Analisis Perbandingan *Behavior User Menggunakan Low Interaction Honeypot* dan IDS pada Sistem *Edge Computing*

Mokhamad Wildan Marzuqon[1], Agus Prihanto[2]
[1,2] Jurusan Teknik Informatika, Prodi Teknik Informatika, Fakultas Teknik, Universitas Negeri Surabaya
[1] mokhamad.18053@mhs.unesa.ac.id
[2] agusprihanto@unesa.ac.id

***Abstrak*— Saat ini perkembangan *Edge computing* semakin pesat, perkembangan ini juga disertai dengan ancaman yang begitu besar. *Egde server* merupakan sistem yang rentan terkena serangan. Serangan tersebut dapat berupa serangan *DoS, Port Scanning, Web Service Intrusion*, dan lain sebagainya. Maka dari itu diperlukan upaya pencegahan untuk meminimalisir risiko yang diakibatkan oleh serangan tersebut dengan cara menganalisis aktivitas *user* saat mengakses *edge server*. Penelitian ini bertujuan untuk mengetahui dan menganalisis aktivitas *user* saat mengakses edge server menggunakan Low Interaction Honeypot dan IDS. Pengujian yang dilakukan ya itu dengan dua skenario yaitu saat honeypot dinyalakan dan dimatikan. Hasil pengujian menunjukkan pada skenario honeypot dinyalakan, beban *edge server* menjadi berat, ditunjukkan dengan rata rata latensi sebesar 0,0085s. Selain itu, port layanan server yang terbuka juga lebih banyak sehingga meningkatkan peluang intruder untuk melakukan penyerangan terhadap *edge server*. Sedangkan pengujian dengan skenario honeypot dimatikan, beban edge server menjadi berkurang, hal ini ditunjukkan dengan rata rata latensi sebesar 0,0055s. Selain itu port layanan server yang terbuka hanya layanan yang berasal dari Windows dan XAMPP, sehingga aktivitas *intruder* yang dilakukan menjadi terbatas. Pengujian tersebut menunjukkan semakin banyak port dan layanan server yang terbuka, semakin tinggi risiko penyerangannya, dan dengan adanya honeypot risiko tersebut dapat dikurangi dengan menganalisis aktivitas intruder dengan menentukan rules yang tepat untuk pencegahan serangan.**

Kata Kunci*— *Edge computing*, Honeypot, IDS, *Bevioral Profiling

I. PENDAHULUAN

Perkembangan teknologi *Internet of Things* (IoT) saat ini semakin pesat, terbukti dengan semakin banyaknya penggunaan perangkat IoT di berbagai sektor kehidupan seperti rumah tangga, instansi pemerintahan, *smart city*, dan lain sebagainya. Hal ini berdampak pada semakin banyaknya data yang diproses dalam jaringan global. *International Data Corporation* (IDC) memperkirakan pertumbuhan datasphere global pada tahun 2025 mencapai 163 Zettabytes dan akan terus bertambah kedepannya [1] . Menjawab fenomena tersebut, saat ini teknologi *edge computing* mulai banyak digunakan, khususnya bagi perusahaan besar yang bergerak dibidang IoT. *Edge computing* merupakan sebuah sistem komputasi pada arsitektur perangkat IoT yang difokuskan untuk memperoleh dan memproses aliran data dan penyimpanan dengan sedekat mungkin dari sumber data atau nodes [2] . Sistem *edge computing* ini berada pada layer *edge side* pada arsitektur IoT. Perangkat *edge computing* dapat memiliki fungsi yang berbeda beda bergantung pada posisi dan role nodes yang bersangkutan [3] .

Menurut data survei dari IBM, kedepannya sebanyak 91% perusahaan dunia akan menerapkan sistem *edge computing* dalam bisnisnya [4] . Sistem *edge computing* memungkinkan pengolahan data, penyimpanan, dan pusat kontrol menjadi lebih dekat dengan *user*. Dengan demikian, pengolahan data dalam jaringan *edge* menjadi lebih efektif dan efisien sekaligus dapat menekan latensi dan bandwidth jaringan seminimal mungkin [5] .

Penggunaan teknologi *edge computing* yang semakin masif, tidak terlepas dari isu keamanan jaringan dan data didalamnya. Banyaknya data yang diproses dan posisi sistem *edge computing* yang dekat dengan *user*, menyebabkan sistem *edge computing* rawan untuk disusupi *intruder*. Menurut data dari Kaspersky, Indonesia menempati urutan terbanyak ke 9 kasus serangan penyusup atau *intrusion attack* dengan serangan terbanyak yakni 484291 kali dalam sehari selama Februari 2022. Hal ini menunjukkan bahwa sistem keamanan jaringan di Indonesia, khususnya jaringan *edge computing* sangat rentan untuk disusupi. Maka dari itu sebagai tindakan preventif untuk mencegah adanya *intruder* dalam sebuah jaringan, khususnya jaringan *edge computing*, diperlukan suatu metode pendeteksi serangan yang baik dengan menganalisis perilaku *user* atau disebut juga metode *user behavior profiling*.

User Behavioral Profiling adalah suatu metode keamanan jaringan tingkat lanjut yang bekerja dengan menganalisis data aktivitas suatu pengguna dan menentukan profil perilaku pengguna tersebut atau sistem komputasi [6]. Teknik ini memungkinkan sistem untuk mendeteksi anomali

tindakan yang dilakukan oleh pengguna atau *intruder*. Penggunaan *Behavioral Profiling* dalam sistem keamanan dapat dilakukan dengan menggunakan honeypot dan Software Intrusion Detection System (IDS).

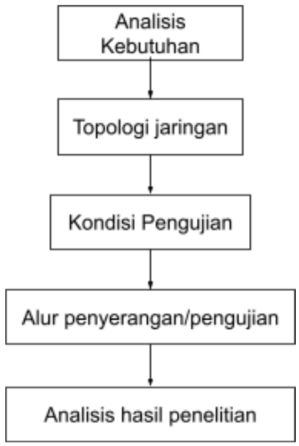
Honeypot merupakan sebuah sistem keamanan jaringan yang dibuat menyerupai lingkungan server atau client yang asli dan berfungsi sebagai umpan atau *decoy* yang dapat menjebak *intruder* dan *intruder* [7] . Honeypot biasanya digunakan sebagai pengalih perhatian, pendeteksi dan analisis serangan, serta sebagai pencegah serangan. Sedangkan *Intrusion Detection System* (IDS) merupakan sebuah sistem keamanan jaringan yang dapat mendeteksi adanya tindakan mencurigakan oleh *intruder* dan dapat melaporkan tindakan tersebut kepada administrator jaringan [8] . Laporan ini biasanya berbentuk log yang memuat data data percobaan serangan oleh *intruder*.

Penelitian sebelumnya telah dilakukan oleh Ernest Bonnah dan Ju Shiguang, 2020 "DecChain: A decentralized security approach in *Edge computing* based on Blockchain" yang menghasilkan simpulan bahwa salah satu cara untuk meningkatkan keamanan dalam *edge computing* salah satunya dapat menggunakan *Decentralized Blockchain* [9] . Penggunaan sistem desentralisasi Blockchain dalam arsitektur jaringan *edge computing* tersebut dapat mengautentikasi setiap elemen yang terdapat dalam jaringan *edge computing* dan menghilangkan *public trusted entity* dalam jaringannya. Mengacu pada penelitian tersebut, sistem keamanan pada *edge computing* selain dapat diterapkan pada arsitektur jaringannya, juga dapat diterapkan pada sistem pencegahan penyusup atau Intrusion Prevention System di setiap node dan server [10] . Hal inilah yang menjadi pembeda dengan penelitian sebelumnya yang berfokus pada penerapan keamanan pada arsitektur jaringan *edge computing* saja.

Pada penelitian ini, difokuskan untuk menganalisis *behavior user* menggunakan *Low Interaction Honeypot* sebagai *decoy* sekaligus menerapkan software *intrusion detection system* (IDS) sebagai alat untuk mendeteksi lalu lintas jaringan. Selain itu peneliti juga akan membandingkan performa jaringan *edge computing* meliputi *opened port* dan latensi saat diterapkan honeypot dan tanpa honeypot dengan skenario serangan web server HTTP, FTP, IP Flooding, dan Port Scanning. *User behavior* yang berbentuk log dari honeypot dan IDS inilah yang akan menjadi dasar administrator jaringan untuk menentukan rules yang tepat pada firewall sistem *edge computing* untuk mencegah adanya *intruder*.

II. METODE PENELITIAN

Jenis penelitian ini merupakan penelitian berbasis eksperimen, yaitu metode penelitian yang bertujuan untuk meneliti dan menganalisis perbandingan *behavior user* menggunakan *Low Interaction Honeypot* dan IDS pada sistem *edge computing*. *Behavior* atau kebiasaan *user* inilah nantinya yang akan digunakan oleh administrator jaringan *edge computing*, khususnya server edge sebagai pertimbangan dalam penyusunan rules pada firewall jaringan. Metode merupakan suatu cara yang disusun sedemikian rupa untuk mencapai tujuan tertentu. Beberapa tahap yang telah dilakukan dalam analisis *behavior user* pada jaringan *edge computing* sebagai berikut :



Gbr 1. Skenario penelitian

A. *Analisis Kebutuhan*

Tahap pertama dalam penelitian ini adalah analisis kebutuhan yang akan digunakan dalam penelitian. Dalam analisis *behavior user* pada sistem *edge computing* ini dibagi menjadi beberapa bagian yaitu :

1) Kebutuhan Data: Data yang digunakan dalam penelitian ini bersumber dari beberapa referensi. Referensi yang diambil berasal dari jurnal nasional dan internasional, serta dokumentasi resmi dari IBM dan Seagate. Penggunaan data yang lengkap dan akurat dapat membuat hasil penelitian ini menjadi lengkap dan terarah. Proses pengumpulan data pada penelitian ini terbagi menjadi dua jenis, yaitu studi literatur dan observasi langsung.

a. Studi Literatur

Penelitian ini mengambil beberapa referensi dari berbagai macam artikel dan literatur yang relevan dengan metode *User Behavioral Profiling* menggunakan Honeypot dan IDS pada sistem *edge computing*. Literatur yang digunakan diantaranya berupa jurnal nasional dan

internasional, video dari Youtube, tesis, situs resmi, dan beberapa sumber di internet

b. Observasi

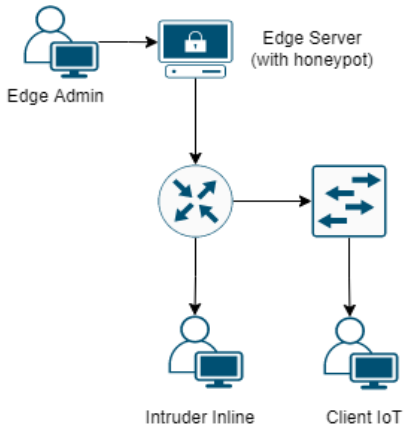
Penelitian ini juga dilakukan observasi dengan mengunjungi beberapa situs referensi mengenai penggunaan Honeypot dan IDS sebagai *User Behavioral Profiling* serta melakukan analisis serangan cyber threat pada situs Cybermap Kaspersky.

2) Kebutuhan Alat: Spesifikasi perangkat pendukung yang dibutuhkan dalam penelitian ini adalah sebagai berikut :

a. Virtualbox sebagai media virtualisasi perangkat client, server, dan router menggunakan sistem operasi Windows XP pada PC *edge server* dan Ubuntu pada PC *intruder*
b. GNS3 sebagai media virtualisasi jaringan *edge computing*
c. Valhala sebagai *Low Interaction Honeypot* yang berperan sebagai server *decoy*
d. Nmap, LOIC, CMD, Web browser, dan Filezilla sebagai tools penyerangan pada *edge server* (*intruder*)
e. Wireshark sebagai IDS dan media monitoring anomali pada lalu lintas jaringan *edge computing*

B. Topologi Jaringan

Desain topologi jaringan menggambarkan perancangan sistem *edge computing* dengan menggunakan honeypot dan IDS.



Gbr 2. Topologi jaringan

Pada gambar topologi diatas, PC *edge server* menggunakan OS Windows XP dengan IP 192.168.20.2 sedangkan PC *intruder* terhubung langsung dengan PC *edge server* melalui router dengan IP 192.168.30.2 menggunakan OS Ubuntu. Penyerangan dilakukan langsung dari PC *intruder* menuju PC *edge server*. Pemantauan serangan dilakukan pada PC *edge server* dengan Valhala Honeypot dan Wireshark sebagai IDS.

C. Kondisi Pengujian

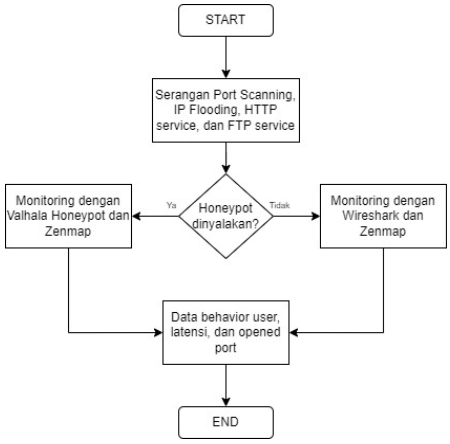
Serangan yang akan dianalisis dalam pengujian ini adalah serangan Port Scanning, DoS (IP Flooding), HTTP service, dan FTP service. Adapun kondisi pengujian pada penelitian ini sebagai berikut:

1) Honeypot Diaktifkan: Kondisi pengujian ini dilakukan dengan mengaktifkan layanan server dari honeypot Valhala dan KfSensor. Layanan server yang diaktifkan yaitu HTTP dan FTP. Layanan server tersebut dibuat semirip mungkin dengan aslinya untuk menjadi umpan bagi penyerang. Penyerang akan melakukan serangan terhadap *edge server* melalui layanan server yang disediakan oleh honeypot. Segala bentuk aktivitas yang coba dilakukan oleh penyerang terhadap layanan server pada honeypot akan otomatis terekam dan tampil dalam bentuk log aktivitas.

2) Honeypot Dimatikan: Kondisi pengujian ini dilakukan dengan menonaktifkan layanan server pada honeypot Valhala dan KfSensor. Penyerang akan berinteraksi dengan *edge server* secara langsung tanpa ada perantara sebelumnya. Pemantauan segala aktivitas yang dilakukan oleh penyerang dilakukan menggunakan aplikasi Wireshark.

D. Alur Pengujian

Untuk memahami alur pengujian pada penelitian ini, maka dibuatlah skema alur pengujian sebagai berikut:



Gbr 3. Alur pengujian

E. Analisis Hasil Penelitian

Penarikan kesimpulan atas pengujian diambil dari data log yang disediakan oleh honeypot Valhala dan KfSensor serta data dari Wireshark. Berdasarkan data tersebut akan diketahui beberapa hasil seperti :

1) User Behavior Analytics: User Behavior Analytics adalah analisis aktivitas apa saja yang dilakukan oleh penyerang terhadap layanan *edge server* dan honeypot. Aktivitas inilah yang akan menjadi acuan dan referensi untuk menentukan *security rule* pada firewall.

2) Latensi: Latensi adalah waktu yang dibutuhkan untuk berkomunikasi dalam suatu jaringan. Latensi merupakan salah satu faktor penting yang perlu diperhatikan dalam komunikasi dalam jaringan. Pada pengujian ini akan dibandingkan kebutuhan latensi saat honeypot diaktifkan dan dimatikan.

3) Opened Port: Opened port merupakan daftar port yang terbuka pada suatu layanan server atau komputer. Semakin banyak port yang terbuka, maka semakin rentan pula sistem tersebut untuk disusupi. Dalam pengujian ini akan dibandingkan port apa saja yang terbuka saat layanan server pada honeypot diaktifkan dan dimatikan.

III. HASIL DAN PEMBAHASAN

Penyerangan / pengujian pada *edge server* menggunakan Virtualbox dan GNS3 sebagai media virtualisasi perangkat dan jaringannya. Peneliti menggunakan Virtualbox versi 6.1 dan GNS3 versi 2.2.31. PC *edge server* menggunakan OS Ubuntu dan PC *intruder* menggunakan OS Windows XP.

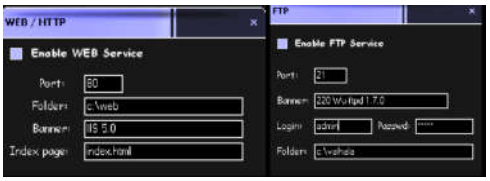
A. Pengujian Port Scanning

Berikut skenario pengujian dengan melakukan port scanning terhadap *edge server*.

1) Honeypot Dinyalakan: Pengujian pertama yaitu Port Scanning dengan honeypot diaktifkan, pengujian ini dilakukan untuk mengetahui port apa saja yang terbuka selama honeypot diaktifkan dan dimatikan. Langkah pertama yaitu pada PC *edge server* buka Valhala Honeypot kemudian pilih layanan server yang diaktifkan pada menu "Server Config".

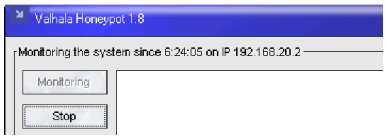
Gbr 4. Server *config* Valhala Honeypot

Pada gambar diatas layanan server honeypot yang diaktifkan dalam pengujian ini adalah layanan Web Server dan FTP Server.



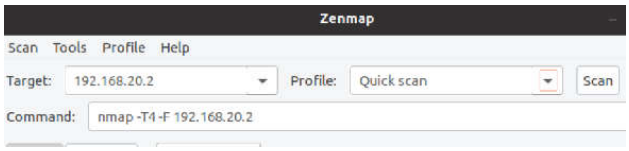
Gbr 5. *Config* HTTP dan FTP Server

Peneliti menggunakan port 80 sebagai Web Server dan port 21 sebagai FTP Server. Setelah layanan server honeypot berhasil terkonfigurasi, selanjutnya aktifkan server honeypot dengan klik tombol "Monitoring".



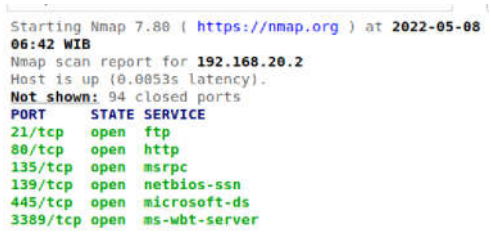
Gbr 6. *Start monitoring*

Pada gambar diatas menunjukkan waktu dimulainya monitoring honeypot beserta IP server saat ini yaitu 192.168.20.2. IP inilah yang akan menjadi target pengujian nantinya. Untuk melakukan pengujian port scanning, pada PC *intruder* buka Zenmap untuk memulai proses scanning.



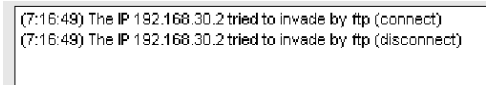
Gbr 7. *Addressbar* Zenmap

Setelah aplikasi Zenmap terbuka, masukkan IP target yaitu 192.168.20.2 dan metode scan "Quick scan" kemudian tekan "Scan". Lalu akan tampil hasil scan dari proses tersebut.



Gbr 8. Hasil *scan* Zenmap

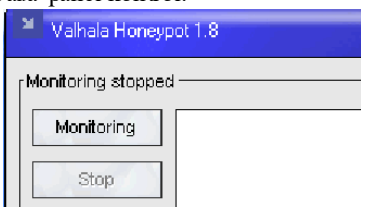
Pada gambar diatas ditampilkan port apa saja yang terbuka pada *edge server*. Port 21 dan 80 merupakan port yang berasal dari honeypot, sedangkan port 135, 139, 445, dan 3389 merupakan port layanan dari Windows XP. Analisis *behavior user* saat terjadinya port scanning dapat diketahui dari hasil respon Valhala honeypot berikut.



Gbr 9. Respon Valhala Honeypot

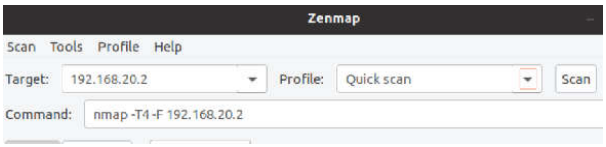
Gambar diatas menunjukkan aktivitas penyerangan meliputi waktu penyerangan, IP penyerang, dan layanan apa yang coba diserang pada server honeypot. Dengan demikian edge admin dapat dengan mudah melacak kemungkinan aktivitas mencurigakan yang dilakukan oleh *intruder*. Selain itu dengan terbukanya port HTTP dan FTP, *intruder* akan mudah melakukan penyerangan terhadap port tersebut. Kebutuhan latensi *edge server* saat honeypot diaktifkan membutuhkan rata rata waktu 8,5 ms dengan tiga kali pengujian.

2) Honeypot Dimatikan: Pengujian selanjutnya yaitu saat honeypot dimatikan. Untuk mematikan honeypot cukup tekan "stop" pada panel kontrol.



Gbr 10. *Stop monitoring*

Setelah di klik "Stop" maka akan ada indikator bahwa proses monitoring sudah berhenti. Untuk memulai proses scanning, kembali ke Zenmap dan klik "Scan".



Gbr 11. Addressbar zenmap

Kemudian akan tampil hasil scanning saat honeypot dimatikan sebagai berikut.

Gbr 12. Hasil scan Zenmap

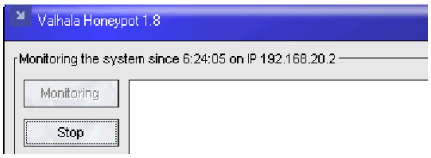
Pada gambar diatas menunjukkan perbedaan port yang terbuka dengan saat honeypot diaktifkan. Port yang terbuka hanya port 135, 139, 445, dan 3389 yang merupakan port layanan dari Windows XP, sedangkan port FTP 21 dan HTTP 80 tertutup.

Behavior user saat honeypot dimatikan hanya bisa melakukan serangan hanya pada port yang terbuka tersebut, sehingga penyerang tidak memiliki akses untuk melakukan penyerangan terhadap layanan HTTP maupun FTP. Kebutuhan latensi *edge server* saat honeypot dimatikan membutuhkan rata rata waktu 5,5 ms dengan tiga kali pengujian.

B. Pengujian Serangan DoS (IP Flooding)

Pengujian selanjutnya yaitu dengan melakukan Dos Attack pada *edge server* menggunakan metode IP Flooding. Pengujian ini memiliki dua kondisi yaitu :

1) Honeypot Dinyalakan: Pengujian menggunakan honeypot Valhala sebagai penyedia layanan FTP dan HTTP server. Aktifkan layanan honeypot pada PC *edge server* dengan klik "Monitoring" pada tombol panel.



Gbr 13. *Start monitoring*

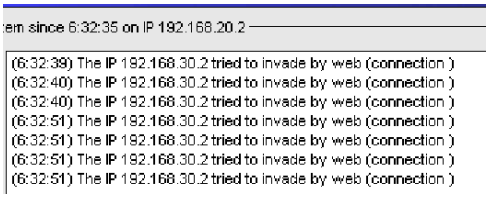
Gambar diatas menunjukkan bahwa Valhala Honeypot sudah berhasil diaktifkan dengan IP 192.168.20.2. Untuk memulai serangan, peneliti menggunakan aplikasi Low Orbit Ion Cannon (LOIC) v1.0.8.0. Penyerangan dilakukan dari PC *intruder* dengan IP 192.168.30.2.

Gbr 14. *Addressbar* LOIC

Pada kolom IP target masukkan IP dari *edge server* kemudian klik "Lock on" untuk mengunci target.

Gbr 15. Konfigurasi serangan LOIC

Kemudian masukkan port tujuan dan method penyerangannya. Peneliti menggunakan port 80 dengan method TCP yang merupakan port layanan HTTP server. Setelah itu dilakukan penyerangan pada *edge server*. Hasil respon dari Valhala honeypot atas penyerangan tersebut dapat dilihat dari gambar berikut.



Gbr 16. Respon Valhala Honeypot HTTP

Pada gambar diatas ditampilkan *behavior user* saat melakukan penyerangan pada layanan HTTP server

honeypot. Log tersebut memuat waktu penyerangan, IP penyerang, dan layanan HTTP server yang coba diserang dengan beberapa kali percobaan. Pengujian juga dilakukan dengan melakukan IP Flooding pada port TCP 21 dengan hasil respon honeypot berikut.

Gbr 17. Respon Valhala Honeypot FTP

Pada gambar diatas ditunjukkan *behavior user* dengan melakukan beberapa kali percobaan penyerangan terhadap layanan FTP pada *edge server*. Pada pengujian Dos Attack dengan metode IP Flooding saat honeypot dinyalakan memiliki waktu rata rata latensi yaitu 8,5 ms dengan tiga kali pengujian.

2) Honeypot Dimatikan: Pengujian selanjutnya yaitu saat layanan honeypot dimatikan. Untuk mematikan honeypot cukup tekan tombol "Stop" dan honeypot akan mati. Untuk melakukan penyerangan IP Flooding, buka aplikasi LOIC pada PC *intruder*.

Gbr 18. *Addressbar* LOIC

Pada gambar diatas IP yang digunakan tetap sama dengan pengujian sebelumnya yaitu 192.168.20.2 yang merupakan IP dari PC *edge server*. Kemudian akan dilakukan penyerangan terhadap port 80 dengan method UDP.

Gbr 19. Konfigurasi serangan LOIC

Untuk mengetahui respon *edge server* terhadap pengujian tersebut, peneliti menggunakan Wireshark sebagai aplikasi monitoringnya. Berikut hasil capture dari Wireshark.

No.	Time	Source	Destination	Protocol	Length
2602…	365.265659	192.168.20.2	192.168.30.2	ICMP	102
2602…	365.265738	192.168.20.2	192.168.30.2	ICMP	102
2602…	365.272539	192.168.30.2	192.168.20.2	UDP	74
2602…	365.272625	192.168.30.2	192.168.20.2	UDP	74
2602…	365.272760	192.168.30.2	192.168.20.2	UDP	74
2602…	365.272836	192.168.30.2	192.168.20.2	UDP	74
2602…	365.273217	192.168.20.2	192.168.30.2	ICMP	102
2602…	365.273336	192.168.20.2	192.168.30.2	ICMP	102
2602…	365.273392	192.168.20.2	192.168.30.2	ICMP	102
2602…	365.273446	192.168.20.2	192.168.30.2	ICMP	102

Gbr 20. Hasil pantauan Wireshark

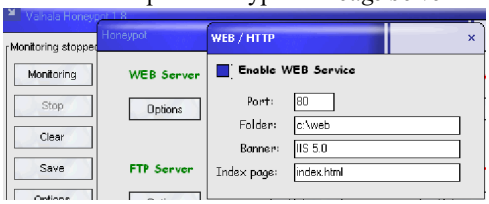
Gambar diatas menunjukkan *behavior user* dengan adanya percobaan penyerangan terhadap *edge server* (IP 192.168.20.2) oleh PC *intruder* (IP 192.168.30.2). PC *intruder* melakukan penyerangan menggunakan method UDP dan mendapat balasan dari PC *edge server* dengan method ICMP.

Pada pengujian ini didapatkan latensi *edge server* dengan rata rata waktu 13,7 ms dengan tiga kali pengujian. Hal ini menunjukkan bahwa server yang tidak menggunakan honeypot akan rentan mengalami down saat terjadi serangan Dos Attack, khususnya IP Flooding.

C. *Pengujian HTTP Service*

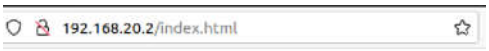
Pengujian HTTP service dilakukan untuk mengetahui *behavior user* saat mengakses suatu website yang di hosting oleh *edge server*.

1) Honeypot Dinyalakan: Pada pengujian ini menggunakan layanan web/HTTP server disediakan oleh Valhala Honeypot. Langkah pertama yaitu menyalakan layanan HTTP server pada honeypot PC *edge server*.



Gbr 21. Konfigurasi HTTP Server Valhala

Pada gambar diatas pengaturan HTTP server pada Valhala Honeypot menggunakan port 80 dengan IP 192.168.20.2. File website disimpan pada folder C:\web dengan Index page yaitu index.html, page inilah yang akan menjadi homepage dari website saat dibuka pertama kali. Untuk mengakses website tersebut, buka browser Mozilla Firefox pada PC *intruder*. dan masukkan IP PC *edge server* sebagai alamat website.

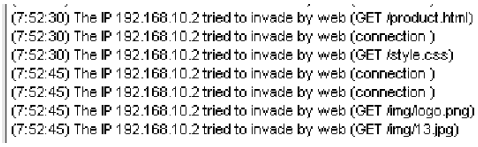


Gbr 22. Alamat web PC Edge Server

Alamat 192.168.20.2/index.html digunakan untuk mengakses file index.html pada PC *edge server*. Jika berhasil terhubung, kemudian akan tampil halaman pertama dari website tersebut. Peneliti menggunakan website pemesanan kopi. Percobaan interaksi dengan mencoba halaman produk dengan klik menu "Product" dan akan tampil halaman produk.

Gbr 23. Halaman "Product"

Interaksi tersebut akan mendapatkan respon dari Valhala honeypot sebagai berikut



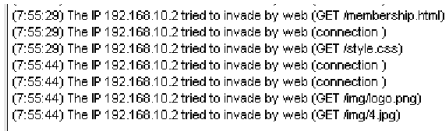
Gbr 24. Respon Valhala Honeypot

Pada gambar diatas akan terlihat *behavior user* dengan adanya waktu penyerangan, IP penyerang, dan apa saja yang coba diakses dari halaman product.html, termasuk gambar dan file yang ada pada halaman tersebut.

Kemudian peneliti mencoba mengakses halaman membership dengan klik tombol "Membership" dan akan tampil halaman berikut

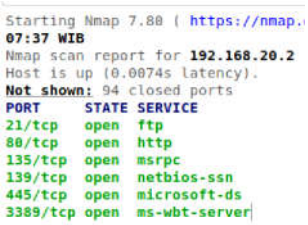
Gbr 25. Halaman "Membership"

Interaksi tersebut akan mendapatkan respon dari Valhala honeypot sebagai berikut



Gbr 26. Respon Valhala Honeypot

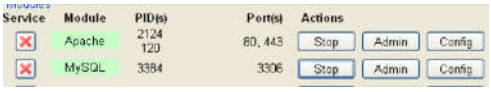
Pada gambar diatas akan terlihat *behavior user* dengan adanya waktu penyerangan, IP penyerang, dan apa saja yang coba diakses dari halaman membership.html, termasuk gambar dan file yang ada pada halaman tersebut. Sehingga akan diketahui aktivitas apa saja yang kemungkinan mencurigakan yang dilakukan oleh *intruder*.



Gbr 27. Port yang terbuka

Gambar diatas menunjukkan port yang terbuka saat pengujian dengan honeypot. Port 21 dan 80 merupakan port dari layanan Valhala Honeypot.

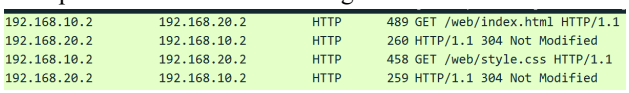
2) Honeypot Dimatikan: Pengujian HTTP service selanjutnya dengan mematikan honeypot. Pengujian HTTP service saat honeypot dimatikan, peneliti menggunakan XAMPP sebagai HTTP server pada PC *edge server*.



Gbr 28. Konfigurasi Server XAMPP

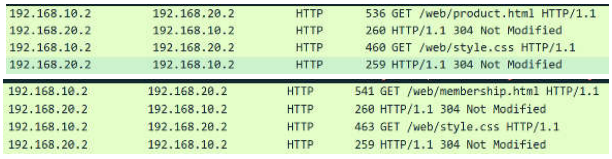
Pada gambar diatas menunjukkan layanan Apache dan MySQL dari XAMPP yang berhasil diaktifkan pada PC *edge server* sebagai HTTP server. File website sebelumnya sudah disimpan pada folder C:\xampp\htdocs agar bisa diakses. Selanjutnya untuk mengakses website tersebut, pada PC *intruder* buka browser Mozilla Firefox dan masukkan alamat web dari *edge server* yaitu 192.168.20.2/web/index.html.

Behavior user saat mengakses halaman index.html akan ter capture dalam Wireshark sebagai berikut



Gbr 29. Hasil *capture* Wireshark

Pada gambar diatas menunjukkan lalu lintas data dan apa saja aktivitas jaringan yang dilakukan antara PC *edge server* dan PC *intruder*. Koneksi tersebut menggunakan protokol HTTP dan PC *intruder* mencoba melakukan akses terhadap file index.html dan style.css Aktivitas selanjutnya yaitu mengakses halaman product dan membership dengan klik menu "Product" dan "Membership" kemudian mendapatkan hasil capture Wireshark sebagai berikut



Gbr 30. Hasil *capture* Wireshark

Gambar diatas menunjukkan aktivitas *user* berupa interaksi PC *intruder* dan PC *edge server* dengan mengakses

file product.html, membership.html, dan style.css dengan menggunakan protokol HTTP.

```
Starting Nmap 7.80 ( https://nmap.or
07:35 WIB
Nmap scan report for 192.168.20.2
Host is up (0.0074s latency).
Not shown: 92 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
3306/tcp open  mysql
3389/tcp open  ms-wbt-server
```

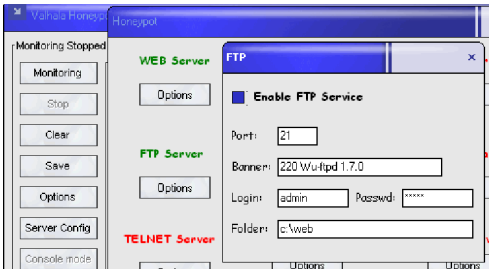
Gbr 31. Port yang terbuka

Gambar diatas menunjukkan port yang terbuka saat honeypot dimatikan. Port 21, 80, dan 3306 merupakan layanan yang terbuka dari XAMPP

D. Pengujian FTP Service

Pengujian terakhir adalah pengujian layanan FTP oleh PC *edge server*. Pengujian ini menggunakan Valhala Honeypot dan XAMPP sebagai FTP servernya. Pengujian ini memiliki dua kondisi sebagai berikut.

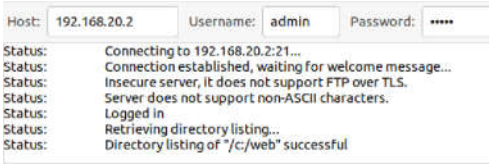
1) Honeypot Dinyalakan: Pengujian ini menggunakan layanan FTP server dari Valhala Honeypot. Aktifkan Valhala Honeypot dari PC *edge server*.



Gbr 32. Konfigurasi FTP Server Valhala

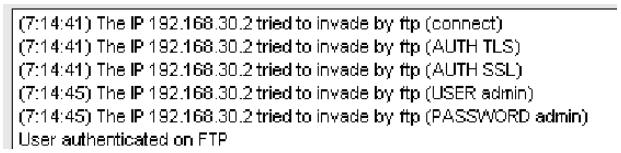
Gambar diatas merupakan tampilan layanan FTP server pada Valhala, kemudian *user*name dan password di set sebagai "admin". Folder akses FTP menggunakan folder "web" pada Local Disk C di PC *edge server*. Pengujian FTP service dilakukan menggunakan aplikasi FileZilla pada PC *intruder*.

Buka FileZilla kemudian masukkan host 192.168.20.2 yang merupakan IP PC *edge server*. Masukkan juga *user*name dan password dengan "admin". Kemudian klik Quick connect. Jika proses berhasil, maka akan tampil respon dari FileZilla sebagai berikut



Gbr 33. Koneksi FTP Berhasil

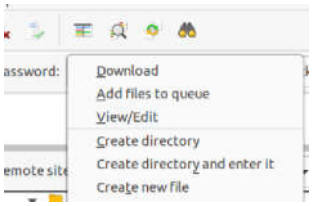
Gambar diatas menunjukkan bahwa proses koneksi FTP dan akses ke folder web pada PC *edge server* berhasil. Pada Valhala Honeypot juga terdapat respon sebagai berikut



Gbr 34. Respon FTP dari Valhala

Gambar tersebut menunjukkan *behavior user* saat mengakses FTP service menggunakan honeypot. Didapatkan waktu akses, IP penyerang, dan aktivitas yang dilakukan oleh penyerang (koneksi dan autentikasi). Setelah FTP service berhasil tersambung, maka peneliti melakukan percobaan

mengunduh file index.html yang ada pada folder "web" di PC *edge server*, dengan cara klik kanan file tersebut kemudian tekan download.



Gbr 35. *Download file* melalui FTP

Setelah proses download selesai, file index.html akan disimpan dalam penyimpanan pada PC *intruder*. Adapun respon dari Valhala sebagai berikut

```
(7:17:16) The IP 192.168.30.2 tried to invade by ftp (CWD /c:/web)
(7:17:16) The IP 192.168.30.2 tried to invade by ftp (SIZE /c:/web/index.html)
(7:17:16) The IP 192.168.30.2 tried to invade by ftp (MDTM /c:/web/index.html)
(7:17:16) The IP 192.168.30.2 tried to invade by ftp (ASCII)
(7:17:16) The IP 192.168.30.2 tried to invade by ftp (PASV )
(7:17:16) The IP 192.168.30.2 tried to invade by ftp (GET /c:/web/index.html)
(7:18:24) The IP 192.168.30.2 tried to invade by ftp (disconnect)
```

Gbr 36. Respon Valhala Honeypot

Gambar tersebut menunjukkan *behavior user* saat mencoba mengunduh file index.html pada PC *edge server*. Adapun port yang terbuka saat pengujian FTP service menggunakan Valhala Honeypot sama dengan port yang terbuka saat pengujian HTTP service yaitu port FTP 21 dan HTTP 80 dari honeypot.

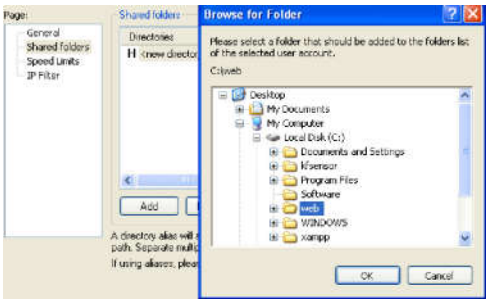
2) Honeypot Dimatikan: Pengujian selanjutnya yaitu dengan mematikan Valhala Honeypot dan mengaktifkan FTP server dari XAMPP sebagai penggantinya.

Gbr 37. Konfigurasi FTP Server XAMPP

Gambar diatas menunjukkan tampilan XAMPP jika FTP server (FileZilla) berhasil diaktifkan. Selanjutnya memulai pengaturan *user* dan folder akses melalui FTP admin dengan klik "Admin".

Gbr 38. Add user account FTP

Gambar tersebut menunjukkan pengaturan akun pada "Account Setting" FTP XAMPP. Untuk menambahkan *user* baru, klik "add *user*" kemudian masukkan *user*name "ftpserver" dan atur password "admin" pada Account Setting. Selanjutnya mengatur folder akses untuk FTP.

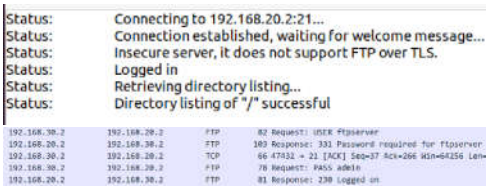


Gbr 39. Pengaturan folder akses FTP

Pengaturan folder akses dilakukan dengan klik "Shared Folders" kemudian ditambahkan folder "web" untuk diberi akses shared via FTP. Kemudian klik "OK" dan proses pengaturan FTP server sudah selesai.

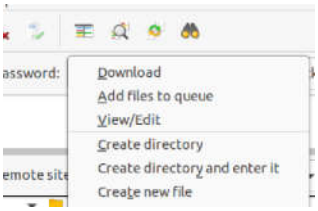
Selanjutnya kembali ke PC *intruder* dan buka FileZilla dan masukkan IP host, *user*name, dan password, kemudian klik "Quick connect"

Setelah percobaan koneksi berhasil, akan tampil respon dari FileZilla dan Wireshark sebagai berikut



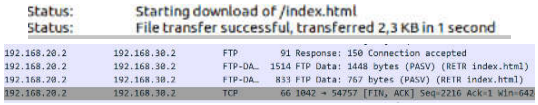
Gbr 40. Respon FileZilla

Setelah koneksi FTP berhasil, maka selanjutnya adalah percobaan mengunduh file index.html yang ada pada folder "web" di PC *edge server*. Pengunduhan dilakukan dengan cara klik kanan file index.html kemudian klik "download"



Gbr 41. Download file melalui FTP

Jika proses pengunduhan berhasil, maka akan mendapatkan repon dari FileZilla dan Wireshark sebagai berikut



Gbr 42. Respon FileZilla dan Wireshark

Percobaan koneksi FTP dan pengunduhan file yang dilakukan oleh PC *intruder* terhadap PC *edge server* merupakan suatu *behavior* yang dapat dianalisis oleh edge admin selanjutnya. Data *behavior user* bisa didapatkan dari

log FileZilla, Wireshark, maupun Valhala Honeypot. Adapun port yang terbuka saat pengujian FTP service menggunakan XAMPP sama dengan port yang terbuka saat pengujian HTTP service yaitu port FTP 21, HTTP 80, dan MySQL 3306 dari layanan XAMPP.

IV. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan penelitian yang telah dilakukan, peneliti berhasil melakukan pemantauan *behavior user* terhadap PC *edge server* pada pengujian *Port scanning, IP Flooding, HTTP service, dan FTP service* menggunakan Valhala Honeypot sebagai *decoy* atau umpan dan Wireshark sebagai alat pemantau lalu lintas jaringan dan IDS. Pada pengujian dengan honeypot didapatkan rata rata latensi server sebesar 0,0085 detik dan pengujian tanpa menggunakan honeypot didapatkan rata rata latensi server sebesar 0,0055 detik. Hal ini menunjukkan bahwa dengan adanya honeypot, beban *edge server* semakin berat dan dapat meningkatkan risiko penyerangan karena port yang terbuka lebih banyak dari biasanya. Akan tetapi, penerapan honeypot dapat membantu meningkatkan keamanan pada *edge server* dan dapat membantu edge admin untuk menganalisis dan melakukan tindakan pencegahan terhadap serangan terhadap *edge server* dengan memanfaatkan log aktivitas *intruder* dan *user* yang dihasilkan oleh Valhala Honeypot dan Wireshark.

B. Saran

Dari hasil penelitian yang didapatkan, peneliti memeberikan saran kedepannya untuk menggunakan *Low Interaction Honeypot* versi lainnya untuk menambah keakuratan dan efisiensi. Selain itu, tipe serangan juga bisa ditambahkan, sehingga *behavior user* yang didapatkan juga semakin banyak dan dapat dilakukan analisis yang lebih mendalam.

UCAPAN TERIMAKASIH

Penulis senantiasa mengucap syukur yang besar kepada Tuhan YME atas segala kekuatan, kesempatan, dan karuniaNya sehingga penulis dapat menyelesaikan penelitian dan penulisan artikel ilmiah ini dengan baik. Penulis juga mengucapkan terimakasih kepada kedua orang tua yang senantiasa mendukung dan mendoakan, Dosen Pembimbing Skripsi yang senantiasa memberikan saran dan masukan kepada penulis, teman teman se-bimbingan dan seluruh pihak yang telah membantu dalam penyusunan artikel ilmiah ini.

REFERENSI

[1]. Reinsel, D., Gantz, J., & Rydning, J. (2017). *Data Age 2025: The Evolution of Data to Life-Critical Don't Focus on Big Data; Focus on the Data That's Big Sponsored by Seagate The Evolution of Data to Life-Critical Don't Focus on Big Data; Focus on the Data That's Big*. www.idc.com

[2]. Ichsan, M. H. H. (2021). *Analisis Kinerja Jaringan Sensor Nirkabel Untuk Edge Computing Menggunakan Lora Sx1278 Performance Analysis of Wireless Sensor Network for Edge Computing Using Lora Sx1278*. *8*(5), 887–894. https://doi.org/10.25126/jtiik.202183631

[3]. Liu, X., Zhang, W., Zhou, X., & Zhou, Q. (2021). MECGuard: GRU enhanced attack detection in Mobile Edge Computing environment. *Computer Communications*, *172*, 1–9. https://doi.org/10.1016/j.comcom.2021.02.022

[4]. Snyder, S., Rob High, K. B., & Marshall, and A. (2019). *Why organizations are betting on edge computing Insights from the edge*.

[5]. Aslanpour, M. S., Gill, S. S., & Toosi, A. N. (2020). Performance evaluation metrics for cloud, fog and edge computing: A review, taxonomy, benchmarks and standards for future research. In *Internet of Things (Netherlands)* (Vol. 12). Elsevier B.V. https://doi.org/10.1016/j.iot.2020.100273

[6]. Najib, W., Ancaman dan Solusi Keamanan, T., Sulistyo, S., & Kunci, K. (2020). Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things (Review on Security Threat and Solution of Internet of Things Technology). In *Jurnal Nasional Teknik Elektro dan Teknologi Informasi* | (Vol. 9, Issue 4).

[7]. Wang, M., Santillan, J., & Kuipers, F. (2018). *ThingPot: an interactive Internet-of-Things honeypot*. http://arxiv.org/abs/1807.04114

[8]. Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep Learning Approach for Intelligent Intrusion Detection System. *IEEE Access*, *7*, 41525–41550. https://doi.org/10.1109/ACCESS.2019.2895334

[9]. Bonnah, E., & Shiguang, J. (2020). DecChain: A decentralized security approach in Edge Computing based on Blockchain. *Future Generation Computer Systems*, *113*, 363–379. https://doi.org/10.1016/j.future.2020.07.009

[10]. Spadaccino, P., & Cuomo, F. (2020). *Intrusion Detection Systems for IoT: opportunities and challenges offered by Edge Computing*. 1–20. http://arxiv.org/abs/2012.01174