IMPLEMENTASI HONEYPOT PADA WEB SERVER AIR TRAFFIC CONTROL (ATC) MENGGUNAKAN KFSENSOR

Hikmah Gatra[1] **Nina Hendrarini**[2] **Anang Sularsa**[3]

[1,2,3]Fakultas Ilmu Terapan - Telkom University

[1]hikmahgatra@gmail.com [2]ninahendrarini@tass.telkomuniversity.ac.id anang@tass.telkomuniversity.ac.id

Abstrak

Teknologi yang berkembang pada saat ini banyak digunakan oleh sebagian perusahaan seperti pada penerbangan yang menggunakan *navigasi* secara terpusat pada menara *air traffic control* (ATC) pada wilayah yang dilalui agar tidak terjadi perubahan jalur yang telah diberikan. Dengan menggunakan *Honeypot* pada KFSensor, serangan yang dilakukan terhadap *server* pada *Air Traffic Control* (ATC) dapat diketahui dengan metode monitoring yang di *install* pada *windows server*, informasi pada monitoring berisi *ip address* penyerang tersebut yang memudahkan untuk dilakukan analisis. Contoh serangan yang sering terjadi seperti *telnet,port scanning* dll.

Kata Kunci : *Honeypot*, ATC, KFSensor

Abstract

Technology is evolving at this point widely used by some companies such as airlines that use centralized on the navigation tower air traffic control (ATC) in the areas traversed in order to avoid the lane change has been given. By using the Honeypot on KFSensor, attacks carried out against the server on the Air Traffic Control (ATC) can be determined by monitoring method is installed on a Windows server, the monitoring information contains the IP address of the attack that makes it easy to do the analysis. Examples of attacks that often occur as telnet, port scanning etc.

Keyword : Honeypot, ATC, KFSensor

1. Pendahuluan

1.1 Latar Belakang

Pentingnya suatu keamanan pada saat kemajuan perkembangan informasi dan teknologi penyimpanan yang berisikan informasi ataupun data yang dapat disalahgunakan untuk kepentingan tertentu sehingga memberikan suatu pencegahan celah keamanan untuk mengurangi kebocoran suatu informasi. Penggunaan sistem keamanan sudah banyak digunakan seperti pada suatu perusahaan, Penerbangan untuk mengontrol sistem keamanan.

Untuk menangani hal ini digunakan metode *honeypot* dengan program tambahan KFSensor untuk mengamankan data asli sehingga serangan yang ditujukan pada *web server* tersebut bukan data yang sebenarnya dan mencari metode yang digunakan untuk menyerang *web server* tersebut sehingga keamanan pada *web Server Air Traffic Controll* (ATC) terlindungi dari serangan *hijacking*.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang diuraikan sebelumnya, maka dapat disimpulkan masalah yang terjadi sebagai berikut:

1. Bagaimana mengamankan *web server* dari berbagai serangan?
2. Bagaimana mengatasi akibat dari serangan pada *web server* tersebut ?

1.3 Tujuan

Tujuan dari Proyek Akhir ini adalah :

1. Mampu membangun *honeypot* untuk perlindungan *web server* dengan KFsensor.
2. Mampu menganalisa hasil serangan pada *web server* untuk meningkatkan keamanan.

1.4 Batasan Masalah

Batasan masalah dapat berisi:

1. Hanya membahas tentang *web server* yang menangani ATC dengan KFSensor.
2. Menganalisa serangan suatu layanan seperti FTP, Telnet, HTTP *Port Scanning*.
3. Tidak membahas tentang IDS terlalu mendalam.
4. Hanya membahas *low-interaction honeypot.*
5. Lebih difungsikan untuk mendeteksi serangan seperti proses *scanning* atau percobaan serangan pada jaringan intranet.

1.5 Definisi Operasional

1. *Honeypot* adalah [1] sumber daya keamanan yang sengaja dengan dibuat untuk menyelediki penyerangan atau membuat *web server* untuk menjebak *attacker* seolah-olah berhasil menjebol dan mengambil data pada sebuah jaringan.
2. *Web Server* adalah [2] sebuah bentuk *server* yang khusus digunakan untuk menyimpan halaman *web site*. Komputer dapat dikatakan sebagai *web server* jika dalam komputer tersebut memiliki program *server* yang bernama *Personal Web Server* (PWS). PWS difungsikan agar komputer klient dapat memanggil halama *web* yang ada di dalam sebuah komputer *server*.
3. *Air Trafic Control* (ATC) [3] adalah profesi yang memberikan lalu lintas di udara terutama pesawat udara untuk mencegah antar pesawat terlalu dekat dengan yang lain, mencegah tabrakan antar

pesawat udara dengan pesawat udara yang lain dan memberikan info navigasi penerbangan.

4. KFSensor adalah [4] *Honeypot* yang berbasis Windows Intrusion Detection System (IDS) yang bertindak sebagan *web server* untuk menarik dan mendeteksi *attacker* dengan mensimulasikan layanan yang diserang.

1.6 Metode Pengerjaan

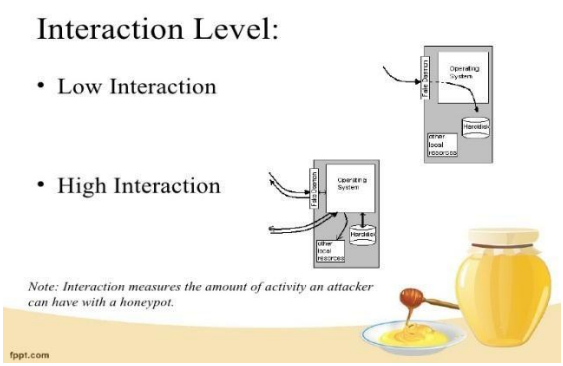
1. Studi Literatur
2. Analisis Kebutuhan
3. Perancangan
4. Implementasi
5. Pengujian
6. Penyusunan Laporan

2. Tinjauan Pustaka

2.1 Honeypot

Honeypot adalah [1] sumber daya keamanan yang sengaja dengan dibuat untuk menyelidiki penyerangan atau membuat *web server* untuk menjebak *attacker* seolah-olah berhasil menjebol dan mengambil data pada sebuah jaringan.

Ada beberapa klasifikasi *honeypot* sebagai berikut:



Gambar 2-1 Honeypot Interaction Level

1. Low-interaction

Low interaction honeypot merupakan *honeypot* dengan tingkat interaksi honeypot yang didesain untuk menganalisa *service* seperti pada *server* yang asli sehinggan penyerang hanya mampu memeriksa dan terkoneksi ke satu atau *port* tertentu. Layanan yang diberikan berupa emulasi yang bertujuan *attacker* tidak dapat berinteraksi secara langsung dengan layanan yang diberikan oleh sistem.

2. High-interaction

High interaction honeypot merupakan *honeypot* di mana attacker dapat berinteraksi secara langsung dan tidak ada batasan yang membatasi interaksi tersebut. Penyerang dapat berinteraksi di dalam *web service*. Sistem tersebut terdiri dari berbagai jenis implementasi dan telknologi keamanan yang banyak digunakan untuk melindungi suatu sistem seperti *firewall*, IDS dan lain-lain.

Dari level interaksi *honeypot* berikut ini perbedaan antara *low-interaction* dan *high interaction*:

Tabel 2-1 Perbedaan Low-interaction dan High-interaction

	Low-interaction	High-interaction
Installation	Easy	More difficult
Maintenance	Easy	Time consuming
Risk	Low	High
Need Control	No	Yes
Data gathering	Limited	Extensive
Interaction	Emulated services	Full control

2.2 Web Server

Web Server adalah [2] sebuah bentuk server yang khusus digunakan untuk menyimpan halaman *web site*. Komputer dapat dikatakan sebagai *web server* jika dalam komputer tersebut memiliki program *server* yang bernama Personal Web Server (PWS). PWS difungsikan agar komputer klient dapat memanggil halaman *web* yang ada di dalam sebuah komputer *server*.

2.3 Air Trafic Control (ATC)

Air Trafic Control (ATC) adalah [3] profesi yang memberikan lalu lintas di udara terutama pesawat udara untuk mencegah antar pesawat terlalu dekat dengan yang lain, mencegah tabrakan antar pesawat udara dengan pesawat udara yang lain dan memberikan info navigasi penerbangan.

Tujuan dari mengamankan *web server* yang mengatur lalu lintas udara menggunakan KFSensor sebagai berikut:

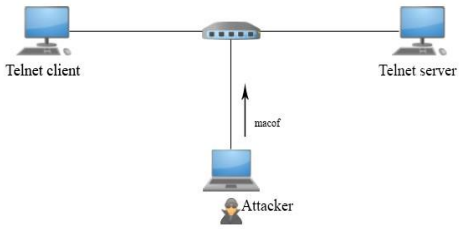
1. Memberikan arah navigasi yang diatur terpusat melalui *web* antar muka yang benar.
2. Mengamankan serangan yang berakibatkan tabrakan lalu lintas udara.

2.4 File Transfer Protocol (FTP)

File transfer protocol adalah [5] protocol jaringan standart yang digunakan untuk mentransfer file dari kumputer dari *host* yang satu ke *host* yang lain melalui jaringan berbasis TCP seperti *internet*. Fungsi dari mengamankan FTP seperti pengamanan pada *server* dari serangan ke FTP dengan menggunakan *keyloger*.

2.5 Telnet

Telnet (*Telecommunication Network*) [6] adalah protokol client-server yang digunakan untuk akses *remote login* komputer tujuan dalam sebuah jaringan yang terhubung pada jaringan *internet* maupun lokal. Fungsi dari telnet sendiri adalah mengakses komputer (*Host/Server*) dari jauh dengan metode *login*.



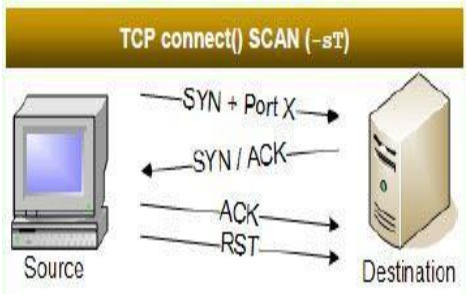
Gambar 2-2 Telnet Skema
(www.ask.wireshark.org)

2.6 Vulnerability

Vulnerability adalah kelemahan yang dapat memungkinkan diakses untuk masuk dan mendapatkan akses kedalam komputer yang akan ditargetkan. *Vulnerability* mengetahui upaya-upaya celah kelemahan sebuah system yang digunakan dalam untuk melakukan exploit dengan kode dalam penyerangan komputer.

2.6.1 Scanning Port

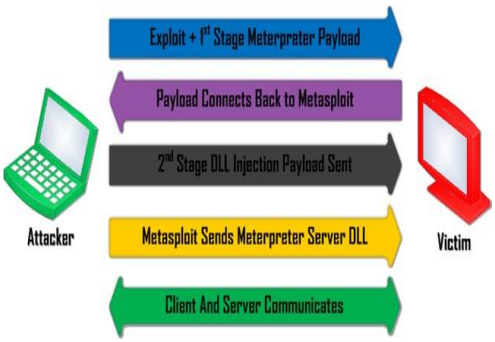
Scanning Port merupakan [7] mencari celah *port* yang terbuka untuk mengetahui kelemahan *service port* yang bisa digunakan untuk masuk kedalam sistem. Scanning port yang sering digunakan dalam linux adalah NMAP. Informasi yang dilakukan menggunakan *scanning port* adalah sebagai berikut :



Gambar 2-3 TCP Scanning

2.6.2 Metasploit System

Metasploit adalah framework yang digunakan sebagai jenis aplikasi, sistem operasi, aplikasi web. Dalam metasploit digunakan module yang terdapat didalam untuk melakukan exploit. Exploit merupakan software yang berfungsi memanfaatkan kelemahan pada web server yang sudah didapatkan melalui kelemahan pada *scanning port.* Dalam *metasploit* terdapat beberapa komponen yang menjadi dasar yaitu payload dan meterpreter. *Payload* merupakan sebuah *file* yang dimiliki oleh penyerang yang akan dijalakan pada komputer target dengan tujuan untuk mengendalikan komputer tersebut secara *remote*. Sedangkan *meterperter* merupakan *payload* yang dimasukan kedalam proses pada saat *exploit* dimana ada tambahan yang dibuat kedalam memori dan dapat menggunakan pada setiap proses. Gambar 2-4 merupakan alur metasploit

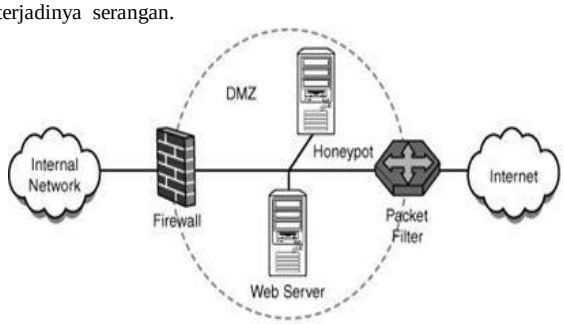


Gambar 2-4 Metasploit skema

3. Analisis dan Perancangan

3.1 Gambaran Sistem saat ini

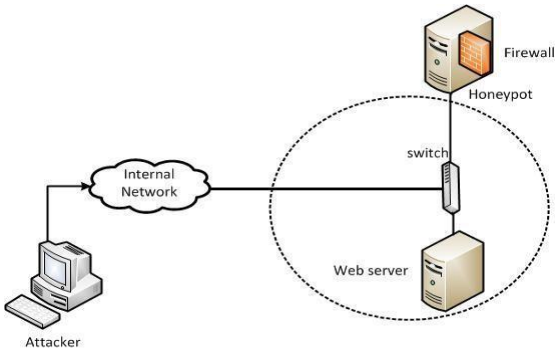
Pada jaringan yang ditunjukan pada Gambar 3-1 adalah jaringan yang sederhana untuk merancang dampak akibat dari serangan *hijacking*, sehingga perancangan kondisi saat ini memungkinkan terjadinya serangan.



Gambar 3-1 Topologi Saat ini

3.2 Sistem Usulan

Rancangan susulan yang telah di analisis pada Gambar 3-1 membedakan letak *web server honeypot* yang beda pada akses pertama kali, sehingga kemungkinan dilakukan *hijacking* akan mengakses terlebih dahulu adalah *server honeypot* bukan pada *server* yang sebenarnya.



Gambar 3-2 Topologi yang diusulkan

3.3 Kebutuhan Perangkat Keras

Dalam pengerjaan proyek akhir ini, digunakan perangkat keras dan spesifikasi minimum sebagai berikut:

Tabel 3-1 Kebutuhan perangkat keras

Jenis	Jumlah	Keterangan
PC Server	1	Intel Corei3; 2 GB DDR3; 500GB HDD
PC Penyerang	1	Intel Corei3; 2 GB DDR3; 500GB HDD
PC Server Honeypot		Intel Corei3; 2 GB DDR3; 500GB HDD

3.4 Kebutuhan Perangkat Lunak

Berikut kebutuhan perangkat lunak yang dibutuhkan:

Tabel 3-2 Kebutuhan Perangkat Lunak

Jenis	Versi	Keterangan
Oracle VM Virtualbox	4.1	Aplikasi Virtualisasi sistem Operasi
KFSensor	4.11.1	Aplikasi Honeypot versi windows
Windows Server 2003		Windows Server Sebagai Honeypot
Ubuntu Server	13.10	Web Server ATC
Backtrack		Sistem Operasi
Nmap		Aplikasi Port scanning

3.5 Langkah Pengerjaan

Adapun tahap pengerjaan proyek akhir ini diantaranya:

1. Melakukan konfigurasi jaringan pada *server honeypot*
2. Melakukan instalasi KFSensor
3. Mengakses jaringan pada *server* dan *client* agar dapat terhubung
4. Melakukan simulasi serangan berupa *scanning port*
5. Melakukan dokumentasi terhadap konfigurasi *honeypot*

3.6 Rencana Pengujian

Pengujian yang dilakukan meliputi

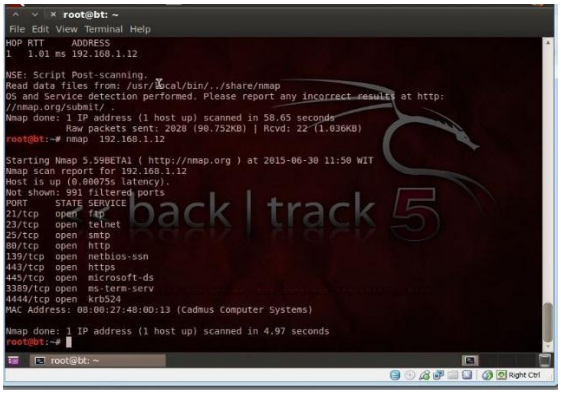
1. Pengecekan konfigurasi jaringan
2. Dilakukanya serangan terhadap *server* yang berupa *Scanning Port,*Telnet,
3. Melakukan remote desktop
4. Melakukan akses halaman web Server.

4. Pengujian

Pada tahap pengujian ini ada beberapa yang dilakukan menjadi tiga tahap, yaitu pengujian *vulnerability, add users login, remote desktop.*

4.1 Vulnerability

Pengujian ini berfungsi untuk mengetahui informasi yang dibutuhkan untuk melakukan akses kedalam server *honeypot* yang telah dikonfigurasi. Hasil pengujian *scanning vulnerability* dengan menggunakan NMAP. Dari gambar dibawah ini didapatkan beberapa *port* yang terbuka seperti Telnet,Ftp,ms-term-serv sehingga server honeypot memiliki beberapa celah melalui *port* yang terbuka.



Gambar 4-1 Scanning dengan NMAP

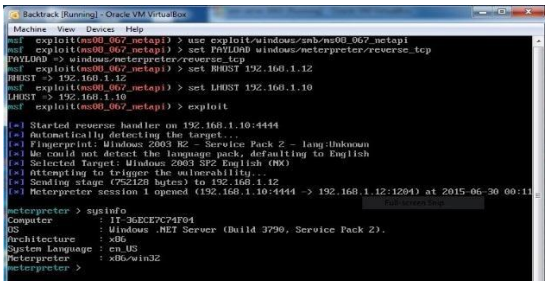
4.2 Metasploit system

Pengujian metasploit system dibagi menjadi beberapa tahap yaitu *exploit system* dan *add user login*.

4.2.1 Exploit system

Pada pengujian ini, *exploit system* yang akan diakses oleh penyerang menggunakan kelemahan *vulnerability* melaluli *port* yang terbuka sebagai contoh serangan *exploit system* menggunakan *msfconsole* yang sudah terinstal terdapat linux.

Pada gambar dibawah ini dijelaskan kode yang digunakan untuk penyerangan exploit/windows/smb/ms_08_067_netapi serta payload yang digunakan payload/windows/meterpreter/reverse_tcp, konfigurasi Rhost 192.168.1.12 adalah target computer sedangkan Lhost ip address penyerang. *Exploit* yang dilakukan setelah mengkonfigurasi *module* dan *IP address* ditandai dengan meterpreter > yang diasumsikan telah memasuki sistem yang ditargetkan. Pada meterpreter dilakukan pengecekan *sysinfo* yang berisikan nama komputer serta *oprating system* yang digunakan.



Gambar 4-2 Gambar Exploit system

4.2.2 Add user login

Setelah melakukan *exploit* pada sistem yang sudah mendapatkan kedalam selanjutnya akan dilakukan untuk membuat *user login* yang akan digunakan untuk melakukan *remote desktop*. Sebagai contoh, pada proyek akhir ini ditambahkan userpa sebagai *usename* dan *password* yang digunakan untuk melakukan *remote desktop* dan

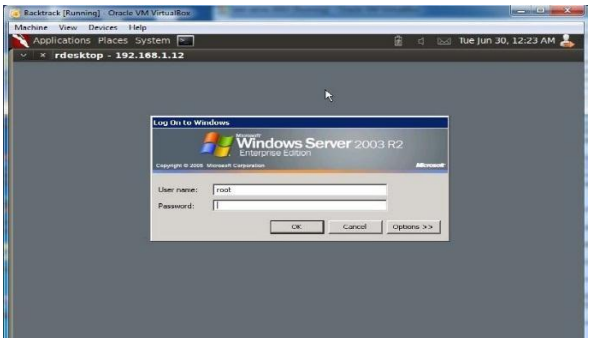
user group untuk menjadikan userpa kedalam *group* hak akses yang ada.

Gambar 4-3 Gambar Add user Remote Desktop

Gambar 4-4 Gambar Add User group

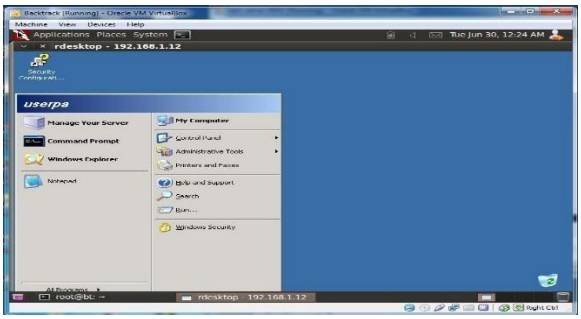
4.2.3 Remote desktop

Pengujian ini dilakukan untuk mencoba *user* yang telah dibuat sebelumnya menggunakan *remote desktop*. Dengan menggunakan terminal pada linux rdesktop 192.168.1.12 yang merupakan target *remote desktop*.



Gambar 4-5 remote desktop login username dan password

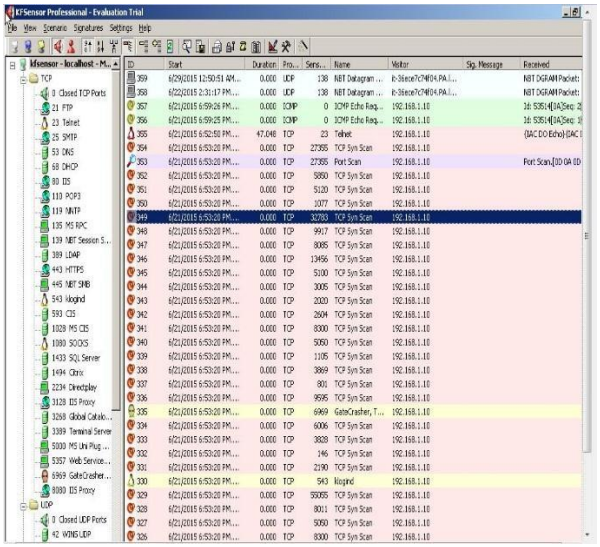
Pada gambar dibawah ini *remote desktop* berhasil masuk pada web server *honeypot* dan dapat digunakan akses yang dilakukan oleh penyerang.



Gambar 4-6 Gambar Remote desktop

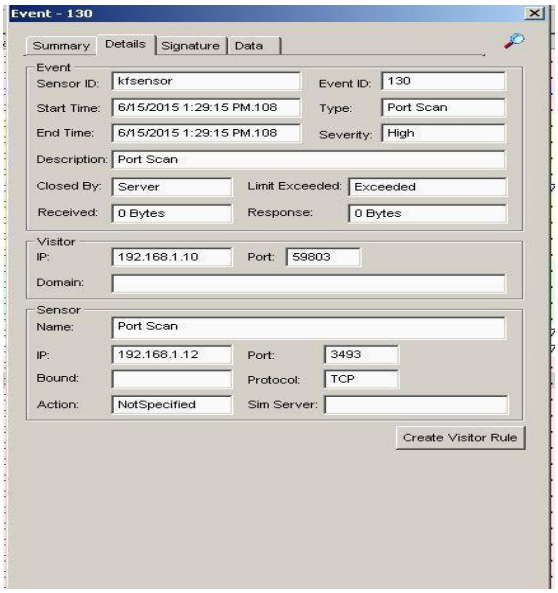
4.3 Pengujian terhadap Server Honeypot

1. Pada pengujian *server honeypot* ini seperti dengan penyerangan menggunakan NMAP yang ditandai dengan *TCP Syn Scan*, serta Telnet



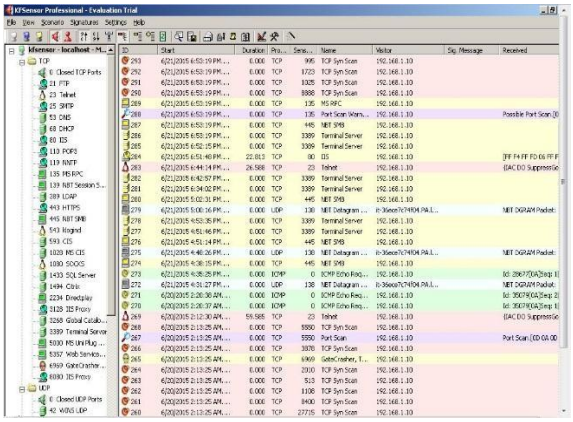
Gambar 4-7 Gambar Alert pada Server Honeypot

2. Pada gambar dibawah ini dijelaskan *port scan* yang artinya telah terjadi *scanning vulnerability* melalui Nmap untuk mencari *port* yang terbuka.



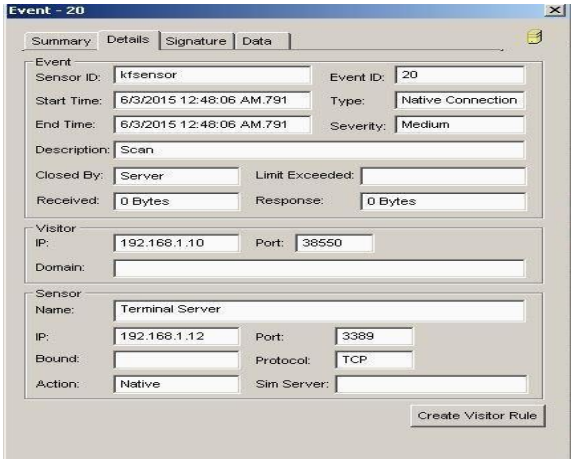
Gambar 4-8 Hasil Port Scan

3. Pengujian yang mengarahkan pada remote desktop yaitu Terminal server yang ditandai dengan warna kuning pada nomor 278 melalui port 3389 yang berdampak pada remote akses sistem.



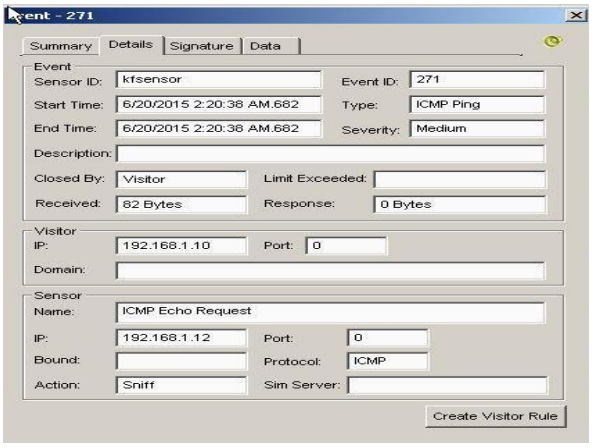
Gambar 4-9 Gambar Alert Remote desktop

Pada hasil pengujian gambar dibawah ini menunjukan jenis serangan yang dilakukan menggunakan remote desktop. Terdapat tanggal diserang dan tanggal berakhir serta IP address yang menyerang ke web server honeypot



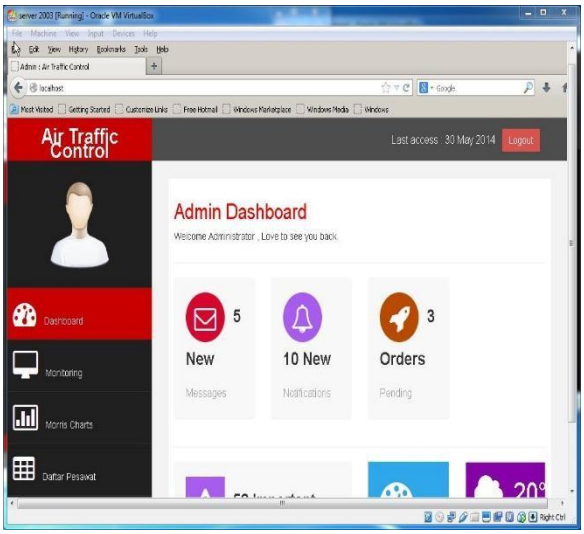
Gambar 4-10 Gambar detail serangan Terminal Server

4. Gambar dibawah ini berkaitan pada gambar 4-17 diatas yang terdapat juga hasil PING yang dilakukan pada web server honeypot sehingga oleh server dianggap serangan.



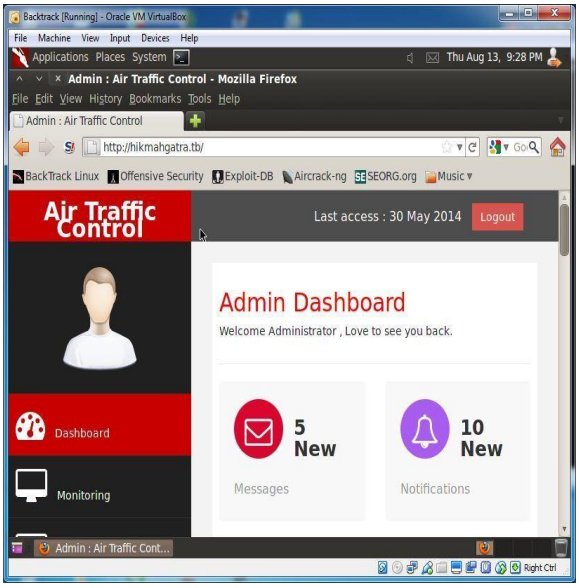
Gambar 4-11 Serangan Ping

5. Akses web server lokal yang tersimpan pada server honeypot berisi halaman web yang diarahkan oleh web server Ubuntu



Gambar 4-12 Akses Web Server melalui lokal

6. Mengalihkan halaman web server yang mengakses web server asli ke arah *web server honeypot* yang di akses oleh *attacker* menggunakan *web browser*.



Gambar 4-13 Akses Web yang dari attacker diarahkan ke web server honeypot

5. Kesimpulan dan Saran

5.1 Kesimpulan

Dari pembahasan dan implementasi serta pengujian diatas maka kesimpulanya adalah :

1. Honeypot yang digunakan pada web server menganalisis serangan yang ditujukan dari penyerang.

2. Penyerangan yang dilakukan mengarahkan attacker ke dalam web server honeypot.

5.2 Saran

Berdasarkan pembahasan dalam penyelesaian proyek akhir ini. Adapun saran yang bertujuan untuk memperkuat keamanan pada server *Air Traffic control* seperti meningkatkan *upgrade oprating system* yang terakhir dikeluarkan. Sehingga web server lebih aman dari penyerangan.

Daftar Pustaka

[1] Anonim, "KeyFocus," [Online]. Available: http://www.keyfocus.net/kfsensor/index.php. [Accessed 12 February 2015].

[2] Anonim, "Pengartian dan Klasifikasi Honeypot," 07 2014. [Online]. Available: http://www.kajianpustaka.com/2014/07/pengertian-dan-klasifikasi-honeypot.html. [Accessed 12 february 2015].

[3] Anonim, "Wikipedia," [Online]. Available: http://en.wikipedia.org/wiki/File_Transfer_Protocol. [Accessed 12 February 2015].

[4] Anonim, "Wikipedia," 12 January 2015. [Online]. Available: http://id.wikipedia.org/wiki/Pemandu_lalu_lintas_udara. [Accessed 12 february 2015].

[5] N. Bunafit, Instalasi dan Konfigurasi Jaringan Windows dan Linux, Yogyakarta: Andi Yogyakarta, 2005.

[6] K. Y. Tung, Teknologi Jaringan IntraNet, Yogyakarta: Andi, 1997.

[7] R. U. Rehman, Intrusion Detection Systems with Snort: Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID, New Jersey: Prentice Hall PTR, 2003.

[8] A. Singh, Metasploit Penetration Testing Cookbook, Birmingham Mumbai: Packt publishing, 2012.