IMPLEMENTASI HONEYPOT DENGAN MODETN HONEY NETWORK

IMPLEMENTATION HONEYPOT WITH MODERN HONEY NETWORK

Dimas Danang Laksana[1], Setia Juli Irzal Ismail, S.T., M.T.[2], Nina Hendrarini, S.T,M.T.[3]

[1,2,3]Prodi D3 Teknik Komputer, Fakultas Ilmu Terapan, Universitas Telkom
dimasdananglaksana@gmail.com

Abstrak

Di era globalisasi saat ini, keamanan jaringan merupakan salah satu hal penting yang harus diperhatikan, karena sangat berguna untuk melindungi suatu sistem computer (host) dari bahaya serangan ataupun oknum penyusup yang tidak bertanggungjawab yang ingin mencuri informasi penting di dalam suatu sistem komputer. Hal itu dapat terjadi karena dalam jaringan tersebut tidak terdapat sistem pengaman yang dapat mengamankan komunikasi data antar host satu dengan host lainnya. Honeypot adalah metode untuk membuat server palsu, dimana penyerang akan menghabiskan waktu untuk melancarkan serangan. Modern Honey Network adalah software open source yang digunakan untuk membangun beberapa sensor honeypot lebih sederhana dan untuk membuat stastistik data dari sensor honeypot. Pada proyek akhir ini, dibangun implementasi honeypot dengan modern honey network yang akan melakukan pengujian dengan melakukan memonitoring sensor kippo. Kippo honeypot merupakan salah satu tools honeypot yang termasuk dalam kategori medium-interaction ssh honeypot yang berfungsi untuk membangun sistem tiruan yang menyerupai aslinya untuk mengalihkan perhatian penyusup yang ingin menyerang sistem server asli. Selain itu, Modern Honey Network dapat membantu kippo honeypot untuk mendeteksi dan memonitoring aktifitas serangan apa saja yang dilakukan penyusup yang ingin menyerang sistem asli, sehingga admin dapat melakukan pencegahan ketika terjadi ancaman serangan.

Kata Kunci: MHN(Modern Honey Network), Kippo Honeypot, honeypot.

Abstract

In the current era of globalization, network security is one of the important things that must be considered, because it is very useful to protect a computer system (host) from the danger of attacks or irregular intruders who want to steal important information in the environment. It can happen because in the network there is no security system that can secure data communication between host one with other host. Honeypot is a method to create a fake server, where the attacker will spend time to launch an attack. The Modern Honey Network is an open source software used to build some simpler honeypot sensors and to create stastistic data from honeypot sensors. In this final project, built honeypot with modern honey network that will do the testing by doing monitor kippo sensor. Kippo honeypot is one of the honeypot tools that belongs to the intermediate category of ssh honeypot interaction that serves to build a full mock system to distract the intruder who wants to attack the original server system. In addition, Modern Honey Network can help kippo honeypot to perform and resolve any attack activity that intruders who want to attack the original system, so the admin can do prevention anytime.

Keywords: MHN(Modern Honey Network), Kippo Honeypot, SSH.

1. Pendahuluan

Seiring dengan perkembangan Teknologi Informasi (TI), menyebabkan keamanan dunia digital yang rentan terhadap hacking atau keamanan yang lemah. Munculnya beberapa kasus CyberCrime di Indonesia pada tahun 2016 cukup banyak seperti peretasan akun sosial media, peretasan situs pornografi, peretasan situs keagamaan, peretasan aplikasi browsing, dan peretasan situs perbankan.

Perkembangan dunia digital saat ini sangat memerlukan suatu sistem keamanan. Pentingnya suatu keamanan agar tidak disalahgunakan oleh seseorang yang tidak bertanggung jawab, sehingga mengakibatkan banyak informasi dan data yang di sabotase. Upaya untuk menangani hal ini digunakan honeypot. Honeypot merupakan metode yang membuat server palsu untuk mengamankan data asli, sehingga serangan yang ditunjukan untuk server tersebut bukan data yang sebenarnya, sehingga data terlindungi dari serangan hijacking. Honeypot sendiri memiliki berbagai macam, salah satunya adalah kippo, kippo adalah jenis honeypot yang bertujuan untuk mengamankan akses SSH.

Sulitnya mengumpulkan data dari honeypot dibutuhkan Modern Honey Network (MHN). MHN digunakan untuk mengatur, mengelola honeypot dan mudah diimplementasikan pada sistem berbasis open source.Untuk menangani masalah di atas membutuhkan honeypot dengan modern honey network, sehingga dapat melindungi server asli dari penyerang

2. Dasar Teori

Honeypot

Honeypot adalah suatu cara untuk menjebak atau menangkal usaha – usaha penggunaan tak terotorisasi dalam sebuah system informasi [1].

Honeypot merupakan pengalih perhatian hacker, agar seolah-olah berhasil menjebol dan mengambil data dari sebuah jaringan, padahal sesungguhnya data tersebut tidak penting dan lokasi tersebut sudah terisolir.

Adapun kegunaan honeypot adalah software keamanan open source yang berguna untuk diserang, diselidiki.

Honeypot terbagi oleh beberapa klasifikasi yaitu :

a. *Low-Interaction Honeypot* merupakan honeypot dengan tingkat interaksi *honeypot*, yang didesain untuk mengemulasikan service (layanan) seperti *server* yang asli. Penyerang hanya mampu memeriksa dan terkoneksi ke satu atau beberapa port
b. *High-interaction honeypot* terdapat system opeasi dimana penyerang dapat berinteraksi langsung dan tidak mempunyai batasan yang dapat membatasi interaksi tersebut. Dengan kata lain jenis *honeypot* ini membuat *server* palsu yang menyerupai dengan *server* asli, sehingga penyerang tidak mencurigai saat terjadi penyerang [2].

Dionaea

Dionaea adalah jenis Honeypot yang dapat memberikan layanan jaringan yang nantinya dapat dieksploitasi. Tujuan dari Dionaea adalah untuk mendapatkan salinan dari malware yang telah dikirim oleh penyerang, sehingga seorang administator dapat memutuskan sesuatu untuk melindungi sistem induk, bahkan menciptakan anti virus baru. [3]

Honeypot Dionaea ini ditaruh dengan pengaman minimal agar mudah diserang hacker dan disusupin segala jenis malware. Server honeypot ini akan mengamati aktivitas malware-malware yang telah tertangkap sebelumnya. Honeypot Dionaea itu fungsinya hanya sebagai perangkap saja, pihak-pihak yang memasang honeypot Dionaea itu sengaja membuat server yang mudah di tembus, sehingga memancing malware untuk menginfeksi komputer itu. Di dalam honeypot ini nanti malware-malware yang sudah masuk akan direkam aktivitasnya dan datanya disimpan. Data ini nantinya dapat dianalisa untuk mempelajari tentang laku malware atau dikirim keperusahaan antivirus untuk dibuat penangkalnya[4].

Kippo

Kippo merupakan salah satu tools honeypot ssh yang berfungsi sebagai server palsu yang termasuk dalam kategori medium-interaction, menurut [5] medium interaction adalah suatu layanan interaksi yang dapat berinteraksi dengan cara memberi tanggapan terhadap serangan yang dilakukan penyerang saat mencoba memberi worm ke dalam sistem komputer. Kippo Honeypot sendiri merupakan sistem yang sengaja dirancang untuk menjebak peretas yang ingin mencoba masuk ke sistem komputer asli, selain berguna sebagai penjebak tools ini juga dapat digunakan untuk membantu para admin untuk memonitoring dan menganalisa apa saja yang dilakukan peretas untuk masuk ke sistem komputer [6].

Modern Honey Network

Modern Honey Network (MHN) adalah software open source yang di buat oleh perusahaan ThreatStream, yang bertujuan untuk mempermudah menginstalasi honeypot. Adapun kegunaan dari Modern Honey Network (MHN) ini adalah mengelola dan menganalisa data dari honeypot tersebut dan mempermudah membangun honeypot baru dan mengambil data. Ada beberapa honeypot yang sudah terintergrasi oleh Modern Honey Network (MHN) antara lain hpfeed, nmomesyne, honeymap, MongoDB, dionaea, conpot, snort, kippo, glastopf, amun, dan wordpot [7].

3. Analisis dan Perancangan

Analisis Gambaran Saat Ini

Berdasarkan dari berbagai informasi sebagai acuan untuk pembuatan Adapun penjelasan dari topologi di atas menjelaskan bahwa internet tidak cukup aman. Karena internet terhubung hanya dengan firewall yang berguna untuk menangkal serangan dari luar. Setelah itu terhubung ke router untuk memasuki ke intranet langsung terhubung ke switch dan komputer. Sebagaimana penjelasan di atas tidaklah terlalu aman, karena jika ada serangan dari luar langsung menyerang ke data yang asli, sehingga data tersebut dapat disalahgunakan.

Analisi Gambaran Sistem Usulan

Pada topologi yang diusulkan ini **bahwa internet terhubung dengan** firewall kemudian terhubungkan dengan router dan server honeypot, MHN, kemudian terhubung dengan switch dan pc, sebagaimana mestinya honeypot berguna untuk menipu penyerang seolah-olah hacker menyerang server asli. Sebenarnya hacker hanya menyerang server palsu, dan pada data server asli aman dari serangan hacker.

Analisi Kebutuhan Sistem

Berikut ini adalah kebutuhan sistem yang diperlukan untuk menyelesaikan Proyek Akhir ini.

a. Sistem ini membutuhkan Ip public untuk server MHN.

b. Honeypot kippo untuk menangkap serangan pada port ssh.

c. Software MHN untuk mengambil data dari sensor honeypot Kippo.

Software Perangkat Lunak

Software atau Perangkat Lunak yang dibutuhkan untuk membangun sistem adalah sebagai berikut

No	Jenis	Versi	Keterangan
1	*Modern Honeypot Network*		Software mengelola honeypot
2	*Kippo*		Software honeypot
3	*Ubuntu*	14.04	Software Operasi system
4	*Virtual Private Server (IP : 103.236.201 .227)*		Server Modern Honey Network
5	*Virtual Private Server (IP : 103.15.226. 90)*		Server honeypot *Dionaea*
6	*VPS (IP 31.220.57.1 9)*		Server *Honeypot Kippo*

Software Perangkat Keras

Hardware atau Perangkat Keras yang digunakan untuk membangun sistem adalah sebagai berikut.

No	Jenis	Jumlah	Keterangan
1	Laptop Acer aspire	1	Intel Core i3, 4 GB DDR, 500GB HDD
2	Modem Handphone	1	*Access point*

Perancangan Rencana Pengerjaan

Adapun tahap pengerjaan proyek akhir ini diantaranya :

a. Installasi ubuntu 14.04

b. Installasi Modern Honey Network (MHN) .

c. Konfigurasi Modern Honey Network (MHN).

d. Deploying sensor honeypot melalui MHN.

e. Melakukan dokumentasi terhadap installansi dan konfigurasi honeypot kippo dan Modern Honey Network (MHN).

Perancangan Rencara Pengujian

Pada Proyek Akhir ini terdapat rencana pengujian yang dilakukan, yaitu:

1. Melakukan serangan DoS attack menggunakan hping3 terhadap sensor honeypot.

2. Melakukan serangan dictionary attack menggunakan hydra terhadap sensor honeypotPerangkat Keras.

4. Implementasi Dan Pengujian

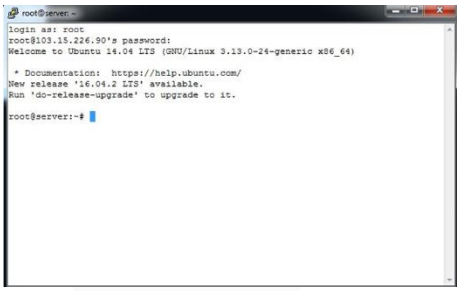
Pada bab ini akan menjelaskan tentang langkah-langkah implementasi honeypot dengan modern honey network terdiri dari installasi ubuntu 14.04, installing modern honey network, konfigurasi modern honey netwrok (MHN), deploying honeypot kippo. Setelah tahap instalasi selesai selanjutnya adalah tahap pengujian dengan melakukan penyerangan dari pihak luar.

Implementasi

Pada tahap ini menjelaskan mengenai langkah-langkah installasi ubuntu 14.04, installing modern honey network, konfigurasi modern honey netwrok (MHN), deploying honeypot kippo.

Installasi Ubuntu

Installasi ubuntu dilakukan dengan layanan VPS.



Instalasi dan Konfigurasi MHN

Pada tahap ini akan dijelaskan tentang instalasi dan konfigurasi Modern honey network.

1. Pilih Terminal Command.
2. Ketikan ssh dimas@93.188.163.149
3. Selanjutnya akan diminta untuk masukan password untuk login ke Virtual Private Server.
4. Ketikan su untuk masuk kedalam super user.
5. Akan dimintai password untuk untuk masuk root/superuser
6. Terlebih dahulu lakukan update dan upgrade sistem dengan perintah :

```
#apt-get update &&  apt-get upgrade
```

7. Setelah itu instalasi git dengan perintah :

```
#apt-get install git –y
```

8. Setelah terinstal git, pindah direktori dan clone mhn dari github.

```
#cd /opt
#git clone https://github.com/threatstream/mhn.git
```

1. Masuk ke dalam direktori mhn dengan perintah:

```
# cd /mhn
```

2. Setelah itu installasi modern honey network dengan perintah:

```
# ./install.sh
```

3. Setelah instalasi maka akan muncul konfigurasi seperti ini :

```
MHN Configuration
Superuser email: dimasdananglaksana@gmail.com
Superuser password :
Superuser password : (again) :
Server base url [http://93.188.163.149] : 93.188.163.149
Honeymap url [93.188.163.149:3000] :
93.188.163.149:3000
Mail server address [“localhost”] : localhost
Mail server port [25] : 25
Use TLS for email ? : y/n n
Use SSl for email ? : y/n n
Mail server username [“ “]:
Mail server password [“ “]:
Mail default sender [“ “]:
Path for log file [“var/log/mhn/mhn.log”]:
/var/log/mhn/mhn.log
```

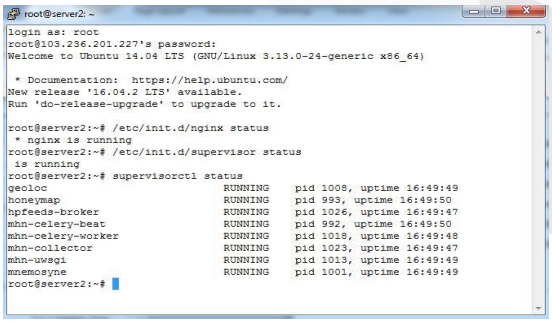
Keterangan:

a) Pada script nomer satu menjelaskan email superuser untuk login pada web modern honey network
b) Pada script nomer 2 dan 3 password untuk login pada web modern honeypot
c) Pada script nomer 4 adalah IP VPS untuk halaman web MHN
d) Selanjutnya IP honeymap
e) Pada script 6 sampai 12 untuk configurasi mail server bisa di kosongkan
f) Dan pada scripts 13 penyimpanan log mhn.

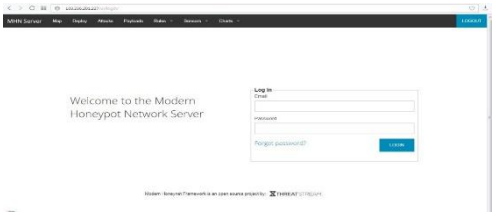
9. Lakukan pengecekan dengan perintah :

```
# /etc/init.d/nginx status
# /etc/init.d/supervisor status
# supervisorctl status
```

10. Setelah menjalankan script di atas akan keluar seperti ini, terdapat pada gambar 4-2:



11. Apabila sudah running, maka buka browser ketikan IP MHN dan masukan email superuser dan password akan muncul seperti ini, terdapat pada gambar 4-3:

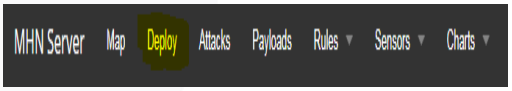


12. Akan muncul beranda seperti ini, terdapat pada gambar 4-4:

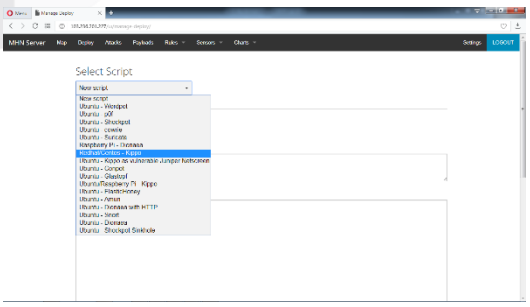
Pada tahap ini akan dijelaskan tentang installasi honeypot kippo melalui modern honey network.

1. Pertama, masuk halaman modern honey network seperti di atas, terdapat pada gambar 4- 5:

2. Klik menu deploy, terdapat pada gambar 4-6.

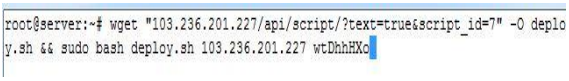


3. Pilih sensor honeypot kippo pada menu select script, terdapat pada gambar 4-7.

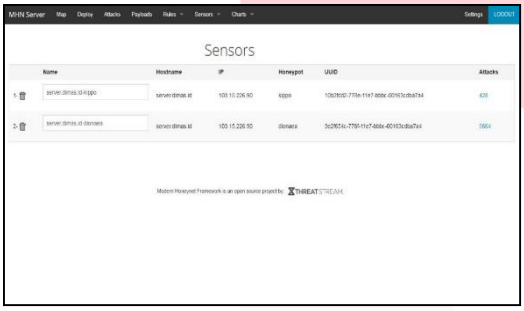


4. Setelah itu akan muncul tampilan seperti di bawah ini, terdapat pada gambar 4-8.

5. Copy deploy command dan paste ke vps sensor honeypot kippo , terdapat pada gambar 4-9.



6. Setelah instalasi kippo selesai cek pada web MHN menu view sensor akan menampilkan seperti ini, terdapat pada gambar 4-10:



7. Setelah menampilkan seperti itu sensor berhasil terinstall di MHN.

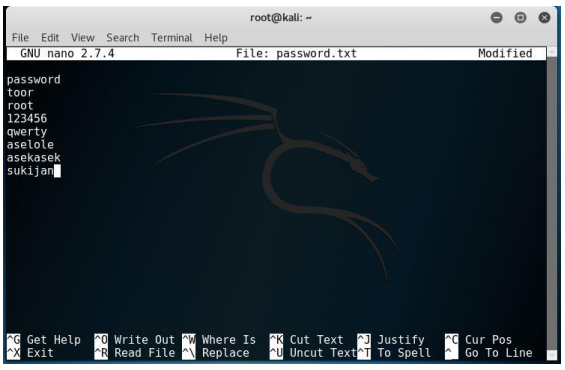
Pengujian

Setelah proses installasi selesai dilakukan selanjutnya adalah proses pengujian untuk mengetahui hasil implementasi yang sudah dikerjakan. Pengujian dilakukan dengan menggunakan tiga teknik serangan yaitu *dictionary attack, DoS attack* dan *Metasploit*.

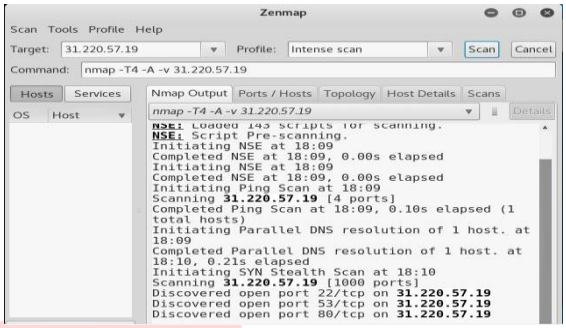
Pengujian pada *Dictionary Attack*

Melakukan pengujian *Dictionary Attack* menggunakan *tools Hydra* untuk mengetahui *username* dan *password* yang digunakan target. Langkah yang dilakukan adalah sebagai berikut :

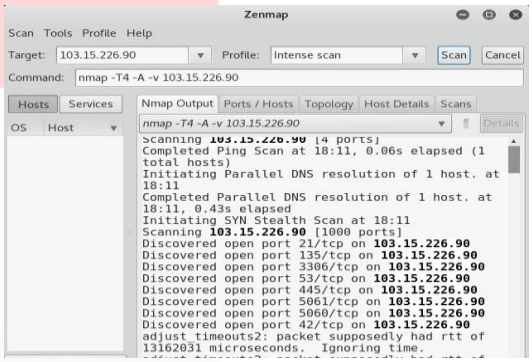
1. Pada gambar 4-11 adalah membuat *wordlist*. Sebelum melakukan serangan, terlebih dahulu membuat *wordlist* (kamus) untuk mencari kemungkinan *password* yang digunakan oleh target.



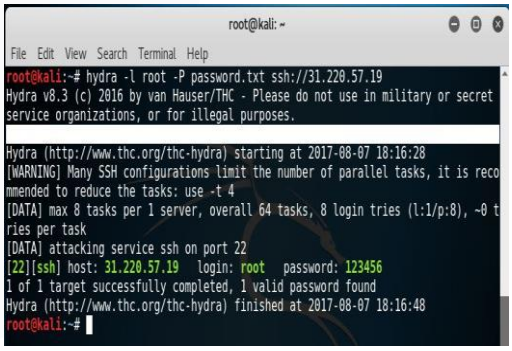
2. Pada gambar 4-12 adalah melakukan *port scanning* dengan menggunakan *zenmap* untuk mencari tahu port apa saja yang terbuka dengan memasukkan IP address *kippo*.



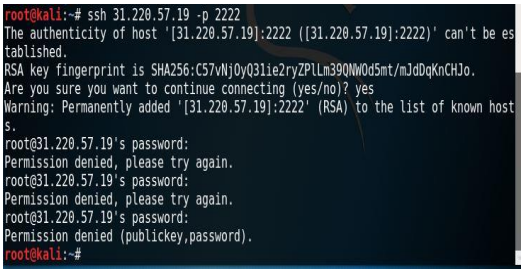
3. Pada gambar 4-13 adalah melakukan *port scanning* dengan menggunakan *zenmap* untuk mencari tahu port apa saja yang terbuka dengan memasukkan IP address *port dionaea*.



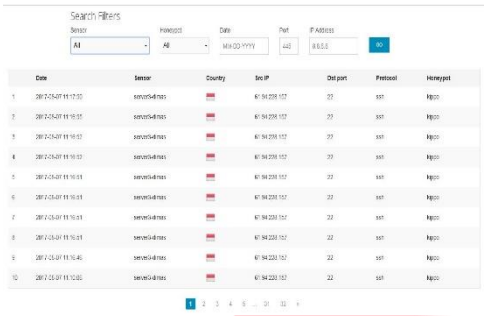
4. **Pada gambar 4-14 adalah melakukan serangan dengan menggunakan *tools hydra*, perintah yang digunakan yaitu #*hydra* –l *user* –P *wordlist.txt port://ip address*. Jika berhasil *hydra* akan menampilkan *password* dan *username* yang digunakan target.**



5. Pada gambar 4-15 adalah *password* dan *username* berhasil diketahui penyerang, selanjutnya penyerang mencoba untuk *login* menggunakan *password* dan *username* pada *server kippo*.



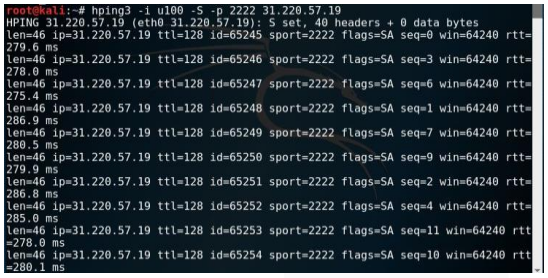
6. Pada gambar 4-16 adalah untuk mendeteksi hasil *login* yang dilakukan penyerang dapat dilihat di *file direktori log* pada *kippo* akan terlihat di *Modern Honey Network* (MHN) .



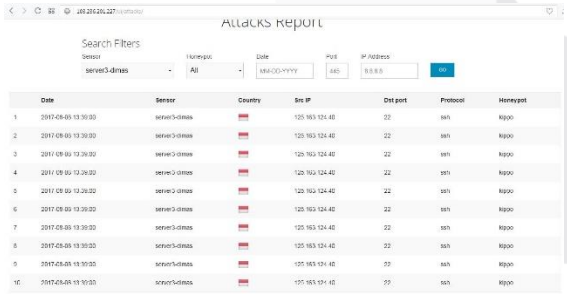
Pengujian pada *DoS Attack*

Pengujian serangan *Denial of Service* atau *DoS* Attack dilakukan dengan menggunakan *tools Hping3*. Serangan ini digunakan untuk mengetahui hasil deteksi yang dilakukan penyerang. Langkah untuk melakukan serangan *DoS* terhadap *Kippo* adalah sebagai berikut :

1. Pada gambar 4-17 adalah melakukan serangan dengan menggunakan perintah hping3 –i u100 –S –p [port] [IP Address]



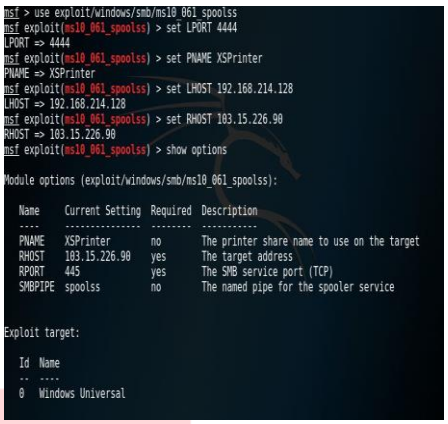
2. Pada gambar 4-18 adalah hasil *log* pada serangan *Denial of Service* terhadap *kippo* di *Modern Honey Network.*



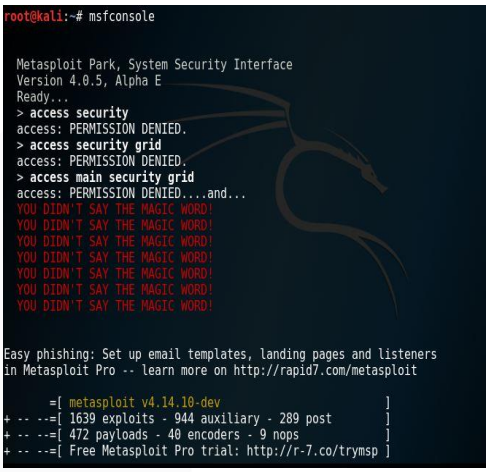
Pengujian pada *Metasploit*

Pengujian serangan pada *metasploit* untuk mengetes *dionaea*, apakah bisa menangkap *malware.* Langkah untuk melakukan serangan *metasploit* adalah sebagai berikut :

1. Pada gambar 4-19 adalah melakukan serangan dengan cara melakukan perintah *#msfconsole* pada kali *linux.*

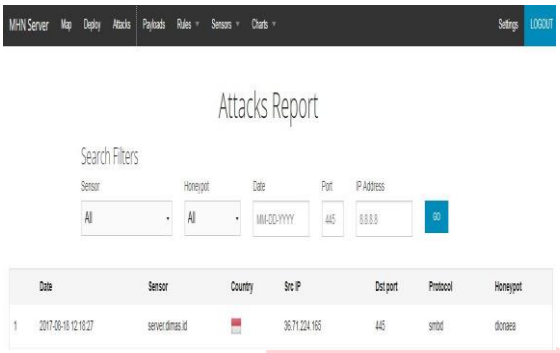


2. Pada gambar 4-20 adalah serangan dengan mengetikan *exploit/windows/smb/ms10_061_spoolss* setelah itu ketikan *set LPORT 4444,* setelah itu masukan set *PNAME* XSPrinter, sebagai nama *malware*, setelah itu masukan *set LHOST IP sendiri/ip* kali dengan cara *ifconfig*, ketikan *set RHOST Ip* korban.

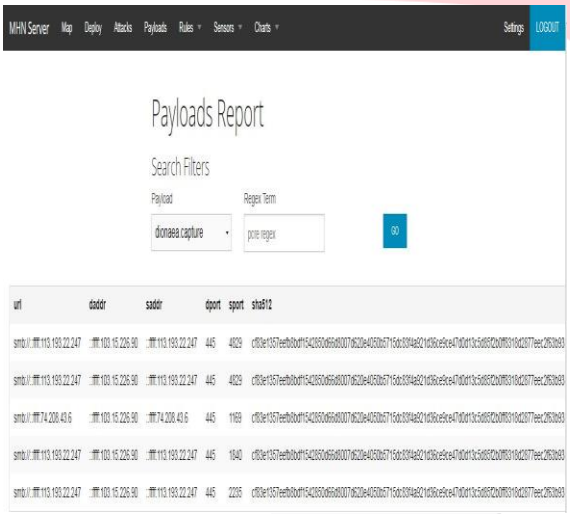


3. Pada gambar 4-21 adalah hasil dari setelah semua setting, untuk mengetikan exploit untuk menyerang korban.

1. Pada gambar 4-22 adalah hasil dari serangan *log dionea* pada MHN.



2. Pada gambar 4-23 adalah hasil serangan *payload dionaea* pada MHN. Akan tetapi sangat di sayangkan, bahwa hasil dari serangan ini tidak sesuai dengan yang diinginkan.



Kesimpulan

Berdasarkan hasil pengujian pada Bab 4, dapat disimpulkan sebagai berikut:

1. Sistem Modern Honey Network bertujuan untuk mengumpulkan log dari sensor kippo seperti negara, IP, waktu, port dan honeypot .
2. Honeypot kippo hanya dapat mendeteksi IP dari serangan.

Saran

Saran dari penulis untuk pengembangan Proyek Akhir ini adalah:

1. Modern honey network menggunakan dua atau lebih sensor honeypot.
2. Memakai sensor medium interaction honeypot atau high interaction honeypot.
3. Data pada MHN dapat terintegrasi dengan mail server.
4. Penjelasan tentang konsep *honeypot* untuk kedepannya lebih terperinci.
5. Diharapkan untuk kedepannya bisa memakai dua *honeypot* untuk satu VPS.

DAFTAR PUSTAKA

[1] L. Spitzner, "Honeypot : Tracking Hacker," in *Honeypot : Tracking Hacker*, Addison Wesley, 2002, p. 58.

[2] M. Riadi, "kajianpustaka.com," kajianpustaka.com, 24 July 2014. [Online]. Available: http://www.kajianpustaka.com/2014/07/pengertian-dan-klasifikasi-honeypot.html. [Accessed 15 januari 2017].

[3] D. Oktavianto, Cuckoo Malware Analysis, Birmingham: packt, 2013.

[4] E. Tan, "edgis-security.org," edgis-sercurity, 13 februari 2014. [Online]. Available: https://www.edgis-security.org/honeypot/dionaea/. [Accessed 15 januari 2017].

[5] A. Wahyuningsih, "Mengenal Honeypot Sebagai Tools Untuk Menjebak Hacker," Netsec.ID, 13 Maret 2017. [Online]. Available: https://netsec.id/honeypot/. [Accessed 26 Juni 2017].

[6] Lanuma Webid, "Pengertian Honeypot," Lanuma Webid, 5 May 2015. [Online]. Available: http://lanuma.web.id/honeypot-introduction/. [Accessed 2017 Juni 26].

[7] K. J. Higgins, "darkreading.com," darkreading.com, 19 juni 2014. [Online]. Available: http://www.darkreading.com/analytics/threat-intelligence/open-source-tool-aimed-at-propelling-honeypots-into-the-mainstream/d/d-id/1278726. [Accessed 15 januari 2017].