Implementasi *Honeypot Dionaea* Sebagai Uji Kerentanan dan Penunjang Keamanan Jaringan

Mohammad Fadhol[1], Ronald David Marcus[2]
[1,2]Sistem Informasi, Universitas Merdeka Malang. Jalan Terusan Dieng No. 62-64 Klojen, Pisang Candi, Kec. Sukun, Kota Malang, Jawa Timur 65146
e-mail: mfadhol07@gmail.com [1], redastrea800@gmail.com [2]

Kata Kunci:

Honeypot
Dionaea
Port
Komputer Server
Peretas

ABSTRAK

Perkembangan sumber daya ilmu pengetahuan yang berkembang pesat dalam dunia teknologi informasi memberikan manfaat yang besar terhadap kemajuan sumber daya manusia ini sendiri. Namun tidak sedikit juga masalah yang ditimbulkan oleh kemajuan ilmu pengetahuan teknologi informasi yang sangat pesat ini, salah satunya penyalahgunaan ilmu tersebut untuk meretas, merusak, dan mencuri sumber daya dari sebuah celah kerentanan *port* komputer *server*.*Honeypot* merupakan sistem yang sengaja digunakan untuk menjadi target sasaran penyerangan dari peretas. *Honeypot* akan menggunakan sumber daya *port* manipulasi sebagai sebuah cara untuk menjebak dan merekam informasi penetrasi dan serangan yang masuk. Implementasi *Honeypot Dionaea* ini sangat penting untuk meningkatkan potensi bertahan dari berbagai jenis serangan yang masuk melalui *port* komputer *server*.Dengan diimplementasikan sistem *Honeypot* tersebut, sebuah port manipulasi dapat melayani serangan yang dilakukan oleh peretas dalam melakukan penetrasi terhadap komputer yang diduga sebagai server tersebut. Sehingga komputer server akan lebih terjaga keamanannya dari segala celah-celah yang ada khususnya celah kerentanan dari sebuah *port*.

Keyword:

Honeypot
Dionaea
Port
Komputer Server
Peretas

ABSTRACT

The development of rapidly growing scientific resources in the world of information technology provides great benefits to the progress of human resources themselves. However, there are also not a few problems caused by the rapid progress of information technology science, one of which is the misuse of this knowledge to hack, destroy, and steal resources from a server computer port vulnerability gap.Honeypot is a system that is deliberately used to become the target of attacks from hackers. Honeypots will use port manipulation resources as a way to trap and record incoming penetration and attack information. Implementation of the Dionaea Honeypot is very important to increase the potential to survive various types of attacks that enter through the server computer port.By implementing the Honeypot system, a port manipulation can serve attacks carried out by hackers in penetrating the computer suspected of being the server. So that the server computer will be more secure from all the gaps that exist, especially the vulnerability gap of a port.

PENDAHULUAN

Sistem komputer menjadi bagian yang sangat penting dan tidak dapat dipisahkan dari bidang pekerjaan manapun. *Internet* merupakan jaringan komputer yang bersifat publik. *Malware*

ISSN: 2598-0076

(*Malicious Software*) merupakan sebuah perangkat lunak yang dirancang dengan tujuan untuk masuk dan menyusupi sebuah sistem komputer, kemudian akan merusak sistem komputer tersebut. *Malware* dapat menyusup ke banyak komputer melalui jaringan *internet* seperti *e-mail*, *download file* dari *internet*, atau melalui program yang terinfeksi [1]. *Malware* yang dimaksut bisa dalam bentuk *virus*, *worm* dan *trojan* merupakan ancaman utama bagi keamanan sistem jaringan komputer. *Honeypot Dionaea* akan berpura-pura menjadi sumber daya yang memikat perhatian penyerang dalam suatu jaringan yang sama.

Honeypot adalah suatu system yang sengaja dikorbankan untuk menjadi sasaran penyerangan dari peretas. *Honeypot* juga berguna untuk membuang-buang sumber daya penyerang atau mengalihkan penyerangan dari sesuatu yang lebih berharga. Sistem tersebut dapat melayani serangan yang dilakukan oleh peretas dalam melakukan penetrasi terhadap server tersebut [2]. Implementasi *Honeypot* low *interaction* memanfaatkan dua aplikasi yang berbeda, yaitu *Dionaea* dan Honeyd berhasil membuat layanan palsu sebagai target serangan dan mencatat aktivitas yang dianggap dapat membahayakan sistem dan jaringan, namun tidak adanya interaksi lebih lanjut ketika penyerang berhasil mengeksploitasi dan masuk dalam *Honeypot* [3]**.**

Port scanning adalah proses yang digunakan untuk mencari *port-port* yang terbuka pada sistem komputer atau jaringan. *Port scanning* merupakan langkah awal serangan terhadap jaringan komputer. Dari keberhasilan melakukan *port scanning*, penyerang dapat melanjutkan serangan lanjutan ke jaringan komputer [4]. Tujuan utama dari setiap uji penetrasi adalah menemukan sistem jaringan yang membalas komunikasi jaringan sehingga dapat diketahui celah dari sistem tersebut dan dengan demikian menarik bagi seorang penguji penetrasi. Hal ini dapat dilakukan dengan menggunakan pemindai jaringan. Pemindai jaringan yang paling dikenal adalah *Nmap* [5].

Metasploit menyediakan antarmuka pengguna grafis dan baris perintah (*command-line interface*) yang memungkinkan para pengguna untuk menentukan dan mengontrol pengujian penetrasi dengan mudah. *Metasploit* juga memiliki *database* celah keamanan yang terus diperbarui, sehingga memudahkan para pengguna untuk menemukan celah keamanan pada sistem yang mereka uji. *Intrusion Detection System* (*IDS*) adalah sebuah sistem yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. Namun *IDS* sendiri tidak serta merta dapat menahan serangan para penyerang. Selain menggunakan cara konvensional tersebut pengamanan sistem jaringan dapat menggunakan *Honeypot* [6].

Dionaea menggunakan Bahasa pemrograman *Python* sebagai Bahasa *shellcode*, mendukung *Ipv6* dan *TLS*. *Dionaea* bertujuan untuk mendapatkan duplikasi data dari *malware* [7]. Perangkat lunak (*software*) cenderung memiliki celah kerentanan yang seringkali dieksploitasi oleh pihak yang tidak bertanggung jawab (peretas) untuk memperoleh informasi, data yang memberikan keuntungan bagi peretas. Dari celah-celah keamanan yang muncul terutama melalui *port* jaringan, maka penulis menggunakan *Honeypot Dionaea* sebagai salah satu terobosan besar dalam menampik kerentanan-

ISSN: 2598-0076

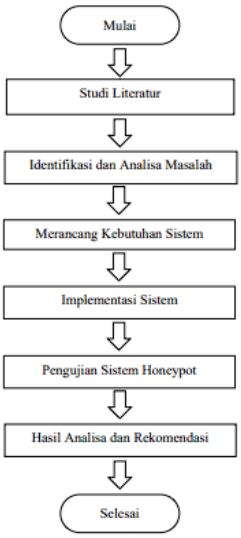
kerentanan *port* jaringan khususnya *port SMB* dan *RPC* yang akan dibahas pada penelitian ini, dan juga lebih meningkatkan keamanan pada komputer, terutama komputer *server*.

METODE

Metode yang digunakan dalam penelitian ini menggunakan 2 metode pengujian kerentanan, yaitu menggunakan *NMAP* dan *Metasploit* untuk mengekspose port dan eksploitasi port tersebut. Dengan menggunakan fitur *Honeypot DionaeaFR* untuk mendeteksi jenis serangan yang masuk pada *port* melalui jaringan.

Honeypot DionaeaFR diimplementasikan sebagai fitur deteksi Alamat *IP* pelaku penyerangan dan jenis eksploitasi yang digunakan untuk berusaha mengambil alih sistem. *Honeypot* adalah layanan *server* yang digunakan sebagai umpan dan perangkap untuk mengelabuhi *hacker*, sehingga *hacker* dapat menyerang target yang salah.

Dalam pengimplementasiannya, penulis menggunakan *Virtualbox* sebagai media untuk mempermudah dalam melakukan praktik dan pengembangan penelitian. Sehingga alat yang dibutuhkan dapat disesuaikan dengan spesifikasi komputer *host* yang ada tanpa merubah atau mengurangi implementasi metode pada keadaan yang sebenarnya.



Gambar 1. Kerangka Penelitian

Kerangka penelitian terdiri dari lima tahapan yang disusun dengan rincian sebagai berikut :

a. Studi literatur yaitu pengumpulan sumber-sumber informasi dan penelitian terdahulu yang berkaitan dengan topik pembahasan.

b. Identifikasi dan Analisa masalah, dilakukan untuk menentukan dan mendalami masalah yang ada, sehingga penulis mengetahui secara terperinci terkait permasalahan tersebut.

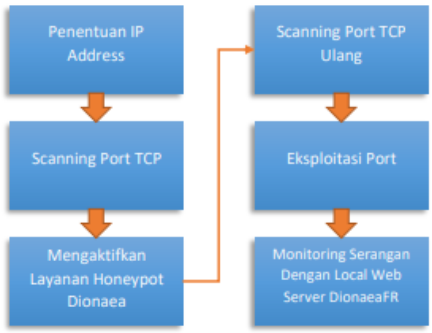
ISSN: 2598-0076

c. Merancang kebutuhan sistem, seperti menyiapkan sistem operasi perangkat lunak yang dibutuhkan untuk menunjang simulasi pemecahan masalah yang telah diidentifikasi dan dianalisa.

d. Implementasi sistem, setelah rancangan kebutuhan sistem siap digunakan, selanjutnya diimplementasikan, sehingga metode pemecahan masalah dapat terlaksana.

e. Pengujian sistem *Honeypot*, pengujian ini dilakukan untuk mengukur seberapa besar pengaruh *Honeypot* dalam mengatasi dan memanipulasi penyerang terhadap port terbuka.

f. Hasil analisa dan rekomendasi, menunjukan hasil temuan permasalahan yang terjadi (mengekspose *port*, serangan *port*, dll) kemudian dari hasil Analisa permasalahan tersebut, penulis akan memberikan rekomendasi berupa *Honeypot Dionaea* untuk memanipulasi dan memikat peretas sehingga *port* yang sebenarnya akan digantikan dengan *port* manipulasi guna menangkap dan melacak pelaku penyerangan jaringan komputer.



Gambar 2. Alur Kerja Penelitian

Adapun alur kerja yang terdapat pada penelian ini terdiri dari 6 (enam) tahapan yang ada dibawah ini, yaitu:

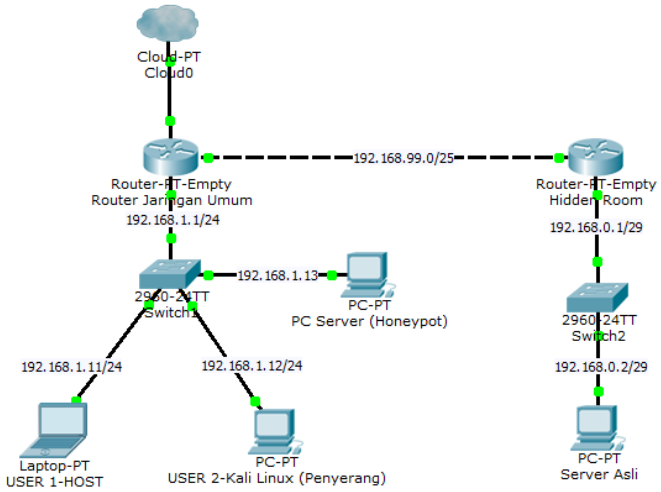
a. Penentuan *IP Address*, yaitu antara penyerang dan *Honeypot* telah terhubung dengan fasilitas jaringan yang sama atau juga dapat berbeda dengan catatan seorang penyerang memperoleh informasi *IP* yang dicurigai sebagai *server* (*honeypot*) sehingga dapat terkoneksi dengan *Honeypot* tersebut.
b. *Scanning Port TCP*, *Scanning port* pada tahap awal ini diperlukan untuk melihat perubahan visibilitas dan kondisi *port* sebelum sebuah *Honeypot* diaktifkan.
c. Mengaktifkan Layanan *Honeypot Dionaea*, Layanan *Honeypot* mulai diaktifkan untuk memikat perhatian dan menjebak seorang penyerang dengan mengekspose *port* manipulasi.

ISSN: 2598-0076

d. *Scanning Port TCP* Ulang, *Scanning port* ulang dilakukan untuk melihat perbedaan setelah layanan *honeypot* mulai diaktifkan.

e. Eksploitasi *Port*, dilakukan untuk mengeksploitasi/menyusupi sebuah serangan atau *malware* pada *port* yang telah diincar oleh penyerang sebagai titik vital untuk dilakukan serangan, dengan harapan dapat melumpuhkan layanan server secara sebagian atau penuh.

f. Monitoring Serangan dengan *Local Web DionaeaFR*, *Monitoring* serangan dengan menggunakan *local web DionaeaFR* ini berguna untuk melacak *port* yang dilakukan penyerangan, mengetahui jejak *IP Address* yang digunakan oleh penyerang dalam melakukan serangannya, jenis serangan yang digunakan, dan status dari serangan tersebut.



Gambar 3. Arsitektur Jaringan

Arsitektur jaringan digunakan untuk menggambarkan kondisi sebenarnya yang terjadi di lapangan, sehingga dapat diketahui dengan mudah posisi peletakan fisik dari *device* yang digunakan beserta pengalamatan *IP* nya.

Pada simulasi serangan yang dilakukan oleh sistem operasi kali linux terhadap *Honeypot* pada sistem operasi Honeydrive menggunakan *network bridge adapter* yang terhubung secara langsung dengan *router* melalui perantara komputer *Host*, sehinga keadaan sebenarnya pada sebuah serangan jaringan dapat digambarkan.

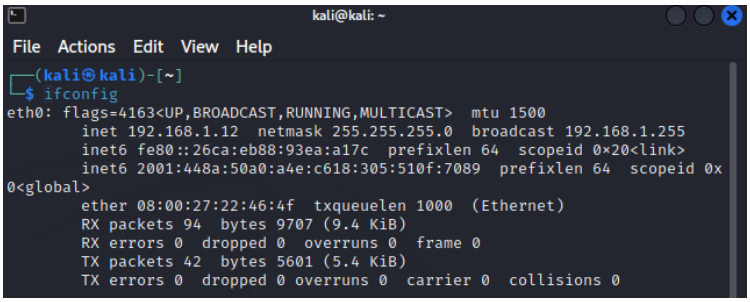
HASIL DAN PEMBAHASAN

1. Penentuan *IP Address*
   a. IP Address Kali Linux (Penyerang)

Penulis menetapkan *IP Address* (192.168.1.12) sebagai penyerang pada jurnal berdasarkan otomatisasi pengalamatan *IP* yang dilakukan oleh *network adapter bridge* pada saat terhubung ke

ISSN: 2598-0076

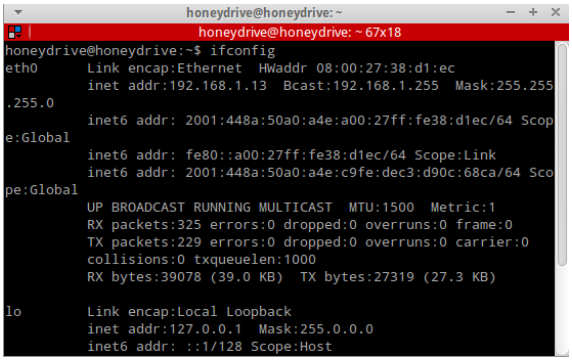
jaringan lokal. Ketikkan perintah "***ifconfig***" untuk memastikan *IP Address* yang diberikan kepada komputer.



Gambar 4. *IP Address Kali Linux*

b. IP Address HoneyDrive (*Honeypot*)

Penulis menetapkan *IP Address* (192.168.1.13) sebagai sasaran pada jurnal berdasarkan *otomatisasi* pengalamatan *IP* yang dilakukan oleh *network adapter bridge* pada saat terhubung ke jaringan lokal. Ketikkan perintah "***ifconfig***" untuk memastikan *IP Address* yang diberikan kepada komputer.



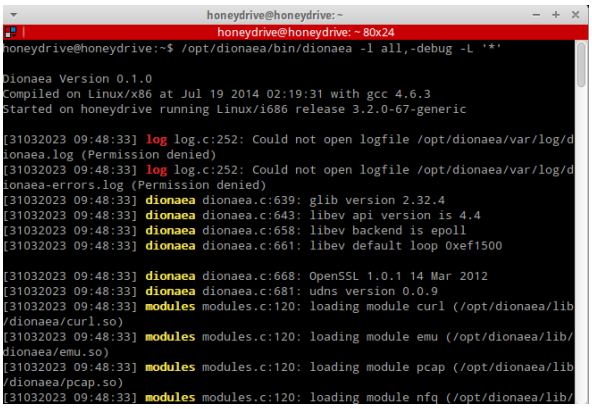
Gambar 5. *IP Address Honeydrive*

2. Implementasi *Honeypot*

a. Menjalankan Layanan *Dionaea*

Dionaea diimplementasikan pada sistem operasi *Honeydrive* yang masih berbasis *Linux* sehingga *command line interface* yang digunakan akan tetap sama dengan *distro linux* lainnya seperti *ubuntu, kali, dll*. Ketikkan perintah *"**/opt/dionaea/bind/dionaea -l all,-debug -L '*'**"*.

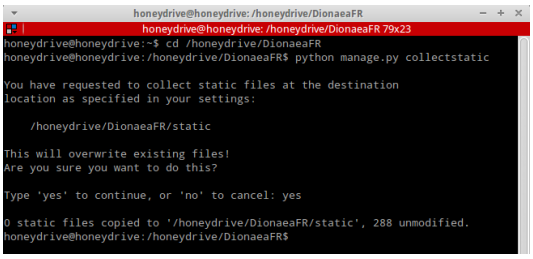
ISSN: 2598-0076



Gambar 6. Mengaktifkan *Dionaea*

Konfigurasi layanan *DionaeaFR*

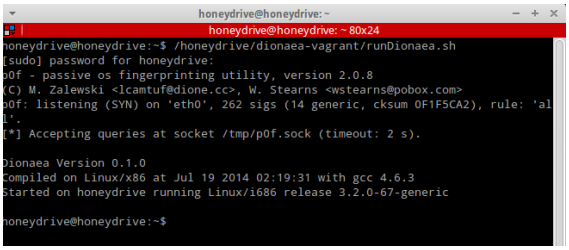
Lakukan pengumpulan data statis pada *DionaeaFR* dengan perintah "***python manage.py collectstatic***".



Gambar 7. Pengumpulan data statis

b. Menjalankan layanan *Dionaea.sh*

Jalankan layanan *Dionaea.sh* dengan perintah "***/honeydrive/Dionaea-vagrant/runDionaea.sh***". Pastikan hasil eksekusi perintah menampilkan pesan *Dionaea* ***compile*** dan ***started*** pada sistem operasi *Honeydrive.*

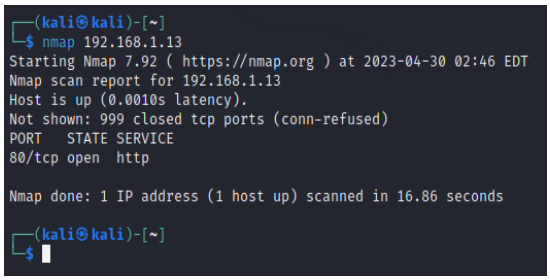


Gambar 8. Aktivasi *Dionaea.sh*

3. Proses penyerangan *Honeypot* menggunakan *Kali Linux*
   a. Pemindaian *port* terbuka menggunakan *NMAP*

Sebelum layanan *Dionaea* secara keseluruhan diaktifkan, maka pada dasarnya hasil *port scanning* yang dilakukan hanya akan menampilkan 1 buah *port* yang terdeteksi sebagai *port* yang terjadi kerentanan, yakni *port* 80 pada sistem operasi *HoneyDrive* yang digunakan oleh sistem tersebut untuk menjalankan layanan *http*.

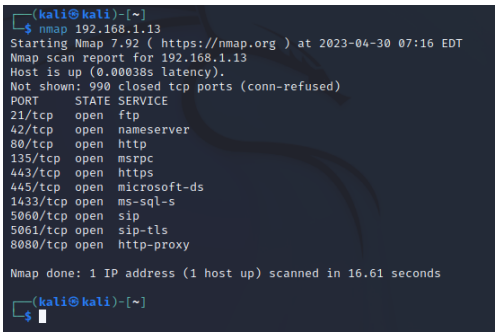
ISSN: 2598-0076



Gambar 9. Sebelum layanan *Dionaea* aktif

Dalam melakukan *port scanning* menggunakan metode *NMAP*, anda dapat dengan atau tanpa menggunakan akses *root*. lakukkan *port scanning* pada *IP* Address sasaran (sistem operasi *HoneyDrive)* dengan perintah **"*nmap 192.168.1.13*"**.

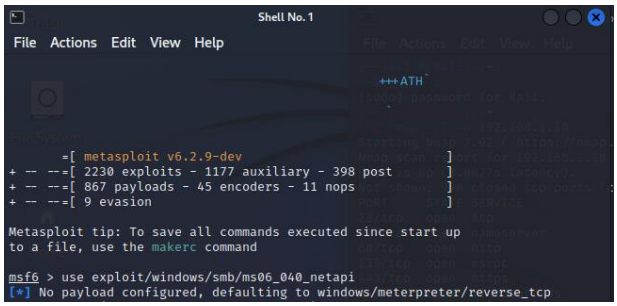
Honeypot akan mengelabuhi musuh atau pelaku yang ingin melakukan kejahatan dengan mengekspos seluruh informasi *port* rentan, sehingga ketika penyerang melakukan serangannya maka informasi penyerang akan tercatat oleh *Honeypot* dan tidak menimbulkan efek apapun setelah penyerang melakukan eksploitasi.



Gambar 10. kondisi setelah *Dionaea* aktif

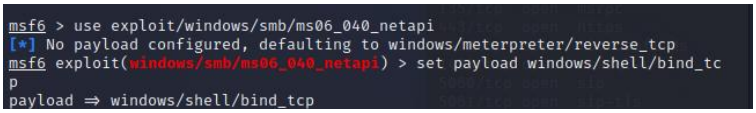
b. Proses penyerangan menggunakan *Metasploit*

Buka *Metasploit Framework* dan masukkan *password* pengguna untuk dapat menjalankan *Metasploit*. Setelah itu ketikkan "***use exploit/windows/smb/ms06_040_netapi"***



Gambar 11. Aktivasi *Metasploit*

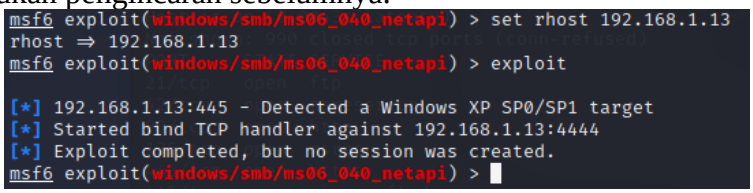
Setelah *console* berada pada *port ms06_040* selanjutnya ketikkan perintah "***set payload windows/shell/bind_tcp***".



Gambar 12. *Input port* untuk di*eksploitasi*

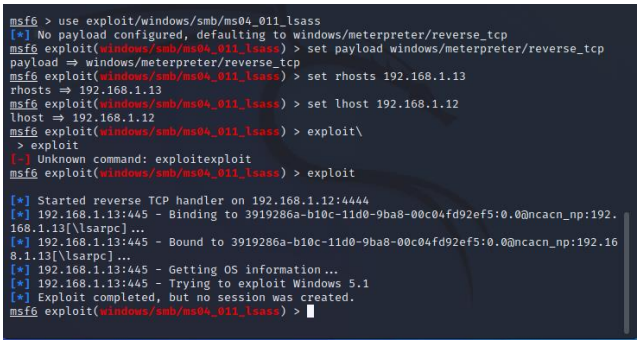
ISSN: 2598-0076

Selanjutnya ketikkan perintah "***set rhost 192.168.1.13***" pastikan *rhost* merupakan *IP Address target*. Lalu ketikkan "*exploit*" untuk mulai melakukan *eksploitasi* pada port yang telah dilakukan pengincaran sebelumnya.



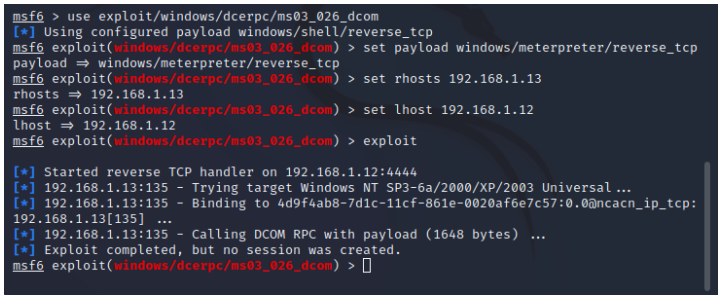
Gambar 13. Eksploitasi *port ms06_040_net*

Serangan kedua, kita akan melakukan eksploitasi terhadap *port ms04_011_lsass*. Ketikkan perintah *"**use exploit/windows/smb/ms_04_011_lsass**"*. Kemudian ketikkan *"**set payload windows/meterpreter/reverse_tcp**"*. Masukkan *IP* target pada ***rhost*** dan masukkan *IP* penyerang pada ***lhost***. Setelah selesai, ketikkan *exploit* untuk memulai eksplotasi terhadap *port smb* sistem operasi *honeydrive*.



Gambar 14. Eksploitasi *port ms04_011_lsass*

Serangan terakhir, eksploitasi menggunakan jenis serangan *dcerpc*. Dengan serangan ini memungkinkan untuk melakukan *remote* komputer lain dalam suatu jaringan. Ketikkan perintah *"**exploit/windows/dcerpc/ms03_026_dcom**"* kemudian ketikkan *"**set payload windows/meterpreter/reverse_tcp**"* lalu set *rhosts* ke *IP* target (192.168.1.13) dan set *lhost* ke *IP* penyerang (192.168.1.12). setelah selesai tahap terakhir yaitu mengetikkan perintah *exploit* untuk mulai mengirimkan serangan ke *IP* tujuan.

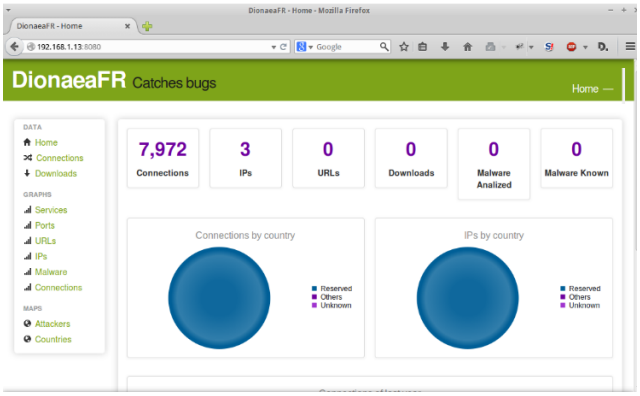


Gambar 15. Eksploitasi *port ms03_026_dcom*

ISSN: 2598-0076

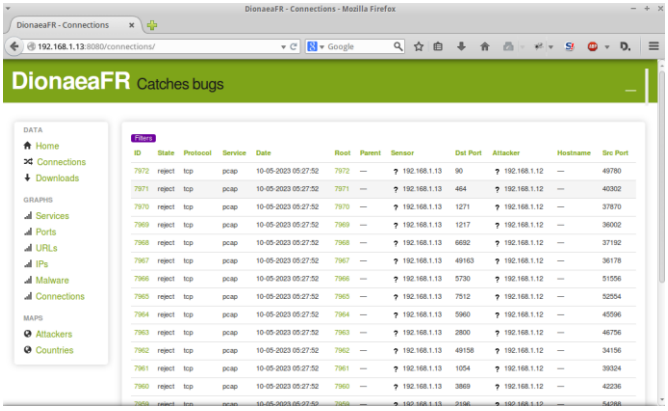
c. Pengecekan aktivitas serangan pada *DionaeaFR*

Setelah *Kali Linux* melancarkan serangan pada port terbuka sistem operasi *HoneyDrive 3* maka layanan *web* lokal *DionaeaFR* akan menunjukan bahwa telah terjadi sebuah serangan yang dilakukan oleh salah satu pengguna jaringan yang sama. Hal ini ditunjukan oleh indikator yang akan menunjukan perubahan data secara *real-time* berdasarkan serangan-serangan yang masuk pada *IP Address* dan *port* terbuka sistem operasi *HoneyDrive 3*.

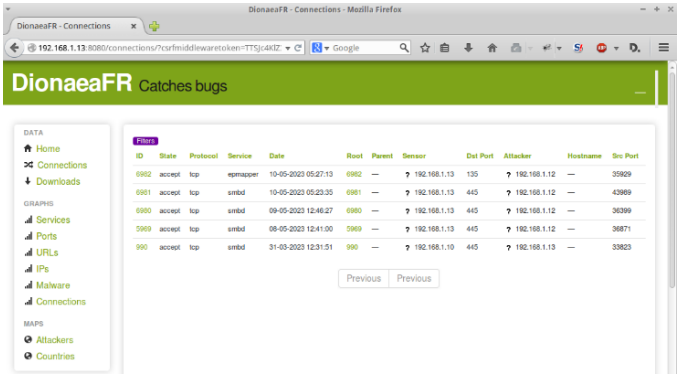


Gambar 16. *Monitoring* serangan

Antarmuka *Web DionaeaFR* akan mencatat seluruh jenis percobaan koneksi dan serangan yang masuk pada *port* manipulasi, sehingga seluruh informasi akan terlacak oleh *DionaeaFR*



Gambar 17. *Menu connection DionaeaFR*



Gambar 18. Slide 2 *menu connection*

ISSN: 2598-0076

SIMPULAN

Berdasarkan hasil perancangan, penilitian, dan pengujian yang telah dilakukan oleh Penulis terhadap **"Implementasi *Honeypot Dionaea* Sebagai Uji Kerentanan dan Penunjang Keamanan Jaringan"** maka dapat disimpulkan bahwa:

1. *Low-interaction Honeypot Dionaea* berhasil membuat layanan palsu berupa port terbuka sebagai penarik perhatian dan target utama serangan. Serta mengumpulkan informasi pelaku penyerangan yang melakukan serangan maupun aktivitas yang dapat membahayakan sistem keamanan jaringan ini sebagai suatu sistem keamanan tambahannya.
2. *NMAP* berhasil mendeteksi perbedaan sebelum dan sesudah layanan *Honeypot* aktif.
3. Serangan terhadap layanan *port* palsu *Dionaea* pada keamanan jaringan *virtual* dalam tingkatan *low interaction*, yakni *port scanning* dan eksploitasi layanan telah berhasil dijalankan dengan menggunakan sistem operasi *Kali Linux*.

DAFTAR RUJUKAN

[1] A. Tedyyana and S. Supria, "Perancangan Sistem Pendeteksi Dan Pencegahan Penyebaran Malware Melalui SMS Gateway," *INOVTEK Polbeng - Seri Inform.*, vol. 3, no. 1, p. 34, 2018, doi: 10.35314/isi.v3i1.340.

[2] P. Diebold, A. Hess, and G. Schäfer, "A honeypot architecture for detecting and analyzing unknown network attacks," *Inform. aktuell*, pp. 245–255, 2005, doi: 10.1007/3-540-27301-8_20.

[3] N. Arkaan and D. V. S. Y. Sakti, "Implementasi Low Interaction Honeypot Untuk Analisa Serangan Pada Protokol SSH," *J. Nas. Teknol. dan Sist. Inf.*, vol. 5, no. 2, pp. 112–120, 2019, doi: 10.25077/teknosi.v5i2.2019.112-120.

[4] M. Anif, S. Hws, and M. D. Huri, "Penerapan Intrusion Detection System (IDS) dengan metode Deteksi Port Scanning pada Jaringan Komputer di Politeknik Negeri Semarang," *J. TELE, Vol. 13 Nomor 1*, vol. 13, no. 1, pp. 25–30, 2015.

[5] F. Holik, J. Horalek, O. Marik, S. Neradova, and S. Zitta, "Effective penetration testing with Metasploit framework and methodologies," *CINTI 2014 - 15th IEEE Int. Symp. Comput. Intell. Informatics, Proc.*, pp. 237–242, 2014, doi: 10.1109/CINTI.2014.7028682.

[6] Sutarti, A. P. Pancaro, and F. I. Saputra, "Implementasi IDS (Intrusion Detection System) Pada Sistem Keamanan Jaringan SMAN 1 Cikeusal," *J. PROSISKO*, vol. 5, no. 1, pp. 1–8, 2018.

[7] Ion, "Visualizing Dionaea's results with DionaeaFR," 2015. https://bruteforce.gr/visualizing-dionaeas-results-with-dionaeafr.html

ISSN: 2598-0076