Jurnal Indonesia : Manajemen Informatika dan Komunikasi
www.journal.amikindonesia.ac.id/jimik/ Vol 4 No 3, September (2023)
E-ISSN: 2723-7079, P-ISSN: 2776-8074

ANALISIS SERANGAN *CYBER* MENGGUNAKAN *HONEYPOT* PADA WEB BERBASIS *CLOUD*

Bayu Setyanto Pamungkas [1*], Irwan Sembiring [2]

[1*, 2] Program Studi Teknik Infomatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Kota Salatiga, Provinsi Jawa Tengah, Indonesia.

Email: 672017268@student.uksw.edu [1*], irwan@uksw.edu [2]

Histori Artikel:
Dikirim 15 Juni 2023; *Diterima dalam bentuk revisi* 5 Juli 2023; *Diterima* 8 Agustus 2023; *Diterbitkan* 10 September 2023.

Abstrak

Cloud computing memiliki sistem keamanan yang cukup tinggi, namun karena dapat diakses dari mana saja melalui jaringan internet, tidak menutup kemungkinan bahwa sistem tersebut sudah aman dari serangan siber, seperti Port Scanning, Brute Force Attack, Malware Attack dan jenis cyberattack lainnya, T-Pot Honeypot adalah sebuah sistem all in one dari Honeypot yang merupakan sebuah sistem keamanan tambahan untuk mendeteksi, menjebak serangan untuk tidak dapat masuk kedalam sistem utama. Berdasarkan hasil penelitian, implementasi dari T-Pot Honeypot ini dapat mendeteksi serangan dan berhasil menjebak penyerang dengan memberikan informasi palsu seperti daftar port terbuka yang menjadi target pencarian penyerang. Data log hasil serangan yang terdeteksi diolah oleh sistem Honeypot dan diteruskan menjadi grafik dan diagram yang dapat dilihat melalui Kibana Dashboard, sehingga memudahkan administrator untuk melakukan monitoring anomali serangan yang dilakukan oleh penyerang sehingga dapat digunakan untuk lebih meningkatkan keamanan.

Kata Kunci: Cloud Computing; Brute Force Attack; Cyber Attack; T-Pot; Honeypot.

Abstract

Cloud computing has a fairly high-security system, however as it can be accessed from anywhere via the internet network, it does not rule out the possibility that the system is safe from cyberattacks, such as Port Scanning, Brute Force Attacks, Malware Attacks, and other types of cyberattacks, T-Pot Honeypot is an all in one system from Honeypot which is an additional security system to detect, trap attacks not to be able to enter the main system. Based on the research results, the implementation of this T-Pot Honeypot can detect attacks and successfully trap attackers by providing false information such as a list of open ports that are the target of the attacker's search. The log data of the detected attack results are processed by the Honeypot system and forwarded into graphs and diagrams that can be seen through the Kibana Dashboard, making it easier for administrators to monitor attack anomalies carried out by attackers so that they can be used to improve security further.

Keyword: Cloud Computing; Brute Force Attack; Cyber Attack; T-Pot; Honeypot.

1. Pendahuluan

Cloud computing saat ini menjadi sebuah teknologi yang banyak digunakan diseluruh dunia, *Data security* dan *network security* adalah sistem keamanan yang dimiliki oleh *cloud computing*, karena sistem *cloud* berada dalam jaringan internet yang mana internet dapat diakses dari mana saja [1]. Namun dengan sistem keamanan tinggi yang dimiliki oleh *cloud computing*, tidak menutup kemungkinan terdapat celah-celah keamanan yang dapat dimanfaatkan, yang mana bisa menyebabkan terjadinya serangan, pencurian data, dan perusakan pada sistem *cloud* yang digunakan, dari laporan data Keamanan Siber Indonesia bulan Agustus 2022, terdapat 7.084.332 *information leak* yang tercatat pada bulan agustus, yang diakibatkan oleh serangan seperti *web weak password login, authentication weak password, SQL injection*. Pada tahun 2021 juga tercatat serangan *brute force* menjadi top anomali *cyberattack* yang terjadi di Indonesia, dengan metode *brute force attack remote desktop protocol (BFA RDP)* [2]. *Brute force attack* merupakan sebuah metode serangan *cracking password,* dimana proses dari serangan ini adalah melakukan segala kemungkinan kombinasi huruf, angka, dan simbol untuk mengetahui *username* dan *password,* serangan ini dilakukan agar *attackers* memiliki akses yang tidak sah untuk dapat masuk kedalam sistem [3]. Serangan *cracking password* memiliki kelemahan yaitu waktu yang digunakan untuk melancarkan serangan ini cukup lama, namun dibalik waktu yang cukup lama ketika melakukan serangan ini, tingkat keberhasilan yang dihasilkan dari teknik serangan ini cukup tinggi [4].

Intrusion Detection and Prevention System (IDPS) adalah sebuah *tools* keamanan yang digunakan untuk mendeteksi dan mencegah aktivitas berbahaya yang terjadi didalam jaringan. *Intrusion Detection System (IDS)* merupakan sebuah *tools* keamanan yang digunakan untuk mendeteksi aktivitas berbahaya, kemudian memberikan peringatan akan aktivitas berbahaya tersebut. Sedangkan *Intrusion Prevention System (IPS)* berbeda dengan *IDS, IPS* dapat menanggapi ancaman yang terdeteksi dengan mencegah serangan dengan cara mengkonfigurasi ulang keamanan, dengan memblokir akses dari penyerang atau mengubah firewall untuk memblokir serangan yang masuk [5] *Honeypot* merupakan sebuah mekanisme sistem keamanan yang digunakan untuk melakukan monitoring pola serangan, mengumpulkan informasi serangan, dan mengumpulkan data kemungkinan serangan yang akan terjadi pada sistem utama [6]. *Honeypot* berisi data-data palsu dengan tujuan untuk menarik perhatian dan mengelabui *attackers,* sistem *Honeypot* dapat mengetahui identitas dan membimbing *attackers* untuk menuju ke dalam sistem *Honeypot* [7].

Berdasarkan uraian diatas maka pada penelitian ini dilakukan implementasi sebuah sistem keamanan untuk mendeteksi, mencegah serangan *cyber* yang terjadi pada web berbasis *cloud* dengan *Intrusion detection and Prevention System (IDPS)* dalam *T-Pot Honeypot* yang dijalankan menggunakan *virtual machines* pada layanan *cloud Microsoft Azure*, serta menganalisis tingkat keberhasilan dari sistem yang dibuat untuk mendeteksi serangan *cyber* yang terjadi.

Pada penelitian yang dilakukan oleh Muhammad [8], penelitian ini mengimplementasikan sistem keamanan dari *Honeypot* untuk mendeteksi adanya serangan yang dilakukan oleh *brute force* dengan menggunakan SSH, semua data informasi terekam dalam *Honeypot* dan dapat berfungsi untuk mengelabuhi penyerang yang menganggap bahwa server *Honeypot* tersebut adalah sistem aslinya dengan membuka beberapa port, namun sistem asli tidak berpengaruh sama sekali dari penyerangan. Pada penelitian yang dilakukan oleh Shivathmika [9], penelitian ini mengungkapkan bahwa *Honeypot* merupakan sistem keamanan atau aset yang dapat membuat keamanan pada sistem *cloud* yang tinggi dapat semakin aman, dan memiliki kemungkinan untuk diserang atau dicuri data-data yang ada pada *cloud* semakin rendah. Selain menjebak dan melakukan monitoring dari serangan yang terjadi, *Honeypot* dapat mengidentifikasi kejanggalan yang terjadi dalam jaringan, dan melakukan antisipasi serangan dari seluruh data yang didapatkan oleh *Honeypot*.

Penelitian yang dilakukan Kahara Wanjau [10], menggunakan CIC-IDS 2018 benchmark dataset, penelitian ini menggunakan performa dari *binary classification*, *classifying network traffic*. Untuk mendeteksi serangan *SSH-Brute force* dengan akurasi tinggi yang sedang melakukan uji coba masuk dengan cara menebak *username* dan *password* pengguna. Dwi & Prakoso [11], melakukan penelitian menambah keamanan yang dilakukan untuk autentikasi ke dalam server, karena *port* yang tersedia

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1284-1295
DOI : https://doi.org/10.35870/jimik.v4i3.325

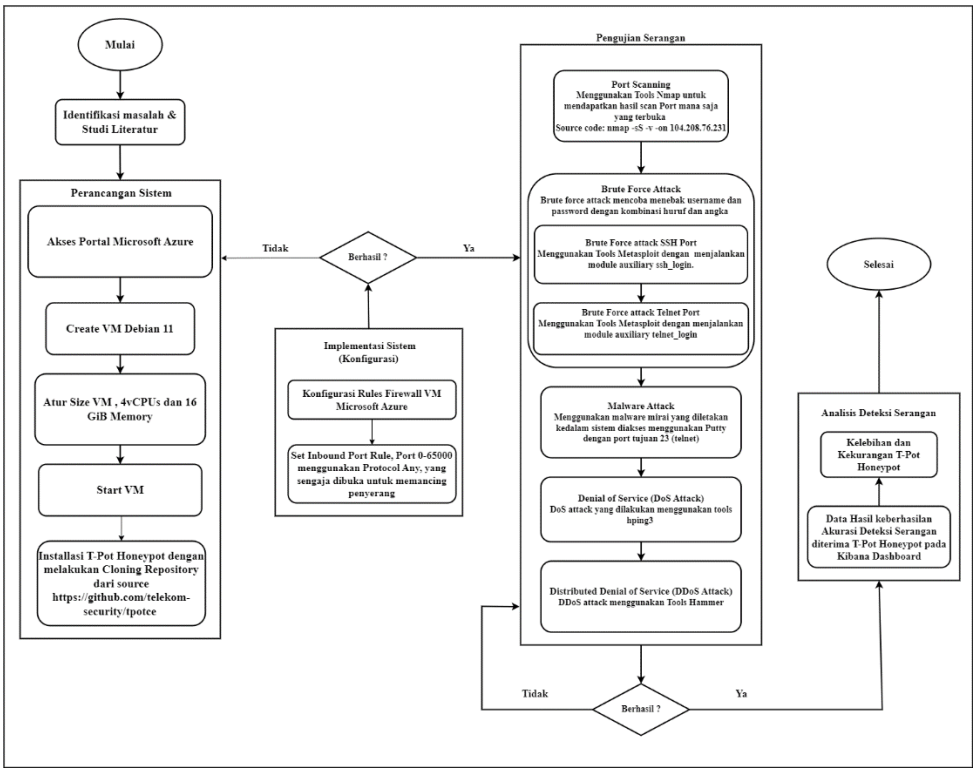
tidak terbuka untuk publik, sehingga perlu ditingkatkan keamanannya. Pada *port knocking* yang dilakukan dalam penelitian tersebut, berhasil mencegah *attackers* dari pemindai SSH. Dengan melakukan *port scanning service SSH* menjadi tidak mudah dilacak dan diakses orang lain, *Honeypot* dapat melakukan pencegahan terhadap upaya dari *attackers* untuk melakukan *scanning port* dan *brute force attack,* maka *attackers* hanya akan melihat *fake ports* yang dibuat oleh *Honeypot.*

Berdasarkan penelitian yang telah dilakukan sebelumnya tentang *honeypot*, maka dilakukan penelitian tentang *T-Pot Honeypot* untuk menganalisa tingkat keberhasilan sistem tersebut dapat mendeteksi serangan *cyber* yang dimana sistem *T-Pot Honeypot* berbasis pada *Cloud,* serangan yang diuji coba pada penelitian ini menggunakan beberapa jenis serangan yaitu *Port Scanning, BFA, Malware Attack, DoS dan DDoS Attack.*

2. Metode Penelitian

Dalam proses penelitian dan perancangan sistem untuk mendeteksi serangan *cyber* dan melakukan analisis terhadap keberhasilan *T-Pot Honeypot* mendeteksi serangan yang terjadi. *Attacker* menggunakan laptop dengan spesifikasi sistem operasi utama menggunakan Kali Linux 2022.4, dengan RAM 8GiB, *Storage* 128 GiB, dengan *IP address* 114.10.125.183 dan 117.74.126.142. *Tools* yang digunakan pada skenario penyerangan yaitu *Nmap, Putty, Hping3, Hammer* dan *Metasploit.*

2.1 Alur Penelitian



Gambar 1. Diagram alur penelitian

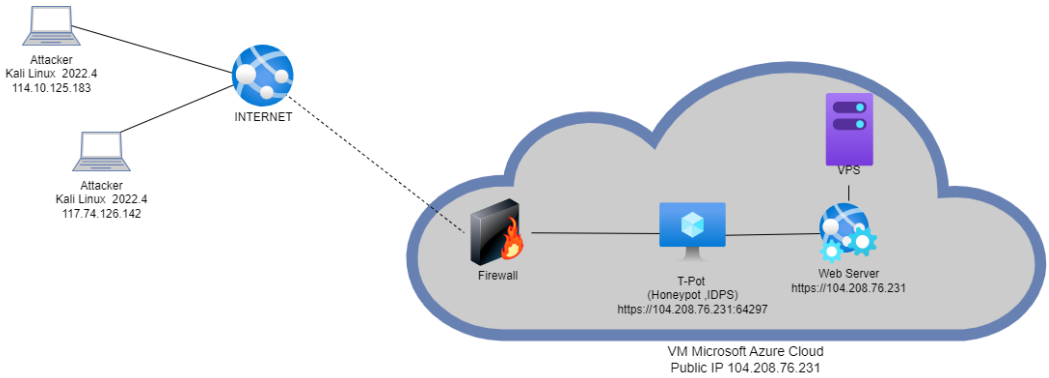
Dalam Gambar 1 dijelaskan bahwa pada penelitian ini melakukan identifikasi masalah & mulai melakukan studi literatur terhadap materi yang berhubungan dengan *Honeypot,* perancangan sistem yang digunakan, melakukan konfigurasi implementasi sistem, pengujian serangan yang dilakukan, kemudian melakukan analisis dari hasil deteksi serangan yang terdeteksi oleh sistem *T-Pot Honeypot.*

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1284-1295
DOI : https://doi.org/10.35870/jimik.v4i3.325

2.2 Perancangan Sistem

Pada tahap ini dilakukan perancangan sistem yang akan digunakan pada penelitian ini pada tahap implementasi dan pengujian, perancangan sistem deteksi serangan berbasis *cloud* ini menggunakan *virtual machines* yang ada pada layanan *cloud service* dari *Microsoft Azure. T-Pot Honeypot* akan dipasang didalam Debian 11 yang telah di install di dalam *virtual machine cloud* dari *azure,* dengan *IP public* 104.208.76.231 yang didapatkan dari *cloud service*, *IP public* ini digunakan untuk mengakses *T-Pot,* dengan spesifikasi vm yang digunakan yaitu *Size Standard D4s v3, vCPUs 4,* dan RAM 16GiB.

Instalasi dan konfigurasi *T-Pot Honeypot* dilakukan dengan cara *cloning repository* dari https://github.com/telekom-security/tpotce, akses melalui port 22 SSH menggunakan putty dengan menuliskan *IP public* 104.208.76.231 yang didapatkan dari *vm azure*, setelah instalasi *T-Pot Honeypot* dapat diakses melalui port 64297 pada *web browser*.

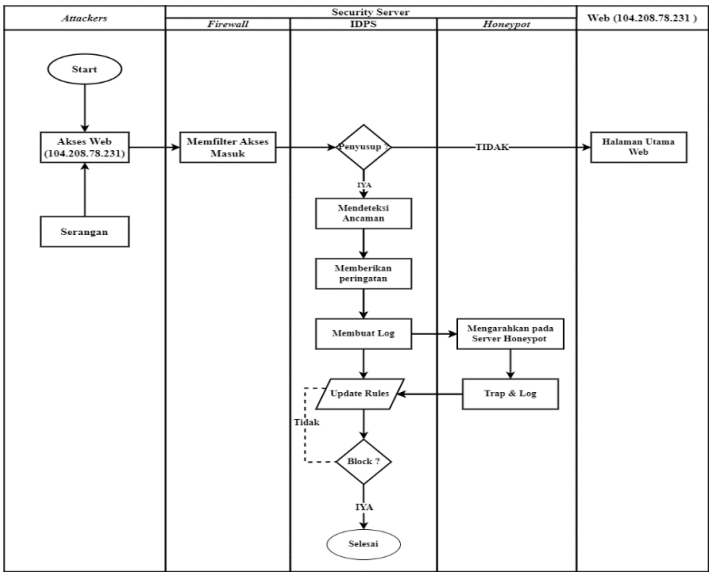


Gambar 2. Topologi Jaringan yang dirancang

Pada Gambar 2 merupakan topologi dari sistem yang dirancang berbasis pada *cloud*, implementasi sistem keamanan untuk mendeteksi *cyber-attack* menggunakan sistem *T-Pot honeypot* untuk mendeteksi serta menjebak penyerang agar tidak dapat masuk kedalam web utama yang dimana penyerang harus melewati *firewall* dan *T-Pot* terlebih dahulu sebelum dapat mengakses web.

2.3 Pengujian Serangan

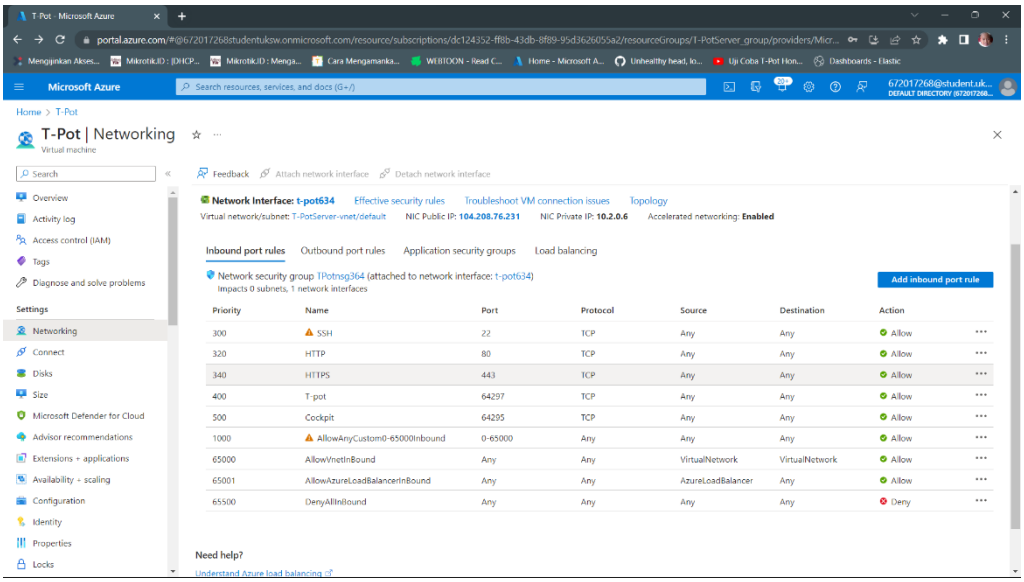
Pada proses ini dilakukan pengujian serangan dilakukan dengan empat skenario serangan. Penyerang akan melakukan serangan tertuju kepada alamat IP target 104.208.76.231.



Gambar 3. Diagram Pengujian Serangan

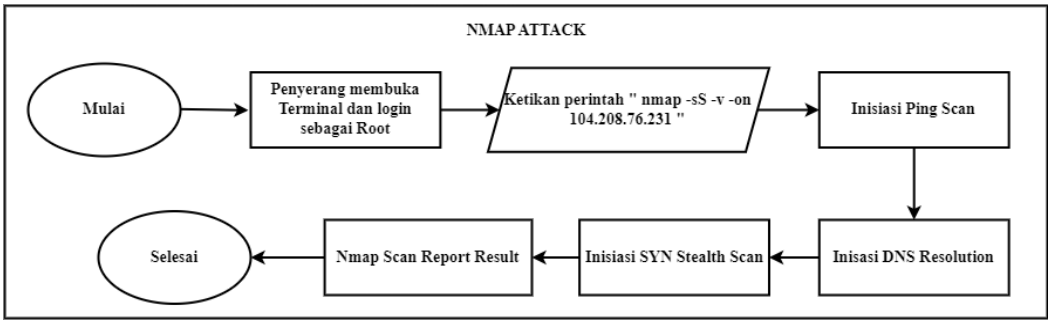
Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1284-1295
DOI : https://doi.org/10.35870/jimik.v4i3.325

Dapat dilihat pada gambar 3, dijelaskan bahwa *client* dan *attacker* akan melewati *Firewall*, T-Pot (IDPS, *Honeypot*) terlebih dahulu sebelum dapat mengakses server sepenuhnya. Ketika melewati IDPS terdeteksi adanya upaya tidak wajar berdasarkan *rules* yang telah dibuat maka IDPS akan mendeteksi dan membuat *log* aktivitas, jika tidak akan diarahkan langsung menuju ke halaman *login*. Untuk serangan yang masih berlanjut diarahkan menuju ke server palsu yang telah dibuat oleh *Honeypot*, kemudian dijebak di dalam server *Honeypot,* dan dihasilkan lah *log* aktivitas yang berisi segala informasi yang didapat dari penyerang. Dari data *log* tersebut akan dikirimkan menuju ke IDPS untuk melakukan *generate rules* baru dan melakukan *blocking* terhadap penyerang.



Gambar 4. Konfigurasi *Port Rule*

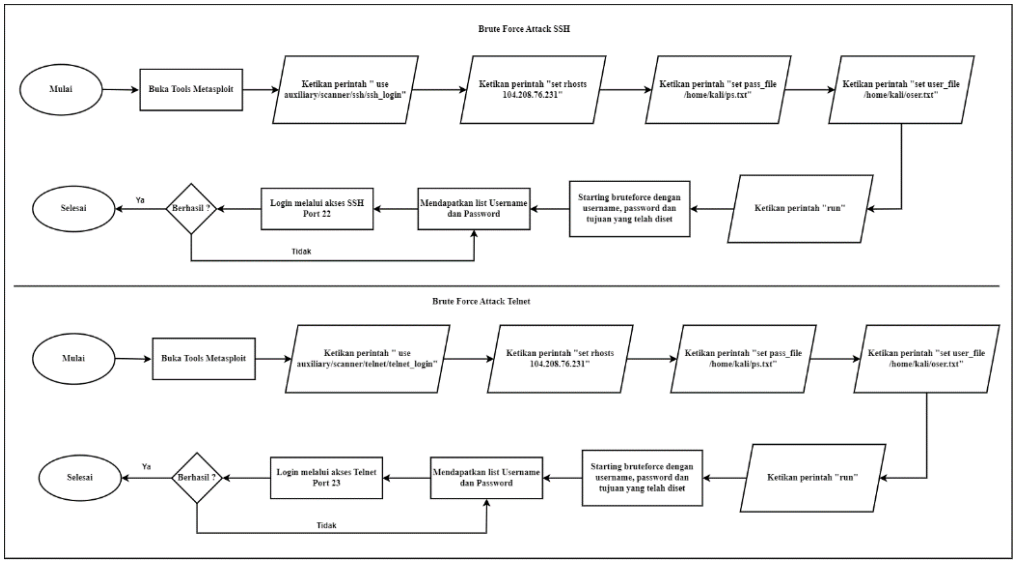
Sebelum dilakukannya pengujian dilakukan terlebih dahulu konfigurasi *rules* terlebih dahulu, dapat dilihat pada Gambar 4 menunjukan terdapat *inbound port rule* yang harus dikonfigurasikan, pada *priority* 1000 dengan port terbuka 0-65000 dibuka dengan sengaja untuk memberikan jalan *attacker* masuk ke dalam jaringan, memungkinkan *attacker* mengetahui bahwa banyak port terbuka sehingga *attacker* dapat merencanakan jenis serangan lainnya, yang dimana sebenarnya *attacker* tersebut masuk kedalam perangkap yang dibuat oleh *Honeypot*. Pada port 64297, dan 64294 dibuka untuk akses ke dalam *cockpit* dan *landing page T-Pot* dengan *protocol* yang diatur yaitu TCP saja.



Gambar 5. Diagram alur skenario serangan *Port Scanning*

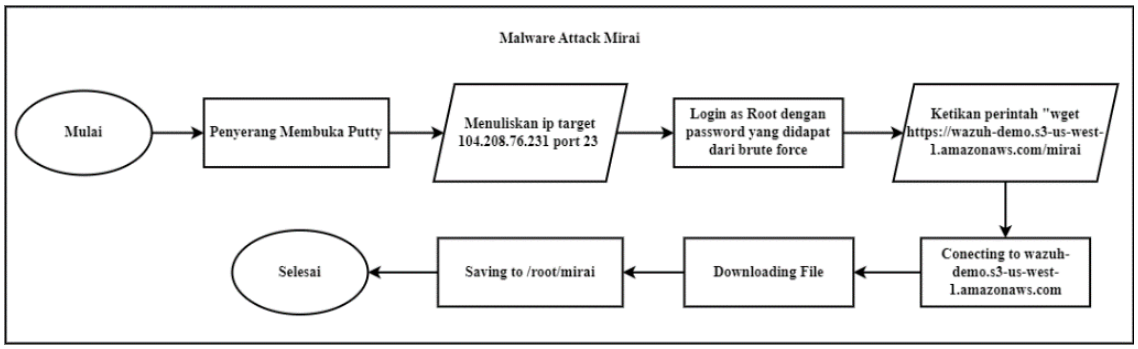
Pada skenario serangan Port Scanning penyerang menggunakan metode serangan Nmap yang berbasis menggunakan terminal dari sistem operasi kali linux, penyerang menginputkan perintah seperti pada gambar 5 untuk menjalankan Nmap dengan *scanning* SYN dan IP target, sehingga Nmap akan memberikan informasi port dan *service* yang ada dimiliki port tersebut.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1284-1295
DOI : https://doi.org/10.35870/jimik.v4i3.325



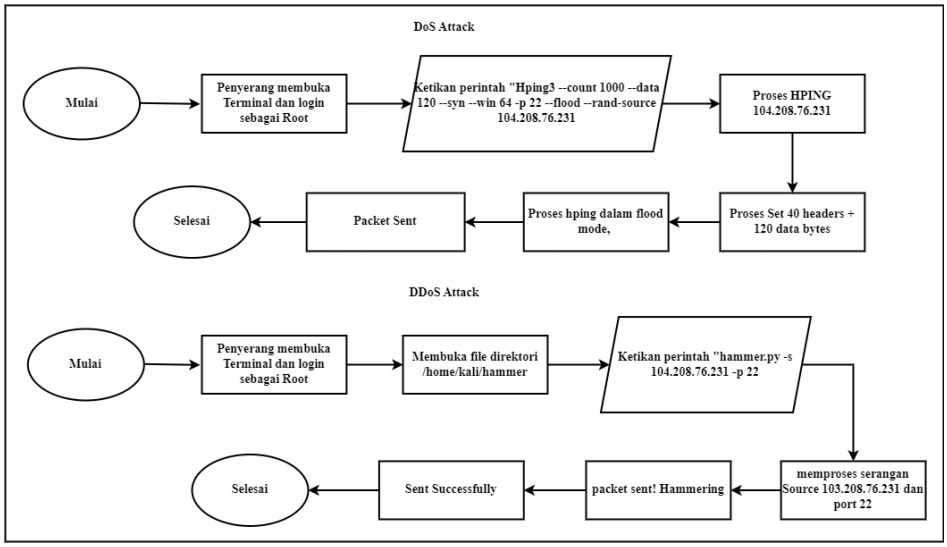
Gambar 6. Diagram alur skenario serangan *brute force* SSH dan Telnet

Pada skenario serangan *brute force* penyerang melakukan dua kali serangan, yang pertama tertuju kepada port ssh dan yang kedua menuju ke port telnet, metode serangan brute force yang dijalankan penyerang dengan memanfaatkan tools metasploit. Penyerang menuliskan perintah seperti yang tertera pada Gambar 6, menggunakan *module auxiliary* untuk melakukan *scanning* dengan melakukan *set IP target*, *set file* untuk *username* dan *password* yang akan di coba dalam serangan *brute force.* Ketika serangan *bruteforce* berjalan dan pada *file username password* yang sudah di set tadi mendapat kecocokan, sistem metasploit akan memberikan *list username* dan *password* yang bisa digunakan untuk *login.*



Gambar 7**.** Diagram alur serangan *Malware attack*

Dalam skenario penyerangan *malware attack,* penyerang memanfaatkan hasil serangan *brute force* yang tertuju pada port 23/telnet. Penyerang menggunakan tools putty untuk mengakses port telnet, dengan login sebagai root dan password toor. Kemudian penyerang melakukan download file yang berisikan malware, dan file yang telah berhasil di download tersebut akan tersimpan pada folder /root/mirai, Alur serangannya dapat dilihat pada Gambar 8.

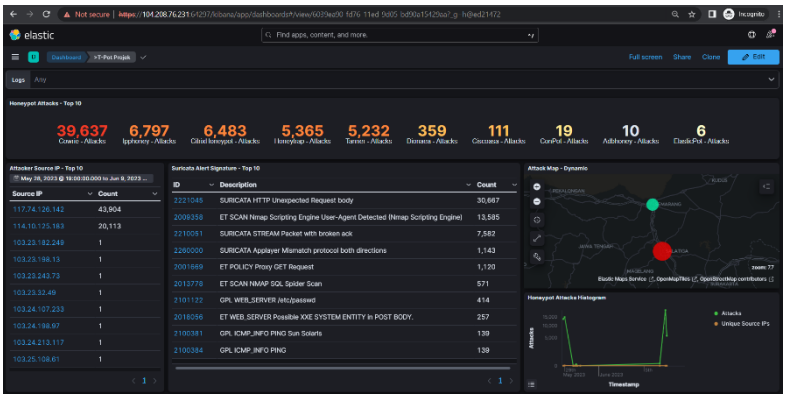


Gambar 8. Diagram alur serangan *DoS & DDoS attack*

Pada Gambar 8 merupakan skenario serangan yang digunakan penyerang untuk melakukan *DoS dan DDoS attack*. Penyerang melakukan akses ke dalam terminal sebagai root terlebih dahulu, kemudian menggunakan tools hping3 untuk *DoS attack* dan hammer untuk *DDoS attack*, pada serangan DoS diatur berapa paket, jumlah data, *SYN flagnya* secara *default* tujuannya pada port 22 dan source yaitu IP target. Kemudian pada serangan DDoS membuka file direktori dimana hammer berada, kemudian penyerang menjalankan tools hammer dan mengatur tujuan nya ke alamat IP target dan port 22 target, serangan DoS dan DDoS mengirimkan jumlah paket secara *flooding* yang telah diatur kedalam sistem secara terus menerus.

3. Hasil dan Pembahasan

Data hasil dari serangan-serangan yang telah dilakukan tercatat dalam log *T-Pot Honeypot* yang ditampilkan dalam kibana dashboard secara visual berbentuk diagram, total serangan terdeteksi yang memudahkan administrator untuk melakukan monitoring serangan yang terjadi.

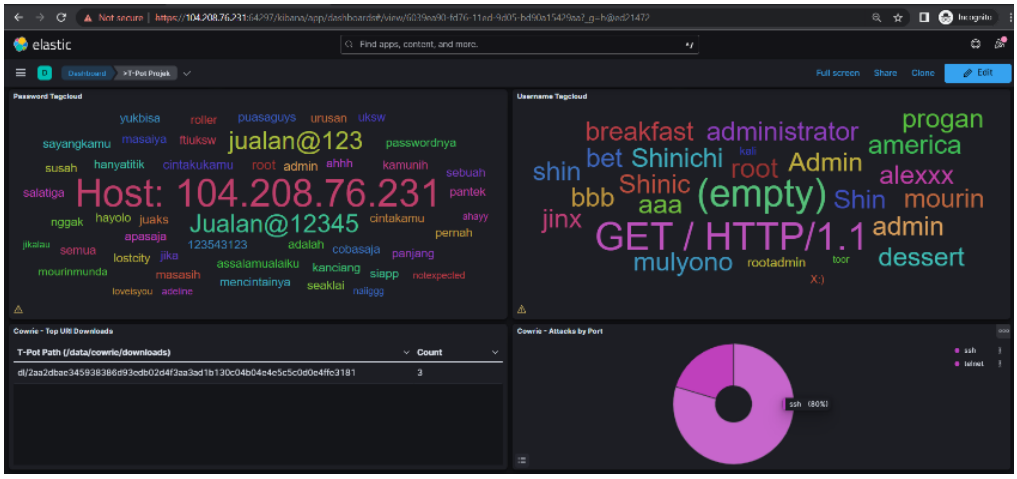


Gambar 9. Tampilan Kibana *Dashboard*

Gambar 9 merupakan tampilan dari Kibana dashboard yang merupakan salah satu tools yang dimiliki oleh *T-Pot Honeypot*, didalam kibana dashboard tercatat segala jenis aktivitas serangan yang terjadi yang mengarah ke *IP* target yang diserang melalui pengujian serangan. Terdapat hasil 10 teratas serangan yang terdeteksi oleh *honeypot* sesuai dengan pengkategorian jenis serangan yang dimiliki oleh

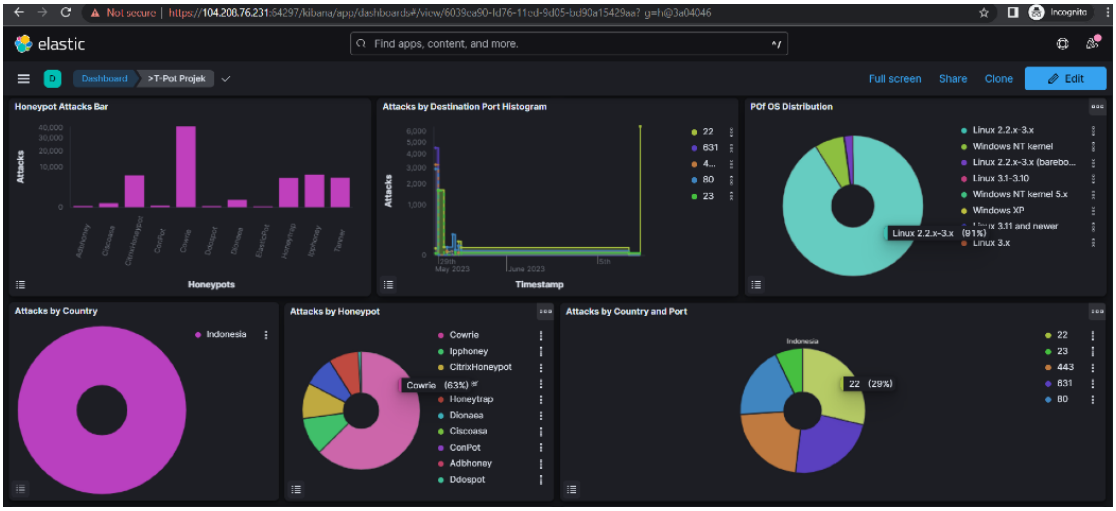
Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1284-1295
DOI : https://doi.org/10.35870/jimik.v4i3.325

honeypot, *cowrie attack* mencatat segala jenis serangan yang menuju ke dalam port, sehingga serangan Port *Scanning*, SSH, Telnet, semua tercatat di dalam *cowrie attack*. Dapat dilihat juga dalam kibana dashboard menampilkan 10 teratas *IP source* penyerang, yang dimana *IP address* 117.74.126.142 dan 114.10.125.183 adalah *IP address DHCP* dari *provider internet* yang digunakan oleh penyerang. Tercatat juga titik lokasi dari *IP address* penyerang di dalam kibana *dashboard*, dimana dua titik tersebut tercatat sebagai titik yang paling banyak melakukan serangan, pada bagian *alert description* tercatat beberapa peringatan akibat serangan yang dilakukan dan terdeteksi oleh sistem keamanan, yaitu *Scan Nmap,Http Request*, akses *password*, *SSH session, Stream packet with broken ack,* yang dimana *alert* tersebut merupakan peringatan dari serangan yang telah diujikan.



Gambar 10. *Kibana Dashboard* Password dan *Username Tag Cloud*

Dalam Kibana Dashboard tercatat *username* dan *password* yang digunakan ketika terdapat anomali, segala aktivitas tercatat oleh Honeypot dan divisualisasikan dalam Kibana Dashboard. Pada bagian diagram *cowrie attack by port* serangan yang dilakukan melalui SSH tercatat 80% serangan dan telnet 20% serangan yang tercatat melalui port tersebut, cowrie top URI download merupakan pencatatan log dari *malware attack*, dalam *T-Pot Path* tercatat nama file dan juga jumlah serangan yang dilakukan menggunakan file tersebut.



Gambar 11. Kibana *Dashboard Diagram Attacks*

Gambar 11 menunjukan bahwa persentase serangan menggunakan sistem operasi paling banyak adalah Linux 2.2x-3.x yaitu 91%, port paling banyak dituju adalah port 22 dengan 29% dan port 631

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1284-1295
DOI : https://doi.org/10.35870/jimik.v4i3.325

dengan 23%, dan serangan paling banyak adalah jenis cowrie dengan 63% dari jumlah serangan yang terdeteksi oleh *T-Pot Honeypot*.

Table 1. Hasil Data 5 deteksi serangan Tertinggi *Honeypot*

No	*IP Address*	Total Serangan Terdeteksi	Attacks				
			Cowrie	*Ipphoney*	*Citrix*	*Tanner*	*Honeytrap*
1	117.74.126.142	43904	33339	2265	3260	2294	2481
2	114.10.125.183	20113	6298	4532	3223	2938	2882
Jumlah Total		64017	39637	6797	6483	5232	5363

Pada Tabel 1 hasil dari serangan yang dilakukan penyerang dan terdeteksi oleh sistem *T-Pot Honeypot*, data serangan tersebut didapatkan dari tampilan *top* 10 serangan yang terjadi dan diolah kedalam tabel menjadi top 5 serangan yang terdeteksi oleh sistem *T-Pot Honeypot* dari 2 *IP Address* penyerang yaitu *cowrie* 39639, *Ipphoney* 6797, *Citrix* 6483, *Tanner* 5232, *Honeytrap* 5363, *attacker* melakukan penyerangan dengan menargetkan port ssh dan telnet sehingga serangan tersebut terdeteksi sebagai *cowrie attack*, *attacker* mengira bahwa *port* tersebut merupakan *port* dari web utama sehingga attacker mengirimkan berbagai serangan dengan tujuan untuk melumpuhkan web utama.

Table 2. Hasil Deteksi Serangan *T-Pot Honeypot*

Skenario Serangan	Jenis Serangan	*Tools*	*T-Pot Honeypot*				
			Jumlah Hit	Jumlah Deteksi	Percent Deteksi Hit (%)	Percent Deteksi (%)	*Alert*
1	*Port Scanning*	*Nmap*	14391	14163	98%	22%	Terdeteksi
2	*Brute Force*	*Metasploit*	25265	24567	97%	38%	Terdeteksi
3	*Malware*	*Mirai*	24	24	100%	0%	Terdeteksi
4	*DoS & DDoS*	*Hping3&Hammer*	26241	25263	96%	39%	Terdeteksi
Jumlah		65921	64017	97%	100 %		
Rata-Rata		16480	16004	98%	25%		

Pada Tabel 2 merupakan hasil pengolahan data dari log kibana dashboard yang digunakan untuk melakukan kalkulasi serangan yang dideteksi oleh *T-Pot Honeypot*. Data diambil dari skenario-skenario serangan yang telah dilakukan, sistem *T-Pot Honeypot* berhasil melakukan deteksi serangan yang diujikan dengan rata-rata persentase mendeteksi serangan dari jumlah hit yang diterima oleh *T-Pot* Honeypot lebih dari 95%, dan sistem T-Pot berhasil juga untuk mengetahui 65921 jumlah hit serangan yang terjadi dan mendeteksi 64017 itu sebagai sebuah ancaman dengan persentase 97% jumlah serangan yang terdeteksi.

Serangan yang dilakukan *attackers* ditujukan untuk mengetahui port mana saja yang terbuka, lalu kemudian memanfaatkan port tersebut untuk mendapatkan akses masuk dengan cara melakukan serangan *brute force*. Namun ketika proses serangan yang dilakukan attacker pada *port scanning*, *T-Pot* telah mendeteksi tersebut sebagai anomali sehingga secara otomatis *T-Pot* memberikan jalan kepada attacker untuk masuk kedalam sistem Honeypot dan memberikan segala informasi yang attacker inginkan seperti port mana saja yang terbuka dan terfilter. Konfigurasi *rules firewall* yang dilakukan

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1284-1295
DOI : https://doi.org/10.35870/jimik.v4i3.325

pada *cloud azure* dengan membuka port 0-65000 untuk dapat dimasuki dari segala jenis *resource*, tujuannya untuk menjebak *attackers* dan mengira bahwa port yang terbuka tersebut adalah akses utama untuk masuk kedalam sistem utama, segala jenis aktivitas yang dilakukan attacker terekam dan ketika attacker mengirimkan serangan kedalam sistem, semua jenis serangan yang dilakukan attacker terekam dan dikategorikan berdasarkan jenis deteksi serangan yang dimiliki oleh *T-Pot Honeypot* dan tersimpan di dalam Log.

Dilanjutkan dengan serangan menggunakan metode *brute force attack* melalui port ssh dan port telnet, dengan tujuan untuk bisa mendapatkan akses masuk kedalam sistem utama dan setelah mendapatkan akses *username* serta *password* melalui telnet. *Attacker* melakukan serangan dengan memberikan sebuah file *malware* ke dalam direktori target, dengan tujuan target tidak mengetahui bahwa terdapat file *malware* yang sangat berbahaya. Kemudian dilakukan serangan *DoS* dan *DDoS attack* dengan mengirimkan secara terus menerus paket data kedalam sistem, dengan tujuan membuat sistem itu menjadi down karena traffic data yang berlebihan. Sehingga ketika attacker melakukan serangan, server sistem utama tidak akan mengalami *down* atau menerima *request* terlalu banyak sehingga menyebabkan server utama menjadi *down*, karena tanpa *attacker* sadari, *attacker* sudah terjebak di dalam *T-Pot Honeypot.*

4. Kesimpulan dan Saran

Berdasarkan hasil dari penelitian, pengujian, dan analisis deteksi serangan *cyber* menggunakan *Honeypot*, dapat diambil kesimpulan bahwa sistem dari *T-Pot Honeypot* dapat mendeteksi secara cepat akurat anomali yang terjadi sehingga *cyberattack* dapat diantisipasi terlebih dahulu, dengan cara memberikan dia akses masuk kedalam sistem *T-Pot Honeypot* melalui port yang telah dibuka sehingga penyerang berfikir telah berhasil untuk masuk kedalam sistem utama. *Tools* yang disediakan oleh *T-Pot* sangat membantu untuk mendeteksi, menganalisa serangan dengan total serangan yang terdeteksi oleh sistem *T-Pot Honeypot* sebanyak 64017 serangan dengan perincian terdeteksi *39637 Cowrie attacks, 6797 Ipphoney attack, 6483 CitrixHoneypot Attacks, 5232 Tanner Attacks, 5363 Honeytrap Attacks, 359 Dionaea Attacks, 111 Ciscoasa Attacks, 19 Conpot Attacks, 10 AdbHoney Attacks, 10 Elasticpot Attacks.* Namun kelemahan yang dimiliki dari sistem *T-Pot Honeypot* ini adalah terdapat 1904 atau 3% Hit yang tidak terdeteksi oleh *T-Pot Honeypot,* yang dimana ini dapat menjadikan celah untuk *attacker* mengetahui bahwa mereka terjebak didalam sistem *Honeypot* dan mencari cara untuk bisa keluar dari jebakan *Honeypot.*

Saran yang dapat diberikan untuk penelitian dan pengembangan *T-Pot Honeypot* sebagai sebuah sistem keamanan yaitu, penambahan *tools* lain agar bisa mencegah dan segala jenis serangan *cyber* yang terjadi, menambahkan fitur untuk block serangan secara otomatis ketika terjadinya anomali tidak wajar yang terdeteksi oleh sistem.

5. Daftar Pustaka

[1] Nadeem, M., Arshad, A., Riaz, S., Band, S. S., & Mosavi, A. (2021). Intercept the cloud network from brute force and DDoS attacks via intrusion detection and prevention system. *IEEE Access*, *9*, 152300-152309. DOI: 10.1109/ACCESS.2021.3126535.

[2] Benyamin, J., Mualim, M., & Duarte, E. P. (2023). MANAJEMEN RISIKO KEAMANAN INFORMASI DALAM MEMINIMALISASI ANCAMAN SIBER PADA PUSAT DATA DAN TEKNOLOGI INFORMASI KOMUNIKASI BADAN SIBER DAN SANDI NEGARA GUNA MENINGKATKAN PERTAHANAN DAN KEAMANAN SIBER. *Manajemen Pertahanan: Jurnal Pemikiran dan Penelitian Manajemen Pertahanan*, *9*(1).

[3] Park, J., Kim, J., Gupta, B. B., & Park, N. (2021). Network log-based SSH brute-force attack detection model. *Computers, Materials & Continua*, *68*(1).

[4] Alam, S., & Kunang, Y. N. (2021). Analisis Serangan Brute Force Pada Ip Address Cctv (Closed Circuit Television) Menggunakan Metode Komputer Forensic. In *Bina Darma Conference on Computer Science (BDCCS)* (Vol. 3, No. 3, pp. 544-553).

[5] Widiyanto, W. W. (2022). SIMRS Network Security Simulation Using Snort IDS and IPS Methods. *Indonesian of Health Information Management Journal (INOHIM)*, *10*(1), 10-17. DOI: https://doi.org/10.47007/inohim.v10i1.396.

[6] TAŞÇI, H., Gönen, S., BARIŞKAN, M. A., KARACAYILMAZ, G., Alhan, B., & YILMAZ, E. N. (2021). Password Attack Analysis Over Honeypot Using Machine Learning Password Attack Analysis. *Turkish Journal of Mathematics and Computer Science*, *13*(2), 388-402.

[7] Amal, M. R., & Venkadesh, P. (2022). Review of cyber attack detection: Honeypot system. *Webology*, *19*(1), 5497-5514.

[8] Muhammad, R. M., Irawati, I. D., & Iqbal, M. (2021). Implementasi Sistem Keamanan Jaringan Lokal Menggunakan Honeypot Dionaea, Dan Ids, Serta Analisis Malware Menggunakan Malware Analysis System. *eProceedings of Applied Science*, *7*(3).

[9] Shivathmika, N., Divya, A., Lakshmi, K. A., & Manikandan, M. L. Intrusion Detection and Prevention Using Honeypot Network for Cloud Security.

[10] Wanjau, S. K., Wambugu, G. M., & Kamau, G. N. (2021). SSH-brute force attack detection model based on deep learning.

[11] Prakoso, R. D. Y. (2022). IMPLEMENTASI LOW INTERACTION HONEYPOT DAN PORT KNOCKING UNTUK MENINGKATKAN KEAMANAN JARINGAN. *Perwira Journal of Science & Engineering*, *2*(1), 16-23. DOI: https://doi.org/10.54199/pjse.v2i1.96.

[12] Duha, T., Setiawan, W., & Fajriyah, N. (2022). Analisis Layanan Cloud Computing Di Era Digital. *Jurnal Informatika*, *1*(1), 32-39. DOI: https://doi.org/10.57094/ji.v1i1.355.

[13] NURILAHI, D. K., MUNADI, R., SYAHRIAL, S., & Bahri, A. L. (2022). Penerapan Metode Naïve Bayes pada Honeypot Dionaea dalam Mendeteksi Serangan Port Scanning. *ELKOMIKA: Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, & Teknik Elektronika*, *10*(2), 309. DOI: https://doi.org/10.26760/elkomika.v10i2.309.

[14] Mulyanto, Y., Herfandi, H., & Kirana, R. C. (2022). Analisis Keamanan Wireless Local Area Network (Wlan) Terhadap Serangan Brute Force Dengan Metode Penetration Testing (Studi Kasus: Rs H. Lmanambai Abdulkadir). *Jurnal Informatika Teknologi dan Sains (Jinteks)*, *4*(1), 26-35. DOI: https://doi.org/10.51401/jinteks.v4i1.1528.

[15] Shurman, M. M., Khrais, R. M., & Yateem, A. A. (2020). DoS and DDoS attack detection using deep learning and IDS. *Int. Arab J. Inf. Technol.*, *17*(4A), 655-661.

[16] Putra, T. H. (2021). *IMPLEMENTASI PORT KNOCKING DAN TPOT HONEYPOT PADA PRIVATE CLOUD SERVER SEBAGAI PENDETEKSI SERANGAN DALAM JARINGAN* (Doctoral dissertation, Universitas Muhammadiyah Malang).

[17] Varma, P., Siddiqui, A., Vadher, P., & Baloda, V. (2020). Snort IDPS using Raspberry Pi 4. *International Journal of Engineering Research Technology (IJERT)*, *9*.

[18] Dermawati, R., & Siregar, M. H. (2020). Implementasi Honeypot Pada Jaringan Internet Labor Fakultas Teknik UNIKS Menggunakan Dionaea Sebagai Keamanan Jaringan. *Jurnal Ilmiah Edutic: Pendidikan dan Informatika*, *7*(1), 20-30. DOI: https://doi.org/10.21107/edutic.v7i1.8660.