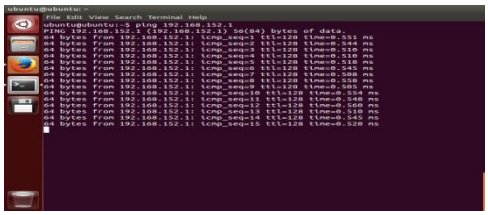
Pada gambar 3.9 menunjukkan langkah verifikasi koneksi antar komputer penyerang dengan *server IPS* dengan utilitas *PING* melalui *server IPS.*

D. Konfigurasi aplikasi *Portsentry* pada *server IPS.*



Gambar 3.10 Melakukan verifikasi konfigurasi *portsentry* pada *Server IPS*

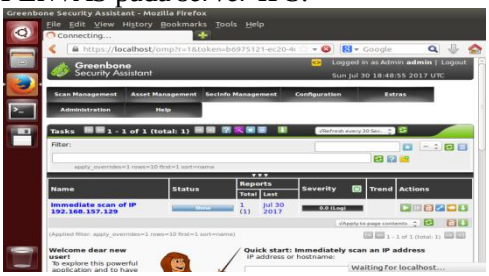
Pada gambar 3.10 penulis melakukan verifikasi konfigurasi portsentry pada *server IPS* setelah melakukan *enable blocking* pada aplikasi *portsentry*.



Gambar 3.11 Melakukan verifikasi Koneksi Antara Komputer Monitoring dengan *Server IPS*

Pada gambar 3.11 menunjukkan langkah verifikasi koneksi antar komputer yang bertindak sebagai *client* monitoring penyerangan dengan *server IPS* dengan utilitas *PING* melalui *server IPS.*

E. Melakukan verifikasi konfigurasi aplikasi *OPENVAS* pada *server IPS.*

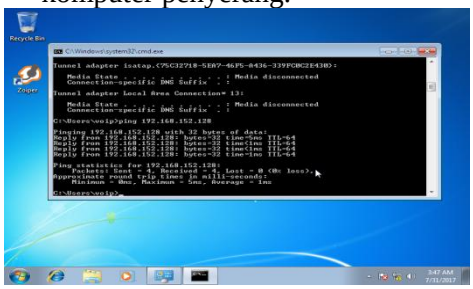


Gambar 3.12 Melakukan verifikasi konfigurasi aplikasi *OPenVAS* pada *Server IPS*

Pada gambar 3.12 menunjukkan langkah verifikasi konfigurasi aplikasi *openvas* pada *server IPS* dengan melakukan running aplikasi melalui fasilitas *browser.*

F. Pengujian serangan dengan melakukan *portscanning*, *Ping Attack*, dan *DDoS* pada *server IPS* sebelum *script Portsentry* dijalankan.

- Melakukan penyerangan dengan menggunakan *ping attack* melalui komputer penyerang.



Gambar 3.13 Melakukan penyerangan pada *server IPS* dengan menggunakan *Ping Attack.*

Pada gambar 3.13 menunjukan penyerangan pada server *IPS* dengan menggunakan *Ping Attack* melakukan *ping* melalui Komputer penyerang ke Komputer *server IPS.*

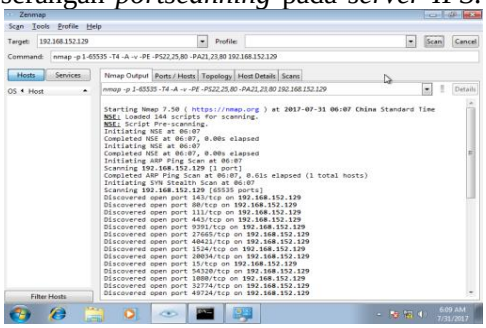
- Proses penyerangan dengan menggunakan aplikasi *xoic* untuk melakukan *ddos* dengan komputer penyerang.

Gambar 3.14 Melakukan

penyerangan pada *server IPS* dengan menggunakan *XOIC* untuk melakukan *DdoS*

Pada gambar 3.14 menunjukkan tentang penyerangan pada *server IPS*dengan menggunakan aplikasi *XOIC* untuk melakukan serangan *DDoS* sebelum dilakukan proteksi *firewall*.

- Penyerangan dengan menggunakan aplikasi *NMAP* untuk melakukan serangan *portscanning* pada *server IPS.*

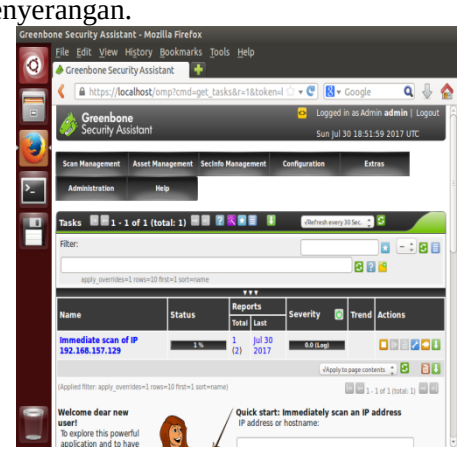


Gambar 3.15 Melakukan penyerangan pada *server IPS* dengan menggunakan *NMAP* untuk melakukan *Port Scanning*

Pada gambar 3.15 menunjukkan penyerangan pada *server IPS* dengan menggunakan aplikasi *NMAP* untuk

melakukan serangan *portscanning* pada *server IPS* sebelum diaktifkan proteksi *firewall* pada *server IPS*.

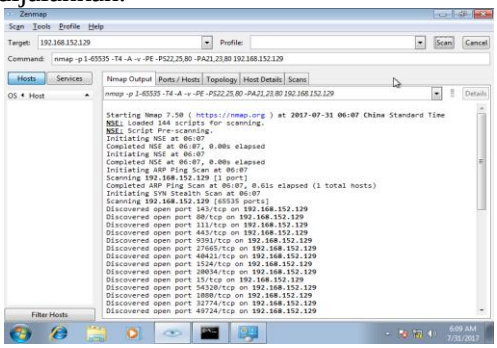
- Proses monitoring dengan menggunakan *OpenVAS* setelah dilakukannya penyerangan.



Gambar 3.16 Melakukan monitoring menggunakan *OPENVAS* setelah dilakukan penyerangan

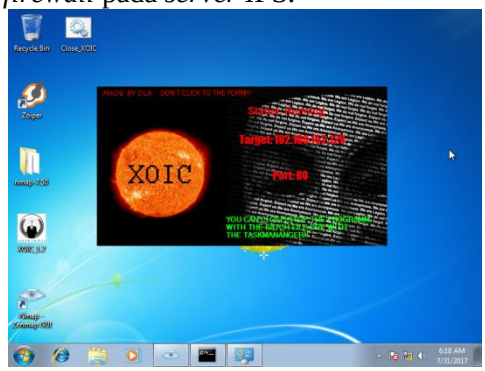
Pada gambar 3.16 menerangkan tentang bagaimana melakukan monitoring dengan menggunakan *OPENVAS* setelah dilakukannya penyerangan. Pada saat melakukan monitoring terjadi hang atau *overload* pada *server IPS* karena serangan *DDoS* yang membuat server *IPS* harus dilakukan *restart*.

G. Pengujian serangan dengan melakukan *Portscanning*, *Ping Attack*, dan *DDoS* pada *server IPS* setelah *Script Portsentry* dijalankan.



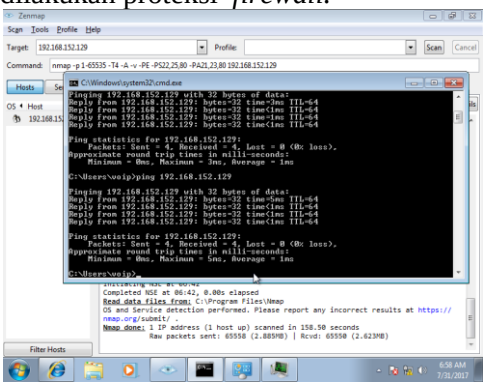
Gambar 3.17 Melakukan penyerangan pada *server IPS* dengan menggunakan *NMAP* untuk melakukan *Port Scanning*

Pada gambar 3.17 menunjukkan penyerangan pada *server IPS* dengan menggunakan aplikasi *NMAP* untuk melakukan serangan *portscanning* pada *server IPS* setelah diaktifkan proteksi *firewall* pada *server IPS*.



Gambar 3.18 Melakukan penyerangan pada *server IPS* dengan menggunakan *XOIC* untuk melakukan *DdoS*.

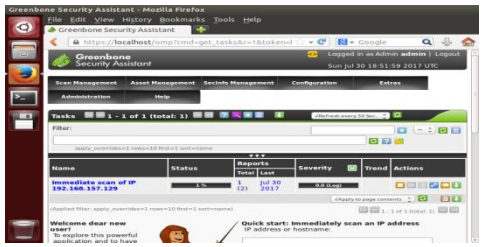
Pada gambar 3.18 menunjukkan tentang penyerangan pada *serverIPS* dengan menggunakan aplikasi *XOIC* untuk melakukan serangan *DDoS* setelah dilakukan proteksi *firewall*.



Gambar 3.19 Melakukan penyerangan pada *server IPS* dengan menggunakan *Ping Attack*

Pada gambar 3.19 Menunjukan penyerangan pada *server IPS* dengan menggunakan *Ping Attack* melakukan ping melalui komputer penyerang ke komputer *server IPS*.

- Melakukan monitoring dengan menggunakan *OpenVAS*.

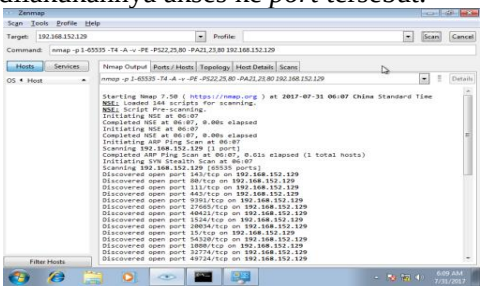


Gambar 3.20 Melakukan monitoring menggunakan *OPenVAS* setelah dilakukan penyerangan

Pada gambar 3.20 menerangkan tentang bagaimana melakukan monitoring dengan menggunakan *OPenVAS* setelah dilakukannya penyerangan pada *server IPS*.

H. Analisa Hasil pengujian sebelum diterapkan *firewall portsentry* dan *IPTables*.

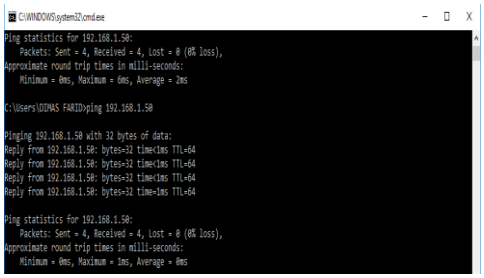
- Pada pengujian dilakukannya portscanning menggunakan *tool nmap* , *port* bisa dibuka seperti *port* 80 untuk internet *ssh* untuk *remote host* dan masih dapat melakukan *ping* dan dapat dilakukannya akses ke *port* tersebut.



Gambar 3.21 Hasil penyerangan dengan *tool nmap*

- Pada saat dilakukannya pengujian *ddos* menggunakan *tool xoic* , *host* atau *server IPS* mengalami hang dan tidak bisa bekerja.

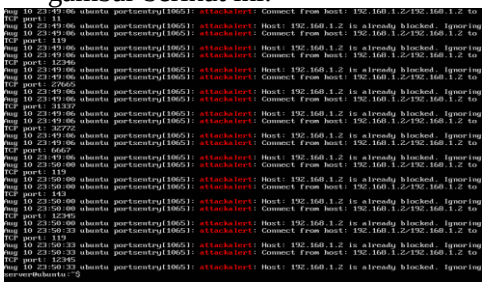
- Pada saat dilakukannya pengujian dengan melakukakan ping melalui host penyerang *server* masih melakukan *replay* sehingga penyerangan dapat dilakukan.



Gambar 3.21 hasil penyerangan dengan *ping attack*

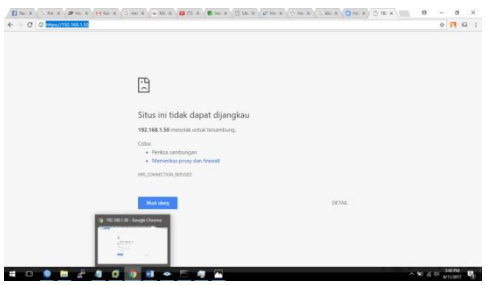
I. Analisa hasil pengujian sesudah diterapkan *firewall portsentry* dan *IPTables*.

- Pada analisa ini dilakukannya pengujian penyerangan dengan menggunakan tool nmap dengan perintah *nmap -p 1-65535 -T4 -A -v -PE -PS22,25,80 -PA21,23,80 192.168.1.10* pada alamat *server IPS* untuk melakukan scaning port dan hasilnya port yang dilakukan *scanning port* tersebut masih terbuka akan tetapi pada saat dilakukan akses, *portsentry* dan *iptables* melakukan *closing* secara otomatis pada *port* tersebut sehingga *port* tersebut tidak dapat dibuka, misalnya *port https* untuk mengakses *openvas* melalui *host* penyerang, dan *putty* untuk *remote* akses *port* 22 untuk mencegah *ssh bruteforce*, seperti gambar berikut ini.

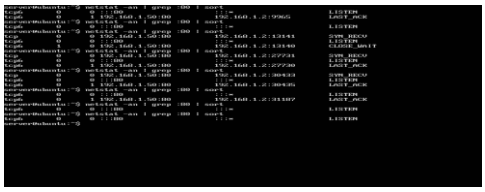


Gambar 3.22 Hasil penyerangan dengan *ping NMAP*

- Pada analisa penyerangan dengan menggunakan *tool xoic* untuk pengujian *ddos* dilakukan pada *port* 80 dan hasilnya *server* langsung melakukan *blocking* dan packet yang dikirimkan secara berlebihan sudah di*bloking* oleh *rule* dari *IPTables* untuk mencegah packet yang berlebihan sehingga performa *server* tetap terjaga. Berikut gambar dari proses *blocking port*.

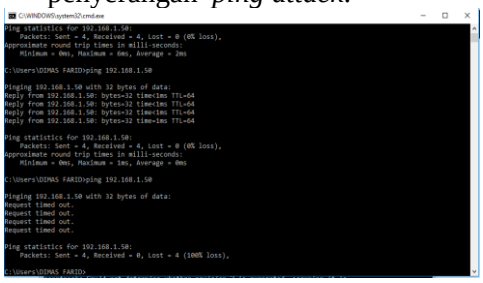


Gambar 3.23 Hasil penyerangan dengan *DDoS XOIC*



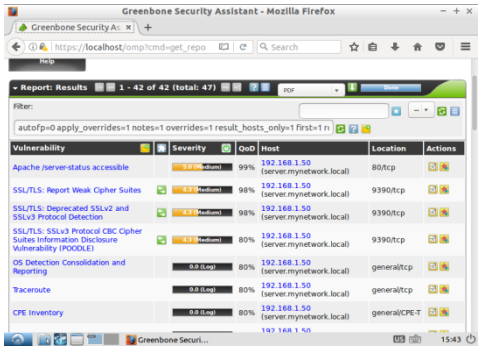
Gambar 3.24 Proses *blocking* penyerangan dengan *DDoS* pada *port* 80

- Pada analisa penyerangan dengan menggunakan *tool ping* untuk melakukan *ping attack* berhasil dilakukan, ini ditandai dengan saat *host* penyerang melakukan *ping* ke *server* maka hasilnya akan *request time out* karena otoritas untuk menjawab dari *server* sudah di *block* oleh *firewall IPTables*. Berikut hasil *capture* dari penyerangan *ping attack*.

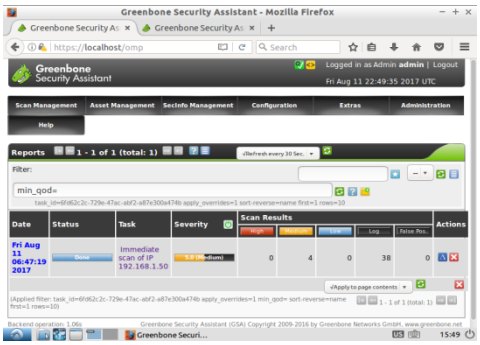


Gambar 3.25 Proses penyerangan dengan *ping attack* pada *ICMP*

- Hasil *scanning* yang ditemukan dengan menggunakan *OpenVAS.*



Gambar 3.26 Hasil *Scanning* menggunakan *Openvas*



Gambar 3.27 Hasil *report scanning* menggunakan *Openvas*

Pada gambar 3.26 dan gambar 3.27 Menerangkan dengan hasil *scanning* yang dibagi menjadi beberapa tingkatan yaitu *High*, *Medium* , dan *Low* dan untuk hasil *scanning* yang dilakukan pada server terdapat 4 *Vulnarebility* dengan tingkatan medium, 0 dengan tingkatan *high* dan 0 dengan tingkatan *low* pada *server IPS* dan *vurnability*nya dapat dilhat pada gambar 3.27.

IV. SIMPULAN DAN SARAN

1. Kesimpulan

Adapun kesimpulan yang dapat diambil dari pengujian yang dilakukan adalah sebagai berikut:

1. Pada analisa penyerangan dengan menggunakan *tool ping* untuk melakukan *ping attack* berhasil dilakukan, ini ditandai dengan saat host penyerang melakukan ping ke *server* maka hasilnya akan *request time out* karena otoritas untuk menjawab dari *server* sudah di *block* oleh *firewall IPTables*.
2. Pada analisa penyerangan dengan menggunakan *tool XOIC* untuk pengujian *DDoS* dilakukan pada *port* 80 dan hasilnya *server* langsung melakukan *blocking* dan *packet* yang dikirimkan secara berlebihan sudah dibloking oleh *rule* dari *IPTables* untuk mencegah *packet* yang berlebihan sehingga performa *server* tetap terjaga dan tidak terjadi hang.
3. Pada analisa ini dilakukannya pengujian penyerangan dengan menggunakan *tool nmap* dengan perintah *nmap -p 1-65535 -T4 -A -v -PE -PS22,25,80 -PA21,23,80*

192.168.1.10 pada alamat *server IPS* untuk melakukan *scaning port* dan hasilnya *port* yang dilakukan *scanning port* tersebut masih terbuka akan tetapi pada saat dilakukan akses, *portsentry* dan iptables melakukan *closing* secara otomatis pada *port* tersebut sehingga *port* tersebut tidak dapat dibuka, misalnya *port https* untuk mengakses *openvas* melalui *host* penyerang, dan *putty* untuk remote akses *port* 22 untuk mencegah *ssh bruteforce*.

4. Berdasarkan hasil pengujian dan dilakukannya *scanning* dengan menggunakan *software OpenVAS,* di dapatkan hasil dengan jumlah *Vulnerability* dengan tingkatan *medium* sebanyak 4, 0 dengan tingkatan *high* dan 0 dengan tingkatan *low* pada *server IPS.*
5. Setelah dilakukannya pengujian terhadap sistem keamanan *web server* dapat disimpulkan bahwa *server* yang telah diberi *firewall Portsentry* dan *iptables* dengan metode *Vulnerability Assesment* menggunakan *OpenVAS* dapat mendeteksi secara langsung kelemahan pada sistem keamanan *web server* tersebut ketika terjadi serangan dan dapat dilakukannya upaya perbaikan terhadap sistem agar menjadi lebih baik.

2. Saran

Adapun saran-saran untuk pengembangan penelitian ini lebih lanjut adalah sebagai berikut:

1. Perlunya pengembangan dalam teknik penyeranganyang lain agar bisa mengetahui apakah sistem yang sudah di amankan sudah tidak mempunyai celah sehingga dapat meminimalisir terjadinya penyusupan.
2. Perlunya pengembangan pada sistem yang real, guna mengetahui apakah penerapan pengamanan pada sistem berjalan dengan baik dalam kehidupan nyata.
3. Perlunya eksplorasi yang lebih terhadap penggunaan *firewall* dalam mengamankan sebuah sistem.

V. UCAPAN TERIMAKASIH

Dengan selesainya penelitian ini, penulis ingin mengucapkan terimakasih kepada pihak-pihak yang telah banyak membantu dalam penyelesaian penelitian ini. Dalam kesempatan ini penulis menyampaikan ucapan terimakasih kepada :

1. Ibu Komariyuli Anwariyah, S.T, M.Kom., selaku Ketua Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Bumigora Mataram.
2. Ibu Ni Gusti Ayu Dasriani, M.Kom., selaku Ketua Program Studi S1 Teknik Informatika pada STMIK Bumigora Mataram.
3. Bapak Raisul Ashar, M.T. selaku Dosen pembimbing yang telah meluangkan waktunya untuk membimbing dan memberikan masukan pada penulisan selama mengerjakan artikel ini.
4. I Putu Hariyadi M.Kom. CCNA, CCAI. selaku Dosen pembimbing II yang telah meluangkan waktunya untuk memberikan masukan pada penulisan selama mengerjakan penelitian ini.
5. Tak terlupakan yang tercinta Bapak dan Ibu yang telah memberikan dukungan moril dan dukungan materi.

REFERENSI

[1] E. Carter, et al, 2006, "*Intrusion Prevention Fundamentals : an introduction to*

[2] Lumy, Gildas Deograt. *Ilusi Test Penetrasi Bagian 1***,** InfoKomputer, April 2010.

[3] Stiawan, Deris. 2009. *Fundamental Interworking Development & Design Life Cycle,* Jurnal, FASILKOM UNSRI.