Paper

Simulasi Pengamanan Virtual Server Menggunakan Dionaea Honeypot Dan Tunneling Sebagai Proses Pengamanan Komunikasi Data

Author: Nauval Alfarizi, T. M. Diansyah, Risko Liza

ISNN: 2964-1950

Simulasi Pengamanan Virtual Server Menggunakan Dionaea Honeypot Dan Tunneling Sebagai Proses Pengamanan Komunikasi Data

Nauval Alfarizi[1*], T. M. Diansyah[2], Risko Liza[3]
[1,2,3]Universitas Harapan, Medan, Indonesia
[1*]nauvalalfarizi026@gmail.com, [2]dian.10.22@gmail.com, [3]risko.liza@gmail.com
[1)] nauvalalfarizi026@gmail.com

Abstrak

kejahatan siber dilakukan bertujuan untuk dapat memperoleh informasi, dimana informasi yang diperoleh dijadikan sebagai suatu sumber *data* dalam melakukan suatu penyerangan. Penyerangan pada umumnya mengarah kedalam berbagai lingkup ruang dimulai dari *server* fisik hingga *virtual server*. Penelitian ini dilakukan penulis untuk dapat melakukan Proses implementasi perancangan berbasis pengembangan kualitatif terhadap teknologi yang sudah ada yaitu rancang bangun sistem *virtual server* menggunakan *dionaea honeypot* dan PPTP *tunneling* dalam melakukan sebuah bentuk pengamanan terhadap komunikasi *data* yang dapat menutupi kerentanan terhadap suatu perangkat pada *virtual server*. Hasil dari penelitian yang penulis lakukan menunjukkan adanya sebuah perbedaan dalam tiap pengujian penyerangan. Ketika sebuah percobaan penyerangan dilakukan kedalam tiap *port* yang tidak terkonfigurasi pada layananan utama pada *virtual server* didapat hasil penyerangan yaitu dapat melakukan pendeteksian terhadap *intruder* dan sebaliknya.

Kata Kunci: Penyimpanan *Virtual, Honeypot,* Terowongan

Abstract

Cybercrime is carried out to obtain information, where the information obtained is used as a source of data in carrying out an attack. Attacks generally lead to various scopes ranging from physical servers to virtual servers. This research was conducted by the author to be able to carry out the implementation process based on qualitative development of existing technology, namely the design of a virtual server system using Dionaea honeypot and PPTP tunneling in carrying out a form of security for data communication that can cover vulnerabilities to a device on a virtual server. The results of the research that the author conducted showed that there was a difference in each attack test. When an attack attempt is carried out into each port that is not configured on the main service on the virtual server, the results of the attack are that it can detect intruders and vice versa.

Keywords: *Virtual Server, Dynamic Honeypot, Tunneling*

1. PENDAHULUAN

Masyarakat semakin bergerak dinamis dan terlibat langsung dalam perkembangan teknologi dalam kehidupan seharinya. Perkembangan teknologi ini tidak hanya menimbulkan dampak positif bagi masyarakat, namun perkembangan teknologi juga menimbulkan dampak yang negatif dengan munculnya bentuk kejahatan baru yang belum pernah terjadi sebelumnya. Salah satu contoh bentuk kejahatan yang sering terjadi adalah dengan melakukan perusakan perangkat pada *virtual server*.

Untuk mengatasi permasalahan yang terjadi akibat penyerangan yang dilakukan pada perangkat *virtual server* tersebut, penulis menerapkan kombinasi pengamanan *data* dengan menggunakan implementasi teknologi berupa aplikasi *dionaea honeypot* dan PPTP *tunnel* sebagai jalur aman dalam melakukan proses komunikasi *data*.

Cara kerja *honeypot* bergantung pada tingkat interaksi yang dilakukan. *Dionaea honeypot* merupakan sebuah aplikasi yang dikategorikan sebagai *low interaction honeypot*, dimana *honeypot* tersebut dapat bekerja dengan menggunakan sistem operasi yang dapat melakukan emulasi dengan meniru berbagai layanan yang ada pada sistem dan membuat *Dionaea* berfungsi sebagai *honeypot* dapat terlihat rentan untuk dilakukan sebuah penyerangan [1].

VPN dibutuhkan untuk dapat melakukan koneksi *dial up* terhadap proses komunikasi. PPTP bekerja dengan sebuah *server* yang dapat berfungsi sebagai penghubung antar komputer yang dapat diketahui sebagai *client*, baik komputer yang berada di wilayah pusat maupun komputer yang berada di wilayah cabang [2].

Pada penelitian yang dilakukan sebelumnya, menyatakan bahwa penggunaan dari *Dionaea honeypot* sebagai sebuah aplikasi yang dapat meniru layanan yang ada pada *virtual server* dapat mampu mendeteksi sebuah proses penyerangan yang dilakukan. Penggunaan dari *virtual server* dapat dilakukan upaya konfigurasi menggunakan *Dionaea honeypot* sebagai proteksi yang bertujuan sebagai sasaran eksploitasi dalam proses penyerangan yang dilakukan oleh *intruder* [3].

ISNN: 2964-1950

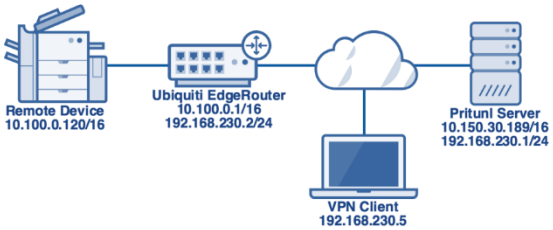
Pada penelitian yang dilakukan sebelumnya, juga mengatakan bahwa penggunaan dari sebuah *firewall* dapat dilakukan dengan proses implementasi penggunaan terhadap aplikasi dari sebuah *honeypot* yang bertujuan untuk memberi proteksi lebih terhadap *virtual server* [4].

Pada penelitian yang dilakukan sebelumnya, mengatakan bahwa teknologi PPTP merupakan sebuah protokol jaringan khusus yang dikembangkan oleh *Microsoft* dan *Cisco* yang bertujuan melakukan proses pengamanan dalam melakukan komunikasi transfer *data* yang dilakukan dari *client* menuju *server* yang dimiliki oleh pribadi ataupun instansi terkait dengan memanfaatkan implementasi PPTP menjadi sebuah perangkat VPN yang dapat digunakan melalui protokol TCP/IP [5].

Untuk menjalankan pengamanan komunikasi *data* terhadap penyerangan yang dilakukan oleh *intruder*, dibutuhkan sebuah aplikasi khusus dalam menjalankan simulasi terkait yaitu sebuah emulasi *Virtual Box 6.1*. Tujuan dari penelitian ini yaitu bertujuan agar dapat melakukan simulasi pengamanan terkait terhadap penyerangan sistem yaitu aplikasi *Dionaea honeypot*, dimana *intruder* dapat terjebak dan masuk kedalam sebuah *honeypot* yang telah dikonfigurasi dengan tujuan agar *intruder* dapat memperlambat aksi peretasan.

1.1 Jaringan Komputer

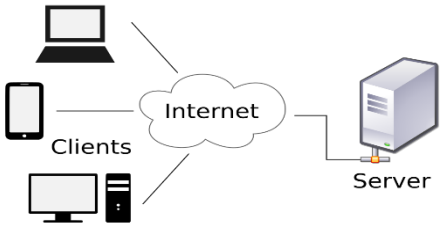
Jaringan komputer merupakan sebuah jaringan komunikasi yang memungkinkan komputer untuk dapat saling berkomunikasi melalui pertukaran *data*. Tujuan dari jaringan komputer untuk dapat memungkinkan bagian dari tiap jaringan komputer untuk dapat meminta dan menyediakan layanan untuk mencapai tujuannya [6].



Gambar 1. Jaringan Komputer

1.2 Server

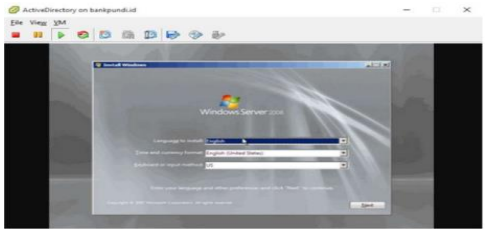
Server adalah pusat kontrol *data* yang dibutuhkan oleh komputer *client*, dan komputer *server* memiliki kendali penuh atas semua *data*. Sistem *backup data* dijalankan secara terpusat oleh kendali penuh *server* [7].



Gambar 2. Server

1.3 Virtual Server

Virtual server merupakan sebuah layanan virtualisasi yang dapat menciptakan wilayah *virtual* yang dapat memungkinkan terjadinya pembagian kumpulan beban sistem operasi aplikasi atau *server* yang dapat berjalan di satu komputer seolah-olah berjalan di komputer yang berbeda [8].

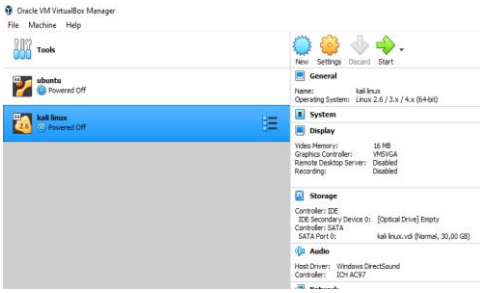


Gambar 3. Virtual Server

ISNN: 2964-1950

1.4 VirtualBox

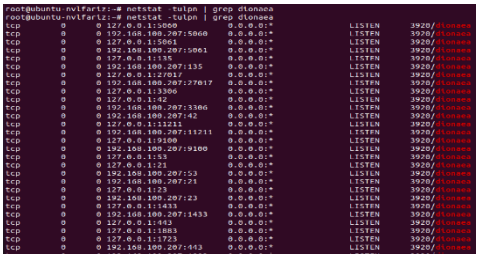
Oracle VM *virtualbox* atau tak jarang diklaim sebagai sebuah produk perangkat lunak yang dikembangkan oleh *Oracle* [9]. *Virtualbox* yang pada pelaksanaan terkait merupakan sebuah *free source machine open source & multi platform* yang bertujuan agar dapat menjalankan fungsi alat agar dapat mejalankan simulator yang pada umumnya merupakan sebuah sistem operasi virtualiasi.



Gambar 4. VirtualBox

1.5 Dionaea honeypot

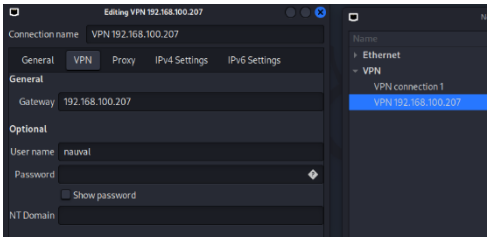
Dionaea merupakan sebuah perangkat *honeypot* yang diciptakan sebagai pewaris pendahulu dari penggunaan *Nepenthes*, *Dionaea* menggunakan *based* bahasa pemrograman *Python* sebagai bahasa *scripting* dalam melakukan pemrosesan *data*. *Dionaea* termasuk kedalam tipe kategori dari *low-interaction honeypot* terbaru yang merupakan pendahulu dari *Nephentes* [10].



Gambar 5. Dionaea Honeypot

1.6 PPTP (Point To Point Protocol)

PPTP adalah pengembangan dari *remote access Point to Point Protocol* yang dikeluarkan oleh *Internet Engineering Task Force* (IETF). PPTP (*Point to Point Tunneling Protocol*). VPN dibangun hanya untuk kepentingan perusahaan besar, militer dan bukan untuk penggunaan komersial [5].



Gambar 6. PPTP VPN

2. METODE PENELITIAN

2.1 Kerangka Penelitian

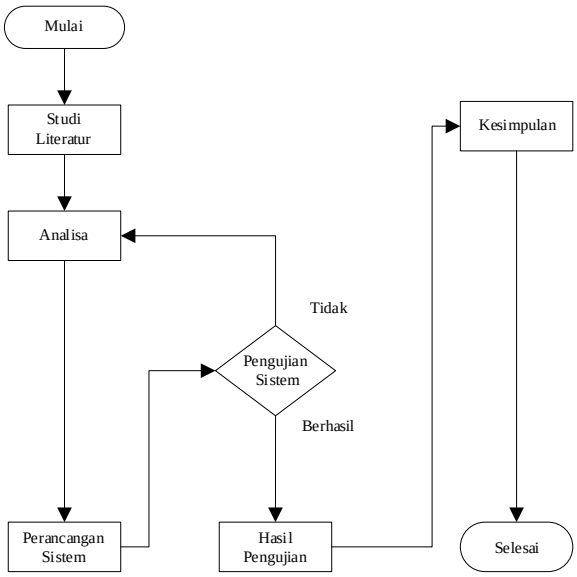
Penelitian yang dilakukan yaitu sebuah bentuk pengamanan dalam melakukan komunikasi *data* yang dilakukan menggunakan aplikasi *Oracle VirtualBox* yang dapat menjalankan sebuah *virtual server* yang memiliki peran sebagai *server* dan *intruder* dalam melakukan simulasi pengamanan *data*. Penggunaan metodologi yang dilakukan menggunakan metodologi pengembangan berbasis kualitatif.

1. Studi Literatur

ISNN: 2964-1950

pengumpulan *data* pendukung berupa jurnal pendukung serta buku terkait yang relevan dengan penggunaan metode studi literatur penelitian pendahulu yang berkaitan dengan topik yang peneliti bahas agar dapat dijadikan sebagai referensi dalam mengembangkan sistem yang akan dirancang dan diuji.

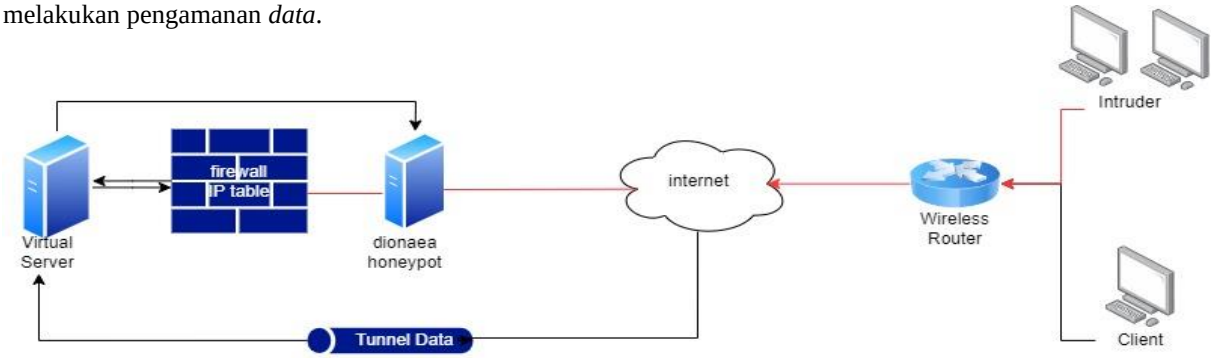
2. Analisa kebutuhan
   Analisa kebutuhan merupakan suatu cara berupa penentuan apa saja hal yang perlu dilakukan berdasarkan tahapan pengumpulan *data* yang dilakukan.
3. Rancang Bangun Sistem
   Rancang bangun *Kali Linux* 20.03 sebagai *intruder* dan *Ubuntu desktop* 20.04.3 sebagai *virtual server* dan aplikasi *Dionaea* sebagai *multiport honeypot* serta PPTP *tunneling*, *firewall* pada sebuah proses pengamanan dalam komunikasi *data*.
4. Pengujian Dan Implementasi Sistem
   Pengujian dan Implementasi dari proses yang dibangun pada saat rancang bangun sistem dilakukan dengan menerapkan pengujian hasil dari penggunaan *Dionaea honeypot*. Serta penerapan dari teknologi *tunnel* PPTP dan *iptables firewall* yang diterapkan dalam proses pengamanan dalam melakukan kegiatan komunikasi *data.*
5. Kesimpulan
   Berisi kesimpulan dan saran mengenai sistem yang telah dibuat dan juga dapat dijadikan sebagai referensi pengambangan bila ada ada peneliti lain yang mengambil topik serupa.



Gambar 7. Flowchart Alur Penelitian

2.2 Rancangan Umum Sistem

Pengembangan sebuah sistem pada penelitian ini berupa pengamanan komunikasi *data* dengan membangun sebuah *dynamic honeypot* dan pemanfaatan teknologi *tunnel* menggunakan *emulator* berupa *VirtualBox* dan juga *tool* pendukung lainnya. Serta memperlihatkan bagaimana terjadinya sebuah proses yang terdapat pada rancangan sistem dengan tujuan mengahasilkan *output* berupa rancangan yang diharapkan sesuai kebutuhan *end user* dalam melakukan pengamanan *data*.



Gambar 8. Perancangan Topologi Pengamanan Dalam Komunikasi Data

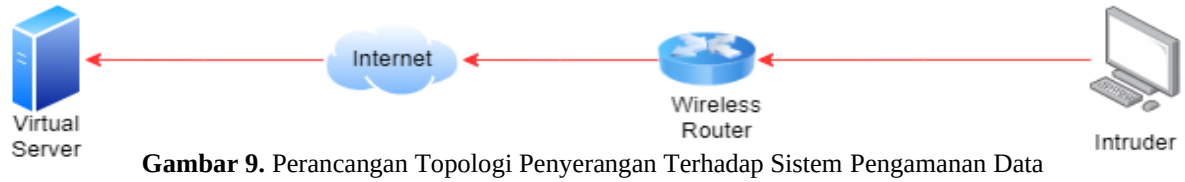
ISNN: 2964-1950

Penjabaran yang dapat dilakukan melalui penggunaan dari tiap perangkat yang terdapat pada gambar.8 dapat dilihat pada tabel 1 dibawah berikut.

Tabel 1. Alat Yang Digunakan Dalam Perancangan Sistem Pengamanan Data

No	Alat Yang Digunakan	Fungsi
1	Komputer	Digunakan untuk melakukan kegiatan berupa pemrosesan *data*.
2	*Virtual server*	Dijadikan sebagai induk *data* yang bertujuan membagikan *resoure* yang diingikan. r*esource* yang dibagikan adalah *web server* dan SSH *server*.
3	*Wireless Router*	Berfungsi untuk dapat melakukan pengaksesan jaringan *internet* .
4	*Internet*	Sebagai sarana dalam mengakses *resource* yang dibutuhkan.
5	*Dionaea Honeypot*	Bertujuan untuk membuat suatu layanan *server* palsu yang digunakan untuk menjebak *intruder*.
6	*Tunnel PPTP*	penulis meletakkan IP PPTP pada *ubuntu* sehingga *client* yang terkoneksi dapat tersambung atas izin yang diberikan pada *virtual server* selaku pemilik hirarki puncak.
7	*Firewall*	*Iptables* yang ada dalam suatu sistem berfungsi sebagai *firewall*.

Perancangan sebuah sistem pada penelitian ini digunakan sebagai bentuk penyerangan yang dilakukan pada topologi pengamanan komunikasi *data* yang membangun sebuah *dynamic honeypot / multiport honeypot* dan *tunnel* menggunakan *emulator* berupa *VirtualBox* yang dilakukan menggunakan sistem operasi kali linux sebagai *intruder*.



Gambar 9. Perancangan Topologi Penyerangan Terhadap Sistem Pengamanan Data

Penjabaran Topologi Penyerangan dapat dilakukan melalui penggunaan dari tiap perangkat yang terdapat pada gambar.9 dapat dilihat pada tabel 2 dibawah berikut.

Tabel 2. Alat Yang Digunakan Dalam Penyerangan Sistem

No	Alat Yang Digunakan	Fungsi
1	Komputer	komputer yang digunakan oleh *intruder* berfungsi untuk melakukan penyerangan berupa *bruteforce* dan DDoS pada *virtual server*.
2	*Virtual server*	Komputer yang digunakan akan menjadi target dari penyerangan yang dilakukan oleh *intruder*.
3	*Wireless Router*	Berfungsi untuk dapat melakukan akses *resource* kedalam jaringan *internet*.
4	*Kali linux 20.3*	Berfungsi sebagai OS yang digunakan untuk melakukan berbagai macam metode penyerangan terhadap *virtual server*.
5	*Internet*	Sebagai sarana dalam mengakses *resource* yang dibutuhkan dan juga sebagai media dalam melakukan serangan penetrasi kedalam *virtual server*.

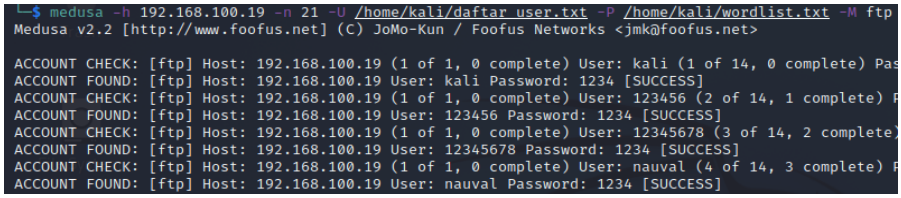
3. HASIL DAN PEMBAHASAN

3.1 Pengujian Multiport Dionaea Honeypot

1. Pengujian Dionaea Honeypot

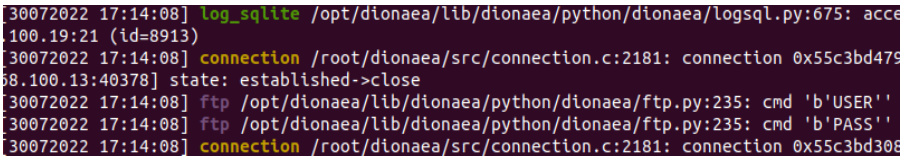
   Pengujian pada *Dionaea honeypot* dilakukan dengan penyerangan *bruteforce* yang dilakukan menggunakan sistem operasi Kali Linux. sebuah pengujian dilakukan dengan melakukan percobaan serangan *medusa* terhadap *port* 21 FTP. *Port* 21 FTP diperoleh dari hasil *port scanning* yang telah dilakukan sebelumnya. Serangan yang dilakukan pada layanan *port* tersebut tidak dalam kondisi terinstalasi dalam layanan utama yang ada pada *virtual server*.

ISNN: 2964-1950



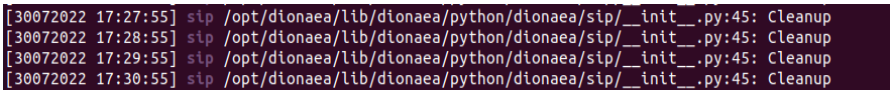
Gambar 10. Implementasi Serangan Bruteforce Pada Port 21 FTP dionaea Honeypot

Dari hasil penyerangan yang terdapat pada gambar 10 dilakukan oleh *intruder*, *Dionaea honeypot* memberikan reaksi dengan memberikan sebuah peringatan alaram telah terjadinya sebuah penyerangan yang dilakukan terhadap sebuah sistem yang ada pada *virtual server* yang dikonfigurasi pada sebuah aplikasi bernama *Dionaea honeypot*.



Gambar 11. Implementasi Serangan Bruteforce Pada Port 21 FTP dionaea Honeypot

Penyerangan yang dilakukan memberikan keterangan tertulis berupa informasi dimana *Dionaea honeypot* dapat menangkap informasi berupa IP *address* dari penyerang. Namun hal ini tidak berlaku ketika layanan yang terkonfigurasi pada *virtual server* seperti SSH tidak dapat melakukan pendeteksian penyerangan.



Gambar 12. Implementasi Serangan Bruteforce Pada Port 22 SSH dionaea Honeypot

Untuk dapat melakukan perhitungan *quality of service*, alat yang digunakan berupa *wireshark*. Perhitungan dilakukan dengan berfokus pada 4 perhitungan utama yang ada yaitu *througput*, *packet loss*, *delay* dan *jitter*.

Rumus

Throughput = Jumlah *bytes* : *timespan*

Packet Loss = Paket dikirim-paket diterima : paket dikirim x 100

Delay = *Timespan* / *packet* x 1000

Jitter = Rata - rata *delay* : jumlah paket x 1000

Tabel 3. Capture Data Pengujian Serangan Port 21 FTP Medusa

Measurement	*Captured*	*Displayed*	*Marked*
Packets	56	56 (100.0%)	—
Time span, s	25.621	25.621	—
Average pps	2.2	2.2	—
Average packet size, B	247	247	—
Bytes	13813	13813 (100.0%)	0
Average bytes/s	539	539	—
Average bits/s	4313	4313	—

Tabel 4. Capture Data Pengujian Serangan Port 22 SSH Medusa

Measurement	*Captured*	*Displayed*	*Marked*
Packets	1203	1203 (100.0%)	—
Time span, s	608.560	608.560	—
Average pps	2.0	2.0	—
Average packet size, B	270	270	—
Bytes	324910	324910 (100.0%)	0
Average bytes/s	533	533	—
Average bits/s	4271	4271	—

ISNN: 2964-1950

3.2 Hasil Perbandingan Pengujian Implementasi Dionaea Honeypot

1. Perbandingan QoS Pengujian Penyerangan *Dionaea Honeypot*
   Pengujian pada *Dionaea honeypot* dilakukan dengan penyerangan *bruteforce* yang dilakukan menggunakan sistem operasi *Kali Linux*. Hasil *capture data* yang dilakukan menampilkan sebuah perbedaan yang dapat dilihat pada tabel dibawah berikut.

Tabel 5. QoS Pengujian Serangan Port 21 FTP Medusa

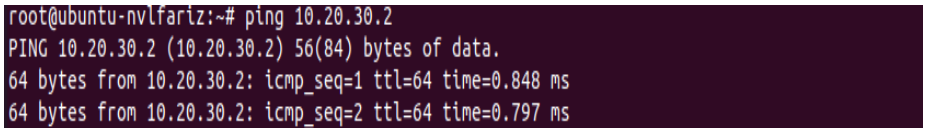
N	*Throughput*	*Packet Loss*	*Delay*	*Jitter*
1	=13813:25.621=0.53912805901 x8= 4.31302447211=*average bits* 4.313	=(56- 54) : 56)x 100 =(5:1780=0.0357142857)x100=(3.5714285713 = 3,6 % *packet loss*)	=5.737:6=956.166666667*sec*,956.166666667*sec*x1000=956166.666667 *ms* = 96 *ms*	956166.666667*s*:(56 =-2=54)= 17706.7901235 17706.7901235x1000= 17706790.1235= 18 *ms*

Tabel 6. QoS Pengujian Serangan Port 22 SSH Medusa

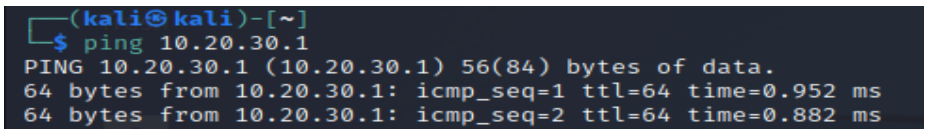
N	*Throughput*	*Packet Loss*	*Delay*	*Jitter*
1	=324910:608.560=0.53389969764 *b* x 8 =4.27119758118=*average bits* 4271	=1203- 1202) : 1203)x 100=(1:1203=0.00083125519)x100=(0.08312551953=0,8% *packet loss*)	=581.207:543=1070.36279926*sec*1070.36279926*sec*x10001070362.79926*ms* = 11 *ms*	= 1070362.79926*s*:(1203 = -2 = 1201) = 1048.34750172 1048.34750172x1000=1048347.50172 = 10 *ms*

3.3 Implementasi PPTP Tunneling

1. Implementasi PPTP *tunnel*
   Implementasi PPTP dilakukan bertujuan untuk memberikan akses jalur koneksi khusus antara *client* yang ingin mencoba melakukan koneksi khusus dan *server* yang memberikan akses jalur komunikasi dengan penerapan konfigurasi teknologi VPN PPTP *static*.



Gambar 13. PING PPTP Client Berhasil



Gambar 14. PING PPTP Server Berhasil

4. KESIMPULAN

Hasil yang didapat setelah perancangan *Dionaea honeypot* akan menampilkan *output* 15 *port* yang ada pada *Dionaea honeypot*. Layanan yang terdiri terdapat pada *port* 21 FTP dan diakhiri dengan *port jetdirect* 9100. Semua *port* terkait berada pada kondisi *open port* untuk memancing penyerang untuk dapat melakukan eksploitasi pada tiap *port* yang diserang. IP *resource* yang digunakan, menggunakan model komunikasi DHCP *server* yang ada pada jaringan yang berada pada *Ubuntu desktop* 20.04.3. sehingga perangkat yang dilakukan konfigurasi pada sistem *honeypot* tersebut seperti *hardware* yang terhubung kedalam koneksi perangkat lain sebagai contoh *router* yang berbeda maka koneksi jaringan yang berada pada IP *address* yang diperoleh otomatis juga berubah. Prinsip ini dikenal dengan *dynamic* IP. Juga penggunaan *tunnel* PPTP yang dilakukan dalam proses komunikasi penulis pilih, dikarenakan konfigurasi PPTP yang mudah serta PPTP tidak memerlukan konfigurasi seperti *tunnel* sejenis lainnya yaitu LPTP dan SSTP yang dimana pengembangan lebih lanjut dari PPTP. Dalam penelitian terkait yang peneliti bawakan, peneliti melakukan perancangan pada konfigurasi PPTP *tunnel*, tidak melakukan kegiatan konfigurasi berupa penyesuaian seperti konfigurasi *port* terkhusus dalam melakukan proses komunikasi *data* dan

hanya menyesuaikan *network* yang sama tetapi hanya berbeda *hostname*. Pengamanan terakhir yang dilakukan yaitu melakukan pemblokiran IP *address* penyerang menggunakan fitur *firewall* yang dimiliki *Ubuntu desktop 20.04.3* yaitu *iptables.*

UCAPAN TERIMAKASIH

Alhamdulillah penulis ucapkan atas rahmat yang diberikan oleh Allah SWT, Tuhan semesta alam atas keberkahan ilmu juga penulis ucapkan terima kasih kepada kedua orang tua yang telah mendukung penulis hingga dapat menyelesaikan pendidikan penulis. Juga penulis berterima kasih kepada penulis kedua yaitu bapak Tengku Mohd Diansyah yang telah melakukan kontribusi sangat baik atas penelitian yang dilakukan dan tak luput juga penulis mengucapkan terima kasih kepada penulis ketiga yaitu bapak Risko Liza atas kontribusi yang diberikan dengan sangat baik serta teman seperjuangan yang telah terkait bersama penulis membantu baik dari segi moril, dukungan finansial, alat dan lainnya yang tidak dapat penulis sebutkan satu persatu. Hingga akhir, terima kasih banyak penulis ucapkan dari lubuk hati yang paling dalam.

DAFTAR PUSTAKA

[1] V. Sethia and A. Jeyasekar, "Malware capturing and analysis using dionaea honeypot," *Proc. - Int. Carnahan Conf. Secur. Technol.*, vol. 2019-Octob, pp. 0–3, 2019, doi: 10.1109/CCST.2019.8888409.

[2] M. Noviansyah and H. Saiyar, "PENCEGAHAN PACKET SNIFFING MENGGUNAKAN METODE VPN TUNNEL UNTUK KEAMANAN JARINGAN KOMPUTER BERBASIS MIKROTIK," vol. 6, no. November, p. 6, 2021.

[3] D. K. Nurilahi, R. Munadi, L. Syahria, and A. L. Bahri, "Penerapan Metode Naïve Bayes pada Honeypot Dionaea dalam Mendeteksi Serangan Port Scanning," vol. 10, no. 2, pp. 309–321, 2022.

[4] T. M. Diansyah, I. Faisal, A. Perdana, B. O. Sembiring, and T. H. Sinaga, "Analysis of Using Firewall and Single Honeypot in Training Attack on Wireless Network," *J. Phys. Conf. Ser.*, vol. 930, no. 1, 2017, doi: 10.1088/1742-6596/930/1/012038.

[5] M. D. Andini, M. Amirulloh, and H. N. Muchtar, "Penggunaan Aplikasi Virtual Private Network (Vpn) Point To Point Tunneling Protocol (Pptp) Dalam Mengakses Situs Terblokir," *Supremasi HukumJurnal Penelit. Huk.*, vol. 29, no. 2, pp. 148–166, 2020, [Online]. Available: https://ditsti.itb.ac.id/layanan-vpn/

[6] I. K. Astuti, "Fakultas Komputer INDAH KUSUMA ASTUTI Section 01," *Jar. Komput.*, p. 8, 2018, [Online]. Available: https://id.scribd.com/document/503304719/jaringan-komputer

[7] A. A. Pangestu, "PENGEMBANGAN SISTEM INFORMASI ADMINISTRASI SEKOLAH BERBASIS CLIENT SERVER (Studi Kasus : SMK Muhammadiyah 2 Borobudur)," 2020.

[8] S. N. Khasanah and S. J. Kuryanti, "Rancangan Virtualisasi Server Menggunakan VMWare Vsphare," *EVOLUSI - J. Sains dan Manaj.*, vol. 7, no. 1, pp. 42–46, 2019, doi: 10.31294/evolusi.v7i1.5091.

[9] A. S. Manalu and S. S. Sitanggang, "Perancangan Dan Implementasi Private Cloud Storage Dengan Owncloud Pada Jaringan Lokal Menggunakan Virtualbox," *J. Comput. Networks, Archit. High-Performance Comput.*, vol. 1, no. 2, pp. 60–71, 2019, doi: 10.47709/cnahpc.v1i2.244.

[10] R. Dermawati and M. H. Siregar, "Implementasi Honeypot Pada Jaringan Internet Labor," *J. Ilm. Edutic*, vol. 7, no. 1, pp. 20–30, 2020.