Analisa Perbandingan *Honeypot Cowrie* Dan *Honeypot Dionaea* Dalam Mendeteksi Serangan *Port Scanning* Dan *Brute Force*

Muhammad Afrinza Ramadhana [1], Atthariq [2], Guntur Syahputra [3]

[1,3] *Jurusan Tekniknologi Informasi dan Komputer Politeknik Negeri Lhokseumawe*
Jln. B.Aceh Medan Km.280 Buketrata 24301 INDONESIA

[1]afrinzam@gmail.com

[2] atthariq.huzaifah@pnl.ac.id

[3] guntursyahputra @pnl.ac.id

***Abstrak*— Teknologi Internet saat ini tidak lepas dari banyak masalah ataupun celah keamanan. Ancaman keamanan jaringan seperti serangan siber, pencurian data, dan gangguan layanan dapat berdampak negatif terhadap SMA Negeri 2 Dewantara. Oleh karena itu, SMA Negeri 2 Dewantara memerlukan penanganan untuk masalah tersebut. *Honeypot* merupakan *server* atau sistem jaringan yang dibuat seakan-akan mirip dengan sistem sebenarnya untuk dikorbankan karena memiliki sumber informasi data palsu untuk menjebak penyerang. Maka penting untuk mengetahui kelebihan dan kekurangan dari *Honeypot Cowrie* dan *Honeypot Dionaea* dalam mendeteksi serangan. Penelitian ini bertujuan untuk melakukan analisa perbandingan antara *Honeypot Cowrie* dan *Honeypot Dionaea* dalam mendeteksi serangan pada lingkungan jaringan. Data aktivitas dan serangan yang terdeteksi oleh kedua *honeypot* dikumpulkan dan dianalisis. Hasil penelitian menunjukkan bahwa pada penyerangan *port scanning*, *honeypot cowrie* memiliki 2 *port* yang terbuka sedangkan pada *honeypot dionaea* memiliki banyak *port* yang terbuka. Pada saat terjadi penyerangan dengan 10 *attacker* pada *server*, *server* menjadi sangat lambat, lumpuh, atau mungkin mati total. Hal ini dilakukan untuk melihat seberapa kuat atau tahan ketika terjadi penyerangan di *server* secara bersamaan. Tingkat keberhasilan *honeypot* dalam mengidentifikasi serangan yaitu *honeypot dionaea* sebanyak 91,8% untuk serangan *port scanning* dan 0% untuk serangan *brute force SSH*. Sedangkan *honeypot cowrie* sebanyak 8,2% untuk serangan *port scanning* dan 100% untuk serangan *brute force SSH*..**
Kata kunci*— *Honeypot, Cowrie, Dionaea, Server, Keamanan Jaringan.

Abstract*— *Current Internet technology is not free from many problems or security gaps. Network security threats such as cyber attacks, data theft, and service disruptions can have a negative impact on SMA Negeri 2 Dewantara. Therefore, SMA Negeri 2 Dewantara needs to address this problem. A honeypot is a server or network system that is made to appear similar to the real system to be sacrificed because it has a source of fake data information to trap attackers. So it is important to know the advantages and disadvantages of Honeypot Cowrie and Honeypot Dionaea in detecting attacks. This research aims to conduct a comparative analysis between Cowrie Honeypot and Dionaea Honeypot in detecting attacks in the network environment. Activity and attack data detected by both honeypots are collected and analyzed. The research results show that in the port scanning attack, the Cowrie honeypot has 2 open ports, while the Dionaea honeypot has many open ports. When an attack occurs with 10 attackers on a server, the server becomes very slow, paralyzed, or maybe completely dead. This is done to see how strong or resistant it is when an attack occurs on the server simultaneously. The honeypot success rate in identifying attacks, namely the dionaea honeypot, was 91.8% for port scanning attacks and 0% for SSH brute force attacks. Meanwhile honeypot cowrie was 8.2% for port scanning attacks and 100% for SSH brute force attacks.
***Keywords*— *Honeypot, Cowrie, Dionaea, Server, Network Security*.**

I. Pendahuluan

Seiring dengan peningkatan penggunaan teknologi di sekolah, muncul risiko yang perlu diatasi secara serius. Ancaman keamanan jaringan seperti serangan siber, pencurian data, dan gangguan layanan dapat berdampak negatif terhadap SMA Negeri 2 Dewantara. Oleh karena itu, penting bagi SMA Negeri 2 Dewantara untuk memahami dan mengelola risiko keamanan jaringan dengan baik.

Berdasarkan Badan Siber dan Sandi Negara (BSSN) mencatat sebanyak tidak kurang dari 370,02 juta serangan siber telah terjadi pada tahun 20222 . Jumlah tersebut meningkat 38,72% dari tahun sebelumnya yang sebanyak 266,74 juta serangan siber di tanah air. Hal tersebut tentu mengkhawatirkan bagi banyak orang, terlebih berbagai ancaman yang menyerang server mulai dari *port scanning* dan *denial of service* dapat membuat *server* lumpuh sehingga tidak dapat melayani berbagai permintaan dari *client*[1].

Dengan adanya permasalahan tersebut, diperlukan sistem keamanan jaringan yang dapat mendeteksi serta mencatat serangan dengan cepat. *Honeypot* merupakan sumber sistem informasi data yang bersifat terbuka, dan dibuat seakan-akan mirip dengan sistem sebenarnya untuk dikorbankan karena memiliki sumber informasi data palsu untuk menjebak penyerang. Dengan adanya *Honeypot*, segala aktivitas ilegal yang dilakukan oleh penyerang dapat digunakan administrator sebagai informasi tentang penyerang untuk menganalisis, serta

mempelajari aktivitas-aktivitas yang cenderung membahayakan sistem.

Penelitian ini bertujuan untuk melakukan analisa perbandingan antara *Honeypot Cowrie* dan *Honeypot Dionaea* dalam mendeteksi serangan pada lingkungan jaringan. Data aktivitas dan serangan yang terdeteksi oleh kedua *honeypot* dikumpulkan dan dianalisis.

Penelitian ini berkaitan dengan penelitian sebelumnya dengan judul "Implementasi *Low Interaction Honeypot* Untuk Peningkatan Keamanan *Server* dan Analisa Serangan Pada *Protokol SSH*.", Metode yang digunakan yaitu Studi Literatur Pada penelitian tersebut terdapat persamaan yaitu menggunakan *Honeypot Dionaea* Perbedaan yang terdapat pada penelitian tersebut adalah hanya memfokuskan pada analisis perbedaan *Honeypot Cowrie* dan *Honeypot Dionaea* [2].

Penelitian ini berkaitan dengan penelitian sebelumnya dengan judul "Implementasi *Low Interaction Honeypot* dan *Port Knocking* Untuk Meningkatkan Keamanan Jaringan". Menggunakan Metode Metode kualitatif Persamaan pada penelitian tersebut ialah menggunakan *Honeypot Dionaea* Perbedaan yang terdapat pada penelitian hanya memfokuskan pada analisis perbedaan Honeypot Cowrie dan Honeypot Dionaea. [3].

Penelitian ini berkaitan dengan penelitian sebelumnya dengan judul "Implementasi *Honeypot* Sebagai Sistem Keamanan Jaringan Pada *Virtual Private Server*" Menggunakan metode Observasi, wawancara dan Studi Literatur Pada penelitian tersebut terdapat persamaan yaitu menggunakan *Honeypot Dionaea* Perbedaan yang terdapat ialah hanya memfokuskan pada analisis perbedaan *Honeypot Cowrie* dan *Honeypot Dionaea*. [4].

Penelitian ini berkaitan dengan penelitian sebelumnya dengan judul "Implementasi *Honeypot* Menggunakan *Dionaea* dan *Kippo* sebagai Penunjang Keamanan Jaringan Komunikasi Komputer" metode yang digunakan Metode Waterfall model Persamaan yang terdapat ialah menggunakan *Honeypot Dionaea* Perbedaan yang terdapat ialah hanya memfokuskan pada analisis perbedaan *Honeypot Cowrie* dan *Honeypot Dionaea*. [5].

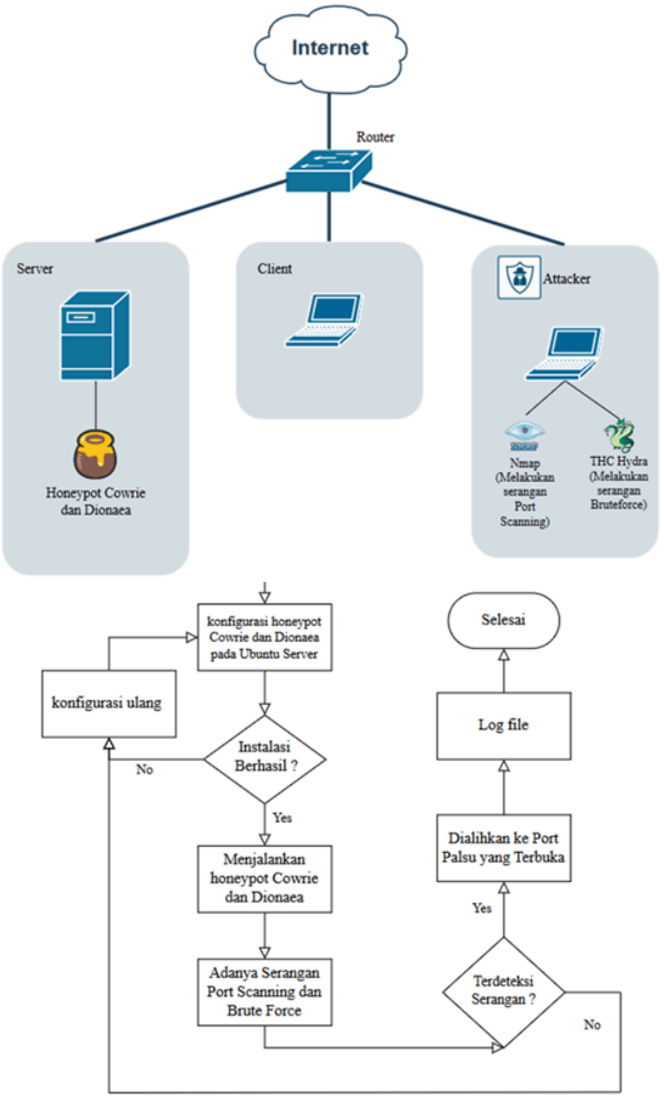
Penelitian ini berkaitan dengan penelitian sebelumnya dengan judul "Analisis Dan Implementasi *Honeypot* Dalam Mendeteksi Serangan *Distributed Denial-Of-Services* (*DDOS*) Pada Jaringan *Wireless*" Metode yang digunakan yaitu Metode kualitatif. Persamaan pada penelitian tersebut menggunakan *Honeypot Dionaea*, perbedaan yang terdapat pada penelitian ialah hanya memfokuskan pada analisis perbedaan *Honeypot Cowrie* dan *Honeypot Dionaea*. [6].

II. Metodologi Penelitian

Penelitian ini menggunakan tahapan pengumpulan data yang diperoleh melalui data primer dan sekunder. Untuk Pengumpulan data primer dilakukan karena data yang nanti akan didapat yaitu setelah melakukan penelitian pada sistem keamanan jaringan dengan pengujian *server Honeypot cowrie* dan *Honeypot Dionaea*. Dalam pengumpulan data yang diperlukan dalam penelitian ini, peneliti menggunakan data primer yakni data yang didapat dengan cara observasi. Dengan melakukan pengamatan secara langsung ke Lab SMA Negeri 2 Dewantara untuk mengumpulkan data yang diperlukan untuk melakukan penelitian.

A. Rancangan Sistem

Topologi yang digunakan adalah bentuk topologi star dimana jenis topologi jaringan komputer yang digunakan untuk menghubungkan perangkat-perangkat dalam jaringan terdapat pada Gambar 1.



Gambar 2. *Flowchart* Konfigurasi Sistem

Berdasarkan rancangan *flowchart* pada Gambar 2, menjelaskan bahwa konfigurasi sistem digunakan untuk membuat sistem pada pc *Server*. Tahap pertama adalah dengan mengkonfigurasi *honeypot cowrie* dan *dionaea* pada *ubuntu server*. Setelah itu apakah instalasi berhasil? jika tidak berhasil, maka harus di intsalasi ulang atau melakukan konfigurasi ulang pada instalasinya. Setelah itu menjalankan *honeypot cowrie* dan dionaea. Kemudian *attacker* menyerang

dengan serangan *port scanning* dan *brtute force.* Jika penyerangan tidak terdeteksi maka harus kembali melakukan instalasi ulang atau konfigurasi ulang. Jika berhasil maka akan dialihkan ke *port* palsu yang terbuka oleh *honeypot*. Kemudian *honeypot* menyimpan hasil serangan pada *server* atau *log file*.

C. *Honeypot*

Honeypot merupakan sumber sistem informasi data yang bersifat terbuka, dan dibuat seakan-akan mirip dengan sistem sebenarnya untuk dikorbankan karena memiliki sumber informasi data palsu untuk menjebak penyerang. Dengan adanya *Honeypot*, segala aktivitas ilegal yang dilakukan oleh penyerang dapat digunakan *administrator* sebagai informasi tentang penyerang untuk menganalisis, serta mempelajari aktivitas-aktivitas yang cenderung membahayakan sistem.

Dalam bahasa sederhana, *Honeypot* adalah sistem atau komputer yang sengaja dikorbankan untuk menjadi target serangan *hacker*. Oleh sebab itu setiap interaksi dengan *Honeypot* patut diduga sebagai aktivitas penyusupan. Misal, jika ada orang yang melakukan *scanning* jaringan untuk mencari komputer yang *vulnerable* (rentan), saat ia mencoba koneksi ke *Honeypot* tersebut, maka *Honeypot* akan mendeteksi dan mencatatnya, karena seharusnya tidak ada *user* yang berinteraksi dengan *Honeypot*[7].

D. *Cowrie*

Cowrie merupakan *honeypot* yang bejalan menyerupai *ssh* dan *telnet*. *Cowrie* akan mencatat serangan yang berasal dari *brute force* dan *shell interaction* kemudian menyimpan serangan *bruteforce* hasil *username* dan *password* yang telah dicobakan ke dalam *honeypot cowrie*. *Cowrie* juga mampu memberikan penyerang halaman *shell* yang berjalan dengan *user root*, *attacker* dapat melakukan apapun dengan *shell* tersebut namun tidak ada efek yang berjalan. Dalam *shell* tersebut semua aktifitas akan di rekam oleh *cowrie*. Serangan yang masuk pada *cowrie* dapat dipelajari dengan memanfaatkan hasil *log* dan *shell* interactionnya.

Cowrie adalah *honeypot* yang didesain untuk mengatasi masalah yang berhubungan dengan *ssh*/*telnet*. Seringkali *cowrie* digunakan untuk merekam aktivitas serangan *bruteforce* maupun *shell interaction*. Pada dasarnya *honeypot* ini merupakan evolusi dari *Kippo*. Namun karena pengumpulan data pada Kippo dirasa lebih sulit dan terlalu banyak *script* maka *cowrie* datang sebagai pembaharuan dari *honeypot* tersebut[8].

E. *Dionaea*

Dionaea adalah sebuah *low interaction honeypot* yang diciptakan sebagai pengganti *Nepenthes*. *Dionaea* menggunakan *python* sebagai bahasa *scripting*, menggunakan libemu untuk mendeteksi *shellcodes*, mendukung *ipv6* dan *tls*. *Dionaea* bertujuan untuk mendapatkan *copy* dari *malware*.

Attacker biasanya berkomunikasi dengan beberapa *service* dengan mengirimkan beberapa paket terlebih dahulu kemudian mengirimkan *payload*. *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 didownload dari *shellcode*, *Dionaea* akan mencoba untuk mendownload file. Setelah *Dionaea* mendapat salinan dari *worm attacker*, *Dionaea* akan menyimpan file lokal untuk analisa lebih lanjut, atau mengirimkan file ke beberapa pihak ke-3 untuk analisis lebih lanjut[9].

III. Hasil dan Pembahasan

Hasil penelitian hendaknya dituliskan secara jelas dan padat. Diskusi hendaknya menguraikan arti pentingnya hasil penelitian, bukan mengulanginya. Hindari penggunaan sitasi dan diskusi yang berlebihan tentang literatur yang telah dipublikasikan.

A. Pengujian *Honeypot Cowrie*

Data yang digunakan dalam analisis ini diperoleh dari implementasi Honeypot cowrie pada lingkungan jaringan lokal penelitian. Data mencakup aktivitas lalu lintas yang diterima oleh Honeypot cowrie selama periode penelitian. Pengujian ini dilakukan dengan 10 penyerang pada tanggal 18 September 2023 dengan beberapa serangan, seperti serangan port scanning dan Brute force.

1. Pengujian *Port Scanning*

Pada *honeypot cowrie* dilakukan pengujian *port scanning* digunakan untuk melihat *port – port* yang terbuka pada *server* yang sudah ditargetkan. Dengan serangan *port scanning* menggunakan *tool Nmap ip address* yang menjadi target serangan adalah 192.168.137.4.

Adapun hasil pengujian *Port Scanning* yang didapatkan selama percobaan sebagai berikut.

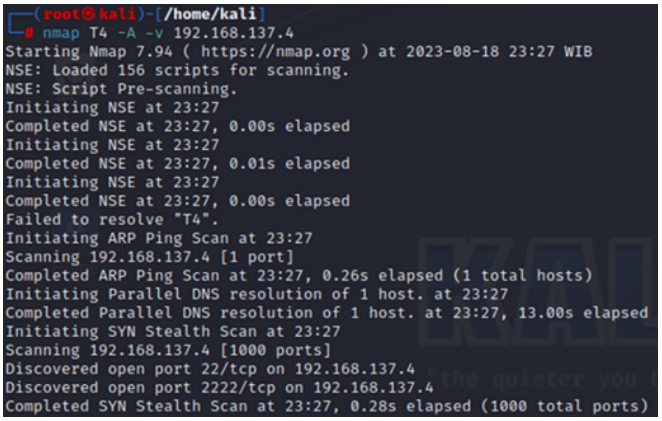
TABEL I

HASIL PENYERANGAN PORT SCANNING

No	Penyerang	Waktu	Ip Address
1	Penyerang ke 1	17 : 34	10.0.5.30
2	Penyerang ke 2	17 : 34	10.0.4.25
3	Penyerang ke 3	17 : 34	10.0.3.20
4	Penyerang ke 4	17 : 34	10.0.2.15
5	Penyerang ke 5	17 : 34	192.168.137.2
6	Penyerang ke 6	17 : 34	192.168.137.6
7	Penyerang ke 7	17 : 34	192.168.137.14
8	Penyerang ke 8	17 : 34	192.168.137.17

9	Penyerang ke 9	17 : 34	192.168.137.20
10	Penyerang ke 10	17 : 34	192.168.137.9

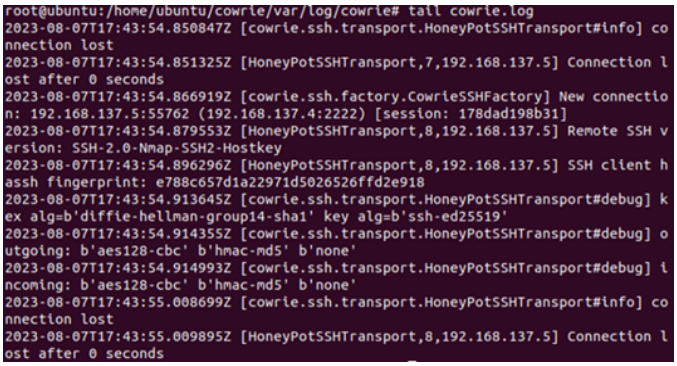
Dapat dilihat pada tabel 1 diatas, telah terjadi 10 penyerangan bersamaan dengan ip address yang berbeda-beda. Hal ini dilakukan untuk melihat seberapa kuat atau tahan ketika terjadi penyerangan di server secara bersamaan. Ketika sepuluh penyerang melancarkan serangan secara bersamaan, server menjadi sangat lamban, lumpuh, atau mungkin mati total.



Gambar 3. Pengujian *Port Scanning*

Dari hasil penyerangan pada gambar 3 dapat diketahui bahwa terdapat beberapa port yang terbuka yaitu port 22 dan port 2222 dimana keduanya termasuk dalam *protocol tcp*.

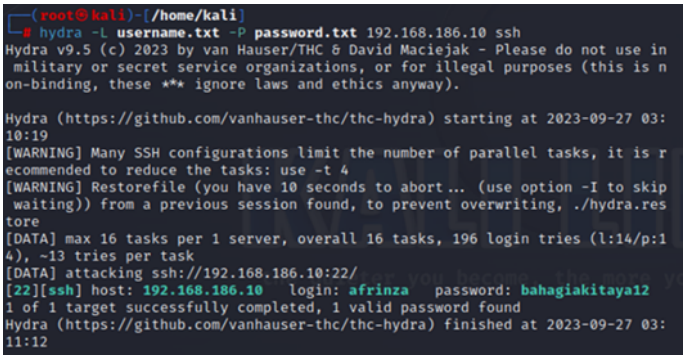
Berikut adalah tampilan dari server *honeypot cowrie* yang berhasil terekam pada saat *attacker* menyerang dengan menggunakan port scanning, bisa dilihat pada gambar 4.



Gambar 4. Hasil Penyerangan *Port Scanning*

2. Pengujian *Brute Force*

Kemudian pengujian selanjutnya adalah serangan *Bruteforce SSH* menggunakan *THC Hydra* seperti pada Gambar 5 *Script* atau perintah yang digunakan untuk melakukan penyerangan adalah '*hydra –L username.txt –P password.txt ssh://192.168.186.10'*. Sesuai dengan perintahnya bahwa penyerang sedang mencoba melakukan serangan *Bruteforce SSH* dengan menggunakan file *'username.txt'*, dimana file tersebut merupakan data list *password* dan *username* dari *attacker* yang sengaja dibuat untuk melakukan serangan *Bruteforce SSH*



Gambar 5. Pegujian *Brute Force*

Dari hasil pengujian penyerangan *Brute Force* pada gambar 5 tersebut dapat dilihat dari *THC Hydra* menampilkan *''[22][ssh] host:192.168.186.10 login:afrinza password:bahagiakitaya12"* dimana dari pernyataan tersebut dapat didapatkan informasi seperti *host* yang menyatakan *ip address* target, *login* yang menyatakan *username* dan *password* yang berisi *password* yang mungkin cocok

B. Pengujian *Honeypot Dionaea*

Sama halnya seperti *Honeypot Cowrie*, data yang digunakan dalam analisis ini diperoleh dari implementasi *Honeypot dionaea* pada lingkungan jaringan lokal penelitian. Data mencakup aktivitas lalu lintas yang diterima oleh *Honeypot dionaea* selama periode penelitian. Pengujian ini dilakukan dengan 10 penyerang pada tanggal 18 September 2023 dengan beberapa serangan, seperti serangan *port scanning* dan *Brute force*

1. Pengujian *Port Scanning*

Sama halnya dengan *cowrie*, pada *dioanea* dilakukan pengujian *port scanning* untuk melihat *port – port* yang terbuka pada *server* yang sudah di targetkan. Dengan serangan *port scanning* menggunakan *tool Nmap ip address* yang menjadi target serangan adalah 192.168.184.4. Adapun hasil pengujian *Port Scanning* yang didapatkan selama percobaan sebagai berikut:

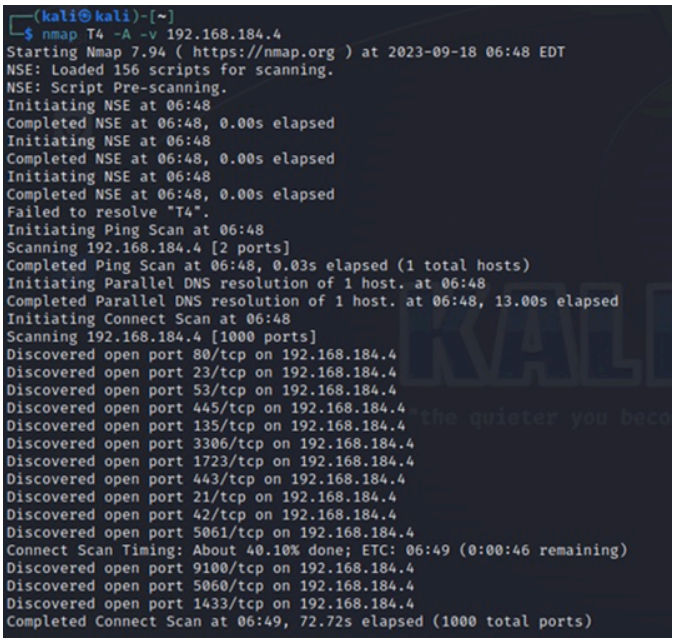
TABEL II

HASIL PENYERANGAN PORT SCANNING

No	Penyerang	Waktu	Ip Address
1	Penyerang ke 1	17 : 34	10.0.5.30
2	Penyerang ke 2	17 : 34	10.0.4.25
3	Penyerang ke 3	17 : 34	10.0.3.20
4	Penyerang ke 4	17 : 34	10.0.2.15

5	Penyerang ke 5	17 : 34	192.168.137.2
6	Penyerang ke 6	17 : 34	192.168.137.6
7	Penyerang ke 7	17 : 34	192.168.137.14
8	Penyerang ke 8	17 : 34	192.168.137.17
9	Penyerang ke 9	17 : 34	192.168.137.20
10	Penyerang ke 10	17 : 34	192.168.137.9

Dapat dilihat pada tabel 2 diatas, telah terjadi 10 penyerangan bersamaan dengan *ip address* yang berbeda-beda sama halnya seperti *Honeypot Cowrie*. Hal ini dilakukan untuk melihat seberapa kuat atau tahan ketika terjadi penyerangan di *server* secara bersamaan. Ketika sepuluh penyerang melancarkan serangan secara bersamaan, *server* menjadi sangat lambat, lumpuh, atau mungkin mati total



Gambar 6. Penyerangan *Port Scanning*

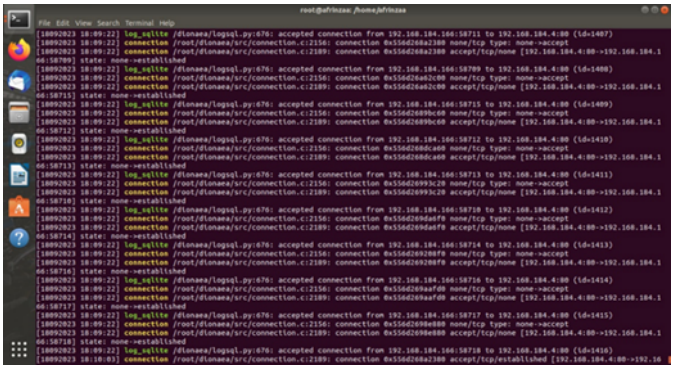
Dari hasil penyerangan pada gambar 6 dapat diketahui bahwa terdapat beberapa port yang terbuka, adapun port yang tercantum pada tabel 3 tersebut :

TABEL III
PORT TERBUKA

No	Port	Protokol
1.	21	ftp
2.	23	telnet
3.	42	Nameserver
4.	53	Domain
5.	80	http
6.	135	Msrpc
7.	443	Ssl/http
8.	445	Microsoft-ds
9.	1723	Pptp
10.	3306	Mysql
11.	5061	Ssl/sip

Beberapa dari *port* ini sengaja dibuat oleh *honeypot* untuk menipu *attacker*, agar *attacker* percaya bahwa semua *port* yang terbuka adalah milik *server* utama yang dibiarkan rentan terhadap penyerangan.

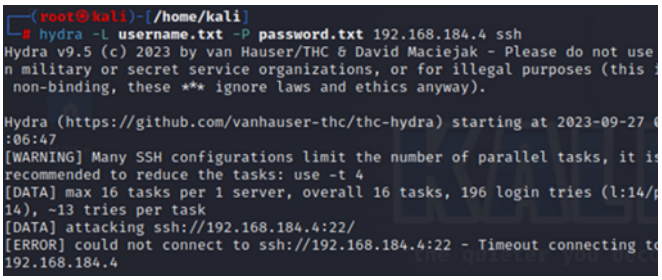
Berikut adalah tampilan dari server *honeypot dionaea* yang berhasil terekam pada saat attacker menyerang, bisa dilihat pada gambar 7.



Gambar 7. Tampilan Hasil Penyerangan

2. Pengujian *Brute Force*

Pengujian selanjutnya adalah serangan *Bruteforce SSH* dengan menggunakan *THC Hydra* seperti pada Gambar 8. Sama halnya seperti *cowrie*, *script* atau perintah yang digunakan untuk melakukan penyerangan adalah *'hydra –L username.txt –P password.txt ssh://192.168.184.4'*. Sesuai dengan perintahnya bahwa penyerang sedang mencoba melakukan serangan *Bruteforce SSH* dengan menggunakan file *'username.txt'*, dimana file tersebut merupakan data list *password* dan *username* dari *attacker* yang sengaja dibuat untuk melakukan serangan *Bruteforce SSH*.



Gambar 8. Penyerangan *Brute Force*

Dari hasil pengujian *brute force* dapat dilihat pada gambar 8. Penyerangan dari *THC Hydra* tidak dapat menampilkan hasil dari *username* dan *password* dari ip target 192.168.186.5 hal ini dikarenakan pada *server honeypot dionaea* tidak memiliki *port ssh*. Maka dari hal itu pada pengujian *brute force* tidak bisa digunakan pada *honeypot dionaea*.

IV. Kesimpulan

Berdasarkan hasil dan pembahasan pada penelitian yang telah dilakukan, maka dapat disimpulkan bahwa :

1. Pada penyerangan port scanning, honeypot cowrie tidak memerlukan waktu yang cukup lama pada saat scaning port dikarenakan hanya memiliki 2 port yang terbuka yaitu port 22 dan 2222. Berbeda halnya dengan honeypot dionaea yang lama dilakukan karena memiliki jumlah port terbuka yang banyak sehingga memerlukan waktu yang lebih lama sekitar 3 menit pada saat scaning port terjadi.
2. Pada saat terjadi penyerangan dengan 10 attacker pada server, server menjadi sangat lambat, lumpuh, atau mungkin mati total. Hal ini dilakukan untuk melihat seberapa kuat atau tahan ketika terjadi penyerangan di server secara bersamaan.
3. Tingkat keberhasilan *honeypot* dalam mengidentifikasi serangan yaitu *honeypot dionaea* sebanyak 91,8% untuk serangan *port scanning* dan 0% untuk serangan *brute force SSH*. Sedangkan *honeypot cowrie* sebanyak 8,2% untuk serangan *port scanning* dan 100% untuk serangan *brute force SSH*.

Referensi

[1] F. S. Pratiwi, "BSSN Catat 370,02 Juta Serangan Siber ke Indonesia pada 2022," *dataindonesia.id*, 2023. https://dataindonesia.id/digital/detail/bssn-catat-37002-juta-serangan-siber-ke-indonesia-pada-2022 (accessed Jul. 09, 2023).

[2] N.Arkaan and D.V. Shaka Yudha, "Implementasi Low Interaction Honeypot Untuk Peningkatan Keamanan Server dan Analisa Serangan Pada Protokol SSH" TEKNOSI, vol. 05, no. 02, 2019.

[3] R.D. Yulian, "Implementasi *Low Interaction Honeypot* dan *Port Knocking* Untuk Meningkatkan Keamanan Jaringan", vol. 02, no. 1. 2022.

[4] W. A. Sulaksono and C. E. Suharyanto, "Implementasi Honeypot Sebagai Sistem Keamanan Jaringan Pada Virtual Private Server," InfoTekJar J. Nas. Inform. dan Teknol. Jar., vol. 5, no. 1, pp. 90–95, 2020.

[5] A. W. Wastumirad and M. I. Darmawan, "Implementasi *Honeypot* Menggunakan *Dionaea* dan *Kippo* sebagai Penunjang Keamanan Jaringan Komunikasi Komputer," Teknologi., vol. 0, no. 1, 2021.

[6] B. Mardiyanto, T. Indriyani, and I. M. Suartana, "Analisis Dan Implementasi *Honeypot* Dalam Mendeteksi Serangan *Distributed Denial-Of-Services* (*DDOS*) Pada Jaringan *Wireless*," Integer Journal., vol. 01, no. 05, pp. 19–23, 2019.

[7] M. Mispriatin, J. G. A. Ginting, and B. Arifwidodo, "Analisis Kinerja Honeypot Dionaea Dan Cowrie Dalam Mendeteksi Serangan," Pros. Semin. Nas. Teknoka, vol. 6, no. 2502, pp. 170–178, 2022.

[8] W. A. Sulaksono and C. E. Suharyanto, "Implementasi Honeypot Sebagai Sistem Keamanan Jaringan Pada Virtual Private Server," InfoTekJar J. Nas. Inform. dan Teknol. Jar., vol. 5, no. 1, pp. 90–95, 2020.

[9] Mispriatin, M., Ginting, J. G. A., & Arifwidodo, B. (2022). Analisis Kinerja Honeypot Dionaea Dan Cowrie Dalam Mendeteksi Serangan. Prosiding Seminar Nasional Teknoka, 6(2502), 170–178.

[10] M. Shell. (2002) IEEEtran homepage on CTAN. [Online]. Available: http://www.ctan.org/tex-archive/macros/latex/contrib/supported/IEEEtran/

[11] *FLEXChip Signal Processor (MC68175/D)*, Motorola, 1996.

[12] "PDCA12-70 data sheet," Opto Speed SA, Mezzovico, Switzerland.

[13] A. Karnik, "Performance of TCP congestion control with rate feedback: TCP/ABR and rate adaptive TCP/IP," M. Eng. thesis, Indian Institute of Science, Bangalore, India, Jan. 1999.

[14] J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control," Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.

[15] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Std. 802.11, 1997.